Научная статья
УДК 343.98
DOI: 10.25683/VOLBI.2026.76.1683

Olesya Vladimirovna Karaulskaya
Inspector at the Material
and Technical Support Department,
Directorate of Non-Departmental Security
of the National Guard Troops of the Russian Federation
for the Irkutsk Region
Irkutsk, Russian Federation
ovk2016@bk.ru

Олеся Владимировна Караульская
инспектор отдела материально-технического
и хозяйственного обеспечения,
Управление вневедомственной охраны
войск национальной гвардии России
по Иркутской области
Иркутск, Российская Федерация
ovk2016@bk.ru

СПОСОБЫ СОКРЫТИЯ МОШЕННИЧЕСТВА ПРИ ПРОВЕДЕНИИ ЗАКРЫТЫХ ЭЛЕКТРОННЫХ ПРОЦЕДУР В СФЕРЕ ГОСУДАРСТВЕННОГО ОБОРОННОГО ЗАКАЗА И ЦИФРОВЫЕ МАРКЕРЫ ЕГО ВЫЯВЛЕНИЯ

5.1.4 — Уголовно-правовые науки

Аннотация. *В статье на основе комплексного криминалистического анализа актуальной правоприменительной практики исследуются способы сокрытия мошеннических посягательств на бюджетные средства в сфере государственного оборонного заказа, совершаемых в условиях закрытых электронных процедур. Методологическую основу работы составили методы системного, сравнительно-правового и типологического анализа судебных приговоров по уголовным делам о корыстных преступлениях в государственных закупках за 2025—2026 гг. Опираясь на теоретические труды В. О. Давыдова и Ф. Г. Аминева, автор детально классифицирует механизмы маскировки преступных действий по этапам непубличного закупочного цикла, последовательно выделяя предконтрактные, организационно-финансовые и технологические составляющие противодействия расследованию.*

В работе подробно раскрыты криминальные схемы умышленного завышения цен, искусственной симуляции конкуренции фирмами-сателлитами, создания видимости легитимности действий участников, а также использования эффекта «отложенного контроля» и тактических приемов введения в заблуждение должностных лиц заказчика. Доказано, что существующий порядок ведомственной приемки носит формально-номинальный характер и способствует камуфлированию дефектов. На основе структуры электронно-цифровых следов, включающих массивы Автоматизированной системы торгов государственного оборонного заказа, лог-файлы и метаданные организаций, предложен комплекс аналитических маркеров детекции обмана и признаков сокрытия преступлений. Для минимизации рисков предложена авторская методика цифрового обнаружения противоправных деяний и создание единой информационной платформы. Обоснована необходимость внедрения в закрытые закупочные системы ИИ-алгоритмов автоматического кросс-анализа учредителей, нормативного закрепления специализированного ведомственного аудита и сквозных цифровых регламентов фиксации результатов с применением технологии распределенного реестра (блокчейн) для повышения эффективности выявления преступлений в стратегическом секторе экономики.

Ключевые слова: *способы сокрытия мошенничества, государственный оборонный заказ, закрытые электронные процедуры, противодействие расследованию, тактические приемы введения в заблуждение, искусственная симуляция конкуренции, электронно-цифровые следы, цифровые маркеры выявления, закрытые закупочные системы, ведомственный цифровой контроль*

Для цитирования: Караульская О. В. Способы сокрытия мошенничества при проведении закрытых электронных процедур в сфере государственного оборонного заказа и цифровые маркеры его выявления // Бизнес. Образование. Право. 2026. № 3(76). С. 204—209. DOI: 10.25683/VOLBI.2026.76.1683.

Original article

WAYS OF CONCEALING FRAUD IN CLOSED ELECTRONIC PROCEDURES WITHIN THE STATE DEFENSE ORDER AND ITS DIGITAL DETECTION MARKERS

5.1.4 — Criminal law sciences

Abstract. *Based on a comprehensive criminological and forensic analysis of current law enforcement practice, the article examines the methods used by unscrupulous entities to conceal fraudulent encroachments on budgetary funds during closed electronic procedures within the State Defense Order. The methodological framework of the research comprises the methods of systemic, comparative legal and typological analysis of court judgments in criminal cases involving acquisitive crimes in public procurement for the period of 2025–2026. Drawing upon the theoretical works of V. O. Davydov and F. G. Aminev, the author provides a detailed classification of the mechanisms for masking criminal actions by the stages*

of the non-public procurement cycle, consistently identifying pre-contractual, organizational, financial, and technological components of countering the investigation.

