Аналитическая статья
УДК 004.056+004.8+339.543; DOI: 10.61260/2218-130X-2026-2-65-81

АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОГО И ОБЪЯСНИМОГО АНАЛИЗА РИСКОВ ДЛЯ КОНТРОЛЯ ПОСЛЕ ВЫПУСКА ТОВАРОВ

✉Грызунов Виталий Владимирович.
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия.
Лемихов Иван Владимирович.
Главное управление МЧС России по Камчатскому краю,
г. Петропавловск-Камчатский, Россия
✉viv1313r@mail.ru

Аннотация. Актуальность исследования обусловлена критической необходимостью перехода таможенного администрирования Российской Федерации от автоматизации отдельных операций к интеллектуальным контурам поддержки принятия решений в соответствии со Стратегией развития до 2030 г. При этом сохраняется высокая цена ошибки должностного лица, растут требования к обоснованности проверок и адресности контроля. Возникает противоречие между необходимостью интеллектуализации постконтроля на основе искусственного интеллекта и высокой ответственностью инспекторов, ограниченностью времени, ростом слабых сигналов риска и недоверием к непрозрачным моделям типа «чёрного ящика». Цель работы – разработка архитектуры системы интеллектуального и объяснимого анализа рисков для контроля после выпуска товаров, ориентированной на безопасную апробацию в формате низкорискового пилота. Метод исследования базируется на проектировании четырёхконтурной микросервисной архитектуры, интегрирующей извлечение открытых сигналов, детерминированную интерпретацию искусственного интеллекта, оркестрацию действий по ситуации и интеллектуальный интерфейс к документам, а также на экономико-математическом моделировании нелинейного риск-скоринга и минимизации функции ожидаемых операционных потерь. В статье впервые обоснована концепция встроенной объяснимости, при которой контекстная компонента данных (источник, доверие, статус) обрабатывается синхронно с числовыми признаками, обеспечивая 100 % воспроизводимый трассировочный след решения. Представлена адаптивная система маршрутизации на основе атрибутированного мультиграфа, переводящая аналитический вывод в параметризованные сценарии реагирования, и когнитивная мультиагентная архитектура, симулирующая работу опытного инспектора с механизмом мета-когнитивной верификации. Показана эффективность трёхклассовой логики принятия решений, при которой промежуточный класс аналитической неопределённости обрабатывается автоматически, что снижает долю необоснованных глубоких проверок. Практическая значимость заключается в предоставлении концептуальной модели для бесшовной интеграции в действующие системы Федеральной таможенной службы Российской Федерации через защищённые API, а также в регламентации безопасного пилотирования в закрытом контуре на базе квантизованных Small Language Models. Экспериментальная апробация на синтетическом датасете подтвердила внутреннюю логическую связность архитектуры, работоспособность сквозной маршрутизации и математическую гарантию аддитивности объяснений детерминированной интерпретации искусственного интеллекта. Предложенный подход позволяет трансформировать стандартный риск-скоринг в процессуально обоснованный полуавтоматический контроль, обеспечивая юридическую значимость выводов искусственного интеллекта. Помимо таможенного администрирования, архитектура может применяться для построения доверенных систем поддержки принятия решений в других регуляторных органах, требующих верифицируемой аналитики и безопасной работы с данными.

Ключевые слова: объяснимый искусственный интеллект, постконтроль, управление рисками на основе данных, оркестрация действий, мультиагентная архитектура

Для цитирования: Грызунов В.В., Лемихов И.В. Архитектура интеллектуального и объяснимого анализа рисков для контроля после выпуска товаров // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2026. № 2. С. 65–81. DOI: 10.61260/2218-130X-2026-2-65-81

Analytical article

ARCHITECTURE OF INTELLIGENT AND EXPLAINABLE RISK ANALYSIS FOR POST-RELEASE CUSTOMS CONTROL

✉**Gryzunov Vitaly V.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia.
Lemikhov Ivan V.
Main Directorate of the Kamchatka Territory of EMERCOM of Russia,
Petropavlovsk-Kamchatsky, Russia
✉***viv1313r@mail.ru***

Abstract. The relevance of the study is driven by the critical need for Russian customs administration to transition from automating individual operations to intelligent decision-support frameworks, in accordance with the Development Strategy until 2030. At the same time, the high cost of official errors persists, while requirements for the justification of inspections and targeted control continue to grow. A contradiction arises between the need to intellectualize post-release control based on artificial intelligence, on the one hand, and the high responsibility of inspectors, time constraints, the growing number of weak risk signals, and mistrust of opaque «black box» models, on the other. The aim of this work is to develop an architecture for an intelligent and explainable risk analysis system for post-release customs control, designed for safe pilot testing in a low-risk environment. The research method is based on designing a four-loop microservice architecture that integrates open-source intelligence extraction, deterministic artificial intelligence interpretation, context-aware action orchestration, and an intelligent document interface, as well as on economic-mathematical modeling of nonlinear risk scoring and minimization of the expected operational loss function. The paper introduces, for the first time, the concept of built-in explainability, in which contextual data components (source, confidence, status) are processed synchronously with numerical features, ensuring a 100 % reproducible traceable decision trail. An adaptive routing system based on an attributed multigraph is presented, which translates analytical output into parameterized response scenarios, along with a cognitive multi-agent architecture that simulates the work of an experienced inspector with a metacognitive verification mechanism. The effectiveness of a three-class decision-making logic is demonstrated, whereby an intermediate class of analytical uncertainty is processed automatically, reducing the proportion of unjustified in-depth inspections. The practical significance lies in providing a conceptual model for seamless integration into existing Federal Customs Service of Russia systems via secure APIs, as well as in regulating safe piloting within a closed loop based on quantized small language models. Experimental validation on a synthetic dataset confirmed the internal logical coherence of the architecture, the operability of end-to-end routing, and the mathematical guarantee of additivity of deterministic artificial intelligence interpretation explanations. The proposed approach makes it possible to transform standard risk scoring into procedurally justified semi-automatic control, ensuring the legal significance of artificial intelligence outputs. Beyond customs administration, the architecture can be applied to build trusted decision-support systems in other regulatory bodies requiring verifiable analytics and secure data handling.

Keywords: explainable artificial intelligence, post-release control, data-driven risk management, action orchestration, multi-agent architecture

For citation: Gryzunov V.V., Lemikhov I.V. Architecture of intelligent and explainable risk analysis for post-release customs control // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2026. № 2. P. 65–81. DOI: 10.61260/2218-130X-2026-2-65-81

Введение

Цифровая трансформация таможенного администрирования в Российской Федерации смещает акцент с автоматизации отдельных операций к построению интеллектуальных контуров поддержки принятия решений[1]. В Стратегии развития таможенной службы Российской Федерации до 2030 года прямо закреплены использование искусственного интеллекта (ИИ) и обработки больших объёмов данных, развитие автоматизированных технологий выбора объектов контроля после выпуска товаров, а также достижение качественно нового уровня такого контроля на основе риск-ориентированного подхода. Одновременно Федеральная таможенная служба Российской Федерации (ФТС России) публично указывает на необходимость максимально автоматизировать выбор объектов контроля так, чтобы это обеспечивало обоснованность проверочных мероприятий.

