ISSN 2949-1150 (online)
2071-8284 (print)

Научная статья
УДК 343

Киберагентурные операции в системе методов оперативно-розыскной деятельности: международный опыт и национальные модели

Владимир Юрьевич Жандров, кандидат юридических наук, доцент

Московский университет МВД России имени В. Я. Кикотя
Москва (117997, ул. Академика Волгина, д. 12), Российская Федерация
vaisvladimir74@gmail.com
https://orcid.org/0000-0002-1353-2837

Аннотация:
Введение. *Трансформация преступности в условиях развития цифровых технологий сформировала потребность адаптации агентурного метода оперативно-розыскной деятельности к новой технологической реальности. Ряд шагов по созданию правовой основы проведения «операций под прикрытием» в интернете предприняты в рамках международных стандартов, на уровне отдельных государств представлены решения сохранения доказательственной пригодности сведений и минимизации рисков недопустимой провокации в цифровой среде. Российская практика реализации агентурного метода в условиях цифровизации складывается неоднозначно, что требует создания прочной теоретической и правовой основы его применения в противодействии киберпреступности.*
Методы. *При формулировании понятия метода киберагентурных операций применялся метод синтеза; подтверждение легитимации и стандартизации особого режима агентурной работы в информационно-телекоммуникационной среде осуществлялось с помощью анализа правовых актов Организации Объединенных Наций; для выявления общих тенденций в правовом регулировании агентурной работы в киберпространстве применялся метод сравнения формирующихся законодательных моделей США и ряда западноевропейских государств; определение границ допустимости и пределов законности агентурных кибероперациий достигалось методом изучения решений Европейского суда по правам человека.*
Результаты. *Обоснована необходимость введения в научный и правовой оборот метода киберагентурных операций (киберагентурного метода) как адаптированной к условиям цифровизации формы агентурной работы. Показано, что эффективность киберагентурных операций достигается при сочетании технических средств разведки с человеческим фактором, а легитимность – при условии четкого нормативного регулирования, многоуровневого надзора и соблюдения принципов необходимости, соразмерности и защиты прав личности. Предлагается основа для формирования российской модели киберагентурного метода ОРД, предусматривающая необходимость: нормативного закрепления конфидента и условий его применения в информационно-телекоммуникационной среде; выстраивания многоуровневой системы санкционирования и двойного контроля; детальную фиксацию всех этапов деятельности конфидента; задействование независимых надзорных и судебных механизмов; защиту конфиденциальности и предотвращение недопустимых провокаций при противодействии киберпреступности.*

Ключевые слова:
киберагентурный метод, методы оперативно-розыскной деятельности, Human Intelligence, киберпреступность, операции под прикрытием, международные стандарты, провокация преступления

Для цитирования:
Жандров В. Ю. Киберагентурные операции в системе методов оперативно-розыскной деятельности: международный опыт и национальные модели // Вестник Санкт-Петербургского университета МВД России. 2025. № 4 (108). С. 127–138.

Статья поступила в редакцию 11.08.2025; одобрена после рецензирования 14.10.2025; принята к публикации 25.12.2025.

Original article

Cyber-enabled human intelligence in law enforcement: international and domestic patterns

Vladimir Yu. Zhandrov, Cand. Sci. (Jurid.), Docent

Moscow University of the MIA of Russia named after V. Ya. Kikot
12, Academician Volgina str., Moscow, 117437, Russian Federation
vaisvladimir74@gmail.com
https://orcid.org/0000-0002-1353-2837

Abstract:
Introduction. *The The transformation of crime in the context of digital technology development has created a need to adapt Human Intelligence methods to the new technological reality. Internationally, there has been a growing movement to codify rules that provide a legal foundation for undercover operations in cyberspace. The implementation of Human Intelligence methods in Russia's digital environment presents a complex and evolving challenge, necessitating the establishment of a robust theoretical and legal foundation for its application in combating cybercrime.*
Methods. *The conceptualisation of the cyber agent operations method was achieved via synthesis. The legitimacy and standardisation of a special regime for agent activities in the information and telecommunications environment were substantiated through an analysis of relevant United Nations legal instruments. To identify common trends in the legal regulation of agent work in cyberspace, the comparative method was applied to emerging legislative models of the United States and a number of Western European states. The determination of the boundaries of permissibility and the limits of legality for agent cyber-operations was achieved through the method of studying decisions of the European Court of Human Rights.*
Results. *The research establishes the necessity of incorporating the method of cyber agent operations (the cyber agent method) into both scholarly and legal frameworks as a form of agent-based activity adapted to the digital environment. The research indicates that the success of such operations relies on synergizing technical tools with human intelligence, whereas their lawfulness requires explicit legal provisions, layered supervision, and compliance with the tenets of necessity, proportionality, and safeguarding fundamental rights. It is proposed to establish a framework for a Russian model of cyber-enabled human intelligence. This framework necessitates the legal recognition and regulation of a "confident" (confidential informant), including the specific conditions for their lawful deployment in the information and telecommunications environment, the implementation of a multi-tiered authorization system with dual oversight mechanisms; and the meticulous documentation of every phase of the confidents' operational involvement; the engagement of independent supervisory and judicial mechanisms; and the protection of confidentiality alongside the prevention of impermissible provocations in countering cybercrime.*

Keywords:
cyber agent-based method; Human Intelligence; cybercrime; undercover operations; international standards; instigation of a crime

Для цитирования:
Zhandrov V. Yu. Cyber-enabled human intelligence in law enforcement: international and domestic patterns // Vestnik of Saint Petersburg University of the MIA of Russia. 2025. № 4 (108). P. 127–138.

The article was submitted August 11, 2025; approved after reviewing October 14, 2025; accepted for publication December 25, 2025.

Введение

Переход значительной части коммуникационных процессов в онлайн-сферу, активное использование зашифрованных мессенджеров, даркнет-площадок и специализированных интернет-форумов существенно изменили характер функционирования как легальных социальных структур, так и криминальных сообществ. Указанные трансформации находят отражение и в статистике. Так, доля соответствующих преступлений, совершаемых в сфере информационных технологий, от общего числа преступлений в 2024 году возросла до 40 %, а общее их количество по сравнению с 2023 года увеличилось на 13,1 % [1, с. 6]. Отчетность фиксирует весьма скромные успехи в раскрываемости киберпреступлений и возмещении причиненного ими вреда, что обусловлено как несовершенством правового регулирования, так и технической и технологической отсталостью правоохранительных органов [2, с. 103]. На этом фоне в литературе высказываются жесткие позиции, призывающие при объявлении войны с киберпреступностью принять чрезвычайные меры, направленные на ограничение банковской тайны и тайны связи, которые сегодня, по оценкам специалистов, существенно препятствуют оперативному получению информации [3, с. 124]. Значительные изменения технологической и социальной среды современного общества требуют адаптации оперативно-розыскной деятельности (далее – ОРД) к новым условиям [4, с. 45], и особенно – ее методов.

