Вестник Евразийской науки / The Eurasian Scientific Journal https://esj.today

2026, Том 18, № 5 / 2026, Vol. 18, Iss. 5 https://esj.today/issue-5-2026.html

URL статьи: https://esj.today/PDF/02ECVN526.pdf

DOI: 10.15862/02ECVN526 (https://doi.org/10.15862/02ECVN526)

5.2.3. Региональная и отраслевая экономика (экономические науки)

Ссылка для цитирования этой статьи:
Максимов, Ю. А. Методологический подход к расчету устойчивости критической инфраструктуры таможенных органов и обеспечению экономической безопасности / Ю. А. Максимов // Вестник евразийской науки. — 2026. — Т. 18. — № 5. — URL: https://esj.today/PDF/02ECVN526.pdf. DOI: 10.15862/02ECVN526.

For citation:
Maximov Yu.A. Methodological approach for calculating the stability of critical infrastructure of customs authorities and ensuring economic security. *The Eurasian Scientific Journal*. 2026;18(5): 02ECVN526. Available at: https://esj.today/PDF/02ECVN526.pdf. DOI: 10.15862/02ECVN526. (In Russ., abstract in Eng.).

УДК 339.543

Максимов Юрий Анатольевич
ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», Санкт-Петербург, Россия
Северо-Западный институт
Доцент кафедры таможенного администрирования факультета безопасности и таможни
Кандидат технических наук, кандидат экономических наук, доцент
E-mail: maximoff2000@mail.ru
РИНЦ: https://elibrary.ru/author_profile.asp?id=637236

Методологический подход к расчету устойчивости критической инфраструктуры таможенных органов и обеспечению экономической безопасности

Аннотация. Разработка методологического подхода к расчету устойчивости критической инфраструктуры таможенных органов — это комплексная задача, находящаяся на стыке нормативного регулирования, теории надежности и практики управления рисками. В условиях цифровой трансформации таможенных органов и роста киберугроз она становится одним из ключевых элементов обеспечения экономической безопасности государства. Существующая правовая база задает обязательные требования к устойчивости критической инфраструктуры таможенных органов, но не предлагает единой количественной методики ее расчета, что оставляет пространство для научно-методологических разработок. Устойчивость критической инфраструктуры таможенных органов — это способность системы сохранять свои функции в условиях внешних и внутренних дестабилизирующих воздействий и восстанавливаться после них. Для оценки устойчивости автоматизированных систем управления критической инфраструктуры применяется логико-вероятностный подход, позволяющий рассчитывать: вероятность сохранения работоспособности программной составляющей и выполнения задачи управления с учетом резервирования. Перспективным направлением является интегральный метод оценки устойчивости, сочетающий многомерную систему показателей, методы нечеткого анализа для работы с неопределенностью, унифицированную нормализацию переменных, категоризацию объектов в соответствии с нормативными документами.

В результате выполненной работы был создан научно обоснованный и практически применимый методический подход, способствующий повышению безопасности, надежности и устойчивости критической инфраструктуры таможенных органов в условиях динамично меняющейся внешнеэкономической среды. Данный подход укрепляет основы эффективного

управления и развития инфраструктуры таможенных органов, обеспечивая их способность своевременно и адекватно реагировать на современные вызовы. Ключевым результатом применения такого подхода становится возможность перехода от реактивного управления инцидентами к проактивному управлению устойчивостью, что в конечном счете укрепляет экономическую безопасность государства в условиях цифровой трансформации и геополитических вызовов.

Ключевые слова: методологический подход; экономическая безопасность; угрозы безопасности; безопасность инфраструктуры; критическая информационная инфраструктура; таможенные органы; эффективное управление

Введение

Развитие международных экономических связей и внешней торговли в настоящее время основано на повсеместной цифровизации и широком внедрении элементов искусственного интеллекта (ИИ).

Система обмена информацией в таможенных органах носит характер критической инфраструктуры, нарушение которой может привести к большим негативным последствиям для экономики, снижению уровня обеспечения экономической и национальной безопасности. В современных условиях инфраструктура таможенных органов построена вокруг интеллектуальных пунктов пропуска (ИПП), которые представляют собой комплексы технологических и организационных решений, объединённых в единую цифровую платформу. Основу информационной структуры ИПП составляют данные автоматизированных контрольно-аналитических комплексов, включающих средства идентификации с большой разрешающей способностью, электронные шлюзы, а также модули управления рисками, функционирующие в едином информационном пространстве. Такой интегрированный комплекс обеспечивает динамический обмен данными между участниками внешнеэкономической деятельности и таможенными органами, что способствует оптимизации процедур контроля и ускорению товарооборота.[1]

Техническая архитектура ИПП включает в себя специализированное оборудование и программные комплексы, позволяющие выполнять комплексный досмотр грузов с минимальным вмешательством человека и сокращением времени обработки. Схема информационных потоков в ИИП представляет собой сложную систему взаимодействия между различными источниками данных и требует отдельного методологического подхода к изучению устойчивости данной структуры.

После внедрения современных программно-технических средств на ряде пунктов пропуска пропускная способность возросла до 500 грузовиков в сутки, а время досмотра сократилось до 10 минут благодаря системе предварительного уведомления и автоматизации проверок.[2] Важной составляющей информационной структуры интеллектуального пункта пропуска (далее ИПП) является применение элементов искусственного интеллекта для анализа рисков и принятия решений в режиме реального времени, что повышает качество оценки безопасности и снижает вероятность ошибок.

[1] Интеллектуальный таможенный пункт пропуска... — Ведомости [Электронный ресурс] // www.vedomosti.ru — Режим доступа: https://www.vedomosti.ru/press_releases/2025/08/27/intellektualnii-tamozhennii-punkt-propuska-realnost-ili-mif. (дата обращения 27.08.2026).

[2] Интеллектуальный пункт пропуска... | Альта-Софт — Режим доступа: https://www.alta.ru/logistics_news/129116/ (дата обращения 27.08.2026).

Архитектура ИПП строится на принципах цифровизации и сервисно-ориентированного подхода, обеспечивая безбумажный документооборот и интеграцию с внешними информационными системами, включая государственные реестры и транспортные платформы [1, с. 58]. Это позволяет формировать единую цифровую экосистему всех заинтересованных сторон — таможенных администраторов, представителей бизнеса, поставщиков и перевозчиков. Сферы применения интеллектуальных пунктов охватывают разные виды транспорта: автомобильный, железнодорожный, морской и воздушный. Такая мультиканальная структура инфраструктуры требует обеспечения надежной синхронизации и обмена информацией между разнородными системами и субъектами управления [2, с. 451].

Ключевые проблемы надежности инфраструктурных элементов ИПП связаны с высокой степенью технологической интеграции и зависимостью от сложного программно-аппаратного комплекса и функционирования системы управления рисками, основанной на методах принятия решения ИИ. Ошибки в работе идентификационных систем или задержки в информационном обмене ведут к снижению эффективности функционирования и увеличению времени таможенного контроля.

Для оценки качества функционирования подобной информационно-технической системы, направленной на обработку информации с применением элементов ИИ и принятие решения о выпуске товара, необходимо создать систему расчета надежности и устойчивости всех системы в целом, без которой невозможна реальная оценка эффективности функционирования [3, с. 8].

Так, снижение уровня надежности, т. е. устойчивости к различным негативным внешним и внутренним деструктивным воздействиям, может привести к компрометации данных, что создает риски нарушения законодательных требований и потерь экономической выгоды. Не меньшую роль играют сбои в модулях управления рисками, где неверная оценка угроз способна приводить к излишним проверкам или, наоборот, пропуску опасных грузов.

Целью исследования является разработка методических положений по оценке надежности функционирования информационной системы таможенных органов и уровня обеспечения экономической безопасности в ходе обработки массива данных, содержащих, в том числе, данные об экономической деятельности государства и субъектов внешнеэкономической деятельности.

Теоретической и методологической основой исследования послужили теория и практика организации и осуществления информационного обмена в таможенных органах и функционирования структуры единой автоматизированной информационной системы таможенных органов (далее ЕАИС ТО) в рамках ИПП таможенной службы России и иностранных государств.