В этих условиях возрастает не только технологическая, но и организационно-правовая нагрузка на должностное лицо таможенного органа. С одной стороны, от него требуется работа в логике цифровизации, аналитической обработки данных и адресного контроля. С другой стороны, сохраняется высокая цена ошибки, поскольку неправомерные решения, действия или бездействие должностных лиц влекут дисциплинарную, административную, уголовную и иную ответственность, а в дисциплинарном контуре возможны взыскания вплоть до увольнения[2].

Проблемный аспект исследования состоит в противоречии между, с одной стороны, растущими требованиями государства к интеллектуализации таможенного контроля, его автоматизации, снижению административной нагрузки на добросовестный бизнес и повышению результативности обязательных требований, а с другой – высокой ценой ошибки должностного лица, ограниченностью времени на анализ ситуации, ростом числа слабых сигналов риска и недоверием к непрозрачным моделям типа «чёрного ящика». В этих условиях одной лишь предиктивной модели недостаточно: необходима архитектура, которая сочетает выявление сигналов риска, объяснимость вывода, особенно сделанного ИИ, маршрутизацию действий и безопасную работу с документами и знаниями.

Цель исследования – разработать архитектуру интеллектуального и объяснимого анализа рисков для контроля после выпуска товаров, ориентированную на безопасную апробацию в формате пилота на базе таможенного органа или профильного вуза.

Общая задача исследования заключается в формировании концептуальной и прикладной модели контура аналитики рисков, сочетающего внешний слой открытых сигналов, объяснимый ИИ, адаптивную обработку ситуаций и защищённый интерфейс к документам и знаниям.

Частные задачи исследования состоят в следующем:

1. Критически проанализировать современные подходы к управлению рисками на основе данных (data-driven customs risk management), постконтролю и объяснимому ИИ (explainable AI, XAI).

2. Предложить функциональную архитектуру интеграции внешних сигналов риска, верифицируемой аналитики, оркестрации действий и RAG-интерфейса.

3. Описать математическую модель нелинейного риск-скоринга и логики обработки ситуации.

[1] Стратегия развития таможенной службы Российской Федерации до 2030 года: распоряжение Правительства Рос. Федерации от 23 мая 2020 г. № 1388-р. Доступ из инф.-правового портала «Гарант»

[2] Ст. 352. Ответственность таможенных органов и их должностных лиц. Таможенный кодекс Евразийского экономического союза. Доступ из инф.-правового портала «Гарант»

4. Оценить согласованность предложенной архитектуры с официальными стратегическими ориентирами ФТС России и доступной статистикой постконтроля;

5. Сформулировать параметры и ожидаемые метрики безопасного пилота.

Обзор литературы

В современной научной и прикладной литературе по таможенному администрированию прослеживается устойчивый сдвиг от классического профилирования риска к data-driven и ИИ-ориентированным моделям. В работе [1] показано, что технологически ориентированное и контролируемое данными управление таможенными рисками усиливает безопасность цепей поставок за счёт интеграции аналитики, ИИ и цифровых источников данных на всех этапах движения товара, включая стадию контроля после выпуска. При этом автор акцентирует внимание не только на предсказательной функции, но и на необходимости архитектурной связности решений в таможенном контуре.

Для непосредственно постконтроля показательна ситуация китайской таможни, исследованная в работе [2]. Автор рассматривает применение RPA + AI для анализа рисковых данных в аудите после выпуска и показывает, что результативность достигается не отдельным алгоритмом, а платформенной организацией слоёв инфраструктуры, данных, сервисов, аналитики и визуализации. Особенно важным для настоящего исследования является тезис о том, что информационная безопасность должна быть встроена в саму архитектуру аналитического робота как характеристика операционной среды, а не рассматриваться постфактум.

В российской профильной литературе также нарастает внимание к цифровизации постконтроля. В публикациях Российской таможенной академии [3, 4] подчёркивается, что применение элементов ИИ в автоматизации таможенных операций и в цифровизации контроля после выпуска товаров становится не факультативным, а стратегически необходимым направлением. Вместе с тем даже в этих работах основной акцент делается либо на автоматизацию контроля достоверности сведений, либо на общее направление цифровизации постконтроля, тогда как проблема объяснимости аналитического вывода и его интеграции с последующими действиями сотрудника остаётся раскрытой лишь частично.

Отдельный пласт исследований связан с XAI в системах поддержки принятия решений. Обзор [5] показывает, что XAI в системах поддержки принятия решений рассматривается как средство не только повышения прозрачности, но и доверия пользователей, операционной пригодности решений и соответствия требованиям подотчётности. Авторы подчёркивают, что в высокозначимых доменах объяснение должно быть связано с контекстом принятия решения, а не ограничиваться постфактум визуализацией важности признаков.

Авторы работы отмечают, что в критических системах поддержки принятия решений XAI повышает безопасность только тогда, когда встроен в трёхслойную модель: качество модели, понятность вывода и управляемость реакции. Иными словами, объяснимость сама по себе не даёт эффекта, если она не связана с процедурой действий после прогноза. Этот вывод непосредственно релевантен таможенному постконтролю, где риск-скоринг без обработки ситуации практически не снижает организационную неопределённость.

В международном таможенном контексте дополнительное значение приобретает использование открытых данных. Отчёт Всемирной таможенной организации (WCO)[3] по применению разведки по открытым источникам (OSINT) для усиления таможенного контроля показывает, что открытые источники уже рассматриваются как источник

[3] STUDY REPORT Unlocking the Value of Open-Source Intelligence for Customs Enforcement JULY 2024. URL: https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/security-programme/osint-report_final.pdf (дата обращения: 14.04.2026)

дополнительных индикаторов риска в системе управления риском (СУР), однако относительно немногие таможни внедряют их системно. Это указывает на противоречие: с одной стороны, направление признано перспективным, с другой – отсутствуют устоявшиеся архитектурные модели его безопасной и объяснимой интеграции в контроль после выпуска.

Отчёт WCO по внедрению AI/ML в таможню[4] подчёркивает, что для практической апробации ИИ необходимы пилотирование, межфункциональные команды, оценка рисков и происхождения данных, правовое и этическое обоснование и повышение квалификации персонала, что подчёркивает актуальность настоящего исследования, поскольку оно ориентировано не на абстрактную модель, а на пилотное внедрение в закрытом и низкорисковом контуре.

