Дата поступления рукописи в редакцию: 26.02.2026 г. DOI: 10.24412/2782-3830-2026-2-276-282
Дата принятия рукописи в печать: 18.03.2026 г.

СТРЕЛЬНИКОВА Анастасия Александровна,
студент кафедры «Уголовное право и прикладная информатика в юриспруденции»
Тамбовский государственный технический университет,
ORCID ID: 0009-0000-1323-2466,
e-mail: n.strelnikova06@yandex.ru

СЕЛЕЗНЁВ Андрей Владимирович,
кандидат технических наук, доцент,
доцент кафедры «Уголовное право и прикладная информатика в юриспруденции»
Тамбовский государственный технический университет,
ORCID ID: 0000-0001-7746-811x,
e-mail: kriminalistik@rambler.ru

ТЕРЕХОВ Алексей Васильевич,
кандидат технических наук, доцент,
доцент кафедры «Уголовное право и прикладная информатика в юриспруденции»
Тамбовский государственный технический университет,
ORCID ID: 0009-0002-8572-9265,
e-mail: a_l_e_x_68@mail.ru

ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ИНСТРУМЕНТОВ В ПРОТИВОДЕЙСТВИИ НАРКОПРЕСТУПНОСТИ

Аннотация. *Статья посвящена комплексному исследованию трансформации методов противодействия незаконному обороту наркотиков в условиях цифровой экономики на примере Тамбовской области. Работа рассматривает эволюцию наркоугрозы от традиционных уличных схем к дистанционным, анонимизированным моделям сбыта через зашифрованные мессенджеры, ресурсы анонимного сегмента сети Интернет и криптовалютные платёжные системы. Особое внимание уделено анализу правовых основ, практической реализации и этико-правовых коллизий, возникающих при применении компьютерно-технических экспертиз и технологий анализа больших данных. В исследовании применяется междисциплинарный подход, объединяющий правовой анализ действующего законодательства (ФЗ об ОРД, УПК РФ, ФЗ о судебно-экспертной деятельности), криминологическую оценку региональной статистики за 2020–2024 гг., изучение конкретных кейсов раскрытых преступлений и выявление системных рисков для конституционных прав граждан. Установлено, что доля преступлений, совершённых с использованием цифровых технологий в Тамбовской области, выросла с 15–20% в 2020 году до более 50% в 2024 году, что подтверждает актуальность темы. Показано, что компьютерно-техническая экспертиза достигла высокой степени зрелости и стала неотъемлемым элементом расследования, тогда как внедрение анализа больших данных сдерживается ресурсными, кадровыми и правовыми ограничениями. Выявлены критические проблемы: правовая неопределённость алгоритмических методов, риск формирования «цифровых профилей» без индивидуализированного обоснования, угроза адвокатской тайне, недостаточная техническая компетентность отдельных участников процесса. На основе проведённого анализа предложены конкретные меры: совершенствование законодательства в части регулирования анализа агрегированных данных, создание межведомственных аналитических центров с протоколами защиты персональной информации, внедрение механизмов общественного контроля, повышение цифровой грамотности сотрудников правоохранительных органов, судей и адвокатов. Исследование подчёркивает необходимость построения сбалансированной модели, в которой технологическая эффективность не противоречит, а служит укреплению конституционных гарантий прав и свобод личности.*

Ключевые слова: *наркопреступность, Тамбовская область, цифровая среда, компьютерно-техническая экспертиза, анализ больших данных, оперативно-розыскная деятельность, права человека, конституционные гарантии, цифровые доказательства, правовая неопределённость.*

STRELNIKOVA Anastasia Aleksandrovna,
Student of the Department
«Criminal Law and Applied Informatics in Jurisprudence»
Tambov State Technical University

SELEZNEV Andrey Vladimirovich,
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department
«Criminal Law and Applied Informatics in Jurisprudence»
Tambov State Technical University

TEREKHOV Aleksey Vasilevich,
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department
«Criminal Law and Applied Informatics in Jurisprudence»
Tambov State Technical University