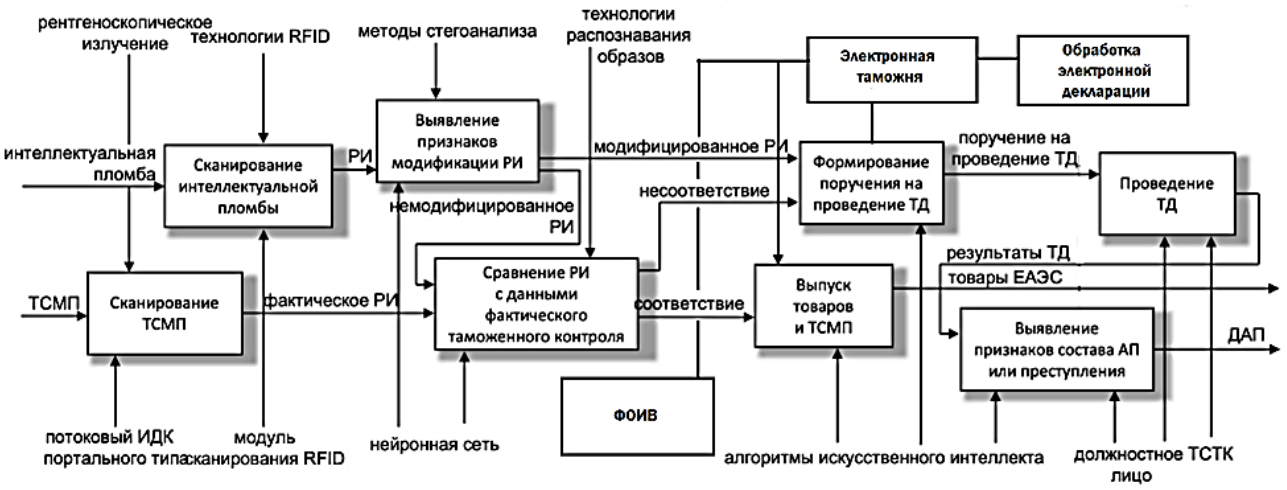
Информационной базой работы послужили аналитические материалы таможенных органов по проведению информационного обмена и концепция функционирования интеллектуального пункта пропуска как перспективного элемента критической инфраструктуры.

В работе использованы методические разработки и фактологические материалы Федеральной таможенной службы (ФТС России), Всемирной таможенной организации, Всемирной торговой организации, Министерства Российской Федерации по налогам и сборам, Федеральной службы по техническому и экспортному контролю, материалы таможенных служб иностранных государств.

Результаты исследования

Исследование устойчивости инфраструктуры таможенных органов требует учета многоуровневой структуры и взаимодействия различных компонентов системы. Инфраструктура таможенных органов включает технические средства таможенного контроля, программное

обеспечение, организационные процессы и человеческий фактор. Особое место в стратегии цифровизации таможенных органов играет создание интеллектуального пункта пропуска, концепция которого подразумевает такую организацию контрольных процедур, при которой все виды государственного контроля проводятся комплексно, с использованием передовых технических средств и применением технологий искусственного интеллекта. [15, с. 43] Для представления об информационном обмене в ходе перемещения товара через таможенную границу можно привести структуру информационных потоков в ИПП. (Рисунок 1). Для анализа устойчивости критической инфраструктуры таможенных органов важно выделить элементы, особо важные для обеспечения надежности и безопасности функционирования таможенных пунктов пропуска.



ТСМП — товары и транспортные средства международной перевозки
ТСТК — технические средства таможенного контроля
RFID — радиочастотная идентификация, т. е. способ автоматической идентификации объектов, в котором посредством радиосигналов считываются или записываются данные, хранящиеся в так называемых транспондерах, или RFID-метках
ТД — таможенная декларация
РИ — рентгеноскопическое изображение
ПФК — пост фактического контроля
АП — административное правонарушение
ДАП — дело об административном правонарушении

Рисунок 1. *Структура информационных потоков в ИПП [4, с. 10]*

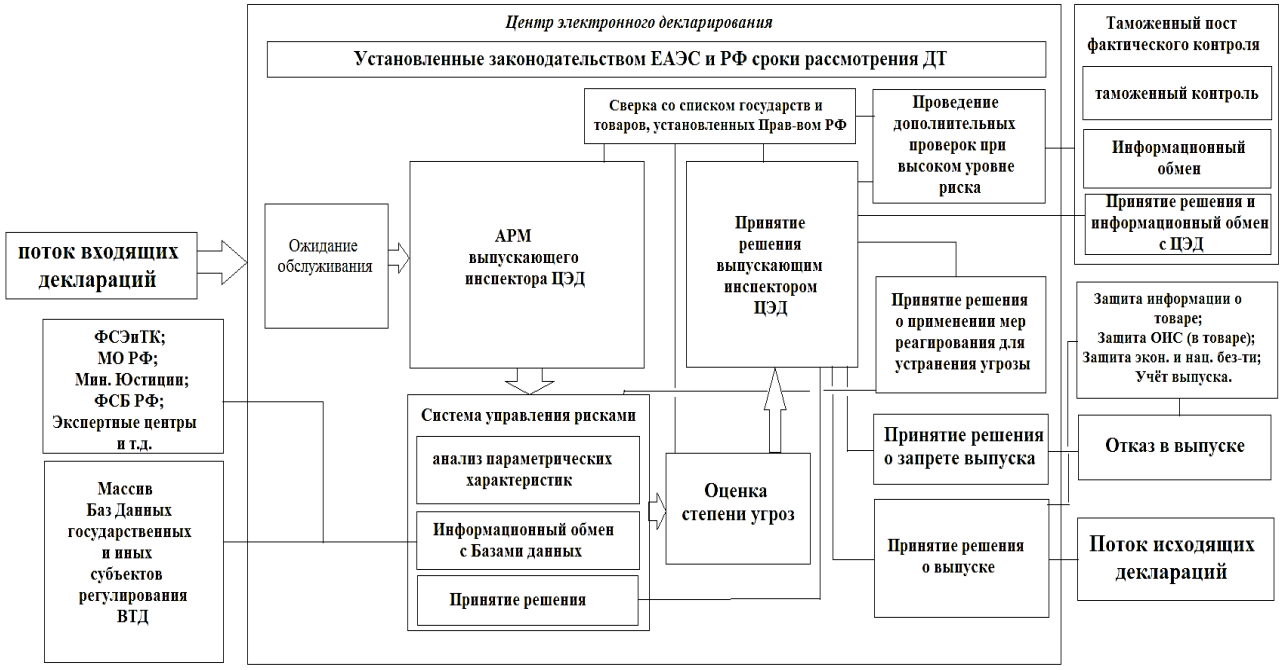
Критическая таможенная инфраструктура функционирует в условиях высокой неопределенности, включающей вариабельность внешних факторов, технические сбои и изменения в нормативно-правовой базе. Оценка устойчивости должна отражать вероятностный характер таких событий и их влияние на обеспечение безопасности и эффективности. Стандартные методы анализа зачастую не учитывают глубину неопределенности и взаимосвязей между элементами системы, что приводит к недостаточной информативности результатов и сложности в принятии управленческих решений. Учитывая отсутствие методологического базиса в оценке состояния устойчивости и надежности функционирования в условиях внешнего и внутреннего деструктивного воздействия, а также наличие значительного методологического базиса только в формировании системы информационно-технического обеспечения, необходимо проведение исследований в этой сфере [5, с. 72].

Логико-вероятностный метод предоставляет инструментарий для формирования формализованных моделей, которые интегрируют логические зависимости и вероятностные оценки параметров системы [6, с. 11]. Такой подход позволяет не только определить вероятность сбоев и отказов отдельных компонентов, но и учесть сложные взаимные влияния

между ними. В результате обеспечивается более точная количественная характеристика устойчивости, что способствует выявлению слабых частей инфраструктуры и направлению ресурсов на их укрепление.