Таким образом, анализ литературы показывает следующее. Во-первых, достаточно хорошо изучены управление риском на основе данных и ИИ-подходы в таможне. Во-вторых, отдельно развиваются исследования по XAI в системах поддержки принятия решений. В-третьих, появляется прикладной интерес к OSINT в ходе усиления таможенного контроля. Однако в литературе практически отсутствует целостная модель, которая одновременно:

1. Использует открытые сигналы риска.
2. Обеспечивает проверяемость и объяснимость вывода.
3. Переводит аналитический вывод в адаптивный сценарий действий по ситуации постконтроля.
4. Содержит безопасный интерфейс к документам и знаниям в изолированном контуре.

На восполнение именно этого пробела и направлено настоящее исследование. Научная новизна состоит в разработке интегральной архитектуры объяснимой аналитики рисков на примере контроля после выпуска.

Материалы и методы

Методологическую основу исследования составили системный, структурно-функциональный, сравнительно-правовой, экономико-математический и проектно-архитектурный подходы.

В качестве общих методов познания использованы анализ, синтез, абстрагирование, классификация, сравнение и моделирование. В качестве частных методов применены:

– контент-анализ стратегических и нормативно-организационных документов ФТС России и Правительства Российской Федерации;

– сравнительный анализ международных практик WCO и научных публикаций по «умной» таможне, контроля после выпуска и XAI;

– архитектурное моделирование контуров анализа рисков;

– математическое описание нелинейного интегрального риск-скоринга и логики обработки ситуации;

– анализ синтетического датасета демонстрационного прототипа.

Эмпирическую базу исследования составили:

– Стратегия развития таможенной службы Российской Федерации до 2030 г. и официальный план её реализации;

– официальные сведения ФТС России о результатах контроля после выпуска товаров за 2024 и 2025 г.;

– официальные материалы ФТС России по цифровизации, автоматизации выбора объектов постконтроля и применению ИИ;

[4] Detailed Report on The Adoption of Artificial Intelligence and Machine Learning in Customs March 2025. URL: https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/smart-customs/public-version_detailed-report-on-the-adoption-of-ai-and-ml-in-customs.pdf?la=en (дата обращения: 14.04.2026)

– отчёты WCO по OSINT и AI/ML в таможне;

– авторский демонстрационный прототип, построенный на синтетическом датасете из 20 000 ситуаций контроля после выпуска с 47 входными признаками и трёхклассовой целевой переменной.

Акцент в прототипе сделан на постконтроле, поскольку контроль после выпуска товаров является одним из наиболее результативных направлений контрольной деятельности. По данным ФТС России, за 2024 г. по результатам контроля после выпуска товаров были выявлены нарушения на сумму 56,4 млрд руб.[5], а за 2025 г. – на сумму 49,3 млрд руб.[6] Эти данные подтверждают и сохраняющуюся значимость постконтроля, и необходимость повышения адресности отбора объектов проверки, поскольку дальнейшее наращивание эффективности невозможно без более качественной риск-аналитики.

Синтетический датасет сгенерирован путём комбинации статистических распределений маргинальных признаков, заданных корреляционных матриц и сценарийной инъекции рисковых паттернов (аффилированность, логистические аномалии, документарные разрывы) с добавлением гауссова шума. Генерация не имела целью воспроизвести реальные риски в потоке ФТС России, синтетический датасет использовался как среда для стресс-тестирования архитектуры, валидации сквозной маршрутизации и демонстрации работы предлагаемой технологии объяснимости VERIDIC.

Архитектурная постановка задачи

Предлагаемая архитектура включает четыре взаимосвязанных контура, проектируемых как микросервисная надстройка (REST/gRPC API) к действующим информационным системам ФТС России (автоматизированные системы управления рисками (АСУ СУР), комплекс программных средств (КПС) «Постконтроль», АИСТ-М), без создания отдельного графического интерфейса.

1. Контур внешних сигналов риска (OSINT). Предназначен для извлечения дополнительных индикаторов из открытых источников: цифрового профиля участника внешнеэкономической деятельности (ВЭД), структуры контрагентов, косвенных признаков аффилированности, логистических аномалий.

В рамках предлагаемой архитектуры процесс OSINT-разведки формализован не как простой парсинг, а как работа абстрактной вычислительной машины на итеративно расширяемом графе знаний $G = (V, E)$ [6].

Задача контура сводится к поиску скрытых (недекларируемых) свойств участника ВЭД, например, теневой аффилированности или реальной логистики X^{conf} на основе известных публичных атрибутов X^{pub} (регистрационные данные, открытые профили контрагентов, логистические треки). Контур использует набор аналитических предикатов (инструментов поиска), порождающих новые ребра графа – семантические связи между публичными фактами.

Важнейшим механизмом работы контура является *триангуляция* – поиск нескольких независимых (непересекающихся) путей в графе G, сходящихся к одному скрытому свойству X^{conf}. Вывод о наличии риска, например, связи импортера с фирмой-однодневкой, считается достоверным только при условии сходимости доказательств из независимых источников.

[5] Итоги деятельности таможенных органов по осуществлению таможенного контроля после выпуска товаров за IV квартал 2024 г. URL: https://customs.gov.ru/activity/results/itogi-deyatel-nosti-tamozhennyx-organov-po-osushhestvleniyu-tamozhennogo-kontrolya-posle-vypuska-tovarov/document/618280 (дата обращения: 15.04.2026)

[6] Итоги деятельности таможенных органов по осуществлению таможенного контроля после выпуска товаров за 2025 г. URL: https://customs.gov.ru/activity/results/itogi-deyatel-nosti-tamozhennyx-organov-po-osushhestvleniyu-tamozhennogo-kontrolya-posle-vypuska-tovarov/document/676258 (дата обращения: 15.04.2026).

Для ограничения потребления вычислительных ресурсов и предотвращения бесконечного поиска в архитектуру контура встроена строгая логическая функция останова (F_{stop}).

Процесс сбора открытых данных рассматривается как управляемая процедура фонового анализа, завершаемость которой определяется системой предельных условий. Завершение процедуры фиксируется при наступлении одного из следующих состояний: Goal Reached – достижение заданного порога уверенности $A_{threshold}$ за счёт комбинирования независимых публичных индикаторов; Lead Exhaustion – исчерпание множества доступных зацепок, при котором расширение графа публичных свойств не приводит к появлению новых информативных признаков; Resource Depletion – исчерпание выделенного ресурса анализа, выраженное в превышении временного лимита T_{limit} либо допустимого числа API-запросов, отведённых на обработку одной декларации.