LEGAL AND TECHNOLOGICAL ASPECTS OF THE USE OF DIGITAL TOOLS IN COUNTERING DRUG CRIME

Annotation. *The article is devoted to a comprehensive study of the transformation of methods of countering illicit drug trafficking in the digital economy, using the example of the Tambov Region. The work examines the evolution of the drug threat from traditional street-based schemes to remote, anonymized models of distribution through encrypted messengers, resources of the anonymous segment of the Internet, and cryptocurrency payment systems. Special attention is paid to the analysis of the legal foundations, practical implementation, and ethical and legal conflicts that arise when using computer-technical expertise and big data analysis technologies. The study uses an interdisciplinary approach that combines a legal analysis of current legislation (Federal Law on Operational Investigative Activities, Criminal Procedure Code of the Russian Federation, Federal Law on Forensic Expert Activity), a criminological assessment of regional statistics for 2020-2024, a study of specific cases of solved crimes, and the identification of systemic risks to the constitutional rights of citizens. It was found that the share of crimes committed.*

Key words: *drug crime, Tambov Region, digital environment, computer and technical expertise, big data analysis, operational and investigative activities, human rights, constitutional guarantees, digital evidence, and legal uncertainty.*

За последние пять лет произошёл качественный скачок в способах распространения запрещённых веществ: если ранее основной акцент делался на личных контактах, уличных точках сбыта и прямых поставках, то сегодня доминирующей моделью становится дистанционный, анонимизированный и децентрализованный сбыт через цифровые платформы. Особую роль в этом процессе играют зашифрованные мессенджеры, социальные сети, форумы в анонимном сегменте Интернета и криптовалютные платёжные системы, которые позволяют организаторам преступных схем минимизировать риски идентификации и задержания [1].

В Российской Федерации обозначенная проблема имеет наиболее выраженный характер. Согласно официальной статистике, в период с 2020 по 2024 год зафиксирован рост числа противоправных действий, связанных с незаконным оборотом наркотиков и совершаемых через информационно-телекоммуникационные сети, в среднем на 35%. Региональная специфика не становится препятствием для данной тенденции: на примере Тамбовской области видно, что даже при менее напряженной криминогенной обстановке по сравнению с мегаполисами ЦФО, доля преступлений с использованием цифровых инструментов выросла с 15–20% до свыше 40%

[2]. Подобная динамика подтверждает, что трансформация способов совершения наркопреступлений носит общенациональный системный характер.

Традиционные методы оперативной работы — патрулирование улиц, задержания с поличным, работа с информаторами — теряют эффективность перед лицом децентрализованных, анонимизированных и трансграничных схем сбыта [3]. В этих условиях правоохранительные органы вынуждены обращаться к технологическим решениям, что, в свою очередь, ставит перед юридической наукой и практикой сложнейшую задачу: как обеспечить безопасность общества, не пожертвовав фундаментальными правами личности. Данная проблема приобретает особую остроту в контексте междисциплинарного характера темы, находящейся на стыке уголовного права, криминалистики, информационной безопасности и этики. Научная новизна настоящего исследования заключается в комплексном региональном анализе, сочетающем правовой, криминологический и технологический аспекты, с акцентом на поиске практических решений для сбалансированного регулирования цифровых методов противодействия наркоугрозе.

Правовую основу деятельности правоохранительных органов в сфере противодействия незаконному обороту наркотиков составляют Федеральный закон от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах», нормы Уголовного кодекса Российской Федерации (статьи 228–234.1), а также Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» [4, 5, 6]. Последний предоставляет правовые основания для проведения оперативно-розыскных мероприятий, включая проверочную закупку в сети Интернет, наведение справок, исследование документов и предметов, контроль почтовых отправлений и иных сообщений (в современной интерпретации — интернет-трафика и электронной переписки), оперативное внедрение и оперативный эксперимент в цифровой среде.