Актуальность применения метода обосновывается необходимостью повышения надежности ИПП, которые представляют собой комплекс технических, программных и организационных средств. Их функционирование тесно связано с анализом потоков данных, идентификацией рисков и осуществлением контроля. Логико-вероятностный подход позволяет моделировать как обычные, так и необычные сценарии развития событий, включая попытки правонарушений и технические сбои, что значительно расширяет возможности мониторинга и управления.

Особое внимание уделяется взаимодействию логико-вероятностного метода (ЛВМ) с динамическими подходами, которые позволяют учитывать временную изменчивость состояния финансовой устойчивости участников внешнеэкономической деятельности, выполнения требований законодательства ими, уплату таможенных платежей, налогов, изменение нормативно-правовой базы, рынок с которого или на который поставляется товар. Их интеграция способствует совершенствованию прогнозирования рисков правонарушений и повышению адаптивности таможенной системы к изменениям во внешней среде.



АРМ — автоматизированное рабочее место
ВТД –внешнеторговая деятельность
ДТ — декларация на товары
ЦЭД — центр электронного декларирования
ОИС — объекты интеллектуальной собственности

Рисунок 2. *Схема предоставления таможенной услуги по оформлению деклараций на товары и принятию решения о выпуске товара (разработана автором)*

Использование ЛВМ открывает новые возможности для комплексного анализа сложных систем, позволяя интегрировать как формальные логические правила, так и оценки вероятностей, что существенно повышает качество принимаемых управленческих решений.

Для успешного применения результатов исследования в практике таможенных органов рекомендуется начать с построения адаптивных моделей оценки устойчивости на основе имеющихся данных об инфраструктуре и рабочих процессах.

При формализации системных зависимостей следует использовать принципы декомпозиции, выделяя автономные подсистемы, что сокращает вычислительные затраты и повышает точность анализа. Схема предоставления таможенной услуги по оформлению деклараций на товары и принятию решения о выпуске в ИПП представлена на рисунке 2. Следует последовательно интегрировать вероятностные параметры, основанные на эмпирическом мониторинге и экспертных оценках, что обеспечит адекватное отражение реального состояния объектов контроля и управления.

Особое внимание необходимо уделить формализации правил принятия решений в системе управления рисками, включающих критерии допуска и ограничения, с учётом вероятностных сценариев возможных сбоев и нарушений. Рекомендуется внедрять накопленные знания в виде логических выражений совместно с вероятностными весами, что позволит создавать рекомендательные системы для поддержки таможенных операторов и автоматизированных подсистем контроля.

Использование ЛВМ в таможенной сфере обеспечивает ряд преимуществ. В первую очередь, это повышение точности оценки устойчивости и надёжности инфраструктуры за счёт комплексного учёта взаимозависимостей и неопределённостей. Метод способствует своевременному выявлению критических уязвимостей и приоритетных направлений развития, что оптимизирует распределение ресурсов. Кроме того, интеграция логических и вероятностных компонентов улучшает адаптивность управления рисками, позволяя гибко реагировать на изменение внешних и внутренних деструктивных факторов.

Таким образом, предложенный подход создает основу для формирования более эффективной системы управления и контроля, сокращения операционных рисков, повышения безопасности и прозрачности таможенных процедур, что в совокупности способствует устойчивому развитию внешнеэкономической деятельности и укреплению доверия между государством и бизнес-сообществом.

Сочетание следующих совокупных показателей деятельности таможенных органов [7, с. 8] при перемещении через таможенную границу товаров придает задаче построения сбалансированной системы таможенного контроля, обеспечивающей заданные параметры экономической безопасности, особую важность:

- эффективность осуществляемого таможенного контроля за перемещением указанных товаров;
- целенаправленное применение системы управления рисками, не допускающей «прорыва» границ экономической и национальной безопасности;
- применение в ходе таможенного контроля информационного обмена огромного массива данных между субъектами, с задачей защиты информационных потоков;
- эффективный контроль за содержанием в товарах объектов интеллектуальной собственности, способствующий защите прав правообладателей и национальной безопасности;
- создание системы управления экономической (внешнеторговой) безопасности, способной оперативно реагировать на возникающие угрозы и определяющей на этапе раннего возникновения угрозы экономической безопасности;
- способность системы управления рисками (далее — СУР) с применением элементов ИИ в таможенной и налоговой сфере адаптировать традиционную теорию риск-менеджмента к специфике управления рисками в таможенном деле при перемещении через таможенную границу товаров.

02ECVN526
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Применение СУР в процессе проведения таможенного контроля товаров сопряжено с необходимостью постоянного повышения эффективности, связанной не столько с техническими особенностями, сколько с применением в ходе информационного обмена части закрытой информации, которая, хотя и входит в перечень таможенной статистики, но в свете применения существующего механизма принятия управленческих решений по отнесению товара к тому или иному уровню риска, может иметь недостатки. При этом недостаток системы принятия решений о выпуске товара на основе применения СУР заложен изначально в соответствии с принципом — чем сложнее система обработки информационных потоков, тем больше она имеет уязвимых мест.

В ходе предоставления таможенных услуг используется сложная организационно-экономическая система с сетевой структурой, которая в то же время является критически важной инфраструктурой. К исследованию такой системы можно применить указанный выше метод структурно-логического моделирования и методику расчета показателей сложных систем с сетевой структурой с учетом вероятностей деструктивного воздействия и устойчивости самой системы и отдельных её структурных элементов, в которых:

- результативность функционирования достигается путем выполнения элементами функций, возложенных на них в соответствии с задачами по принятию решения о выпуске в установленное время. При этом выполнение работ должно производиться в строго определенной, детерминированной последовательности, закрепленной порядком действий выпускающего должностного лица центра электронного декларирования (далее — ЦЭД), ИПП;
- условия реализации своих функций всеми элементами и подсистемами описываются последовательными и/или параллельными причинно-следственными связями.

Организационную систему, процесс функционирования ЦЭД и ИПП на этапе прохождения товаров можно представить в виде структурно-логической схемы, представленной на рисунке 3.

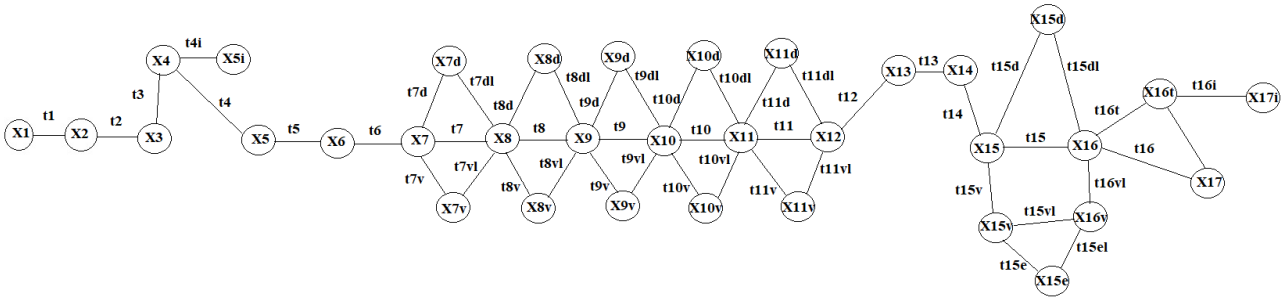


Рисунок 3. *Структурно-логическая схема функционирования ЦЭД на этапе прохождения товаров (разработана автором)*

В данной схеме выделяются следующие вершины:

X1 — поступление декларации в ЦЭД;

X2 — принятие декларации к рассмотрению (время t_1);

X3 — проверки соблюдения условий регистрации ДТ (время t_2);

X4 — запрос информации о нахождении товаров на временном хранении на склад временного хранения (СВХ) в таможенный орган, в регионе которого расположен СВХ (время t_3);

X5 — принятие решения о регистрации поданной ДТ (время t_4);

X5i — решение об отказе в регистрации ДТ (время t_{4i});

X6 — направление информационного пакета данных на сверку внешнему таможенному органу для осуществления документального контроля и принятие решения по ДТ (время t_5), принятие декларации для проведения форматно-логического контроля (время t_6);

X7–X12 проведение форматно-логического контроля ДТ (время: $t_7 + t_8 + t_9 + t_{10} + t_{11}$). В данный этап входит: проверка соответствия заявленных в ДТ сведений о наименовании товаров, их количественных данных (количество мест, вес и пр.), проверка правильности определения классификационного кода товара по Единой Товарной номенклатуре внешнеэкономической деятельности Евразийского экономического союза (далее — ТН ВЭД ЕАЭС) и Единому таможенному тарифу Евразийского экономического союза[3], проверка правильности определения страны происхождения товаров и проверка соблюдения законодательства, устанавливающего запреты и ограничения на перемещение через таможенную границу ЕАЭС, проверка, осуществляемая в целях применения мер, связанных с защитой прав интеллектуальной собственности.