Выявленные в контуре OSINT графовые связи не рассматриваются как самостоятельное юридическое основание для начисления таможенных платежей либо назначения мер процессуального характера. Их функция сводится к формированию дополнительного слоя признаков, статистически и логически значимых для последующего скоринга. Следовательно, указанные связи выступают не доказательственным, а триггерным элементом: они обеспечивают передачу обогащённого вектора признаков в контур VERIDIC, после чего становятся основанием для инициации запроса документов в порядке ст. 326 Таможенного кодекса Евразийского экономического союза (ТК ЕАЭС) либо для аналитической подготовки решения, предшествующей назначению таможенной проверки по ст. 331 ТК ЕАЭС.

Функционирование контура реализуется в режиме однонаправленного парсинга открытых источников. При этом выполняется фильтрация персональных данных, а также ограничение на обработку сведений, не относящихся к допустимому множеству открытых признаков. Такое построение контура обеспечивает отделение внешнего аналитического слоя от чувствительных внутренних данных и, тем самым, создаёт условия для его использования в закрытой архитектуре таможенного анализа.

2. Контур объяснимого и верифицируемого анализа VERIDIC предназначен для совместного вычисления риск-балла и интерпретации полученного результата. В отличие от аппроксимационных методов объяснимого ИИ, таких как SHAP и LIME, функционирующих как внешняя надстройка над уже сформированным прогнозом, VERIDIC реализует внутреннюю двухконтурную схему вычислений. В рамках данной схемы каждое основное числовое значение v, соответствующее признаку декларации, агрегированному показателю либо промежуточному параметру модели, обрабатывается синхронно с контекстной компонентой γ, логически связанной с данным значением.

Под контекстной компонентой γ понимается структурированный метапризнак, инкапсулирующий происхождение значения, уровень доверия к источнику, признак валидности и статус безопасности. Тогда выполнение любой вычислительной операции в модели, в том числе прохождение по ансамблю деревьев решений или по слоям иной нелинейной структуры, представляется как преобразование пары $(v_{in}, \gamma_{in}) \rightarrow (v_{res}, \gamma_{res})$. Из этого следует, что объяснимость не добавляется к результату постфактум, а формируется непосредственно в процессе вычисления.

В результате основной контур формирует итоговый риск-балл v_{res}, характеризующий вероятность нарушения, контекстный контур формирует структуру γ_{res}, которая содержит точный, детерминированный и 100 % воспроизводимый трассировочный след: какие именно данные, из каких источников и с каким процессуальным статусом привели к данному баллу.

Дополнительно в контур интегрирован многоуровневый протокол защиты Tiered Protection Protocol (TTP). В базовом режиме (Уровень 0) система обрабатывает тривиальные декларации с максимальной производительностью. При обнаружении аномалий, например, подозрительных инъекций в метаданных документов или попытках численных атак на модель типа Numerical DoS, система динамически повышает уровень TTP, включая углубленный аудит и отслеживание помеченных данных (taint tracking).

Для должностного лица таможенного органа архитектура VERIDIC решает главную проблему применения ИИ: она обеспечивает юридическую значимость вывода. Инспектор получает не абстрактное «влияние признака», а строгий аудит вычислительной траектории, гарантирующий, что рассчитанный риск опирается на целостные и допустимые данные. То есть, если ИИ говорит: «Цена занижена», инспектор спросит: «Откуда ты взял базовую цену? Из контракта (высокое доверие) или нашел на китайском сайте через OSINT (низкое доверие)?». Архитектура VERIDIC благодаря компоненте γ автоматически выведет на экран инспектора уровень доверия и источник данных, что позволит легко сформировать рапорт на проверку.

3. Контур оркестрации действий по ситуации (ONYX). Переводит аналитический вывод в сценарий реагирования: автоматическая генерация запроса пояснений, фоновый мониторинг, аналитическая оценка инспектором или эскалация на назначение проверки. Задача контура – преодолеть разрыв между выявлением риска и операционным действием, минимизируя ручной разбор пограничных ситуаций.

Данный контур базируется на архитектурной модели X-адаптивного управления (Organizational-technical Networked Yield X-adaptive system). В рамках ONYX таможенный постконтроль рассматривается как единое вычислимое пространство состояний, формализованное в виде атрибутированного мультиграфа S, где вершинами (V) выступают элементы разной природы (участники ВЭД, должностные лица, документы, контуры VERIDIC и AIVANT), а рёбрами (E) – связи между ними, например, «администрирует», «ожидает пояснений».

В нормальном режиме работы, когда риски приемлемы, система находится во множестве штатных состояний $S_{intended}$. Обнаружение сигнала риска контуром VERIDIC (переход риск-балла в классы $Y_i = 1$ или $Y_i = 2$) математически трактуется как переход графа ситуации в инцидентное состояние $S_{incident}$.

Обнаружение значимого сигнала риска в контуре VERIDIC, сопровождающееся переходом риск-балла в классы $Y_i = 1$ или $Y_i = 2$, трактуется как перевод графа ситуации в инцидентное состояние $S_{incident}$. Возврат к целевому режиму функционирования обеспечивается оператором управления R, который применяет к текущему состоянию параметризованные шаблоны восстановления из множества P.

Каждый шаблон задаётся парой (предусловие; постусловие), где предусловие определяет конфигурацию состояния, при которой шаблон является допустимым, а трансформация описывает детерминированное изменение графа. Постусловие является критерием успешного применения шаблона восстановления. Для случая среднего риска, соответствующего $Y_i = 1$, механизм обработки реализуется как кросс-уровневая компенсация в логике ONYX. Если риск-балл требует аналитической отработки, но текущая пропускная способность узлов типа «Сотрудник» (уровень персонала модели ONYX) оказывается ниже требуемой вследствие высокой загрузки инспектора, то направление ситуации в очередь ручного анализа не выполняется.

Вместо этого оператор R осуществляет перенастройку маршрута обработки: к графу добавляется связь с программным узлом (уровень программного обеспечения), то есть результат детерминированной интерпретации VERIDIC передаётся в контур AIVANT для формирования проекта запроса документов и фоновой аналитической подготовки. Следовательно, достигается реакция на сигнал риска без превышения допустимой когнитивной нагрузки на должностное лицо и без разрушения общей производительности системы.

Использование мультиграфовой модели ONYX обеспечивает выполнение инварианта безопасности. Под данным инвариантом понимается невозможность формирования управляющего воздействия, если не выполнены предикаты валидности соответствующего состояния. В частности, назначение проверки не допускается в ситуации, когда в графе отсутствует связка с подтверждёнными индикаторами риска либо нарушена допустимая конфигурация источников аналитического вывода.

Таким образом, маршрутизация реакции осуществляется не произвольно, а в пределах формально определённого множества допустимых состояний. Это исключает хаотичную генерацию требований к бизнесу и минимизирует ручной разбор пограничных ситуаций.

Элементы ONYX успешно апробированы при создании киберполигона МЧС России как системы, адаптирующейся к разноплановой нагрузке в ходе целенаправленных разрушающих воздействий злоумышленников [7].