Статья 8 Федерального закона «Об оперативно-розыскной деятельности» устанавливает, что проведение оперативно-розыскных мероприятий, связанных с ограничением прав граждан, допускается только на основании судебного решения, что формально обеспечивает гарантию против произвольного вмешательства [6]. Однако на практике суды зачастую выносят решения на основе формальных ходатайств без детального анализа пропорциональности вмешательства, что отмечается в многочисленных обзорах судебной практики Верховного Суда Российской Федерации. Производство компьютерно-технической экспертизы регулируется Федеральным законом от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации», что позволяет устанавливать факты хранения, распространения запрещённых веществ через цифровые каналы, идентифицировать пользователей, восстанавливать удалённую информацию и цепочки коммуникации [7].

Процессуальный порядок извлечения и изучения цифровых носителей регламентирован Уголовно-процессуальным кодексом РФ в рамках таких следственных действий, как обыск, выемка и осмотр доказательств [8]. Хотя ст. 182 УПК РФ предписывает конкретизировать изымаемые объекты, техническая специфика электронных устройств, хранящих массивы файлов, часто приводит к формальному соблюдению этого правила и чрезмерному сбору информации [9]. Правовое регулирование анализа больших данных базируется на Федеральном законе № 149-ФЗ «Об информации...» (ст. 10.1) и Федеральном законе № 374-ФЗ. Эти нормативные акты возлагают на организаторов распространения информации обязанность по сохранению сведений о приеме, передаче и обработке пользовательских сообщений [10-11].

При этом принципиально важно отметить, что действующая нормативная база не предусматривает специальных правил для регулирования алгоритмических методов анализа информации, включая машинное обучение, построение поведенческих моделей и прогнозную аналитику [12]. В законодательстве отсутствуют чёткие критерии допустимости таких методов, порядок минимизации собираемых данных, определённые сроки их хранения и обязательные процедуры уничтожения после достижения целей расследования. Такая правовая неопределённость создаёт условия, при которых применение технологий анализа больших данных происходит в «серой зоне», где отсутствуют надёжные гарантии против произвольного вмешательства в частную жизнь граждан [13]. Отсутствие прозрачных стандартов затрудняет как оценку законности проводимых мероприятий со стороны суда, так и возможность для граждан защитить свои права в случае необоснованного включения в сферу оперативного интереса. В условиях, когда алгоритмы способны обрабатывать миллионы записей и выявлять корреляции, неочевидные для человека, отсутствие правовых рамок превращает технологический инструмент в потенциальный источник системных нарушений, где эффективность борьбы с преступностью может достигаться ценой неоправданного ограничения свободы невиновных лиц. Эта коллизия требует скорейшего нормативного урегулирования, учитывающего как потреб-

ности правоохранительной деятельности, так и необходимость защиты конституционных прав в цифровую эпоху.

В Тамбовской области практика применения компьютерно-технической экспертизы достигла высокого уровня зрелости и стала одним из главных элементов расследования дел о незаконном обороте наркотиков [14]. При изъятии электронных устройств у подозреваемых регулярно назначаются экспертизы, позволяющие восстанавливать переписку в мессенджерах (Telegram, WhatsApp, MAX), выявлять фотографии и описания наркотических средств, устанавливать геолокационные данные, подтверждающие присутствие лица в месте совершения преступления, а также идентифицировать криптокошельки и цепочки транзакций. Технологическая база экспертиз включает использование специализированных программных комплексов, таких как Cellebrite UFED, Magnet AXIOM, Belkasoft Evidence Center, позволяющих работать с зашифрованными устройствами, восстанавливать удалённые данные, анализировать артефакты операционных систем и приложений [15]. Эксперты применяют методы криминалистического анализа файловых систем, извлечения данных из резервных копий облачных сервисов, декодирования временных меток и сопоставления цифровых следов с объективными обстоятельствами дела.

Ярким подтверждением эффективности данного подхода стало расследование деятельности организованной преступной группы в Мичуринском муниципальном округе Тамбовской области, занимавшейся производством и сбытом синтетических наркотиков. Комплексная компьютерно-техническая экспертиза изъятых устройств позволила восстановить детали организации нарколаборатории, установить круг участников преступной деятельности через анализ контактных списков и истории коммуникаций, документально подтвердить закупку оборудования и химических компонентов, а также выявить электронные финансовые операции [16].