The paper uncovers in detail the criminal schemes of deliberate price inflation, artificial simulation of competition by satellite companies, creation of a semblance of legitimacy for the participants' actions, as well as the exploitation of the "delayed control" effect and tactical methods of misleading the customer's officials. It is proved that the existing procedure of departmental acceptance is of a formal and nominal nature and contributes to the camouflaging of defects. Based on the structure of_electronic-digital footprints, including AST GOZ datasets, log files, and corporate metadata, a complex of analytical markers for deception detection and signs of crime concealment is proposed. To minimize risks, the author introduces a proprietary methodology for the digital detection of unlawful acts and the establishment of a unified information platform. The study substantiates the necessity of integrating AI algorithms for automated cross-analysis of founders into closed procurement systems, establishing a regulatory framework for specialized departmental auditing, and introducing end-to-end digital regulations for recording results using distributed ledger technology (blockchain) to enhance the efficiency of crime detection in the strategic sector of the economy.

Keywords: *ways of concealing fraud, State Defense Order, closed electronic procedures, countering investigation, tactical methods of misleading, artificial simulation of competition, electronic-digital footprints, digital detection markers, closed procurement systems, departmental digital control*

For citation: Karaulskaya O. V. Ways of concealing fraud in closed electronic procedures within the state defense order and its digital detection markers. *Biznes. Obrazovanie. Pravo = Business. Education. Law*. 2026;3(76):204—209. DOI: 10.25683/VOLBI.2026.76.1683.

Введение

Актуальность. Надежность тылового обеспечения прямо определяет состояние национальной безопасности. Специфика оборонно-промышленного комплекса (далее — ОПК) обусловливает применение закрытых процедур и ограничение публичности закупок согласно федеральным законам от 5 апреля 2013 г. № 44-ФЗ и от 29 декабря 2012 г. № 275-ФЗ. Режим секретности минимизирует внешний контроль, формируя «слепые зоны».

Режим государственной тайны и стратегическая значимость сведений об обеспечении обороны страны и безопасности государства обусловливают ограничение публичного доступа к сводной статистической отчетности о преступности в сфере государственного оборонного заказа (далее — ГОЗ). Тем не менее официальные доклады руководителей надзорных и следственных ведомств (Генеральной прокуратуры РФ, Следственного комитета РФ) по итогам 2025 г. констатируют сохранение значительных объемов причиняемого государству материального ущерба в ОПК. Анализ правоприменительной практики в данном секторе указывает на усложнение криминальных механизмов сокрытия преступлений. Мошеннические схемы умышленно камуфлируются под легитимную хозяйственную деятельность, исключая детекцию стандартными методами ведомственного аудита. В связи с этим возникает острая необходимость разработки научно обоснованных технико-криминалистических инструментов и маркеров для своевременного обнаружения признаков преступной деятельности в условиях закрытых электронных систем.

Изученность проблемы. Превенция, уголовно-правовое противодействие преступлениям в сфере ГОЗ, дифференциация ответственности за мошенничество и уклонение от исполнения оборонных контрактов исследованы Е. В. Шмировым [1], В. Н. Борковым [2], М. М. Исаичевой [3] и А. Р. Садвакасовым [4]. Социальная обусловленность введения уголовной ответственности за срыв договорных обязательств в контрактной системе ОПК отражена в работах А. Н. Каменевой [5]. Организационно-финансовая безопасность, казначейское сопровождение закупок и административное принуждение при контроле бюджетных средств проанализированы С. М. Рукавишниковым [6], О. В. Сергеевым и В. А. Шишковым [7].

Методологический базис криминалистического анализа, системно-информационный подход к виртуальной среде и экспертно-профилактическая деятельность при выявлении скрытых угроз в условиях цифровизации обоснованы В. О. Давыдовым [8] и Ф. Г. Аминевым [9]. Криминалистическая характеристика злоупотреблений и вопросы фиксации цифровых следов при расследовании мошенничества подробно рассмотрены Р. А. Дерюгиным [10], В. А. Очаковским и А. С. Усенко [11].