4. Контур интеллектуального интерфейса к документам и знаниям (AIVANT). В отличие от стандартных систем информационного поиска (RAG), которые способны транслировать только эксплицитное знание (цитирование нормативных актов), AIVANT представляет собой мультиагентную когнитивную архитектуру, предназначенную для извлечения и применения имплицитных (неформализованных) стратегий таможенного контроля [8].

Основываясь на дуальной теории когнитивных процессов (Канеман), архитектура AIVANT симулирует работу опытного инспектора через взаимодействие двух агентов:

1. Агент-интуит (System 1): опирается на граф когнитивных операторов, обученный на паттернах принятия решений опытными должностными лицами (тактика выбора документов для запроса, распознавание логистических аномалий, стратегии сужения зоны неопределенности). Агент осуществляет быстрое распознавание паттернов в данных, поступающих от контуров OSINT и VERIDIC, и генерирует гипотезу проверки.

2. Агент-критик (System 2): осуществляет медленную фактологическую кросс-валидацию гипотезы. При обработке ситуации агент AIVANT реализует гибридный ретривал, сочетающий векторный поиск по телу документов и онтологическую навигацию по графу базы знаний ФТС России. Такое комбинирование позволяет не ограничиваться семантической близостью текстовых фрагментов, а проверять гипотезу на соответствие нормативным и процедурным ограничениям, включая положения ТК ЕАЭС, локальные регламенты и профили риска. Следовательно, результат поиска определяется не только языковой релевантностью, но и структурной согласованностью с нормативной средой.

Ключевая особенность AIVANT состоит в наличии механизма метакогнитивной верификации вывода. Под данным механизмом понимается оценка пределов собственной применимости модели в конкретной аналитической ситуации. Если объём и качество доступного контекста недостаточны для формирования устойчивого ответа, система не переходит к генерации правдоподобного, но непроверенного вывода. Вместо этого выполняется расчёт доверительного интервала интерпретации и формируется ответ с явным указанием степени достоверности, ограничений применимости и требуемых дополнительных данных.

В результате инспектор получает не категоричное утверждение, а калиброванный аналитический вывод, например: «С высокой вероятностью выявлено занижение таможенной стоимости; для перехода к применению метода 6 требуется запрос экспортной декларации». Такая форма ответа реализует функцию управляемого отказа, при которой система не подменяет отсутствующие основания генеративной догадкой, а фиксирует границы допустимого вывода. Следовательно, уменьшается вероятность принятия неправомерных решений в условиях неполного информационного обеспечения.

Развёртывание AIVANT предполагается осуществлять исключительно в закрытом контуре на базе ведомственных центров обработки данных ФТС России. Вычислительная обработка, хранение базы знаний и генерация ответов не должны переноситься на локальные рабочие места инспекторов, поскольку в противном случае возрастает риск фрагментации контекста, нарушения требований информационной безопасности и снижения управляемости обновления моделей.

Использование квантизованных моделей малого размера (Small Language Models, 7B–8B параметров) в связке с фреймворками, оптимизированными для серверных CPU-вычислений, например, OpenVINO или Llama.cpp, позволяет отказаться от дорогостоящих внешних GPU-кластеров. Для компенсации ограничений скорости инференса (генерации токенов в секунду) на процессорных мощностях, обработка массивов документов

по ситуации «Класса 1» (аналитическая неопределенность) реализуется через механизм асинхронных фоновых очередей. Нагрузка на элементы системы распределяется согласно модели, приведённой в работе [9].

Таким образом, система заранее формирует справку-обоснование до того, как инспектор откроет дело, что полностью сохраняет оперативность работы должностного лица.

В совокупности архитектура реализует переход от простого риск-скоринга к объяснимому полуавтоматическому контролю после выпуска.

Экономико-математическая модель риска и обработки ситуации

Для формализации решения по ситуации i используется нелинейная функция скоринга:

$$R_i = F(O_i, D_i, C_i, B_i),$$

где F– обучаемая нелинейная модель, которая в прототипе реализована на базе градиентного бустинга над деревьями решений (CatBoost); O_i, D_i, C_i, B_i – агрегированные блоки признаков (OSINT, документарный, цепочки поставок, поведенческий).

Решение по ситуации Y_i (обработка) формируется путём разбиения непрерывной оценки R_i на три класса с помощью пороговых значений τ_1, τ_2:

$$Y_i = \begin{cases} 0, & R_i < \tau_1, \\ 1, & \tau_1 \le R_i < \tau_2, \\ 2, & R_i \ge \tau_2. \end{cases}$$

где $Y_i = 0$ соответствует состоянию, при котором контроль после выпуска не требуется; $Y_i = 1$ соответствует состоянию автоматизированной предварительной обработки, включающей генерацию запросов и фоновый мониторинг; $Y_i = 2$ соответствует состоянию, при котором рекомендуется контроль после выпуска.

Пороговые значения τ_1 и τ_2 определяются не эвристически, а посредством минимизации функции ожидаемых операционных потерь $L(\tau_1, \tau_2)$ на валидационной выборке. Поскольку фактическое наличие риска описывается бинарной переменной $y_i \in \{0,1\}$, а множество управляющих решений включает три альтернативы, функция потерь должна учитывать стоимость каждого типа управленческого отклонения. В этом случае потери от решения Y_i относительно фактического класса y_i могут быть заданы выражением:

$$L(\tau_1, \tau_2) = \sum_{i=1}^{N} \big(c_{FN} \cdot I(Y_i = 0 \wedge y_i = 1) + c_{process} \cdot I(Y_i = 1) + c_{FP} \cdot I(Y_i = 2 \wedge y_i = 0) \big),$$

где $I(\cdot)$ – индикаторная функция, принимающая значение 1 при истинности условия и 0 в противном случае; c_{FN} – стоимость пропуска реального риска, интерпретируемая как потенциальный ущерб бюджету или недоимка; $c_{process}$ – стоимость автоматизированной аналитической обработки, включающая вычислительную нагрузку и временные издержки; c_{FP} – стоимость ложного срабатывания, выражающаяся в избыточной административной нагрузке на добросовестный бизнес и инспекторский контур.

Оптимальные значения порогов находятся как решение задачи

$$(\tau_1^*, \tau_2^*) = \arg\min_{\tau_1, \tau_2} L(\tau_1, \tau_2).$$

Такая постановка позволяет не только формировать решение по классу риска, но и балансировать нагрузку между автоматизированным и ручным контурами обработки. Следовательно, снижение числа необоснованных глубоких проверок достигается не за счёт произвольного ужесточения порогов, а за счёт оптимизации на множестве стоимостных ограничений.