X13 — осуществление валютного контроля и контроля за исполнением внешнеторговых бартерных сделок;

X14 — оформление таможенной расписки и списание денежных средств со счета участника ВЭД;

X15 — определение категории риска по данной поставке товаров;

X16 — внесение отметок в декларацию таможенной стоимости и принятие решения о выпуске товаров;

X17 — выпуск товара.

Всё время прохождения операций от t_1 до t_{16} составляет около 4 часов.

В представленной структурно-логической схеме могут возникать дополнительные временные издержки, возникающие при обращении к внешнему таможенному посту фактического контроля для производства дополнительных мероприятий; отмечены на схеме литерой «v» с потерей времени ($t_{xv} + t_{xvl}$). Вторая составляющая — формирование запроса участнику внешнеэкономической деятельности (далее — ВЭД) для представления дополнительных документов; их обработка указана на схеме литерой «d», со временем потери ($t_{xd} + t_{xdl}$). Проведение осмотра и экспертизы на внешней таможенном посту отмечена литерой «e» и соответствующими временными потерями.

Информационную систему, созданную в рамках цифровизации ФТС России, можно отнести к киберфизической системе[4], объединяющей информационно-технологическую составляющую, взаимодействие физических объектов товарных поставок и процессов таможенного оформления с цифровыми элементами и ИИ. Для исследования устойчивости киберфизической системы таможенных органов на предмет оценки надежности отдельных её элементов и системы в целом при влиянии внешних и внутренних деструктивных воздействий необходимо построение структурно-логической схемы функционирования [8, с. 17]. Обеспечение устойчивости функционирования такой сложной киберфизической системы является важным элементом обеспечения экономической безопасности и требует соответствующего подхода к расчетам таких параметров, как живучесть отдельных элементов и всей системы в целом, а также вероятности функционирования в условиях деструктивного воздействия.

[3] Официальный сайт Евразийской экономической комиссии. Единая Товарная номенклатура внешнеэкономической деятельности Евразийского экономического союза и Единый таможенный тариф Евразийского экономического союза. https://eec.eaeunion.org/comission/department/catr/ett/?ysclid=mufemkzowq771571802 (дата обращения 24.09.2026).

[4] Современные технологии. Киберфизические системы: учебное пособие / Авт.-сост. Е. И. Громаков, А. А. Сидорова; Томский политехнический университет. — Томск: Изд-во Томского политехнического университета, 2021. — 166 с. С. 7.

Современные тенденции развития методов оценки устойчивости ориентированы на интеграцию классических математических подходов с передовыми цифровыми технологиями. Традиционные методы Ляпунова и энергетические функционалы дополняются спектральным и структурным анализом, основанным на теории графов и методе субграмианов, что позволяет детальнее учитывать сложную взаимозависимость компонентов систем большой размерности и многоуровневой структуры [9, с. 34]. Применение численного моделирования в режиме реального времени и программно-аппаратных комплексов цифрового моделирования открывает новые возможности для мониторинга и оперативного анализа состояния инфраструктуры таможенных органов, повышая скорость и точность оценки устойчивости.

Одним из перспективных направлений является расширение сферы применения методов на киберфизические системы, где технические средства интегрированы с человеческим и организационным факторами. Особое значение приобретают инструменты оценки экономической и информационной устойчивости, учитывающие защиту информационных потоков в условиях усиливающихся киберугроз и необходимого цифрового взаимодействия между субъектами функционирования единой автоматизированной информационной системы таможенных органов (ЕАИС ТО). Разработка универсальных методик, объединяющих вероятностно-статистические модели с экспертным оцениванием, обеспечивает более комплексный анализ, адаптивный к неопределённости и динамичности внешней среды.[5]

Предварительная оценка устойчивости системы в рамках функционирующих цифровых платформ и систем управления таможенными процессами способствует переходу от пассивного мониторинга к активному прогнозированию возможных сбоев и формированию модельных сценариев развития инцидентов. Это вызывает необходимость совершенствовать алгоритмы обработки больших данных и применять методы ИИ и машинного обучения для выявления скрытых закономерностей и своевременного принятия управленческих решений, что является важным шагом в развитии интеллектуальной таможенной инфраструктуры.

В связи с усложнением геополитической ситуации и нарастающими вызовами безопасности, связанными с кибератаками и мошенническими схемами, становится критически важным развивать методы, способные обеспечивать информационную и организационную устойчивость таможенных систем.[6] В этом контексте перспективным является применение гибридных моделей, сочетающих формальные аналитические методы с эвристическими и адаптивными механизмами, что повысит надежность и оперативность реакций на новые угрозы.

Сложность структурно-логического моделирования информационных систем таможенных органов как объектов критической инфраструктуры государства определяется еще и многообразием используемых программных средств и платформ. Так, на текущий момент под управлением отечественной систем управления базами данных (далее — СУБД) уже функционируют: автоматизированная информационная система (далее — АИС) «Электронное представление сведений (за исключением КПС «ЭАД» — комплекс программных средств (далее — КПС), обеспечивающая хранение документов участника ВЭД «Электронный архив декларанта»), КПС «Web сервер ФТС России», автоматизированная программная среда (далее — АПС)

[5] Евсеева О. О. Развитие методов оценки устойчивости крупномасштабных проектов по производству сжиженного природного газа. Диссертация на соискание ученой степени кандидата экономических наук. СПб. — 2022. 147 с. — С. 21. URL: https://spmi.ru/sites/default/files/imci_images/sciens/dissertacii/2021/evseeva_dissertaciya.pdf (дата обращения 16.09.2026).

[6] Евсеев К., Исаев М., Мурзина А., Муфлиханова А., Шакирзянова Д. Данные без опасности. Сборник аналитических данных. Центр информационной Безопасности Университета Иннополис. Университет Иннополис. 2023. — 92 с. С. 11 URL: https://innopolis.university/filespublic/dannye_bez_opasnosti.pdf (дата обращения 24.09.2026).

«Электронные госуслуги», сервер картографии информационно-справочная система (далее ИСС) «Малахит», ИСС «Портал ФТС России», КПС «Внешний шлюз», автоматизированная система учета и контроля исполнения документов (АС «УКИД-2») [10, с. 108.], АИС «ДИСОРИ» — это автоматизированная информационная система «Документирование и систематизация оперативно-розыскной информации» и КПС «КАСКАД» и другие.[7]

Таким образом, дальнейшие исследования должны быть направлены на разработку комплексных, многоуровневых и интегрированных подходов к оценке устойчивости ЕАИС ТО, способных адаптироваться к быстро меняющейся технологической и информационной среде таможенной деятельности. Это обеспечит повышение эффективности управления рисками, снизит вероятность сбоев и инцидентов, а также создаст основу для формирования прорывных технологий в обеспечении безопасности и стабильности инфраструктуры таможенных органов.

Разработка модели расчёта устойчивости ИПП осуществляется с использованием многоуровневого подхода, основанного на декомпозиции системы на ключевые функциональные блоки [14, с. 387–388]. Каждый блок отражает отдельный аспект функционирования пункта пропуска: техническое оснащение, программное обеспечение и административно-организационные процедуры. Для моделирования используется построенная логико-вероятностная структура, в которой логические зависимости между элементами интегрировались с вероятностными характеристиками на основе статистических данных и экспертных оценок с учетом современных правил применения логико-вероятностного метода [11, с. 23].