Агентурный метод исторически составляет центральный элемент системы оперативно-розыскной, разведывательной и контрразведывательной деятельности. Конфиденты – одни из основных источников оперативно-значимой информации, которая ложится в основу для реализации практически всех форм оперативно-розыскной деятельности. Раскрыть сложное преступление без использования агентуры сегодня практически невозможно [5, с. 216].

Традиционные практики агентурной работы в новых технологических условиях оказываются ограниченными по эффективности, что объективно обусловливает необходимость разработки и внедрения новых форм скрытого взаимодействия. Одним из таких инструментов выступает метод киберагентурных операций (киберагентурный метод) – регулируемый правом и этикой комплекс приемов и способов оперативно-розыскной деятельности, в котором уполномоченный субъект ОРД, используя легендированную цифровую идентичность, целенаправленно вступает во взаимодействие с лицами в информационно-телекоммуникационной среде

ISSN 2949-1150 (online)
2071-8284 (print)

(включая закрытые и анонимные площадки) для получения, документирования и верификации оперативно значимой информации при обязательном соблюдении принципов законности, необходимости, соразмерности, запрета провокации и независимого надзора. Его практическая ценность заключается в возможности получения уникальных сведений посредством управляемого человеческого взаимодействия, тогда как технические способы разведки зачастую не обеспечивают необходимой глубины и достоверности информации. При этом опыт работы оперативных подразделений органов внутренних дел показывает, что нельзя обеспечить неотвратимость ответственности преступников без противопоставления их криминальной деятельности целенаправленного комплекса оперативно-розыскных мер и следственных действий, без использования в качестве вспомогательной информации данных, полученных оперативно-розыскным путем, без привлечения граждан к противодействию преступности [6, с. 16].

Несмотря на актуальность проблемы совершенствования оперативно-розыскных мер в противодействии киберпреступности, степень научной разработанности поднимаемой проблемы представляется недостаточной. В широком перечне исследований, посвященных эволюции и общим вопросам кибербезопасности, комплексный анализ киберагентурного метода как самостоятельного инструмента оперативно-розыскной деятельности фактически отсутствует. В отечественной литературе данная тематика лишь намечается, тогда как зарубежные публикации заметно погрузились в вопросы правовых и этических аспектов скрытых операций в интернете. В отсутствие прочной теоретической основы практика вынуждена становиться на зыбкую почву экспериментального накопления опыта. В результате складывается ситуация, при которой практическое развитие киберагентурного метода опережает его научно-теоретическое осмысление и нормативное закрепление. Подобные методологические проблемы фиксируются и в более широком научном дискурсе по вопросам ОРД. В частности, отмечается некритическое воспроизводство устаревших научных позиций и недостаточная проработка современных направлений исследований [7, с. 65].

Массовый уход коммуникаций в «тень» зашифрованных алгоритмов связи снизил результативность классических приемов и поставил перед практикой задачу модернизации агентурной работы. При этом именно в российской научной и нормативной плоскости фиксируется разрыв: практика киберагентурных операций опережает теоретическое осмысление, стандарты фиксации/верификации действий агента и механизмы надзора сформулированы неполно, что повышает риски недопустимой провокации и утраты доказательственной пригодности. Необходима модель, которая соединяет человеческое взаимодействие в сети с техническими средствами, но при этом жестко встраивает вмешательство в правовые и этические рамки (законность, необходимость, соразмерность, запрет провокации, многоуровневый контроль).

Метод киберагентурных операций заслуживает самостоятельного научного исследования, в рамках которого актуальность приобретают вопросы оценки правовых, организационных и этических основ его применения. Вполне созрела потребность выявления особенностей и границ допустимости киберагентурного метода, а также разработка предложений по формированию его российской модели.

Методы

Исследование построено на введении в научный и правовой оборот адаптированной к условиям цифровизации новой формы агентурной работы – метода киберагентурных операций (киберагентурного метода), что потребовало анализа зарубежных и российских как литературных, так и нормативно-правовых источников. Это позволило выделить существенные признаки нового метода и с помощью синтеза сформулировать его дефиницию.

Подтверждение легитимации и определение возможностей стандартизации особого режима агентурной работы в информационно-телекоммуникационной среде осуществлялось с помощью анализа положений Конвенции Организации Объединенных Наций (далее – ООН) против транснациональной организованной преступности[1]. При выявлении общих тенденций в правовом регулировании агентурной работы в киберпространстве применялся метод сравнения формирующихся законодательных моделей США, Франции, Испании, Германии и Великобритании. Определение границ допустимости и пределов законности агентурных кибероперации достигалось методом изучения решений Европейского суда по правам человека (далее – ЕСПЧ).

[1] Конвенция против транснациональной организованной преступности (принята в г. Нью-Йорке 15.11.2000 Резолюцией 55/25 на 62-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН) (ред. от 15.11.2000) // Собрание законодательства Российской Федерации (далее – СЗ РФ). 2004. № 40. Ст. 3882.

Результаты

Эволюция агентурного метода в киберагентурный тесно связана с развитием концепции *Human Intelligence* (*HUMINT*) – направления, традиционно охватывающего методы получения информации через непосредственное взаимодействие с людьми [8, с. 161]. В классической разведывательной парадигме оно реализуется через агентурную работу, вербовку, наблюдение, опросы и внедрение. Однако в условиях стремительного усложнения цифровой преступности и трансформации средств коммуникации *HUMINT* получает новое практическое наполнение, расширяя поле своего применения.

Все чаще концепция выступает как интеллектуальный компонент кибероперации, обеспечивающий доступ к закрытым виртуальным пространствам, в которых технические средства разведки либо неприменимы, либо ограничены в эффективности. Если ранее рассматриваемое направление охватывало личные взаимодействия с источниками, то сегодня данная работа все чаще перемещается в виртуальную плоскость, формируя гибридные модели взаимодействия с фигурантами в даркнете, на форумах, в зашифрованных чатах и закрытых сетевых сообществах. В открытых источниках подчеркивается – *HUMINT* в киберпространстве представляет собой операционную дисциплину, ориентированную на получение уникальных сведений через взаимодействие с людьми (чаще всего злоумышленниками) на платформах, недоступных для пассивного мониторинга средствами *OSINT* (разведки по открытым источникам) и *SIGINT* (технической разведки)[2]. В условиях, когда автоматические средства мониторинга ограничены рамками публичного пространства, только методы цифрового *HUMINT* способны восполнить критически важные пробелы в аналитике и предупреждении преступлений в интернете.