Предупредительный потенциал цифровых криминалистических методов, автоматизированного мониторинга, программного контроля и использования защищенных распределенных баз данных в правоприменительной деятельности исследовали В. В. Астанин [12], Д. В. Меняйло и К. К. Крупенникова [13], Р. В. Иванов [14] и Л. В. Каширская [15]. Однако комплексный криминалистический анализ способов сокрытия мошенничества в закрытых процедурах ГОЗ и механизмов их выявления не проводился.

Целесообразность разработки темы. Своевременное выявление скрываемых правонарушений, посягающих на бюджет ГОЗ, взаимосвязано с необходимостью постоянного совершенствования методов их обнаружения, поскольку маскировка преступных схем и специфика изолированных систем требуют адаптации экспертно-криминалистической деятельности к цифровым вызовам [6; 7]. Обусловленная процессами цифровизации трансформация посягательств и их укоренение в электронной среде предопределяют разработку маркеров детекции обмана [12; 15] для развития методики расследования и предупреждения данных преступлений.

Ключевая научная проблема исследования заключается в возникновении «слепых зон» в сфере ГОЗ, где режим секретности и формальный характер контроля создают условия для сокрытия криминальных схем.

Цель исследования — на основе правоприменительной практики систематизировать способы сокрытия закупочного мошенничества и определить маркеры его обнаружения.

Задачи исследования:

1. Дифференцировать механизмы сокрытия по этапам контрактного цикла (предконтрактный, организационно-финансовый, технологический).

2. Раскрыть алгоритмы симуляции конкуренции фирмами-сателлитами и имитации легитимности действий.

3. Обосновать цифровую детекцию криминальных рисков для преодоления формальной приемки и выявления мошенничества.

Научная новизна исследования заключается в том, что автором осуществлена классификация способов сокрытия мошенничества по этапам непубличного цикла ГОЗ, а также раскрыты механизмы обмана на основе симуляции конкуренции аффилированными структурами, «отложенного контроля» и камуфлирования дефектов. Кроме того, в работе доказана упреждающая роль цифровых следов как маркеров своевременной верификации рисков и преодоления номинальной приемки.

Теоретическая значимость исследования заключается в углублении криминалистических представлений о механизмах сокрытия и детерминации скрытого характера мошенничества при проведении закрытых электронных процедур в сфере ГОЗ в условиях общей цифровизации.

Практическая значимость исследования заключается в том, что разработанные автором криминалистические рекомендации и аналитические маркеры цифровой детекции обмана могут быть непосредственно внедрены в деятельность следственных органов, экспертных подразделений и контролирующих органов для оперативного предупреждения и выявления признаков мошенничества при проведении закрытых электронных процедур в сфере ГОЗ.

Методологическая основа исследования сформирована методами системного, структурно-функционального и сравнительно-правового анализа, а его эмпирическую базу составил криминалистический анализ материалов судебной практики по уголовным делам о мошенничестве в сфере закупок для нужд ГОЗ за 2025—2026 гг., позволивший выявить устойчивые криминальные механизмы сокрытия указанных преступных посягательств.

Основная часть

Правоприменительная практика позволяет классифицировать факторы, способствующие совершению мошенничества по этапам контрактного цикла.

Первые — предконтрактные факторы, действующие при обосновании начальной (максимальной) цены контракта и проведении торгов за счет информационной асимметрии и имитации конкуренции.

Предконтрактные факторы наглядно раскрывает уголовное дело ООО «СпецТрансСервис» (ГУ МЧС России по Тамбовской области). Пользуясь дефицитом ведомственной экспертизы, подрядчик завысил начальную (максимальную) цену контракта (далее — НМЦК) до 7,1 млн руб. Должностные лица, стремясь формально закрыть показатели ГОЗ, отказались от аудита цен. Сокрытие преступного умысла обеспечила подача скоординированных заявок от трех аффилированных структур (ООО «СпецТрансСервис», ООО «АвтоСпецЦентр», ООО «АвтоТехЦентр»), создавших в закрытом аукционе ложную видимость состязательности и позволивших завысить стоимость контракта на 34 % до начала работ.