Для слоя объяснимости вводится функция интерпретации VERIDIC:

$$E_i = \{(f_j, s_j, p_j, c_j)\}_{j=1}^{m},$$

где f_j – признак; s_j – его детерминированный вклад в итоговое решение; p_j – происхождение признака; c_j – уровень доверия к источнику, соответствующий контекстной компоненте γ. В отличие от аппроксимационных методов, основанных на вероятностном семплировании и допускающих стохастическую вариативность результата, алгоритм VERIDIC опирается на структурную трассировку путей в ансамбле деревьев решений. Это обеспечивает аддитивную декомпозицию прогноза, задаваемую равенством:

$$R_i = F_{base} + \sum_{j=1}^{m} s_j,$$

где F_{base} – базовое значение модели. Из данного равенства следует, что суммарный вклад признаков полностью воспроизводит отклонение прогноза от базового уровня. Отсутствие аппроксимационной погрешности создаёт условия для полной воспроизводимости результата при повторном запуске на одном и том же наборе данных, что критично для аудита решений в таможенных органах.

Следовательно, итоговое решение по ситуации представляется как расширенная структура:

$$\Omega_i = (R_i, Y_i, E_i),$$

где R_i – риск-балл; Y_i – решение по обработке; E_i – вектор детерминированных объяснений. Именно наличие структуры Ω_i, а не только значения R_i, делает систему пригодной для контуров, в которых прогноз должен сопровождаться проверяемым основанием.

Численная апробация экономико-математической модели выполняется на контрольной выборке из 10 ситуаций. В качестве условных стоимостных коэффициентов принимаются: $c_{FN} = 500\,000$ руб. – стоимость пропуска реального риска; $c_{FP} = 50\,000$ руб. – издержки необоснованной проверки добросовестного участника ВЭД; $c_{process} = 5\,000$ руб. – стоимость автоматизированной предварительной обработки средствами AIVANT. Указанный набор коэффициентов используется исключительно как формализованный пример для демонстрации механизма минимизации потерь.

Пошаговый расчёт функции потерь для различных сценариев работы модели представлен в таблице.

Таблица

Расчет вклада ситуаций в функцию операционных потерь

№	Истинный класс (y_i)	Решение модели (Y_i)	Статус классификации	Потери (ℓ_i), руб.
1	0 (нет риска)	0 (нет контроля)	True Negative (Верно)	0
2	1 (риск есть)	2 (проверка)	True Positive (Верно)	0
3	0 (нет риска)	2 (проверка)	False Positive (Ложное срабатывание)	50 000
4	1 (риск есть)	0 (нет контроля)	False Negative (Пропуск риска)	500 000
5	0 (нет риска)	1 (предобработка)	Буферная зона (безопасная проверка)	5 000
6	1 (риск есть)	1 (предобработка)	Буферная зона (безопасная проверка)	5 000

№	Истинный класс (y_i)	Решение модели (Y_i)	Статус классификации	Потери (ℓ_i), руб.
7	0 (нет риска)	0 (нет контроля)	True Negative (Верно)	0
8	1 (риск есть)	2 (проверка)	True Positive (Верно)	0
9	0 (нет риска)	1 (предобработка)	Буферная зона (безопасная проверка)	5 000
10	1 (риск есть)	1 (предобработка)	Буферная зона (безопасная проверка)	5 000

Итоговое значение функции потерь $L(\tau_1, \tau_2)$ для данной конфигурации составит 570 000 руб. Доминирующий вклад в потери вносит пропуск одного реального риска (ситуация № 4). Применение промежуточного класса 1 обходится системе всего в 5 000 руб. за ситуацию, что позволяет направлять сомнительные ситуации на машинную аналитику (генерацию запросов) без критических финансовых и репутационных потерь.

На валидационной выборке алгоритм перебирает пары порогов (τ_1, τ_2), находя оптимум. Например, смещение порогов к значениям (0,45; 0,75) в симуляции снижает ожидаемые потери до 412 000 руб. за счет балансировки между c_{FN} и c_{FP}.

Формирование структуры Ω_i на примере реальной ситуации

Далее представлено практическое формирование вектора объяснений E_i для декларации на ввоз микросхем (ТН ВЭД 8542):

– риск-балл (R_i): 0,73 (базовое значение модели $F_{base} = 0{,}14$);

– обработка (Y_i): поскольку $0{,}73 \geq \tau_2 = 0{,}65$, принимается решение $Y_i = 2$ (рекомендуется контроль).

Вектор объяснений (E_i). Система генерирует следующий детерминированный набор атрибутов:

– price_deviation: вклад $s_1 = +0{,}28$; происхождение $p_1 = \text{FTS\_price\_db}$; доверие $c_1 = 0{,}95$;

– hidden_affiliation: вклад $s_2 = +0{,}31$; происхождение $p_2 = \text{OSINT\_triangulation}$; доверие $c_2 = 0{,}82$;

– route_anomaly: вклад $s_3 = +0{,}19$; происхождение $p_3 = \text{OSINT\_graph}$; доверие $c_3 = 0{,}78$;

– counterparty_age: вклад $s_4 = -0{,}12$; происхождение $p_4 = \text{EGRUL\_database}$; доверие $c_4 = 0{,}99$;

– importer_experience: вклад $s_5 = -0{,}07$; происхождение $p_5 = \text{customs\_history}$; доверие $c_5 = 0{,}97$.

Проверка аддитивности (математическая гарантия VERIDIC) выполняется абсолютно точно:

$$R_i = 0{,}14 + (0{,}28 + 0{,}31 + 0{,}19 - 0{,}12 - 0{,}07) = 0{,}73.$$

В машинном представлении структура Ω_i транслируется в систему АИСТ-М в формате JSON с хэшем воспроизводимости (audit trail). При этом к инспектору попадает на один агрегированный балл, а расшифровка, почему именно такой балл получен: *«Рост риска вызван занижением цены на 34 % (база ФТС России, доверие 95 %), аффилированность контрагентов (OSINT, доверие 82 %). Факторы, влияющие на снижение риска – срок существования контрагента (ЕГРЮЛ, доверие 99 %). Рекомендовано запросить экспортную декларацию поставщика».*

Описанная архитектура предоставляет возможность проводить аудит каждого решения ИИ и конкретные проверяемые аргументы для составления отчёта о проведении таможенной проверки.

Исследовательский прототип и распределение решений

Прототип, представленный в настоящей работе, использует синтетический датасет из 20 000 ситуаций контроля после выпуска, каждая из которых оценивалась по 47 входным признакам. Целевая переменная включает три класса:

– класс 0 (низкий риск) – 7 696 ситуаций (38,48 %);

– класс 1 (средний риск) – 10 080 ситуаций (50,40 %);

– класс 2 (высокий риск) – 2 224 ситуации (11,12 %).