Процесс создания модели начинается с идентификации критически значимых компонентов и установления взаимосвязей между ними. Для каждого компонента должны быть заданы вероятности нормального функционирования с учётом различных факторов риска, включая потенциальные сбои оборудования, ошибки должностных лиц таможенных органов, сбои ИИ и угрозы информационной безопасности. Далее на основе построенных логических выражений формировалась агрегированная функция работоспособности пункта пропуска, которая позволяла определить общую вероятность поддержания устойчивого состояния системы.

На следующем этапе применяется компьютерное моделирование с учётом стохастических воздействий, что позволило учесть случайные изменения условий функционирования и их влияние на надёжность системы в целом. В ходе исследования использовался байесовский подход для обновления вероятностей с учётом экспериментальных данных и мониторинга, что повышало адаптивность модели к меняющимся условиям эксплуатации. Кроме того, проводилась идентификация минимальных критических сечений системы, что обеспечивало выявление наиболее уязвимых элементов и направляло усилия на их усиление в соответствии с правилами моделирования устойчивости сложных организационно-технических систем [9, с. 41].

Автором была разработана комплексная методика оценки эффективности обеспечения экономической безопасности при информационном взаимодействии между участниками внешнеторговой деятельности в условиях электронного документооборота с учетом особенностей перемещения товаров через таможенную границу и вероятностью деструктивного воздействия. В методике учитываются особенности информационного обмена и фактического контроля, производимого на таможенных постах, а также методы идентификации продукции и товаров двойного назначения при перемещении через таможенную границу.

Система предлагаемых автором показателей позволяет осуществить эмпирическую оценку эффективности обеспечения информационной безопасности в ходе межведомственного взаимодействия в условиях внешнего негативного воздействия и осуществлении комплексных мероприятий, направленных защиту информации.

[7] Архитектура Единой автоматизированной информационной системы таможенных органов 2025. Реестровый номер ФГИС 0152. Версия 2 (с 01.01.2025). Издание ФТС РФ. 2025г. — 127 с. — Лист 26.

Так, предлагаются следующие обозначения:

R — количество органов управления, привлекаемых к решению задачи электронного документооборота при перемещении товаров военно-технического и двойного назначения через таможенную границу;

|R| — мощность множества R (с учетом имеющегося количества элементов);

n — идентификатор каждого элемента (n = 1, 2, …, N) элемента из множества R;

Zn — множество задач, решаемых каждым n-м (n = 1, 2, …, N) органом-участником информационного обмена управления, в интересах обеспечения экономической и национальной безопасности;

|Zn| — мощность (количество элементов) множества Zn;

k — идентификатор (k = 1, 2, …, Kn) задачи из множества |Zn|;

Для определения количества времени, являющегося одним из определяющих факторов выполнения таможенных операций, введем временную характеристику выполнения одной операции из массива Zn каждым элементом государственного управления из множества n. Таким параметром является допустимое время выполнения операции по таможенному или иному государственному виду контроля в ходе принятия решения о выпуске товара, относящегося к исследуемым, при соблюдении требований экономической и национальной безопасности. Такой параметр обозначим t_{nk}. Величина t_{nk} представляет собой допустимое время принятия управленческого решения при выполнении задачи обеспечения информационной безопасности потока электронного документооборота между участниками ВЭД.

Для каждого отдельного z-го органа информационное взаимодействие с другим n-м органом внешнеэкономического электронного документооборота при выполнениик-й задачи будем характеризовать временем τ_{nz}^{k} формирования и доведения до n-го органа информации, необходимой для полной реализации задачи передачи и получения информации для оформления сделки с товарами военно-технического и двойного назначения, а также соблюдения условий защиты экономической и национальной безопасности.

Величина определяется соотношением

$$\tau_{nz}^{k} = \tau_{nz}^{k*} + T_{nz}^{k}, \quad (1)$$

$$z, n = 1, 2, \dots |R|,$$

$$z \neq n, k = 1, 2, \dots, Kn,$$

где:

τ_{nz}^{k*} — нормативное время формирования и доведения от z-го до n-го органа информации, необходимой для полной реализации задачи передачи и получения информации для оформления сделки с товарами военно-технического и двойного назначения, а также соблюдения условий защиты экономической и национальной безопасности с применением средств защиты информационных потоков, имеющихся в распоряжении, n-му органу управления, при решении k-й задачи;

T_{nz}^{k} — приращение времени электронного документооборота за счет внешних деструктивных воздействий и проведения мероприятий защиты от них, времени формирования и доведения от z-го до n-го органа информации, необходимой для принятия решений уполномоченным на это n-м органом на данном этапе таможенного декларирования, при решении k-й задачи.

02ECVN526
Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

В соответствии с нормативами времени, установленными в рамках формирования нормативно-правовой базы ЕАЭС [8] для реализации задач, стоящих перед таможенными органами по защите экономической и национальной безопасности, в ходе принятия решений необходимых для выпуска товаров, подведомственных n-му органу управления, время формирования и доведения до него информации от z-го органа управления, необходимой для решения k-й задачи, должно удовлетворять условию:

$$\tau_{nz}^{k} \leq t_{nk}, \quad (2)$$

$$n, z = 1, 2, \ldots, N,$$

$$z \neq n, k = 1, 2, \ldots, Kn$$

Оценка выполнимости этого условия опирается на определение величины T_{nz}^{k}. Исходя из случайности негативного воздействия на обмен информационными потоками, следует признать, что данная величина является случайной и определяется соотношением:

$$T_{nz}^{k}. = \sum_{r=0}^{R_{zn}^{k}} \vartheta_{zn}^{k}(r), \quad (3)$$

$$n, z = 1, 2, \ldots, N,$$

$$z \neq n, k = 1, 2, \ldots, Kn,$$

где:

r — идентификатор (порядковый номер) внешнего негативного воздействия угрозы на информационные потоки;

R_{zn}^{k} — случайная величина, отражающая количество внешних негативных воздействий на информационные потоки за время электронного документооборота между z-м и n-м субъектами внешнеэкономической деятельности, принимающими решение, влияющее на выпуск товара;

ϑ_{zn}^{k} — случайная величина, характеризующая время ликвидации последствий r-х негативных воздействий при электронном документообороте между z-м и n-м субъектами внешнеэкономической деятельности, принимающими решение, влияющее на выпуск товара.

Так, как ϑ_{zn}^{k} является вероятностной величиной, которая носит случайный характер и зависит, во-первых, от количества негативных воздействий на систему обмена информацией, во-вторых, зависит от времени устранения угрозы и её негативного воздействия, то в отношении ϑ_{zn}^{k}, r = 1, 2, …, m, можно предположить, что она независима от величины R_{zn}^{k}. В этом случае, как и в большинстве существующих методик [13, с. 84–85], для построения функции случайной величины T_{nz}^{k}, зависящей, в свою очередь, от случайных величин ϑ_{zn}^{k} *и* R_{zn}^{k}, можно использовать математический аппарат характеристических функций. Так, на основе мультипликативного свойства характеристических функций можно записать:

$$\varphi_{zn}^{k}(t) = \sum_{r=0}^{\infty} p_r[\hat{\varphi}_{zn}^{k}(t)]\text{r}, \quad (4)$$

$$n, z = 1, 2, \ldots, N,$$

$$z \neq n, k = 1, 2, \ldots, Kn,$$

где:

[8] Таможенный кодекс Евразийского экономического союза (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза от 11 апреля 2017 г.) — Режим доступа: URL: https://base.garant.ru/71652992/65d319556446be991febc269ec46d49b/?ysclid=mui47n3p240092554. (дата обращения:04.10.2026). — Статья 119. Сроки выпуска товаров.

$\varphi_{zn}^{k}(t)$ — характеристическая функция величины T_{nz}^{k};

$\hat{\varphi}_{zn}^{k}(t)$ — характеристическая функция величин ϑ_{zn}^{k}, r = 1,2,…m;

p_r — вероятность наступления события, состоящего в том, что $R_{zn}^{k} = r$.