Организационно-финансовые факторы, способствующие совершению мошенничества (эффект «отложенного контроля» и транзитное дробление) отражены в деле ООО «АлтайПромАльп» (Бийский городской суд). Используя закрытый статус единственного поставщика в сфере ГОЗ, субъекты получили максимальный аванс (70 % от цены контракта, или 49 млн руб.), причем скрытый характер хищения обеспечил пятимесячный временной лаг до сдачи объекта. Период «отложенного контроля» использовался для транзитного вывода средств по схеме «веера» через фиктивных соисполнителей и индивидуальных предпринимателей, **а** частичные перечисления на Единый налоговый счет служили маскировкой перед финансовым мониторингом.

Другую группу образуют технологические и социально-психологические способы сокрытия преступления при исполнении и приемке контракта за счет искажения параметров, маскировки дефектов и эксплуатации лояльности. Механизмы отражены в материалах дел ООО «АсСтрой» и ООО «СпецТрансСервис». При строительстве ангара преступники заменяли проектный профлист и проволоку тонкими аналогами, скрывая недостатки последующим монтажом, а при ремонте автоцистерн подлог выразился в поверхностном окрашивании вместо капитального восстановления. Судебная экспертиза подтвердила невозможность проверки скрытых работ, поскольку комиссия заказчика не имеет возможности выявить подлог без демонтажа конструкций ангара и разборки узлов автоцистерн.

Криминогенные риски усугубляются авторитетом подрядчиков, работающих с ведомством более десяти лет. Неформальный «кредит доверия» размывает границы контроля, детерминируя устные договоренности. Ведомственная приемка приобретает номинальный характер, оценивая объем бумаг (акты КС-3, накладные), а не реальные свойства объекта. Нейтрализация факторов обеспечивается анализом вещественных доказательств, где инструментом выступают цифровые маркеры мобильных устройств и переговоров.

Результаты исследования и их обсуждение. Перенос активности в виртуальную среду требует модернизации подходов. В. О. Давыдов отмечает, что цифровизация выводит исследование виртуальных объектов на первый план [8]. Мошеннические схемы в ГОЗ аккумулируются в закрытых системах, лог-файлах площадок и метаданных. Их раскрытие требует системно-информационного анализа следов. Практическая реализация методики предполагает упреждающую детекцию рисков сопоставлением действий участников с моделями добросовестного поведения и НМЦК. Базу составляют мониторинг Автоматизированной системы торгов государственного оборонного заказа (АСТ ГОЗ), каналы межведомственного обмена, программы анализа больших данных и неразрушающий контроль объектов.

Изоляция закрытых торгов преодолевается автоматизированным анализом скрытых массивов, реконструирующим ход закупок. Девиации обнаруживаются при изучении коммуникации участников: вербальные следы фиксируют сговоры о завышении цен или игнорировании дефектов. При компьютерно-технической экспертизе скриншоты писем и данные флеш-накопителей доказывают создание мнимо конкурирующих предложений на одном устройстве и их отправку с единого *IP*-адреса. Интеграция распределенных реестров значима для профилактики и доказывания мошенничества: неизменяемые цифровые следы блокчейн-систем выступают допустимыми доказательствами, оптимизируя расследование.

Финансово-хозяйственные риски выявляются анализом первичных бухгалтерских документов (книги учета, счета-фактуры поставщиков, выписки бенефициаров). Логистические маркеры (накладные, путевые листы, формуляры) позволяют сопоставить реальный маршрут

с задекларированными фиктивными затратами. Материально-технические маркеры (паспорта качества, серверы учета, оттиски печатей, демонтированные изношенные агрегаты) формируют эмпирическую базу строительно- и автотехнических экспертиз, доказывающих параметрический подлог. Вещественные и документальные индикаторы исследуются взаимосвязанно как единый цифровой объект. В концепции В. О. Давыдова [8] под цифровым объектом в ГОЗ понимается любая криминалистически значимая электронная информация, связанная с посягательством.

Исследование цифровых объектов сопряжено с организационно-методическими сложностями. Ф. Г. Аминев указывает, что цифровизация криминальной сферы требует адаптации экспертной системы [9]. Главная проблема — дефицит единых стандартов исследования комплексных улик, сочетающих признаки ПО, строительной документации и финансового аудита. При махинациях в сфере ГОЗ данная разобщенность вынуждает назначать несколько изолированных экспертиз, результаты которых сложно увязать.