В частности, эксперты восстановили переписку в зашифрованном мессенджере, где обсуждались рецептуры синтеза, локации закладок и распределение ролей; проанализировали геоданные фотографий, подтверждающих факт закладки веществ в конкретных точках города; установили связь между криптокошельком и банковскими переводами через обменные сервисы. Полученные цифровые доказательства легли в основу обвинительного приговора, по которому организатор преступной группы был осуждён на 17 лет лишения свободы в колонии строгого режима. Данный кейс демонстрирует не только техническую состоятельность современных методов экспертизы, но и их процессуальную значимость: цифровые доказательства были признаны судом допустимыми, поскольку процедура изъятия и исследования соответствовала требованиям УПК РФ, а заключение эксперта содержало чёткое описание методики, результатов и выводов [17].

Вместе с тем внедрение технологий анализа больших данных в регионе находится на начальной стадии. Сдерживающими факторами выступают недостаточное ресурсное обеспечение (отсутствие высокопроизводительных вычислительных мощностей и специализированного программного обеспечения), острый дефицит квалифицированных аналитиков, предпочитающих работать в коммерческом секторе, а также ведомственная разобщённость информационных систем УМВД, Роскомнадзора, Федеральной налоговой службы и финансовых организаций [18].

В отличие от Москвы или Санкт-Петербурга, где реализуются пилотные проекты по интеграции данных из различных источников и применению алгоритмов машинного обучения для выявления аномалий в поведении пользователей, в Тамбовской области подобные инициативы носят единичный характер и зависят от федеральной поддержки. Например, в рамках программы «Цифровой регион» в 2023 году был проведён эксперимент по анализу анонимных агрегированных данных трафика в социальных сетях для выявления точек концентрации наркоугрозы, однако его результаты не были систематизированы и внедрены в постоянную практику из-за отсутствия методических рекомендаций и финансирования на последующие этапы.

Применение цифровых инструментов в условиях недостаточной правовой урегулированности порождает серьёзные риски для прав и свобод граждан. Массовый сбор метаданных под предлогом борьбы с наркоугрозой фактически формирует режим тотального наблюдения, что ставит под сомнение соблюдение принципа соразмерности вмешательства в частную жизнь, закреплённого в статье 23 Конституции Российской Федерации [13]. Алгоритмические системы анализа могут формировать «цифровой профиль» лица на основе поведенческих паттернов — использования анонимных браузеров, посещения определённых ресурсов, применения шифрования, — что не является правонарушением, но может стать основанием для необоснованного оперативного интереса и подрыва презумпции невиновности.

В научной литературе этот феномен получил название «алгоритмической дискриминации»

или «профилирования по признаку поведения», что противоречит принципу индивидуальной ответственности [12]. Особую тревогу вызывает потенциальная угроза адвокатской тайне при массовом мониторинге коммуникаций, что противоречит конституционному праву на защиту и статье 53 УПК РФ [8]. Даже при наличии судебного решения на контроль сообщений, техническая невозможность точечного фильтра переписки адвоката и подзащитного создаёт риск непреднамеренного доступа к конфиденциальной информации.

Недостаточная техническая компетентность судебных органов при рассмотрении ходатайств о проведении оперативно-розыскных мероприятий, связанных с глубоким анализом данных, снижает эффективность судебного контроля. Судьи, не обладающие знаниями в области информационных технологий, вынуждены полагаться на технические заключения следственных органов, что нарушает баланс властей [9]. В Тамбовской области эти риски усугубляются относительно низким уровнем цифровой грамотности среди отдельных представителей судейского корпуса и адвокатского сообщества, что затрудняет квалифицированную оценку законности и обоснованности цифровых доказательств на всех стадиях уголовного судопроизводства. Позиция правозащитных организаций подчёркивает необходимость введения независимого надзора за применением технологий массового анализа данных. Отмечается, что отсутствие публичной статистики по количеству и результатам ОРМ, связанных с анализом больших данных, препятствует общественному контролю. Международный опыт демонстрирует эффективность обязательная оценка воздействия на защиту данных перед запуском новых систем анализа, а также участие уполномоченных по защите данных в процессе принятия решений. В Российской Федерации подобные институты находятся в зачаточном состоянии, что создаёт дополнительные барьеры для обеспечения правовой определённости.