Соотношение для плотности распределения $f_{zn}^{k}(g)$ случайной величины T_{nz}^{k} с учетом (3) может быть представлено в следующем виде:

$$f_{zn}^{k}(g) = \frac{1}{2\pi}\int_{-\infty}^{\infty} e^{-ing} \sum_{r=0}^{\infty} p_r[\hat{\varphi}_{zn}^{k}(t)]\mathrm{rdt}, \quad (5)$$

n, z = 1, 2, …, N,

z ≠ n, k = 1, 2, …, Kn.

Вследствие конечности величин получаем:

$$\sum_{r=0}^{\infty} p_r[\hat{\varphi}_{zn}^{k}(t)]\mathrm{r} \le \sum_{r=0}^{\infty} p_r[\hat{\varphi}_{zn}^{k}(t0)]\mathrm{r} < \infty. \quad (6)$$

Если в уравнении (6) поменять порядок суммирования и интегрирования, что допускается, то получим следующее уравнение:

$$f_{zn}^{k}(g) = \frac{1}{2\pi}\sum_{r=0}^{\infty} p_r \int_{-\infty}^{\infty} e^{-ing}\,[\hat{\varphi}_{zn}^{k}(t)]^r\,\mathrm{dt}, \quad (7)$$

n, z = 1, 2, …, N,

z ≠ n, k = 1, 2, …, Kn.

На основе мультипликативного свойства характеристической функции и теоремы единственности из (6), следует:

$$f_{zn}^{k}(g) = \sum_{r=0}^{\infty} p_r f_{zn}^{k}(g,r), \quad (8)$$

n, z = 1, 2, …, N,

z ≠ n, k = 1, 2, …, Kn,

где:

$f_{zn}^{k}(g,r)$ — функция плотности распределения суммы r случайных величин ϑ_{zn}^{k}, r = 1, 2, …, m.

В условиях внешних негативных воздействий вероятность своевременного выполнения своих функций и доведения от z-го органа информационного обмена до соответствующего ему контрагента выработки информационного массива данных, на основе которых принимается решение о выпуске товара n-гоэлемента, необходимой для успешного решения k-й задачи, определяется соотношением:

$$\Psi_{zn}^{k}(g \le t_{nk} - \tau_{nz}^{k*}) = \sum_{r=0}^{\infty} p_r \int_{0}^{t_{nk}-\tau_{nz}^{k*}} f_{zn}^{k}(g,r)\,dg, \quad (9)$$

n, z = 1, 2, …, N,

z ≠ n, k = 1, 2, …, Kn.

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Все органы информационного обмена должны в полном объеме предоставлять весь массив данных n-му органу принятия решения на выпуск товара, несмотря на негативное воздействие со стороны, и только в данном случае обеспечивается экономическая и национальная безопасность.

Учитывая решение задачи информирования таможенных органов с учетом всех информационных массивов данных, находящихся в открытом и закрытом доступе, выполнение ими своих функций по своевременному принятию решения относительно поданных деклараций, соблюдение установленных сроков принятия решения и защита экономических интересов возможны только в том случае, если все элементы информационного обмена решают заданное количество задач при возможности негативного воздействия на информационные потоки.

Так как все возможные события, состоящие в реализации задач при информационном обмене и при решении каждой отдельной задачи независимы, можно представить соотношения:

$$\Psi_n^k = \prod_{z=1, z\neq n}^{|R|} \Psi_{zn}^k \left(g \leq t_{nk} - \tau_{nz}^{k*}\right), \tag{10}$$

$$n = 1, 2, \ldots, N,$$

$$k = 1, 2, \ldots, Kn$$

$$\Psi_n = \prod_{k=1}^{|Zn|} \Psi_n^k, \tag{11}$$

$$n = 1, 2, \ldots, N,$$

$$\Psi = \prod_{n=1}^{|R|} \Psi_n, \tag{12}$$

где:

Ψ_n^k — вероятность информационной обеспеченности, необходимой для полной реализации своих задач, подведомственных n-му органу информационного обмена в условиях электронного документооборота, при решении k-й задачи в интересах достижения цели своевременного выполнения функций таможенного контроля и оформления;

Ψ_n — вероятность информационной обеспеченности, необходимой для полной реализации задач, подведомственных уполномоченному n-му органу информационного обмена в условиях электронного документооборота, при решении всех задач, стоящих перед ним;

Ψ — вероятность информационной обеспеченности, необходимой для выполнения функций по своевременному принятию решения относительно поданных деклараций, соблюдение установленных сроков принятия решения и защита экономических интересов, при возможности негативного воздействия на информационные потоки.

Возможно применение указанного метода расчета оценки эффективности информационного взаимодействия государственных органов при осуществлении внешней торговли товарами военно-технического и двойного назначения, осуществляемого в целях обеспечения защиты военно-технической и интеллектуальной составляющих экономической безопасности в случае, когда поток внешних негативных воздействий на информационные потоки, возникающие в ходе электронного декларирования, подчиняется закону Пуассона со средними значениями: μ_{zn}^k, n, z = 1, 2, …, N, z ≠ n, k = 1, 2, …, Kn, а время ликвидации последствий внешних негативных воздействий на информационные потоки распределено по экспоненциальному закону с соответствующими параметрами λ_{zn}^k.

В данном случае характеристические функции $\hat{\varphi}_{zn}^{k}(t)$ экспоненциально распределенных случайных величин $\vartheta_{zn}^{k}(r), (n, z = 1,2,\dots,N, z \neq n, k = 1,2,\dots,Kn)$ длительности ликвидации внешних негативных воздействий на информационные потоки, возникающие в ходе электронного декларирования при информационном обмене между z-м и n-м органами управления определяется соотношением:

$$\hat{\varphi}_{zn}^{k}(t) = [1 - it\left(\lambda_{zn}^{k}\right)^{-1}]^{-1}, \quad (13)$$
$$(n, z = 1,2,\dots,N, z \neq n, k = 1,2,\dots,Kn).$$

Подставив эти функции и величину p_r, определяемую законом Пуассона со средним значением μ, в (3), получим характеристические функции величин $T_{zn}^{k}, n, z = 1,2,\dots,N, z \neq n, k = = 1,2,\dots,Kn$:

$$\hat{\varphi}_{zn}^{k}(t) = \sum_{r=0}^{\infty} \frac{(\mu_{zn}^{k})^{r} e^{-\mu_{zn}^{k}}}{r!} [1 - it\left(\lambda_{zn}^{k}\right)^{-1}]^{-r}, \quad (14)$$
$$n, z = 1,2,\dots,N, z \neq n, k = 1,2,\dots,Kn.$$

Подставив функции (13, 14) в (8), получим уравнение:

$$f_{zn}^{k}(g) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{-ing} \sum_{r=0}^{\infty} \frac{(\mu_{zn}^{k})^{r} e^{-\mu_{zn}^{k}}}{r!} [1 - it\left(\lambda_{zn}^{k}\right)^{-1}]^{-r} dt, \quad (15)$$
$$n, z = 1,2,\dots,N, z \neq n, k = 1,2,\dots,Kn.$$