Для преодоления барьеров необходима Концепция цифрового развития судебно-экспертной деятельности в Российской Федерации. Первоочередной шаг — создание межведомственного координационного совета по цифровому развитию судебной экспертизы (Минюст, Верховный суд, Генеральная прокуратура, научные организации) для интеграции ведомственных усилий и формирования фундамента исследования цифровых следов. Пилотное внедрение Концепции обеспечит апробацию стандартов и обязательную сертификацию методик, а итогом станет развертывание единой цифровой платформы судебно-экспертных организаций. Общая среда и унифицированная аккредитация лабораторий позволят сопоставлять данные финансового аудита с лазерным сканированием и системными логами, ускоряя расследование должностных преступлений в ОПК.

Платформа позволит структурировать информацию на материальные свидетельства и смысловые маркеры. К первым относятся параметры документов, история авторизации на АСТ ГОЗ и хэш-суммы файлов исполнительной документации (акты КС-2, КС-3), фиксирующие ручные исправления. Смысловые маркеры отражают скрытые договоренности в метаданных и завышение цен через зеркальные заявки подставных структур. Выявление обеих составляющих позволяет контролирующим органам реконструировать механизм подлога, трансформируя разрозненные логи и метаданные в верифицированную доказательственную базу умысла.

Выводы

Закупочное мошенничество в закрытых электронных процедурах имеет системную структуру и не локализуется силами штатного ведомственного контроля. Текущий регламент приемки при отсутствии верификации детерминирует информационную асимметрию, позволяя фальсифицировать документацию. Для ликвидации криминогенных факторов на всех этапах ГОЗ обоснован комплекс мер:

• На предконтрактной стадии — автоматизация мониторинга рисков закрытых площадок ИИ-алгоритмами для выявления аффилированности контрагентов и предотвращения симуляции конкуренции.

• На стадии исполнения и приемки — нормативное закрепление объективного экспертно-инструментального контроля (дефектоскопия, лазерное сканирование) как базового источника данных для исключения номинальной проверки объектов

• На стадии фиксации результатов — внедрение цифровых регламентов фото- и видеофиксации скрытых работ с заверением усиленной квалифицированной электронной подписью и трансляцией данных в блокчейн-реестры.

Заключение

Для модернизации превенции мошенничества в сфере ГОЗ необходима интеграция в закрытые торговые системы ИИ-алгоритмов. Программные комплексы призваны осуществлять кросс-анализ учредителей, бенефициаров, метаданных и *IP*-адресов участников для обнаружения симуляции конкуренции и завышения НМЦК. Данная мера минимизирует влияние субъективных факторов на этапе отбора исполнителей и обеспечит проактивный мониторинг рисков.

Для нейтрализации условий, способствующих сокрытию преступлений, на стадии исполнения контрактов необходимо модернизировать существующие процедуры ведомственного контроля. Предлагается внедрить сквозной цифровой регламент фиксации результатов промежуточных проверок и актов скрытых работ. Регламент приемки должен опираться на методы цифровой фото- и видеофиксации, верификацию георасределенных метаданных (координат и точного времени проведения работ), а также аппаратный контроль физических параметров объектов с автоматическим занесением информации в защищенные информационные системы заказчика.

Технологическим базисом достоверности информации должен стать сквозной цифровой регламент, предусматривающий применение технологии блокчейн от начала закрытых процедур до подписания актов. Материалы фото- и видеоконтроля скрытых работ с привязкой к навигационным координатам заверяются электронной подписью инспектора и экспортируются в децентрализованную базу данных. Архитектура распределенного реестра исключает удаление или подмену сведений, блокируя манипулирование отчетностью. Данный подход соответствует передовому опыту прозрачности военных закупок.

Внедрение стандартов должно сопровождаться развитием нормативно-правовой базы, регламентирующей использование систем распределенных данных и ужесточающей ответственность за искажение метаданных. Создание сквозной цифровой архитектуры контроля позволит ликвидировать «слепые зоны» закрытых торгов и трансформировать превенцию корыстной преступности, защитив бюджетные ассигнования в стратегическом секторе экономики.