С позиций теоретико-прикладного измерения цифровизация *HUMINT* превратила его в комплекс способов получения информации, основанный на непосредственном или опосредованном взаимодействии с людьми в информационно-телекоммуникационной среде. Особое внимание в современных подходах уделяется сочетанию такого взаимодействия с техническими средствами. Мониторинг даркнета с помощью систем цифровой защиты (*Digital Risk Protection Services*, *DRPS*) – перехват интернет-трафика, криптоанализ и инструменты *OSINT* – формируют многослойную архитектуру разведывательного цикла. В этой системе *HUMINT* играет критически важную роль в восполнении информационных пустот, остающихся за пределами досягаемости технической разведки. Однако эффективность этой модели зависит не только от технологической поддержки, но и от способности выстраивать доверительное взаимодействие в цифровой среде. Поэтому значительный объем содержания рассматриваемого подхода будет наращивать применение легендированных цифровых личностей, установление доверительных контактов с преступниками на форумах и в закрытых каналах, а также долгосрочную разработку фигурантов с целью получения оперативно значимой информации.

В научной литературе подчеркивается методологическая универсальность агентурного метода в системе ОРД. Так, И. А. Климов, Г. К. Синилов и Л. Л. Тузов [9, с. 18–19] обоснованно доказывают, что он одновременно выступает как способ получения оперативной информации, форма тактической реализации ОРМ и канал ее документированной фиксации. Такое многоаспектное понимание позволяет отнести агентурный метод к наиболее гибким и адаптируемым инструментам ОРД, сочетающим элементы психологии, правовой тактики и оперативной техники. Очевидно, в условиях радикального усложнения киберугроз и использования преступниками зашифрованных платформ, даркнета и виртуальных коммуникаций, меняется логика самой оперативной деятельности: от сбора эпизодических данных к глубокой цифровой разработке фигурантов. К сожалению, это закономерно приводит к существенному возрастанию рисков недопустимой провокации, нарушения границ частной жизни и непропорционального вмешательства. Вот почему применение агентурных кибероперации требует не только организационной проработанности и надежной конспирации, но и наличия самостоятельного нормативно-правового механизма, обеспечивающего законность, и как следствие – этическую оправданность и доказательственную пригодность получаемой информации. Эта необходимость подтверждается и практикой: как показывает весь опыт работы полиции, без использования комплексных негласных действий противодействие организованной преступной деятельности малоэффективно [10, с. 187].

Целенаправленный сбор, обработка и анализ информации в цифровом пространстве демонстрируют все большую сложность в части соблюдения баланса между эффективностью

[2] HUMINT and its Role within Cybersecurity // SANS : [website]. URL: https://www.sans.org/blog/humint-and-its-role-within-cybersecurity (дата обращения: 08.07.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

оперативной работы и необходимостью защиты прав человека. Поддерживать равновесие между интересами правопорядка и правами личности призваны международно-правовые стандарты, определяющие пределы допустимости HUMINT-практик в интернете.

Ключевую роль в легитимации и стандартизации агентурного метода, особенно в условиях расширения его применения в информационно-телекоммуникационной среде, играют международные правовые акты ООН. Одним из базовых международных документов, закрепляющих возможность применения специальных методов расследования, включая внедрение агентов под прикрытием, является Конвенция ООН против транснациональной организованной преступности[3]. Государства-участники могут предусматривать использование скрытых методов, включая «операции под прикрытием» (англ. *undercoveroperations*), в рамках своей правовой системы при условии, что такие меры четко закреплены законом, соответствуют принципам необходимости, соразмерности и реализуются под эффективным контролем соответствующих государственных органов (ст. 20 Конвенции).

Особая актуальность положений данной Конвенции прослеживается при рассмотрении правовых основ проведения агентурных операций в информационно-коммуникационной среде, где традиционные методы правового контроля сталкиваются с новыми вызовами – трансграничным характером коммуникаций и высокой степенью анонимности действий субъектов. Особое значение здесь приобретает вопрос экстерриториального доступа к цифровым данным и необходимости судебного контроля за действиями агентов. Как полагают D. Andrees и B. Schreij, отсутствие международного механизма принудительного исполнения запросов создает правовую неопределенность и увеличивает соблазн «нелегального взлома» без санкции принимающей стороны[4]. Поэтому закономерным шагом стало объединение, например, в рамках Европейской сети надзора за разведкой (англ. *European Intelligence Oversight Network*, EION) органов парламентского и специализированного надзора более чем из 18 стран, что позволяет им осуществлять обмен практиками по контролю за цифровыми методами разведывательной деятельности, включая правовую верификацию массового сбора данных[5].

Принципы юридической определенности, необходимости, пропорциональности и судебного надзора, закрепленные в Конвенции, служат ориентиром для национальных законодательств особенно в контексте регулирования кибероперациий с участием агентов, осуществляющих свою деятельность через социальные сети, зашифрованные мессенджеры или даркнет-форумы. Весьма обширный опыт законодательного регулирования агентурной работы в киберпространстве имеют США и страны Западной Европы.

В США деятельность агентов под прикрытием детально регламентирована на федеральном уровне. Основу нормативного регулирования составляет Руководство Генерального прокурора по тайным операциям ФБР[6] (далее – Руководство), разработанное Министерством юстиции США и Федеральным бюро расследований США. Согласно данному документу, агент под прикрытием определяется как лицо, действующее под вымышленной личностью и скрывающий свою аффилированность с ФБР от третьих лиц. Руководство устанавливает многоуровневую процедуру санкционирования операций, включая предварительное одобрение на уровне территориального управления (англ. *Special Agentin Charge*), а в особо чувствительных случаях – на уровне специального федерального комитета.

Особое внимание документ уделяет недопущению участия агента в нелегальной деятельности (англ. *other wise illegal activity*) без соответствующего разрешения, а также ограничению действий, способных квалифицироваться как провокация преступления или недобросовестное вмешательство в личную жизнь. Кроме того, Руководство обязывает фиксировать ключевые элементы взаимодействия *undercover*-агента с объектом и проводить внутренний аудит завершенных операций. Важным элементом контроля является разрешение на временное установление цифрового контакта с фигурантом в течение 30 дней до получения окончательного разрешения на операцию, что особенно актуально в контексте инфильтрации в интернет-среду.

---

[3] СЗ РФ. 2004. № 40. Ст. 3882.

[4] Grabosky P., Urbas G. Online Undercover Investigations and The Role of Private Third Parties // International Journal of Cyber Criminology. 2019. Vol. 13. Is. 1. P. 38–54.

[5] European Intelligence Oversight Network (EION) // Interface [website]. URL: https://www.interface-eu.org/focus-area/european-intelligence-oversight-network-eion (дата обращения: 17.07.2025).