Цели эксперимента на тестовых данных носят архитектурно-методологический характер, а не оценочно-превентивный. Исследование не ставило задачей отразить реальную долю рискованных ситуаций в потоке ФТС России или спрогнозировать их процентное соотношение. Задачи прототипа:

1. Доказать работоспособность VERIDIC в интерпретации нелинейных решений и генерации человеко-читаемых, процессуально обоснованных пояснений («почему инспектор может прийти с проверкой»);

2. Продемонстрировать сквозную отработку всех элементов архитектуры: расследование OSINT → нелинейный скоринг → детерминированное объяснение → маршрутизация ONYX → контекстная поддержка AIVANT.

В отличие от реальной операционной среды ФТС России в моделировании намеренно используется увеличенная доля класса 1 (50,4 %) как стресс-тест для контура ONYX и AIVANT: система должна не «сваливать» половину массива на ручную проверку, а автоматически фильтровать пограничные ситуации через генерацию запросов пояснений и фоновый мониторинг. Такая форма распределения согласуется с официальной логикой ФТС России, согласно которой качественно новый контроль после выпуска должен сочетать риск-ориентированный подход, повышение эффективности проверочных мероприятий и снижение их количества.

Контрольные ситуации и логика объяснения

Наиболее показательна ситуация с высоким риском, когда итоговое решение «рекомендуется контроль после выпуска» формируется по совокупности факторов. VERIDIC выводит детерминированный набор (f_j, s_j, p_j, c_j), в котором каждый признак сопровождается его происхождением (декларация, логистический трек, открытый реестр, контрагент) и указанием точного вклада в итоговый результат. Это разрешает проблему «чёрного ящика» в работе с ИИ и соответствует многофакторной логике действий инспектора.

Ситуация с низким риском может описывать импортёр с большой предысторией, давней регистрацией, постоянным адресом, низкой ценовой волатильностью и тривиальной логистикой. Ситуация со средним риском характеризует зону неопределённости, в которой некоторые факторы увеличивают риск, а некоторые – снижают его. Именно для такого класса ONYX рекомендует запрос уточняющих документов или выполнение других уточняющих действий через интеллектуальный интерфейс AIVANT, сокращая необходимость ручного вмешательства.

Ограничения исследования и логика дальнейшей проверки

Настоящее исследование имеет очевидные ограничения:

1. Эмпирическая часть основана на синтетическом датасете, а не на историческом массиве ФТС России.

2. Количественные эффекты пока не могут рассматриваться как эксплуатационно подтверждённые KPIs.

3. Архитектура проверена на демонстрационном уровне, а не в реальном процессе.

Именно поэтому корректно говорить не о достигнутом экономическом эффекте, а об ожидаемых метриках пилота. В качестве таких метрик целесообразно рассматривать:

– формальные метрики классификации: точность, полнота, F1-score для высокорискового класса (2), ROC-AUC, калибровочная ошибка;

– операционные метрики: изменение точности доотбора объектов контроля после выпуска, снижение времени первичной аналитической обработки ситуаций, снижение доли необоснованных направлений в глубокий постконтроль, оценка понятности вывода пользователями (Likert-шкала), удобство работы с документами и основаниями.

Все метрики должны фиксироваться на изолированном пилоте, не влияющем на реальные решения в режиме онлайн. Интеграция с АСУ СУР/КПС «Постконтроль» должна осуществляться исключительно через защищённые API с журналированием всех вызовов и результатов в соответствии с требованиями Федеральной службы по техническому и экспортному контролю и внутренними регламентами информационной безопасности ФТС России.

Практические рекомендации

1. Рассматривать внедрение предложенной архитектуры не как масштабный проект, а как низкорисковую пилотную апробацию. Наиболее рациональный формат – изолированный пилот длительностью 3–4 мес. на синтетическом, обезличенном или историческом учебном массиве.

2. Разворачивать пилот исключительно в закрытом контуре. Никакие служебные данные, профили участников ВЭД и результаты аналитики не должны передаваться во внешние облачные сервисы. OSINT-контур должен работать как однонаправленный парсер открытых сигналов, а LLM/RAG-компоненты – как локальное решение на базе квантизованных Small Language Models, оптимизированных под ведомственные вычислительные ресурсы.

3. Запускать пилот по двухэтапной схеме. На первом этапе – апробация на базе профильного вуза или академической площадки с использованием синтетических и обезличенных данных; на втором – ретроспективное тестирование на историческом массиве конкретного таможенного органа под контролем экспертной группы.

4. Обмен данными с АСУ СУР и КПС «Постконтроль» целесообразно реализовать через внутренние защищённые API, в частности REST/gRPC-интерфейсы. Поскольку интерфейсы действующих таможенных систем характеризуются жёсткой табличной структурой и ограниченной изменяемостью экранных форм, интеграция предлагаемой архитектуры не должна предполагать модификацию пользовательского фронтенда АИСТ-М. В противном случае возрастает стоимость внедрения и снижается организационная приемлемость пилота. Текстовые объяснения VERIDIC и сценарии, формируемые средствами RAG-контуров, могут транслироваться двумя способами. Во-первых, краткие выводы могут маршрутизироваться в существующие штатные поля, например, в разделы служебных отметок или описания профиля риска. Во-вторых, развернутый аналитический вывод может формироваться в виде машиночитаемого документа формата XML/PDF с последующим автоматическим прикреплением к электронному досье по конкретной декларации. Такая схема обеспечивает бесшовную доставку сложной аналитики в привычную рабочую среду инспектора без необходимости переработки интерфейсного слоя информационных систем ФТС России.

5. Для таможенного органа польза пилота должна фиксироваться в измеримых категориях. К таким категориям относятся: увеличение адресности контроля, выражаемое как рост доли подтверждённых нарушений при проведении контроля после выпуска; сокращение времени первичной обработки ситуации; сокращение доли решений, впоследствии отменённых по жалобам; число положительных оценок пользователей о том, насколько аргументирован и понятен вывод системы.

6. Для вуза формулировать пользу как формирование центра компетенций. Апробация такой архитектуры на академической площадке даёт базу для магистерских и аспирантских исследований, прикладной учебный стенд по цифровой таможне и возможность стать пилотной площадкой по применению объяснимого ИИ в таможенном контроле.

7. Фиксировать заранее ожидаемые, а не вымышленные KPIs пилота. Корректно задавать диапазоны проверки гипотез: целевой прирост F1-score для класса 2, сокращение времени обработки ситуации на 15–30 %, снижение доли ложных срабатываний класса 2 до <8%, рост пользовательской оценки понятности вывода до > 4.0/5.0. Конкретные значения определяются только после фиксации базовой линии на историческом или учебном массиве.

Заключение

Проведённое исследование позволяет сделать следующие выводы:

1. Цифровая трансформация таможенного контроля в Российской Федерации объективно требует перехода от разрозненных автоматизированных модулей к связанным архитектурам интеллектуальной поддержки принятия решений. Стратегические документы ФТС России и Правительства Российской Федерации прямо закрепляют курс на ИИ, большие данные, автоматизацию контроля после выпуска и повышение обоснованности проверок.