Для преодоления выявленных противоречий и формирования сбалансированной модели противодействия цифровой наркопреступности предлагаются следующие меры. Уполномоченному по правам человека в Тамбовской области целесообразно инициировать проведение межведомственных дискуссионных площадок с участием представителей УМВД, судебного сообщества, адвокатуры и независимых IT-экспертов с целью выработки единых подходов к применению цифровых доказательств и укрепления гарантий прав граждан [1]. Такие площадки могут быть оформлены в виде ежегодного регионального форума или семинара, где будут обсуждаться кейсы, этические дилеммы и лучшие практики.

Необходимо подготовить экспертные рекомендации для федеральных законодательных органов, направленные на детализацию процедур сбора, хранения и анализа больших данных, включая обязательное указание конкретных целей, сроков и критериев минимизации обрабатываемой информации. В частности, предлагается установить чёткий перечень случаев, при которых допускается анализ агрегированных данных без индивидуализации субъекта, а также ввести обязательное уведомление граждан о факте включения их данных в аналитические выборки (за исключением случаев, угрожающих раскрытию оперативной информации).

Правоохранительным органам региона рекомендуется активизировать программы повышения квалификации сотрудников в области цифровой криминалистики, этики работы с персональными данными и интерпретации результатов алгоритмического анализа [15]. Перспективным шагом может стать создание на базе УМВД межведомственного аналитического центра с чётко прописанными протоколами защиты персональной информации и межведомственного взаимодействия. При обращении в суд с ходатайствами о проведении оперативно-розыскных мероприятий, затрагивающих обработку массивов данных, следует обеспечивать содержательное обоснование — с указанием методологии, масштаба вмешательства и связи с конкретным уголовным делом.

Образовательным организациям области, реализующим программы подготовки юристов и IT специалистов с юридической направленностью, рекомендуется включить в учебные планы модули, посвящённые цифровой грамотности, основам киберправа и этическим аспектам применения больших данных в правоохранительной деятельности [3]. Дополнительно следует рассмотреть возможность внедрения в региональную практику механизмов «тестовых зон», где новые методы анализа данных будут апробироваться в ограниченном масштабе с обязательным мониторингом их воздействия на права граждан и публичной отчётностью. Такой подход позволит накопить эмпирические данные для последующего нормативного закрепления успешных практик и распространения их в других регионах Российской Федерации.

Таким образом, цифровые инструменты, в частности компьютерно-техническая экспертиза, доказали свою незаменимость в раскрытии современных форм наркопреступности в Тамбовской области [14]. Одновременно анализ больших данных требует дальнейшего развития как в технологическом, так и в правовом измерении. Ключевым условием устойчивого прогресса выступает не технологическое превосходство как тако-

вое, а его гармоничное встраивание в систему конституционных ценностей [13]. Только при условии строгого соблюдения принципов законности, соразмерности и подотчётности цифровые методы станут не угрозой, а надёжным инструментом обеспечения безопасности общества без ущерба для прав и свобод личности.

Достижение этого баланса требует совместных усилий законодателя, правоохранительных органов, судебной власти, гражданского общества и научного сообщества. Перспективы дальнейших исследований видятся в разработке методик оценки эффективности цифровых методов с учётом не только раскрываемости преступлений, но и степени соблюдения прав граждан, а также в создании межрегиональных баз данных анонимизированных кейсов для обмена опытом и выработки единых стандартов.

Список литературы:

[1] Готчина, Л. В. Цифровизация наркопреступлений и противодействия им / Л. В. Готчина // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 32-36.