[6] The Attorney General's Guidelines on FBI Undercover Operations United States Department of Justice // U.S. Department of Justice : [website]. URL: https://www.justice.gov/sites/default/files/ag/legacy/2013/09/24/undercover-fbi-operations.pdf (дата обращения: 14.07.2025).

Во Франции с принятием закона от 5 марта 2007 г. № 2007–297 «О предупреждении преступности»[7] появилось правовое основание для применения undercover агентурных методов в онлайн-пространстве, включая скрытое участие на форумах, в чатах и приватных группах при расследовании тяжких преступлений, таких как торговля наркотиками и распространение детской порнографии. Несколько позднее закон от 13 ноября 2014 г. № 2014–1353[8], направленный на усиление антитеррористических мер, расширил эти возможности, официально легализовав использование легендированных цифровых профилей в интернете и закрепив модель разведки в правоохранительных целях (франц. *Intelligence-ledPolicing*) с акцентом на проактивное вмешательство и интеграцию *HUMINT* совместно с технологическими средствами анализа угроз.

Закон **Испании** от 5 октября 2015 г. № 13/2015[9] установил строгий судебный контроль за тайными операциями в интернете – внедрение агента может происходить лишь по предварительному судебному ордеру, оно ограничивается по времени и должно быть оправдано необходимостью применения цифровых методов. Вся деятельность скрытого агента фиксируется и подлежат судебному пересмотру в целях защиты прав субъектов.

Федеративная Республика Германия все агентурные операции (нем. *Einsatzverdeckter Ermittler*) поставила в рамки норм Уголовно-процессуального кодекса[10] (*StPO*). Положения § 110a–110d *StPO* допускают использование официальным сотрудником полиции (нем. *verdeckter Ermittler*) постоянной легенды и при необходимости поддельных документов. Такие действия допустимы только при расследовании особо тяжких преступлений, включая организованную преступность, торговлю наркотиками, оружием, людьми и терроризм и в случае, если иные методы оказались неэффективными.

Применение агентов под прикрытием возможно исключительно по судебному разрешению, полученному в ходе согласования с прокуратурой. В экстренных случаях допускается временное внедрение с последующим подтверждением в течение трех рабочих дней (§ 110b *StPO*). Закон также требует документировать действия *undercover*-агента: фиксировать сроки операции, условия внедрения и использовать методы, исключающие нарушение конституционных прав граждан (§ 110c *StPO*). Кроме того, закон прямо запрещает провокации преступлений, ограничивая участие undercover-сотрудника ролью наблюдателя или контролируемого участника, не формирующего у фигуранта преступного умысла (§ 110a (1) *StPO*).

Правовая модель ФРГ подчеркивает значимость соблюдения принципов соразмерности и судебного контроля. Например, внедрение в жилые помещения требует дополнительного согласования с судом (§ 110b (2) *StPO*), а раскрытие личности агента после завершения операции допускается только при соблюдении условий сохранения его безопасности (§ 110d *StPO*). Кроме того, существует прецедентная практика Федерального Конституционного суда Германии (нем. *Bundesverfassungsgericht*, *BVerfG*) и Федерального верховного суда Германии (нем. *Bundesgerichtshof*, *BGH*), подтверждающая недопустимость провокации: доказательства, полученные с ее помощью, признаются недействительными, а наказание может быть смягчено.

Таким образом, ФРГ демонстрирует высокую степень правовой определенности и институциональной прозрачности в части использования *undercover*-методов, что делает ее правоприменительную практику значимой для сравнительного анализа и разработки нормативных моделей в других странах, включая Российскую Федерацию. Особенно важно, что положения § 110a–110d *StPO* (включая требования к судебному разрешению, ограничение целей и условий внедрения, запрет провокации и механизм документирования), распространяются не только на физическое пространство, но и полностью охватывают действия агентов под прикрытием в информационно-телекоммуникационной среде. Немецкие правоохранительные органы могут применять *undercover*-инструменты на форумах, в мессенджерах, игровых платформах и социальных сетях, однако только при условии соблюдения тех же правовых процедур и гарантий, которые предусмотрены для офлайн-среды. Такой подход обеспечивает непрерывность правового контроля вне зависимости от среды осуществления вмешательства, позволяя

[7] Loi n° 2007 297 du 5 mars 2007 relative à la prévention de la délinquance (dernière mise à jour des données de ce texte : 01 janvier 2016) // Journal officiel de la République française. 2007. n°0056 : [site web]. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000615568 (дата обращения: 13.07.2025).

[8] Loi n° 2014 1353 du 13 novembre 2014 renforçant les dispositions relatives à la luttecontre le terrorisme (dernière mise à jour des données de ce texte : 15 novembre 2014) // Journal officiel de la République française. 2014. n°0263. [site web]. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000029754374 (дата обращения: 13.07.2025).

[9] Ley Orgánica 13/2015, de 5 de octubre, para elfortalecimiento de las garantíasprocesales y la regulación de las medidas de investigacióntecnológicas // BoletínOficial del Estado. 2015. № 244. [sitio web]. URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725 (дата обращения: 13.07.2025).

[10] Strafprozessordnung (StPO) = [Уголовно-процессуальный кодекс Германии] // Bundesamt für Justi : [webseite]. URL: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html (дата обращения: 14.07.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

эффективно бороться с киберпреступностью, не нарушая при этом фундаментальные права личности. Схожие процессуальные ограничения закреплены и в российском законодательстве, где «оперативное внедрение» допустимо только на основании постановления, утвержденного руководителем оперативно-розыскного органа согласно ч. 5 ст. 8 Федерального закона «Об оперативно-розыскной деятельности»[11] [11, с. 177].

Особый интерес представляет сформировавшаяся нормативная база **Великобритании**, где деятельность агентов под прикрытием в цифровой среде урегулирована через развитую законодательную систему, базирующуюся на принципах законности, пропорциональности и независимого надзора. Основу такой системы составляет Закон о регулировании следственных полномочий 2000 года (*RIPA*), в рамках которого вводится правовое определение "*covert human intelligence source*" (*CHIS*) – скрытого агента, действующего на постоянной или временной основе, в т. ч. в киберпространстве[12]. Согласно положениям *RIPA*, проведение любой операции, связанной с внедрением агента в виртуальные сообщества (форумы, соцсети, платформы даркнета), требует предварительного санкционирования и точного документирования целей, методов и продолжительности операции; такое санкционирование осуществляется специально уполномоченными должностными лицами ("*designated persons*") в соответствующих государственных органах – от старших офицеров полиции (не ниже *Superintendent*) до руководителей и назначенных старших должностных лиц спецслужб (*MI5*, *MI6*, *GCHQ*, *NCA*, *HMRC* и др.), при обязательном последующем контроле со стороны Комиссара по полномочиям в сфере расследований (*Investigatory Powers Commissioner*)[13].