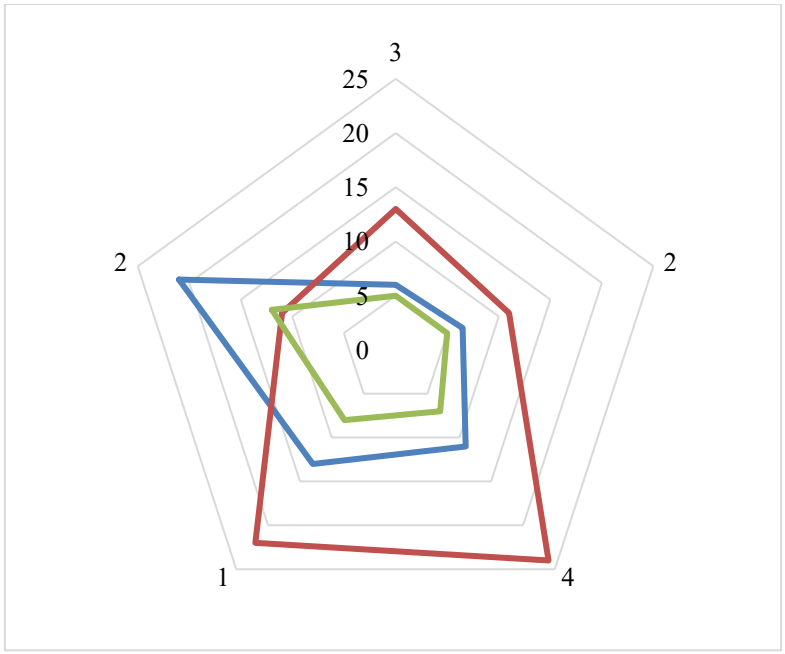
Проведя необходимые преобразования, получаем следующее уравнение:

$$f_{zn}^{k}(g) = \sum_{r=0}^{\infty} \frac{(\lambda_{zn}^{k} \mu_{zn}^{k})^{r} e^{-\mu}}{r! 2\pi} \int_{-\infty}^{\infty} e^{-ing} \left(\lambda_{zn}^{k} - it\right) dt = \sum_{z=0}^{\infty} \frac{(\mu_{zn}^{k})^{r} e^{-\mu_{zn}^{k}} (\lambda_{zn}^{k} g)^{r-1} e^{\lambda_{zn}^{k} g}}{r!\, \lambda_{zn}^{k}\, R(r)}, \quad (16)$$
$$n, z = 1,2,\dots,N, z \neq n, k = 1,2,\dots,Kn.$$

Из предыдущего уравнения следует, что при принятых в ходе проведения данного исследования допущениях вероятность своевременного формирования информационной базы и передачи её от k-го органа информационного обмена до органа n-го органа принятия решений в области таможенного оформления и контроля, необходимая для успешного решения k-й задачи, определяется соотношением:

$$\Psi_{n}^{k}(g \leq t_{nk} - \tau_{nz}^{k*}) = \sum_{r=0}^{\infty} \frac{e^{-\mu_{zn}^{k}} (\mu_{zn}^{k})^{r} e^{-\mu}}{r!\, 2\pi} \int_{-\infty}^{\infty} e^{-ing} \left(\lambda_{zn}^{k} - it\right) dt = \sum_{z=0}^{\infty} \frac{(\mu_{zn}^{k})^{r} e^{-\mu_{zn}^{k}} (\lambda_{zn}^{k} g)^{r-1} e^{\lambda_{zn}^{k} g}}{r!\, \lambda_{zn}^{k}\, R(r)}. \quad (17)$$
$$n, z = 1,2,\dots,N, z \neq n, k = 1,2,\dots,Kn.$$

На основании полученного уравнения и соотношений (14–16), получим соответствующие принятым допущениям вероятности обеспечения передачи информации без негативных последствий внешних угроз в результате информационного межведомственного взаимодействия, возникающего при таможенном оформлении и контроле между задействованными органами государства для достижения целей обеспечения информационной, экономической и национальной безопасности (рис. 4, 5).



Красный цвет — надежность функционирования; синий — устойчивость; зеленый — целостность

Рисунок 4. *Вероятности обеспечения устойчивости передачи информации (получено автором в результате расчетов)*

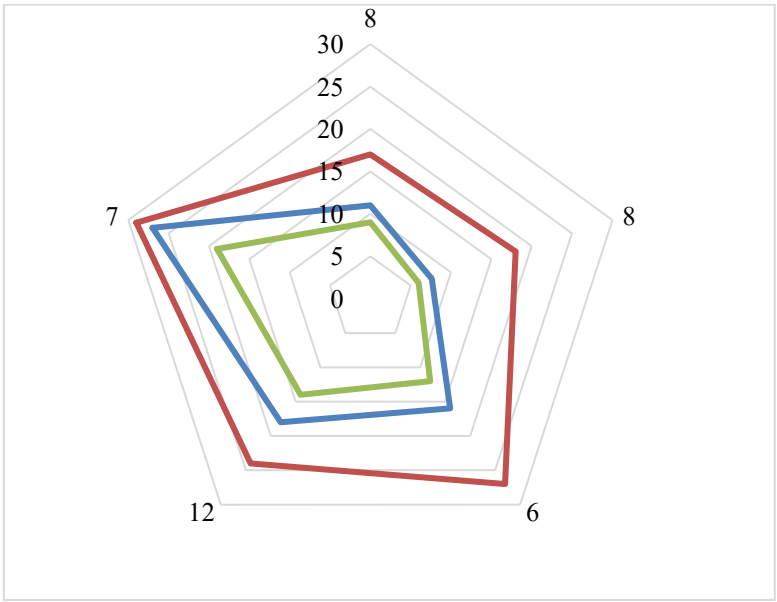


Рисунок 5. *Вероятности устойчивости информационной обеспеченности по расчетам при предотвращенном деструктивном воздействии на систему «Электронной таможни» (получено автором в результате расчетов)*

Данные расчетов позволяют говорить о вероятности успешного обеспечения передачи информации без негативных последствий внешних угроз в результате информационного межведомственного взаимодействия, возникающего при таможенном оформлении и контроле между задействованными органами государства для достижения целей обеспечения информационной, экономической и национальной безопасности. В части латентного эффекта указанная цель достигается уменьшением ущерба, обусловленного эффективным функционированием системы защиты информационных потоков при применении предлагаемого методического подхода к расчету надежности и устойчивости самой системы.

Выводы

Таким образом, новизна предлагаемого метода расчета для приближенной оценки эффективности защиты информации при межведомственном обмене информацией, возникающем при таможенном оформлении и контроле, в том числе, при перемещении через границу ЕАЭС товаров, заключается, в первую очередь, в её применении в случае электронного документооборота в таможенных отношениях и, во-вторую, в возможности повышения эффективности взаимодействия государственных органов при осуществлении внешней торговли товарами военно-технического и двойного назначения, осуществляемых в целях обеспечения защиты экономической безопасности.

В результате моделирования были получены количественные показатели вероятности сбоев и отказов, а также выделены приоритеты для мероприятий по техническому обслуживанию и модернизации. Модель продемонстрировала высокую чувствительность к изменениям в параметрах, что свидетельствует о её пригодности для адаптивного управления инфраструктурой и прогнозирования устойчивости при различных сценариях эксплуатации.

Оценка корректности модели проводилась через сравнение результатов с реальными данными мониторинга функционирования интеллектуального пункта пропуска. Полученные показатели достоверно отражает фактическое состояние системы и позволяет обоснованно планировать управленческие решения. Таким образом, созданная модель адекватно описывает поведение сложной системы и может использоваться для повышения уровня её устойчивости в условиях многофакторных воздействий и неопределённости.

В ходе проведённого исследования была сформирована комплексная методология применения логико-вероятностного метода для количественной оценки устойчивости критической инфраструктуры таможенных органов. Разработанный подход учитывает не только структуру и функциональные взаимосвязи элементов информационного обмена интеллектуальных пунктов пропуска, но и вероятностный характер данных, а также неопределённость, которая неизбежна при анализе сложных технических и организационных систем.

Полученная модель устойчивости демонстрирует высокую адекватность отражению реального состояния защищенности и устойчивости таможенной инфраструктуры, что позволяет выявлять критические узлы и минимальные сечения отказов, что обеспечивает целенаправленное выделение ресурсов на укрепление наиболее уязвимых компонентов системы. Адаптивность модели подтверждена возможностью интеграции динамических методов оценки финансовой устойчивости участников внешнеэкономической деятельности, что расширяет горизонты анализа и дает инструменты для прогнозирования и снижения рисков деструктивных воздействий.

Научная новизна работы заключается в разработке нового подхода к расчету оценки обеспечения устойчивости и надежности в области защиты ЕАИС ТО. Он может быть использован для расчетов состояния защищенности и устойчивости таможенной инфраструктуры, что позволяет выявлять критические узлы и минимальные сечения отказов, что обеспечивает целенаправленное выделение ресурсов на укрепление наиболее уязвимых компонентов системы.

ЛИТЕРАТУРА

1. Башлы, П. Н. О реализации модели интеллектуального пункта пропуска / П. Н. Башлы // Особенности государственного регулирования внешнеэкономической деятельности в современных условиях: материалы VII Всероссийской научно-практической конференции. — Ростов-на-Дону: Ростовский филиал государственного казенного образовательного учреждения высшего образования "Российская таможенная академия", 2020. — С. 55–61. — EDN: XUARMU.