[2] Доклад о наркоситуации в Тамбовской области в 2022 году [Электронный ресурс] // Правительство Тамбовской области: [официальный сайт]. 2023. Режим доступа: https://www.tambov.gov.ru/assets/files/ank/doklad-2022.pdf (дата обращения: 16.02.2026)

[3] Грогуль, А. А. Цифровые технологии и наркопреступность: проблемы противодействия незаконному обороту наркотиков, совершаемому с использованием глобальной сети интернет / А. А. Грогуль, Ю. А. Сидоренко // Сборник статей XIV Международной научно-практической конференции «Научные междисциплинарные исследования». Саратов, 2021. С. 271-276

[4] О наркотических средствах и психотропных веществах: Федеральный закон от 08.01.1998 № 3-ФЗ (ред. 25.12.2023) // Собрание законодательства Российской Федерации. 1998. № 2. Ст. 219.

[5] Уголовный кодекс Российской Федерации: федеральный закон от 13.06.1996 № 63–ФЗ (ред. от 31.07.2025) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[6] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 № 144-ФЗ (ред. 01.04.2025) // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

[7] О государственной судебно-экспертной деятельности в Российской Федерации: Федеральный закон от 31.05.2001 № 73-ФЗ (ред. 22.07.2024) // Собрание законодательства Российской Федерации. 2001. № 23. Ст. 2291

[8] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174–ФЗ (ред. от 31.07.2025) // Собрание законодательства РФ. 2001. № 52. (ч.1). Ст. 282.

[9] Решетняк, О. А. Использование компьютерных технологий при расследовании преступлений в сфере незаконного оборота опасных психоактивных веществ: дис. ... канд. юрид. наук / О. А. Решетняк // Волгоград, 2020. 220 с.

[10] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. 24.06.2025) // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

[11] О внесении изменений в Федеральный закон «О противодействии терроризму»: Федеральный закон от 06.07.2016 № 374-ФЗ (ред. 29.12.2022) // Собрание законодательства Российской Федерации. 2016. № 28. Ст. 4558.

[12] Меняйло, Д. В. Использование цифровых технологий для противодействия наркопреступлениям в современной России / Д. В. Меняйло, И. С. Назаренко, А. Э. Федосеев, К. К. Крупенникова // Право и государство: теория и практика. 2025. № 3. С. 467-470.

[13] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законом РФ о поправках к Конституции РФ от 14.03.2020 г. № 1–ФКЗ) // Собрание законодательства РФ. 2014. №31. Ст. 4398.

[14] Веденин, Д. А. Возможности компьютерной экспертизы при расследовании преступлений, связанных с незаконным оборотом наркотиков, совершенных и использованием информационно-телекоммуникационных сетей, включая сеть Интернет / Д. А. Веденин // Молодой ученый. 2022. № 48 (443). С. 211-214.

[15] Россинская, Е. Р. Теория информационно-компьютерного обеспечения судебно-экспертной деятельности как новая частная теория судебной экспертологии / Е. Р. Россинская // Вестник Университета имени О. Е. Кутафина. 2022. № 2 (90). С. 27-40.

[16] Владимиров, В.Ю. Кибериcточник как современный способ получения криминалистически значимой информации об особенностях функционирования транснационального наркотрафика / В. Ю. Владимиров, Е. А. Манакова // Наркоконтроль. 2023. № 2. С. 20–23.

[17] Куликов, А. В. Проблемы квалификации сбыта наркотиков, совершенного группой лиц с использованием информационно-телекоммуникационных технологий / А.В. Куликов, И.Ю. Железняк // Наркоконтроль. 2024. № 4. С. 9–12.

[18] Столбанов, Р. А. Использование современных технологий в борьбе с незаконным наркооборотом / Р. А. Столбанов // Молодой ученый. 2024. № 22 (521). С. 437-439.

References:

[1] Gotchina, L. V. Digitalization of drug crimes and counteraction to them / L. V. Gotchina // Criminology: yesterday, today, tomorrow. 2019. No. 4 (55). pp. 32-36.