Дальнейшее развитие регулирования данной сферы произошло с принятием закона о следственных полномочиях 2016 года (*IPA*), который расширил сферу регулирования на цифровое пространство, включая механизмы перехвата интернет-трафика, внедрения в шифрованные каналы связи и скрытого анализа цифровых следов[14]. *IPA* ввел принцип так называемого «двойного замка» (англ. *double lock*), при котором каждая операция подлежит не только административному согласованию, но и обязательному судебному одобрению. Таким образом обеспечивается системный контроль и соответствие вмешательства требованиям необходимости и соразмерности.

Сегодня ключевую роль в обеспечении легитимности деятельности под прикрытием играют Офис комиссара по следственным полномочиям (*IPCO*)[15] и Трибунал по следственным полномочиям (*IPT*)[16]. *IPCO* осуществляет регулярный надзор за действиями спецслужб, включая аудит операций с участием *CHIS*, а *IPT* предоставляет гражданам возможность обжаловать действия государства в случае подозрения на нарушение прав человека, включая вмешательство в частную жизнь.

Практические аспекты киберагентурной работы регламентируются также утверждаемым Министерством внутренних дел Великобритании Кодексом практики агентурной разведки. В данном документе подробно изложены правила выбора, подготовки и управления *CHIS*, включая допустимые формы взаимодействия, обязательства по фиксации контактов, сохранению конфиденциальности и ограничения на участие агента в потенциально преступной деятельности[17]. Специальное внимание уделяется цифровому взаимодействию: установлены протоколы легендирования, правила поведения в онлайн-группах, а также процедуры реагирования на риски провокаций и компрометации агента.

Дополнительным шагом стало принятие закона о тайных источниках агентурной разведки 2021 года, который легализовал возможность совершения undercover-агентом ограниченного круга действий, формально подпадающих под уголовную ответственность (например, покупка наркотиков или участие в фиктивных сговорах), при условии получения санкции и соблюдения

[11] Об оперативно-розыскной деятельности : Федеральный закон от 12 августа1995 г. № 144-ФЗ (ред. от 01.04.2025) // СЗ РФ. 1995. № 33. Ст. 3349.

[12] Regulation of Investigatory Powers Act 2000 // Legislation.gov.uk : [website]. URL: https://www.legislation.gov.uk/ukpga/2000/23/contents (дата обращения: 14.07.2025).

[13] Regulation of Investigatory Powers Act 2000 : Section 29, 30: Authorisation of covert human intelligence sources // Ibid. [website]. URL: https://www.legislation.gov.uk/ukpga/2000/23/contents (дата обращения: 14.07.2025).

[14] Investigatory Powers Act 2016 // Ibid. [website]. URL:https://www.legislation.gov.uk/ukpga/2016/25/contents (дата обращения: 14.07.2025).

[15] Investigatory Powers Commissioner's Office (IPCO) // Investigatory Powers Commissioner's Office (IPCO) : [website]. URL: https://www.ipco.org.uk (дата обращения: 31.07.2025).

[16] The Investigatory Powers Tribunal (IPT) : [website]. URL: https://investigatorypowerstribunal.org.uk/about-the-tribunal (дата обращения: 31.07.2025).

[17] Covert Surveillance and CHIS Code of Practice // Legislation.gov.uk : Legislation.gov.uk : [website]. URL: https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice (дата обращения: 14.07.2025).

процедурных гарантий. Такая практика признана допустимой при условии соблюдения правовых рамок и тщательного независимого контроля[18].

Опыт нормативно-правового регулирования агентурной деятельности в интернете не является безупречным. В научной литературе подчеркивается, что киберагентурные операции могут вступать в противоречие с действующим законодательством, если отсутствует четкое разграничение между допустимым наблюдением и недопустимой провокацией преступления [12, с. 821]. При этом основной акцент делается на необходимости демонстрации «обоснованного подозрения» и минимизации вмешательства в частную жизнь субъектов наблюдения.

Как подчеркивает С. Ланнье, в цифровой среде граница между допустимым скрытым наблюдением и недопустимой провокацией оказывается очень размыта, особенно в случаях длительного участия агента в закрытых виртуальных сообществах [13, с. 4]. Такая ситуация может привести к трансформации из наблюдателя в участника, чьи действия провоцируют или усиливают преступную активность фигурантов. В связи с этим возникает необходимость введения не только внешней судебной и прокурорской проверки подобных действий, но и формализованных критериев оценки допустимости вмешательства: обоснования необходимости операции, формулирования ее целей и сроков, оценки риска посягательства на частную жизнь, разработки критериев оценки «уязвимости» вмешательства для прав фигуранта. Подобный подход соответствует как международным стандартам прав человека, так и требованиям процессуальной справедливости, особенно в случаях, когда результаты кибероперации могут быть использованы в уголовном преследовании. Более того, усиление независимого надзора и отчетности способствует не только легитимности действий оперативных подразделений, но и укреплению общественного доверия к правоохранительным институтам в цифровую эпоху.

Использование конфидентов в онлайн-среде нуждается в установлении четкой процедуры и прозрачных протоколов взаимодействия – особенно при проникновении в защищенные паролем сообщества или осуществлении «оперативной игры». Особого внимания требует проблема цифровых ловушек (англ. *honeypots*) и фишинговых платформ, которые, несмотря на эффективность, могут нарушать рассматриваемый принцип [6].

В настоящее время оперативно-розыскная деятельность в целом и в частности содействие граждан органам, ее осуществляющим, регулируются в Российской Федерации целым рядом законов, основным из которых является Федеральный закон «Об оперативно-розыскной деятельности»[19] [14]. Содействие является одной из форм реализации гражданами своих конституционных прав и свобод; «право свободно искать, получать, передавать, производить и распространять информацию» обусловливает правомерность поиска информации и ее последующей передачи в оперативные подразделения [14, с. 208]. Результаты социологических опросов свидетельствуют о наличии объективной основы для реализации института содействия граждан органам, осуществляющим оперативно-розыскную деятельность: 48–52 % респондентов выразили готовность к конфиденциальному сотрудничеству, еще 23–26 % – при определенных условиях [15, с. 72].

На этом фоне остро встает вопрос не только о правовых, но и об этических границах *HUMINT* в киберпространстве. Очевидно, что даже при наличии формального процессуального основания оперативное внедрение агентов в цифровые сообщества с целью получения разведывательной информации должно оцениваться не только с точки зрения допустимости, но и с позиций соразмерности, предсказуемости и уважения к достоинству личности. При этом особую озабоченность вызывает практика активного манипулирования фигурантами, например, через подстрекательство, искажение мотивов или эксплуатацию уязвимости.