2. Фильчакова, В. А. Интеллектуальные пункты пропуска: перспективы внедрения и ключевые проблемные вопросы / В. А. Фильчакова // Экономика: вчера, сегодня, завтра. — 2025. — Т. 15, № 7А. — С. 444–454. — URL: http://publishing-vak.ru/file/archive-economy-2025-7/d3-filchakova.pdf (дата обращения: 10.09.2026).
3. Гамидуллаев, С. Н., Ю. А. Максимов. Направления применения технологий искусственного интеллекта при осуществлении таможенной деятельности при создании интеллектуальных пунктов пропуска в Российской Федерации / С. Н. Гамидуллаев, Ю. А. Максимов // Вестник евразийской науки. — 2022. — Т. 14, № 5. — URL: https://esj.today/PDF/09ECVN522.pdf (дата обращения: 10.09.2026).
4. Максимов, Ю. А. Обеспечение экономической безопасности внешней торговли и информационной защиты критической инфраструктуры таможенных органов / Ю. А. Максимов // Вестник евразийской науки. — 2025. — Т. 17, № 1. — URL: https://esj.today/PDF/30ECVN125.pdf (дата обращения: 10.08.2026).
5. Афонин, П. Н., Е. В. Кисилева. Применение структурно-семантической модели эвристического анализа для формирования модели "интеллектуального" пункта пропуска / П. Н. Афонин, Е. В. Кисилева // Бюллетень инновационных технологий. — 2021. — Т. 5, № 2(18). — URL: https://bitjournal.ru/index.php/BIT/article/view/207 (дата обращения: 10.09.2026).
6. Викторова, В. С., А. С. Степанянц. Модели и методы расчета надежности технических систем / В. С. Викторова, А. С. Степанянц. — Москва: Ленанд, 2013. — URL: https://www.ipu.ru/sites/default/files/card_file/Viktorova&Stepanyants.pdf (дата обращения: 15.09.2026).
7. Протасов, М. Н. Состояние и перспективы развития современной системы показателей оценки процесса оказания государственных таможенных услуг / М. Н. Протасов // Вестник евразийской науки. — 2024. — Т. 16, № 2. — URL: https://esj.today/PDF/39ECVN224.pdf (дата обращения: 18.09.2026).
8. Билятдинов, К. З. Модель обеспечения и методика оценки устойчивости больших технических систем в процессе эксплуатации / К. З. Билятдинов // International Journal of Open Information Technologies. — 2022. — Т. 10, № 9. — С. 32–39. — URL: https://cyberleninka.ru/article/n/model-obespecheniya-i-metodika-otsenki-ustoychivosti-bolshih-tehnicheskih-sistem-v-protsesse-ekspluatatsii/viewer (дата обращения: 03.09.2026).
9. Кривчун, Е. А., К. З. Билятдинов. Интеграция методологических решений по оценке устойчивости функционирования больших технических систем / Е.А. Кривчун, К.З. Билятдинов // Моделирование, оптимизация и информационные технологии. — 2021. — Т. 9, № 4. — DOI: 10.26102/2310-6018/2021.35.4.003. — URL: https://moitvivt.ru/ru/journal/article?id=974 (дата обращения: 10.08.2026).
10. Элова, Г. В., М. В. Какорина. Совершенствование управленческих процессов в таможенных органах России посредством внедрения автоматизированной системы электронного документооборота / Г. В. Элова, М. В. Какорина // Мировая экономика и международные экономические отношения. — 2014. — № 3(112). — С. 106–111. — URL: https://ecsn.ru/wp-content/uploads/201403_106.pdf (дата обращения: 17.08.2026).
11. Можаев, А. С. Общий логико-вероятностный метод анализа надежности сложных систем / А. С. Можаев. — Ленинград: Издательство Военно-Морской Академии имени Маршала Советского Союза Гречко А. А., 1988. — 68 с. — URL: http://www.ifel.ru/surv/Res_9.pdf (дата обращения: 06.08.2026).

12. Морозов, В. В. Моделирование устойчивости сложных организационно-технических систем / В. В. Морозов // Управление организационно-экономическими системами: моделирование взаимодействий, принятие решений: сборник научных статей. — Самара: СГАУ, 2005. — Вып. 4. — С. 40–43. — URL: https://repo.ssau.ru/jspui/bitstream/123456789/1578/1/Стр.-40-43.pdf (дата обращения: 10.08.2026).
13. Анисимов, В. Г., Е. Г. Анисимов, Е. С. Родионова, Т. Н. Сауренко. Стохастическая модель для оценки эффективности управления таможенными рисками / В. Г. Анисимов, Е. Г. Анисимов, Е. С. Родионова, Т. Н. Сауренко // Управленческое консультирование. — 2016. — № 9. — С. 83–94. — URL: https://cyberleninka.ru/article/n/stohasticheskaya-model-dlya-otsenki-effektivnosti-upravleniya-tamozhennymi-riskami/viewer (дата обращения: 17.09.2026).
14. Поленин, В. И., И. А. Гладкова. Логико-детерминированные разделы структурно-логического анализа сложных систем / В. И. Поленин, И. А. Гладкова // Труды Международной Научной Школы МАБР — 2011 / под редакцией И. А. Рябинина, Е. Д. Соложенцева. — Санкт-Петербург: Институт проблем машиноведения Российской академии наук, 2011. — С. 386–394. — URL: https://docs.360.yandex.ru/docs/view?tm=1791448406&tld=ru&lang=ru&name=polenin_gladkova.pdf (дата обращения: 08.10.2026).
15. Кондрашова, В. А. Внедрение интеллектуального пункта пропуска через государственную границу Российской Федерации — динамика, проблемы и перспективы / В. А. Кондрашова // Бюллетень инновационных технологий. — 2024. — Т. 8, № 4(32). — С. 43–45. — EDN: PZFIQN. — URL: https://bitjournal.ru/index.php/BIT/article/view/388/660 (дата обращения: 08.10.2026).

Maximov Yuri Anatolyevich
The Russian Presidential Academy of National Economy and Public Administration, Saint Petersburg, Russia
North-Western Institute
E-mail: maximoff2000@mail.ru
RSCI: https://elibrary.ru/author_profile.asp?id=637236

Methodological approach for calculating the stability of critical infrastructure of customs authorities and ensuring economic security

Abstract. Developing a methodological approach to calculating the resilience of critical infrastructure of customs authorities is a complex task that lies at the intersection of regulatory frameworks, reliability theory, and risk management practices. In the context of the digital transformation of customs authorities and the growing cyber threats, it becomes one of the key elements of ensuring the economic security of the state.

The existing legal framework sets mandatory requirements for the resilience of the critical infrastructure of customs authorities, but it does not offer a unified quantitative methodology for calculating it, which leaves room for scientific and methodological developments. The stability of the critical infrastructure of customs authorities is the ability of the system to maintain its functions in the face of external and internal destabilizing influences and recover from them.

To assess the stability of automated control systems, a logical-probabilistic approach is used to calculate: the probability of maintaining the functionality of the software component and completing the management task, taking into account redundancy.

A promising direction is an integral method of assessing sustainability, combining: a multidimensional system of indicators, methods of fuzzy analysis for dealing with uncertainty, unified normalization of variables, categorization of objects in accordance with regulatory documents.

As a result of the work carried out, a scientifically grounded and practically applicable methodological approach was developed, which helps to improve the safety, reliability, and resilience of the critical infrastructure of customs authorities in a dynamically changing external economic environment. This approach strengthens the foundations for effective management and development of the infrastructure of customs authorities, ensuring their ability to respond timely and adequately to modern challenges.

The key outcome of applying this approach is the possibility of transitioning from reactive incident management to proactive resilience management, which ultimately strengthens the economic security of the state in the context of digital transformation and geopolitical challenges.

Keywords: methodological approach; economic security; security threats; infrastructure security; critical information infrastructure; customs authorities; effective governance