СПИСОК ИСТОЧНИКОВ

1. Шмиров Е. В. Некоторых особенностях противодействия преступлениям, совершаемым в сфере государственного оборонного заказа, при помощи уголовно-правовых средств // Вестник Университета прокуратуры Российской Федерации. 2026. № 1(111). С. 78—91.

2. Борков В. Н. Применение уголовного закона при посягательствах на контрактную систему и государственный оборонный заказ // Правоприменение. 2018. Т. 2. № 2. С. 56—63. DOI: 10.24147/2542-1514.2018.2(2).56-63.

3. Исаичева М. М. Особенности уголовно-правовой оценки преступлений в сфере государственного оборонного заказа // Закон и право. 2025. № 9. С. 212—218. DOI: 10.24412/2073-3313-2025-9-212-218.

4. Садвакасов А. Р. Некоторые проблемы установления уголовной ответственности за злоупотребление служебными полномочиями при выполнении государственного оборонного заказа // Вестник Университета прокуратуры Российской Федерации. 2025. № 5(109). С. 152—159.

5. Каменева А. Н. Социальная обусловленность введения уголовной ответственности за отказ или уклонение лица, подвергнутого административному наказанию, от заключения государственного контракта по государственному оборонному заказу либо договора, необходимого для выполнения государственного оборонного заказа // Пробелы в российском законодательстве. 2023. № 7. С. 200—204. DOI: 10.33693/2072-3164-2023-16-7-200-204.

6. Рукавишников С. М. Меры административного принуждения, направленные на обеспечение соблюдения законодательства о государственном оборонном заказе // Вестник Саратовской государственной юридической академии. 2023. № 4(153). С. 162—166. DOI: 10.24412/2227-7315-2023-4-162-167.

7. Сергеев О. В., Шишков В. А. Проблемные вопросы гособоронзаказа, предложения по их решению и повышению эффективности выделяемых средств // Научный вестник оборонно-промышленного комплекса России. 2019. № 1. С. 27—33.

8. Давыдов В. О. Системно-информационный подход как методологическая база исследования цифровых информационных объектов в парадигме развития системы криминалистического обеспечения расследования преступлений // Всероссийский криминологический журнал. 2026. Т. 20. № 2. С. 184—193. DOI: 10.17150/2500-4255.2026.20(2).184-193.

9. Аминев Ф. Г. Проблемы совершенствования судебно-экспертной деятельности в условиях цифровизации и пути их решения // Всероссийский криминологический журнал. 2026. Т. 20. № 1. С. 74—83. DOI: 10.17150/2500-4255.2026.20(1).74-83.

10. Дерюгин Р. А. Некоторые аспекты исследования цифровых следов в процессе расследования мошенничеств, совершаемых с использованием сведений о пользователях средств сотовой связи // Вестник Уральского юридического института МВД России. 2023. № 4. С. 72—76.

11. Очаковский В. А., Усенко А. С. Криминалистическая характеристика злоупотреблений в сфере государственных закупок товаров, работ услуг для обеспечения государственных или муниципальных нужд // Вестник Краснодарского университета МВД. 2023. № 3(61). С. 82—89.

12. Астанин В. В. Антикоррупция в ограничениях естественного и стимулах искусственного интеллекта // Журнал Сибирского федерального университета. Гуманитарные науки. 2024. Т. 17. № 6. С. 1163—1173.

13. Меняйло Д. В., Крупенникова К. К. О противодействии коррупции в условиях цифровой трансформации // Проблемы правоохранительной деятельности. 2022. № 3. С. 28—32.

14. Иванов Р. В. Перспективы использования технологии блокчейн для противодействия коррупции в сфере государственного оборонного заказа // Военное право. 2025. № 5(93). С. 62—65.

15. Каширская Л. В. Внутренний контроль процесса закупок в окружении информационных технологий // Учет. Анализ. Аудит. 2025. Т. 12. № 5. С. 75—91. DOI: 10.26794/2408-9303-2025-12-5-75-91.

REFERENCES

1. Shmirov E. V. On some features of countering crimes committed in the field of state defence order using criminal law remedies. *Vestnik Universiteta prokuratury Rossiiskoi Federatsii = Bulletin of the University of the prosecutor's office*. 2026;1(111):78—91. (In Russ.)