В условиях цифровой среды, где идентичность легко маскируется, а контакты с фигурантами происходят через платформы, лишенные традиционных механизмов верификации, особенно остро встает вопрос об информированном согласии и праве на неприкосновенность приватной цифровой среды. Например, создание агентом имитирующего реальную личность цифрового профиля (англ. *deepfakeprofile*) с целью получения доверия может не нарушать закон, но порождает моральный риск, особенно если результатом становится психологическая травма или искусственно сформированное поведение со стороны наблюдаемого субъекта. Такие действия могут формально не нарушать закон, но вступают в противоречие с принципами этической правоприменительной деятельности.

В странах с развитой правовой системой формируются надзорные механизмы, отслеживающие правомерность агентурной деятельности в киберпространстве. Развивается практика

[18] Covert Human Intelligence Sources (Criminal Conduct) Act 2021 // Ibid. [website]. URL: https://www.legislation.gov.uk/ukpga/2021/4/contents (дата обращения: 14.07.2025).

[19] СЗ РФ. 1995. № 33. Ст. 3349.

ISSN 2949-1150 (online)
2071-8284 (print)

многоуровневой этической оценки, предполагающая вовлечение не только непосредственных исполнителей и юридических консультантов, но и независимых экспертных групп, а также институциональных надзорных органов, аналогичных тем, что действуют при национальных разведслужбах или органах внутренней безопасности в странах с развитой системой «сдержек и противовесов» (англ. *checks and balances*). Особенно важно это при использовании социальной инженерии, цифровых профилей интернет-персонажей и иных имитационных методов.

Так, в Германии действует Парламентская комиссия по надзору за разведслужбами (*PKGr*), которая после реформы 2014 года получила полномочия инициировать проверки, назначать уполномоченного по контролю и обеспечивать постоянную парламентскую подотчетность[20]. Аналогичный механизм реализован в Норвегии через Парламентский комитет по надзору за разведкой (англ. *Norwegian Parliamentary Intelligence Oversight Committee* (*EOS Committee*)) – независимый надзорный орган, функционирующий с 1996 года и обладающий полномочиями инспектировать спецслужбы, инициировать расследования и предоставлять ежегодные отчеты в парламент[21]. Внимания заслуживает и французская модель, в рамках которой функционирует Национальная комиссия по контролю за методами разведки (франц. *Commission nationale de contrôl edes techniques derenseignement*, *CNCTR*), включающая судей, депутатов и технических экспертов, уполномоченных осуществлять как предварительный, так и последующий надзор с возможностью доступа к логам операций и вынесения обязательных рекомендаций[22]. Указанные примеры показывают, что современные формы надзора в киберсфере ориентированы не только на судебную санкцию, но и на институционализированное экспертное сопровождение, технический аудит и участие независимых структур в контроле за правомерностью и пропорциональностью вмешательства.

Многоуровневые модели надзора за оперативной деятельностью весьма результативны, но, как показывает практика, эффективный контроль возможен только при наличии независимых и технически компетентных надзорных органов, обладающих достаточными ресурсами, правом на инициативное расследование, доступ к закрытой информации и полномочиями на применение санкций.

Достижение легитимности и эффективности *HUMINT*-операций возможно только при соблюдении следующих условий: международной согласованности правовых стандартов, институциональной подотчетности, технической транспарентности и правовой защиты цифровой неприкосновенности личности. Развитие этической инфраструктуры не менее значимый элемент, чем нормативное регулирование, особенно в условиях усиления автоматизации разведывательной деятельности. Признание этих требований должно стать основой для формирования справедливой, предсказуемой и правомерной модели киберагентурной работы на современном этапе. Как отмечает А. Л. Осипенко, «во многих ситуациях производства следственных действий копирование информации в электронном виде, имеющей значение для расследования, является приемлемой альтернативой изъятию электронных носителей этой информации, а в ряде случаев – единственно возможной формой фиксации» [16, с. 47]. В случае если оперативная информация, полученная с помощью специальных знаний, не может быть легализована, она не будет иметь и процессуальной значимости в качестве доказательств [17, с. 64].

Таким образом, в контексте *HUMINT* в киберпространстве этика становится не факультативным элементом, а необходимым уровнем правовой культуры, направленным на защиту не только целостности оперативной работы, но и доверия общества к инструментам цифровой безопасности. Подобные действия относятся к оперативно-розыскным мероприятиям и должны осуществляться исключительно уполномоченными правоохранительными органами в рамках действующего законодательства [1, с. 10]. Как отмечается в литературе, законодатель уже закрепил значимость общественного восприятия результатов правоохранительной деятельности: «Общественное мнение является одним из основных критериев официальной оценки деятельности полиции» (п. 6 ст. 9 Федерального закона «О полиции»[23]) [18, с. 66].

По мнению исследователей, «большинство проблем фиксации доказательственной информации связано не с противоречивостью норм и пробелами правового регулирования, а с поверхностной, формальной их оценкой без учета уровня развития теории доказывания» [16, с. 45]. Правомерность применения агентурного метода в цифровом пространстве неоднократно

[20] Parliamentary Oversight Panel (Germany) // Deutscher Bundestag : [webseite]. URL: https://www.bundestag.de/resource/blob/537938/d52afbcb73b53eea59511515a1dd40a5/go_pkgr-data.pdf (дата обращения: 08.09.2025).

[21] Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee) // EOS- Committee : [webseite]. URL: https://eos-utvalget.no/en/home (дата обращения: 17.07.2025).

[22] Commission nationale de contrôle des techniques de renseignement (CNCTR) // CNCTR : [webseite]. URL: https://www.cnctr.fr/en/statut (дата обращения: 17.07.2025).

[23] О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 31.07.2025) // СЗ РФ. 2011. № 7. Ст. 900.

становилась предметом рассмотрения ЕСПЧ, который в ряде решений установил правовые ориентиры допустимости использования скрытых агентов с учетом требований ст. 8 Европейской конвенции о защите прав человека и основных свобод (*ECHR*) – права на уважение частной и семейной жизни[24]. Так, в прецедентном деле *Klass v. Germany* ЕСПЧ подтвердил, что вмешательство государства в частную жизнь через скрытое наблюдение допустимо, но только при наличии надлежащей правовой базы, строгой системы контроля и гарантий от злоупотреблений[25]. При этом особое внимание было уделено прозрачности процедуры санкционирования, необходимости информирования надзорных органов, а также временным ограничениям на проведение тайных мероприятий. С учетом этого важно, чтобы применение специального программного обеспечения для негласного дистанционного доступа к компьютерной информации преследовало законные цели, было необходимым и соразмерным общественной опасности преступлений, осуществлялось грамотно и осторожно [19, с. 52].