2. Научная и прикладная литература подтверждает перспективность управления рисками на основе данных, применения ИИ в постконтроле, расширение системы поддержки принятия решения за счёт интеграции объяснимого ИИ и OSINT. Однако интегральная модель, объединяющая эти контуры в единую доверенную архитектуру постконтроля, требует снятия введённых ограничений.

3. Предложенная архитектура, включающая контуры OSINT, VERIDIC, ONYX и AIVANT, устраняет разрыв между выявлением сигнала риска, объяснением вывода, выбором операционного сценария и работой с документами и знаниями. VERIDIC обеспечивает детерминированную и воспроизводимую интерпретацию нелинейных решений, выступая альтернативой стохастическим методам атрибуции.

4. Экономико-математическая модель нелинейного риск-скоринга и трёхклассовой маршрутизации показывает, что для постконтроля более адекватна не бинарная логика, а выделение промежуточного класса аналитической неопределённости с автоматизированной предварительной обработкой.

5. Результаты демонстрационного прототипа на синтетических данных нельзя интерпретировать как доказанное внедренческое преимущество, однако они подтверждают внутреннюю логическую связность архитектуры, работоспособность VERIDIC в генерации процессуально значимых объяснений и соответствие стратегическому вектору ФТС России: адресность контроля, объяснимость вывода и снижение числа необоснованных глубоких проверок.

Список источников

1. Vijayakumar S. Technology–centric and Data‑Driven Customs Risk Management for Supply Chain Security // World Customs Journal. 2025. Vol. 19. № 1. P. 38–63.

2. Gao Q., Kuang Z. Can robotic process automation technology enable risk data analysis for customs' post-clearance audit: a China customs case study // World Customs Journal. 2023. Vol. 17. № 2. P. 93–104.

3. Афонин П.Н., Лебедева А.Ю. Применение искусственного интеллекта для анализа массива данных, формируемых с использованием интегрированной информационной системы пункта пропуска // Вестник Российской таможенной академии. 2024. № 1. С. 97–112.

4. Прокопенко А.А. Концептуальная модель развития сквозного процесса документального и фактического таможенного контроля // Вестник Российской таможенной академии. 2024. № 1. С. 173–182.

5. Kostopoulos G., Davrazos G., Kotsiantis S. Explainable artificial intelligence–based decision support systems: a recent review // Electronics. 2024. Vol. 13. № 14. P. 2842.

6. Грызунов В.В. Формальный фреймворк для OSINT-нарушителя и защитника // Информационно-управляющие системы. 2025. № 5 (138). С. 22–34. DOI 10.31799/1684-8853-2025-5-22-34

7. Грызунов В.В., Шестаков А.В. Модель системы адаптивного управления киберполигоном МЧС России на основе операторного уравнения // Вопросы кибербезопасности. 2024. № 6. С. 140–149. DOI: 10.21681/2311-3456-2024-6-140-149

8. Интеллектуальная система AIVANT для поддержки пользователей и автоматизации продаж: свидетельство о государственной регистрации программы для ЭВМ № 2026619865, 08.04.2026. Заявка № 2026618861.

9. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability // Information and Control Systems. 2022. № 1 (116). P. 19–29. DOI 10.31799/1684-8853-2022-1-19-29

References

1. Vijayakumar S. Technology–centric and Data‑Driven Customs Risk Management for Supply Chain Security // World Customs Journal. 2025. Vol. 19. № 1. P. 38–63.

2. Gao Q., Kuang Z. Can robotic process automation technology enable risk data analysis for customs' post-clearance audit: a China customs case study // World Customs Journal. 2023. Vol. 17. № 2. P. 93–104.

3. Afonin P.N., Lebedeva A.Yu. Primenenie iskusstvennogo intellekta dlya analiza massiva dannyh, formiruemyh s ispol'zovaniem integrirovannoj informacionnoj sistemy punkta propuska // Vestnik Rossijskoj tamozhennoj akademii. 2024. № 1. S. 97–112.

4. Prokopenko A.A. Konceptual'naya model' razvitiya skvoznogo processa dokumental'nogo i fakticheskogo tamozhennogo kontrolya // Vestnik Rossijskoj tamozhennoj akademii. 2024. № 1. S. 173–182.

5. Kostopoulos G., Davrazos G., Kotsiantis S. Explainable artificial intelligence–based decision support systems: a recent review // Electronics. 2024. Vol. 13. № 14. P. 2842.

6. Gryzunov V.V. Formal'nyj frejmvork dlya OSINT-narushitelya i zashchitnika // Informacionno-upravlyayushchie sistemy. 2025. № 5 (138). S. 22–34. DOI 10.31799/1684-8853-2025-5-22-34

7. Gryzunov V.V., Shestakov A.V. Model' sistemy adaptivnogo upravleniya kiberpoligonom MChS Rossii na osnove operatornogo uravneniya // Voprosy kiberbezopasnosti. 2024. № 6. S. 140–149. DOI: 10.21681/2311-3456-2024-6-140-149

8. Intellektual'naya sistema AIVANT dlya podderzhki pol'zovatelej i avtomatizacii prodazh: svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM № 2026619865, 08.04.2026. Zayavka № 2026618861.

9. Gryzunov V.V. Model of a distributed information system solving tasks with the required probability // Information and Control Systems. 2022. № 1 (116). P. 19–29. DOI 10.31799/1684-8853-2022-1-19-29

Информация о статье:
Статья поступила в редакцию: 25.03.2026; одобрена после рецензирования: 27.04.2026;
принята к публикации: 29.04.2026

Information about the article:
The article was submitted to the editorial office: 25.03.2026; approved after review: 27.04.2026;
accepted for publication: 29.04.2026

Информация об авторах:
Грызунов Виталий Владимирович, профессор кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, доцент, e-mail: viv1313r@mail.ru, https://orcid.org/0000-0003-4866-217X
Лемихов Иван Владимирович, заместитель начальника центра управления в кризисных ситуациях Главного управления МЧС России по Камчатскому краю (683003, г. Петропавловск-Камчатский, ул. Ленинградская, д. 25), e-mail: bezemo@mail.ru, https://orcid.org/0009-0001-7712-4277

Information about authors:
Gryzunov Vitaliy V., professor of the department of applied mathematics and information technology security of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, associate professor, e-mail: viv1313r@mail.ru, https://orcid.org/0000-0003-4866-217X
Lemikhov Ivan V., deputy head of the crisis management center of Main Directorate of the Kamchatka Territory of EMERCOM of Russia (683003, Petropavlovsk-Kamchatsky, Leningradskaya st., 25), e-mail: bezemo@mail.ru, https://orcid.org/0009-0001-7712-4277