2. Borkov V. N. Application of the criminal law in contracting system and state defense order violations. *Pravoprimenenie = Law Enforcement Review*. 2018;2(2):56—63. DOI: 10.24147/2542-1514.2018.2(2).56-63.

3. Isaicheva M. M. Features of the criminal law assessment of offences in the sphere of the state defense order. *Zakon i pravo*. 2025;9:212—218. (In Russ.) DOI: 10.24412/2073-3313-2025-9-212-218.

4. Sadvakasov A. R. Certain issues of establishing criminal liability for abuse of official powers in the execution of state defense contracts. *Vestnik Universiteta prokuratury Rossiiskoi Federatsii = Bulletin of the University of the prosecutor's office*. 2025;5(109):152—159. (In Russ.)

5. Kameneva A. N. The social conditionality of the introduction of criminal liability for the refusal or evasion of a person subjected to administrative punishment from concluding a state contract under a state defense order or a contract necessary to fulfill a state defense order. *Probely v rossiiskom zakonodatel'stve = Gaps in Russian legislation*. 2023;7:200—204. (In Russ.) DOI: 10.33693/2072-3164-2023-16-7-200-204.

6. Rukavishnikov S. M. Administrative coercive measures aimed at ensuring compliance with legislation on state defense orders. *Vestnik Saratovskoi gosudarstvennoi yuridicheskoi akademii = Saratov State Law Academy Bulletin*. 2023;4(153): 162—166. (In Russ.) DOI: 10.24412/2227-7315-2023-4-162-167.

7. Sergeev O. V., Shishkov V. A. Problematic questions of the state defense order, proposals to address them and improve the efficiency of the allocated funds. *Nauchnyi vestnik oboronno-promyshlennogo kompleksa Rossii = Scientific bulletin of the military-industrial complex of Russia*. 2019;1:27 — 33. (In Russ.)

8. Davydov V. O. A System-Information Approach as a Methodological Basis for Researching Digital Information Objects Within the Paradigm of Developing a System of Criminalistic Support of Crime Investigation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*. 2026;20(2):184—193. (In Russ.) DOI: 10.17150/2500-4255.2026.20(2).184-193.

9. Aminev F. G. Problems of Improving Forensic Expertise in the Context of Digitalization and Ways of Solving Them. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*. 2026;20(1):74—83. (In Russ.) DOI: 10.17150/2500-4255.2026.20(1).74-83.

10. Deryugin R. A. Some aspects of researching digital trails in the process of investigating frauds committed using information about cellular communication users. *Vestnik Ural`skogo yuridicheskogo instituta MVD Rossii = Bulletin of the Ural Law Institute of the Ministry of the of the Interior of the Russian Federation*. 2023;4:72—76. (In Russ.)

11. Ochakovskii V. A., Usenko A. S. Criminalistic characteristics of abuse in the field of public procurement of goods, works, services for state or municipal needs. *Vestnik Krasnodarskogo universiteta MVD Rossii = Bulletin of Krasnodar university of Russian MIA*. 2023;3(61):82—89. (In Russ.)

12. Astanin V. V. Anti-corruption in the constraints of natural and incentives of artificial intelligence. *Zhurnal Sibirskogo federal`nogo universiteta. Gumanitarnye nauki = Journal of Siberian federal university. Humanities & social sciences*. 2024;17(6):1163—1173. (In Russ.)

13. Menyailo D. V., Krupennikova K. K. On combating corruption in the context of digital transformation. *Problemy pravookhranitel`noi deyatel`nosti = Problems of Law Enforcement Activity*. 2022;3:28—32. (In Russ.)

14. Ivanov R. V. Prospects of using blockchain technology to counter corruption in the field of state defense procurement. *Voennoe pravo = Military Law*. 2025;5(93):62—65. (In Russ.)

15. Kashirskaya L. V. Internal control of the procurement process in the framework of information technology. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing*. 2025;12(5):75—91. (In Russ.) DOI: 10.26794/2408-9303-2025-12-5-75-91.

Статья поступила в редакцию 05.06.2026; одобрена после рецензирования 26.06.2026; принята к публикации 29.06.2026.
The article was submitted 05.06.2026; approved after reviewing 26.06.2026; accepted for publication 29.06.2026.