Другим значимым решением, формирующим подход к правомерности скрытых оперативных действий в цифровом пространстве, стало дело *Zakharov v. Russia* (2015)[26]. В данном деле ЕСПЧ установил, что законодательство и практика Российской Федерации в сфере прослушивания телефонных переговоров и слежки за цифровыми коммуникациями нарушают ст. 8 Конвенции, поскольку не обеспечивают достаточных гарантий от злоупотреблений со стороны государственных органов[27]. Суд подчеркнул необходимость четкой нормативной базы, содержащей: (а) критерии допустимости вмешательства; (б) процедуры получения санкции; (в) независимый и эффективный надзор как до, так и после проведения мероприятия; (г) механизм уведомления постфактум. Хотя дело непосредственно касалось технического перехвата, его правовые положения в полной мере применимы и к *undercover*-операциям в киберсреде, где действия агентов могут затрагивать переписку, цифровую идентичность и приватное онлайн-присутствие лица. Принципы, сформулированные судом, требуют, чтобы любые формы тайного взаимодействия, включая внедрение *undercover*-агентов в цифровые сообщества, проводились на основе закона, были пропорциональны цели вмешательства и находились под эффективным внешним контролем. Данные положения особенно важны в контексте современной оперативно-розыскной деятельности, где границы между наблюдением и провокацией, сбором информации и нарушением фундаментальных прав легко размываются в условиях анонимности и удаленности виртуального пространства.

Данные выводы находят подтверждение и развитие в более широком контексте международной правовой дискуссии. Так, согласно данным обзора, проведенного D. Murray, P. Fussey и L. McGregor в 2021 году, устойчивость и легитимность надзора над разведывательной деятельностью зависят от наличия действенных институциональных гарантий, включая четко определенные мандаты, технически оснащенные независимые органы и возможность как предварительного, так и последующего контроля [20]. В отсутствие таких механизмов цифровой надзор рискует утратить законность и превратиться в инструмент неконтролируемого вмешательства. Аналогичные проблемы выявлены и в отчете Агентства по фундаментальным правам ЕС (FRA) за 2023 год, в котором указано, что, несмотря на наличие формальных структур надзора во многих странах ЕС, часто этим органам не хватает ресурсов, технической экспертизы и санкционных полномочий для обеспечения реального контроля над агентурной деятельностью в интернете[28]. FRA подчеркивает необходимость укрепления правовой базы и внедрения многоуровневой модели контроля, способной гарантировать соблюдение прав человека даже в условиях быстро развивающихся технологий.

Обобщение опыта США и западноевропейских государств по регулированию *undercover*-операций в цифровой среде позволяет выделить следующие его ключевые признаки: нормативное закрепление статуса агента под прикрытием и условий его применения; выстраивание многоуровневой системы санкционирования и двойного контроля; детальная фиксация всех этапов

[24] European Convention for the Protection of Human Rights and Fundamental Freedoms// European Court of Human Rights : [website]. URL: https://www.echr.coe.int/documents/convention_eng.pdf (дата обращения: 16.07.2025).

[25] European Court of Human Rights. Case of Klass and Others v. Germany, App. № 5029/71, Judgementof 6 September 1978 // Ibid. URL: https://hudoc.echr.coe.int/eng?i=001-57510 (дата обращения: 14.07.2025).

[26] European Court of Human Rights. Case of Roman Zakharov v. Russia. Application no. 47143/06. Jadgment Strasbourg. 4 December 2015 // Ibid. URL: https://www.statewatch.org/media/documents/news/2015/dec/echr-russian-secret-surveillance-judgment.pdf (дата обращения: 31.07.2025).

[27] European Court of Human Rights. Case of Roman Zakharov v. Russia, App. № 47143/06, Judgementof 4 December 2015 // Ibid. URL: https://hudoc.echr.coe.int/eng?i=001-159324 (дата обращения: 14.07.2025).

[28] FRA Opinion Bulletin: Surveillance by intelligence services: Fundamental rights safeguards // European Union Agency for Fundamental Rights. [website]. URL: https://fra.europa.eu/en/publication/2023/surveillance-update (дата обращения: 17.07.2025).

ISSN 2949-1150 (online)
2071-8284 (print)

деятельности конфидента; задействование независимых надзорных и судебных механизмов; защита конфиденциальности и предотвращение недопустимых провокаций. Эта модель находится в границах международных стандартов, представляет собой разумный баланс между оперативной необходимостью и защитой прав человека в условиях стремительной цифровизации, а ее регулятивный инструментарий может служить полезной демонстрацией при разработке нормативной базы киберагентурных операций, проводимых российскими субъектами ОРД.

Заключение

Проведенное исследование подтвердило, что киберагентурный метод является естественным этапом эволюции классического HUMINT и отражает необходимость адаптации агентурных практик к цифровой среде. Перенос коммуникаций в зашифрованные мессенджеры, даркнет и закрытые онлайн-сообщества предопределил создание новых форм скрытого взаимодействия, в которых именно человеческий фактор обеспечивает доступ к информации, не достижимой для технической разведки. В условиях цифровизации агентурный метод ОРД не только не теряет, но и значительно повышает актуальность применения. Именно синтез агентурной работы с технологиями цифровой инфильтрации и анонимного присутствия создает уникальные возможности для получения оперативно значимой информации. Трансформируясь из агентурного в киберагентурный, рассматриваемый метод становится специализированной формой HUMINT, приспособленной к особенностям сетевой среды, и потому претендует на роль ключевого компонента современной разведывательной модели в ОРД.

В целом международные правовые стандарты устанавливают четкие рамки, в которых допустимо осуществление операций под прикрытием в условиях цифровизации, включая: наличие специального закона, определяющего допустимые формы и цели скрытых методов; обеспечение процессуальной прозрачности и контроля (предпочтительно судебного) на всех этапах операции; запрет на провокацию преступления, особенно при дистанционном контакте в цифровой среде; защиту прав на неприкосновенность частной жизни как в офлайн-, так и в онлайн-пространстве. Указанные принципы универсальны и подлежат применению независимо от формы и характера среды, в которой действуют агенты.

Анализ имеющейся практики показывает, что внедрение конфидентов в цифровую среду регулируется в большинстве развитых законодательств строго ограниченными правовыми рамками, требующими соблюдения принципов пропорциональности, субсидиарности и независимого надзора.

Сравнительный анализ международных моделей показал, что устойчивость и легитимность киберагентурных операций зависят от четкой нормативной базы, процедур санкционирования и эффективного независимого контроля. Опыт США, Франции, Испании, Германии и Великобритании демонстрирует, что ключевыми гарантиями являются принцип законности, судебный надзор, запрет провокации и документированность действий агента. Данные подходы позволяют сбалансировать интересы безопасности и защиту прав личности, что особенно важно в условиях цифровизации.

Тайные киберагентурные операции должны иметь четкую правовую регламентацию, касающуюся не только начала и целей вмешательства, но и критериев завершения, а также механизмов отчетности и последующего анализа воздействия на права лиц. В связи с этим актуальность приобретает вопрос «этической сертификации» агентурных методик, в т. ч. при участии представителей гражданского общества.