[2] Report on the drug situation in the Tambov region in 2022 [Electronic resource] // Government of the Tambov region: [official website]. 2023. Access mode: https://www.tambov.gov.ru/assets/files/ank/doklad-2022.pdf (date of request: 02/16/2026)

[3] Grogul, A. A. Digital technologies and drug crime: problems of countering drug trafficking committed using the global Internet / A. A. Grogul, Yu. A. Sidorenko // Collection of articles of the XIV International Scientific and Practical Conference "Scientific interdisciplinary research". Saratov, 2021. pp. 271-276

[4] On narcotic drugs and psychotropic substances: Federal Law No. 3-FZ of 08.01.1998 (as amended on 25.12.2023) // Collection of Legislation of the Russian Federation. 1998. No. 2. Article 219.

[5] The Criminal Code of the Russian Federation: Federal Law No. 63–FZ of 13.06.1996 (as amended on 31.07.2025) // Collection of Legislation of the Russian Federation. 1996. No. 25. Article 2954.

[6] On operational investigative activities: Federal Law No. 144-FZ dated 08/12/1995 (as amended on 04/01/2025) // Collection of Legislation of the Russian Federation. 1995. No. 33. Article 3349.

[7] On state forensic expertise in the Russian Federation: Federal Law No. 73-FZ dated 05/31/2001 (as amended on 07/22/2024) // Collection of Legislation of the Russian Federation. 2001. No. 23. St. 2291

[8] Code of Criminal Procedure of the Russian Federation No. 174-FZ dated 12/18/2001 (as amended on 07/31/2025) // Collection of Legislation of the Russian Federation. 2001. No. 52. (part 1). Article 282.

[9] Reshetnyak, O. A. The use of computer technologies in the investigation of crimes in the field of trafficking in dangerous psychoactive substances: dis. ... kand. jurid. Sciences / O. A. Reshetnyak // Volgograd, 2020. 220 p.

[10] On information, information technologies and information protection: Federal Law No. 149-FZ of 27.07.2006 (as amended on 24.06.2025) // Collection of Legislation of the Russian Federation. 2006. No. 31. St. 3448.

[11] On amendments to the Federal Law "On Combating Terrorism": Federal Law No. 374-FZ of 07/06/2016 (as amended on 12/29/2022) // Collection of Legislation of the Russian Federation. 2016. No. 28. Art. 4558.

[12] Menyailo, D. V. The use of digital technologies to counter drug crimes in modern Russia / D. V. Menyailo, I. S. Nazarenko, A. E. Fedoseev, K. K. Krupennikova // Law and the State: theory and practice. 2025. No. 3. pp. 467-470.

[13] The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993) (as amended by the Law of the Russian Federation on Amendments to the Constitution of the Russian Federation dated 14.03.2020 No. 1–FKZ) // Collection of Legislation of the Russian Federation. 2014. No. 31, Article 4398.

[14] Vedenin, D. A. Possibilities of computer expertise in the investigation of crimes related to drug trafficking committed and the use of information and telecommunication networks, including the Internet / D. A. Vedenin // Young Scientist. 2022. No. 48 (443). pp. 211-214.

[15] Rossinskaya, E. R. Theory of information and computer support for forensic expertise as a new private theory of forensic expertise / E. R. Rossinskaya // Bulletin of the O. E. Kutafin University. 2022. No. 2 (90). pp. 27-40.

[16] Vladimirov, V.Y. Cyber source as a modern way to obtain criminalistically significant information about the functioning of transnational drug trafficking / V. Y. Vladimirov, E. A. Manakova // Drug Control. 2023. No. 2. pp. 20-23.

[17] Kulikov, A.V. Problems of qualification of drug sales committed by a group of persons using information and telecommunication technologies / A.V. Kulikov, I.Yu. Zheleznyak // Drug control. 2024. No. 4. pp. 9-12.

[18] Stolbanov, R. A. The use of modern technologies in the fight against illicit drug trafficking / R. A. Stolbanov // Young Scientist. 2024. No. 22 (521). pp. 437-439.