Таким образом, значимым условием легитимности HUMINT в цифровую эпоху становится не только формальное соблюдение процедур, но и включение оперативной практики в систему этического, международно-правового и технически подкрепленного надзора, обеспечивающего баланс между интересами безопасности и правами личности. Анализ международных подходов к HUMINT-деятельности в цифровом пространстве показывает растущую необходимость юридической и этической переоценки традиционных агентурных практик. Современные вызовы, связанные с трансграничным характером операций, использованием методов социальной инженерии, симуляцией цифровых личностей и внедрением в закрытые виртуальные сообщества, требуют системной нормативной реакции.

Для российской практики очевидна потребность в дальнейшем уточнении правовых и организационных оснований применения киберагентурного метода. Представляются перспективными развитие механизмов контроля, выработка критериев допустимости вмешательства, а также создание процедур фиксации и верификации действий киберагентов в сети. Не менее

значимой задачей становится формирование профессиональной подготовки, сочетающей технические компетенции с пониманием правовых и этических ограничений.

В целом киберагентурный метод следует рассматривать как междисциплинарный инструмент, соединяющий технические, правовые и этические элементы. Его дальнейшее развитие возможно лишь при условии международной согласованности стандартов, институциональной прозрачности и уважения фундаментальных прав личности, что позволит не только повысить эффективность борьбы с киберпреступностью, но и укрепить доверие общества к институтам цифровой безопасности.

Список источников

1. *Осипенко А. Л.* Участие граждан в противодействии преступности в сфере информационных технологий // Вестник Краснодарского университета МВД России. 2025. № 2 (68). С. 6–15.

2. *Гусев В. А.* Цифровая гигиена vs. киберпреступность // Психопедагогика в правоохранительных органах. 2022. Т. 27, № 1 (88). С. 102–108. https://doi.org/10. 24412/1999-6241-2022-188-102-10

3. *Чечетин А. Е.* Борьба с киберпреступностью требует наращивания усилий // Актуальные проблемы борьбы с преступлениями и иными правонарушениями. 2025. № 25. С. 123–125.

4. *Осипенко А. Л.* Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской академии МВД России. 2019. № 4 (75). С. 38–46. https://doi.org/10.24411/1999-625X-2019-14007

5. *Шахматов А. В.* Современное состояние и проблемы конфиденциального содействия граждан оперативным подразделениям органов внутренних дел / Оперативно-разыскное противодействие преступлениям экономической направленности и коррупции: передовой опыт, проблемы и пути их решения : материалы всероссийской научно-практической конференции, г. Санкт-Петербург, 29 мая 2020 г. Санкт-Петербург : Санкт-Петербургский университет МВД России, 2020. С. 214–220.

6. *Шахматов А. В.* Содействие граждан в правоприменительной практике предупреждения и раскрытия преступлений органами внутренних дел / Актуальные вопросы противодействия организованной преступности в России (памяти профессора Д. В. Ривмана) : материалы региональной научно-практической конференции, г. Санкт-Петербург, 28 ноября 2014 г. Санкт-Петербург: Санкт-Петербургский университет МВД России, 2014. С. 16–19.

7. *Румянцев Н. В., Шкабин Г. С.* Научный дискурс в сфере оперативно-разыскной деятельности : обзор докладов Межведомственной научно-практической конференции в НИИ ФСИН России // Научные исследования преступления и наказания. 2025. № 2 (22). С. 63–74.

8. *Лымарев А. В.* Агентурная разведка (HUMINT) в борьбе с международным терроризмом: опыт США // Ярославский педагогический вестник. 2011. Т. 1, № 4. С. 160–163.

9. *Климов И. А., Синилов Г. К., Тузов Л. Л.* Агентурный метод защиты интересов личности, общества, государства и борьбы с преступностью : монография / под общ. ред. Г. К. Синилова. Калининград : Калининградский юридический институт МВД России, 2002. 334 с.

10. *Осипенко А. Л.* Организованная преступная деятельность в киберпространстве: тенденции и противодействие // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 181–188.

11. *Латынин Е. В.* Реализация агентурного метода в следственных изоляторах на примере оперативно-розыскного мероприятия «оперативное внедрение» / Уголовно-исполнительная система: педагогика, психология и право : материалы Всероссийской научно-практической конференции, г. Томск, 10–11 октября 2019 г. Томск : Томский институт повышения квалификации работников ФСИН, 2019. Вып. 7. С. 174–180.

12. *Tetzlaff-Bemiller M. J.* Undercover Online: An Extension of Traditional Policing in the United States // International Journal of Cyber Criminology. 2011. Vol 5. Is. 2. P. 813–824.

13. *Lannier S.* Infiltrating virtual worlds. The regulation of undercover agents through fundamental rights // Revista Brasileira de Direito Processual Penal. 2024. T. 10, Is. 3. P. 1–12. https://doi.org/10.22197/rbdpp.v10i3.1066

14. *Шахматов А. В.* Некоторые вопросы правового регулирования содействия граждан оперативным подразделениям ОВД // Оперативно-розыскная деятельность в современных условиях : материалы межведомственной научно-практической конференции, г. Санкт-Петербург, 22–23 июня 2023 г. Санкт-Петербург : Санкт-Петербургский университет МВД России, 2023. С. 208–212.

15. *Луговик В. Ф., Важенин В. В.* Развитие осведомительства как мировая тенденция // Общество и право. 2020. № 4 (74). С. 71–75.

16. *Осипенко А. Л., Гайдин А. И.* Проблемы фиксации доказательственной информации в электронном виде // Общественная безопасность, законность и правопорядок в III тысячелетии. 2015. № 1-1. С. 44–51.

17. *Хромов И. Л., Эзрохин П. В.* Использование специальных знаний в оперативно-розыскной деятельности // Научный портал МВД России. 2018. № 1 (41). С. 62–66.

18. *Самоделкин А. С.* Объективные критерии оценки деятельности органов, осуществляющих оперативно-розыскную деятельность, и их значение в борьбе с преступностью // Общество и право. 2025. № 2 (92). С. 65–75.

19. *Осипенко А. Л.* Сбор информации и полицейские операции по противодействию организованной преступности в киберпространстве: зарубежный опыт // Общество и право. 2021. № 1 (75). С. 47–55.

20. *Murray D., Fussey P., McGregor L.* Effective Oversight of Large Scale Surveillance Activities: A Human Rights Perspective // Journal of National Security Law & Policy. 2021. No. 11. URL: https://jnslp.com/wp-content/uploads/2021/09/Effective_Oversight_of_Large_Scale_Surveillance_Activities_2.pdf (дата обращения: 17.07.2025).