Эшелон
комплексная безопасность

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ПРОИЗВОДСТВЕННОЕ ОБЪЕДИНЕНИЕ «ЭШЕЛОН»

107023, г. Москва, ул. Электрозаводская, д. 24, стр. 1, тел.: +7 (495) 223 23 92, факс: +7 (499) 753-04-14, mail@npo-echelon.ru, npo-echelon.ru

Исх. № 17921 от 02.11.2026

# ОТЗЫВ

члена диссертационного совета НТУ.2.3.6.23
Маркова Алексея Сергеевича
на диссертацию Балябина Артёма Алексеевича
«Метод обеспечения киберустойчивости облачных платформ критической информационной инфраструктуры на основе теории подобия и размерностей», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

## 1. Актуальность избранной темы

Во исполнение Указа Президента РФ от 07.05.2024 г. № 309 реализуется национальный проект «Экономика данных и цифровая трансформация государства», в рамках которого ведется активная разработка и внедрение современных прорывных технологий, к которым относятся технологии искусственного интеллекта (ИИ), больших данных, квантовых вычислений, распределенного реестра, интернета вещей и другие. При этом облачные вычисления играют ключевую роль в создании инфраструктурной основы для реализации и внедрения современных технологий. Например, в соответствии с Распоряжением Правительства РФ от 21.10.2022 № 3102-р ведется разработка цифровой платформы, обеспечивающей развертывание и управление государственными информационными системами и цифровыми сервисами на базе облачных платформ, имеющих высокую значимость для государства и общества.

С другой стороны, сейчас наблюдается резкий рост количества выявленных уязвимостей, их доли в реальной эксплуатации в критических системах и сервисах, а также проявления разного рода инцидентов информационной безопасности облачных платформ критической информационной инфраструктуры (КИИ), особенно с развитием агентов ИИ. Например, по оценкам IBM X-Force[1], в позапрошлом году 70% расследованных кибератак приходились на организации КИИ, а конкретно процент скомпрометированных учетных данных облачных хранилищ составил почти 30%. Увеличение же числа уязвимостей, по оценкам MITRE, составляет за пять лет более 24% в год[2], причем ожидается экспоненциальный рост по той же причине развития технологий ИИ.

[1] X-Force Threat Intelligence Index 2025 highlights attackers steal, and sell, user identities at scale. IBM, 2025.
[2] 25th Anniversary Report, MITRE Corporation, 2024.

Следует отметить, что соискатель основное внимание уделяет именно не зафиксированным ранее классам кибератак (и не имеющим описания в систематиках MITRE CAPEC и ATT@CK), что обуславливает оригинальность и научный интерес к работе.

Таким образом, научная тема, направление исследований и научные результаты работы являются безусловно актуальными и востребованными.

## 2. Научная новизна результатов диссертационной работы

Судя по рукописи, оригинальность работы состоит в предложении нового подхода к обеспечению киберустойчивости вычислительных процессов облачных платформ КИИ, основанного на выявлении нарушений контролируемых семантических инвариантов с использованием аппарата теории подобия и размерностей, определении необходимого уровня покрытия вычислительных программ проверками и организации восстановления штатного выполнения вычислений в рамках принятой модели угроз и установленных ограничений.

Представляется, что работа направлена на разрешение фундаментального противоречия между увеличением вероятности достижения цели обнаружения и ростом времени выполнения программного цикла. На этом противоречии построены необходимое и достаточное значения коэффициента покрытия и критерий.

Следует согласиться с автором, что к новым научным результатам, полученным в диссертационном исследовании, следует отнести следующие:

1. Разработка математической модели киберустойчивой облачной платформы КИИ с самовосстановлением на основе теории подобия, позволяющей исследовать устойчивость ее функционирования в условиях компьютерных атак, направленных на нарушение целостности вычислений;

2. Разработка адаптивного алгоритмического метода обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением, позволяющего управлять устойчивостью их функционирования в зависимости от параметров интенсивности и повторяемости компьютерных атак за счет варьирования коэффициента покрытия облачных вычислительных программ проверками подобия;

3. Разработка методики синтеза и настройки средств обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей, позволяющей наделять их способностью обнаруживать известные и новые, ранее неизвестные компьютерные атаки, направленные на нарушение целостности вычислений, восстанавливать штатное функционирование и самообучаться;

4. Проектирование модульной многоуровневой архитектуры (с разделением функций и замкнутым контуром управления) прототипа программного комплекса обеспечения киберустойчивости облачных платформ КИИ в условиях роста угроз безопасности информации для экспериментального исследования предложенной модели, метода и методики.

Новизна по первому положению, выносимому на защиту, состоит в учете разработанной моделью киберустойчивой облачной платформы формальных операций обнаружения и восстановления штатного функционирования на основе теории подобия и внедрении впервые предложенного соискателем варьируемого коэффициента покрытия программ проверками подобия для управления киберустойчивостью.

Новизна по второму защищаемому научному положению состоит в применении в рамках предложенного метода обеспечения киберустойчивости облачных платформ модифицированного соискателем метода бисекции для оценивания необходимого значения коэффициента покрытия вычислительных программ проверками подобия, а также критерия устойчивости облачных платформ, впервые сформулированного и доказанного соискателем.

Новизна по третьему научному положению заключается в разработке методики формирования подмножества контролируемых линейных блоков вычислительных программ, позволяющей организовать выявление нарушений контролируемых семантических инвариантов с учётом заданного коэффициента покрытия вычислительного процесса.

Новизна четвертого научного результата состоит в разработке оригинальной архитектуры обеспечения киберустойчивости облачных платформ КИИ, включающей программные модули трансляции для синтеза эталонных семантических моделей программ, оценивания и управления киберустойчивостью, обнаружения нарушений и самовосстановления облачных платформ на основе теории подобия и размерностей, а также базы данных «приобретаемого кибериммунитета» для самообучения системы защиты.

В целом можно заключить, что в работе сформулирована и решена новая научная задача разработки методического аппарата обнаружения нарушений целостности и восстановления вычислительных процессов многоуровневой облачной платформы КИИ при известных и неизвестных компьютерных воздействиях, обеспечивающего заданную вероятность достижения цели функционирования при ограничении на допустимые временные затраты за счет управляемого выбора полноты контроля семантических инвариантов вычислений.

### 3. Теоретическая значимость и практическая ценность исследования

Предложенные в диссертационной работе математическая модель, метод и методика обеспечения киберустойчивости облачных платформ являются развитием инвариантных подходов к обнаружению киберугроз, накладывающих систему ограничений (инвариантов) на пространство допустимых состояний вычислительных процессов так, чтобы выделить подмножества штатных и «аварийных» состояний.

Любопытным является то, что используемая в работе теория размерностей позволяет осуществлять контроль вычислений на семантическом уровне, выявляя отклонения контролируемых инвариантов от модели штатного функционирования

независимо от конкретных сигнатур компьютерных атак. Такой подход создает предпосылки для обнаружения в том числе ранее неизвестных кибератак, приводящих к нарушениям контролируемых свойств вычислительных процессов. Применение положений теории подобия позволяет формализовать условия соответствия вычислительных процессов модели штатного функционирования и использовать их при реализации механизмов обнаружения нарушений и последующего восстановления.

Указанное позволяет сделать вывод, что теоретическая значимость работы состоит в дополнении теории защиты информации новыми вероятностной математической моделью, методом и методикой обеспечения заданной степени киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей, что позволило получить эффект выявления в том числе ранее неизвестных кибератак.

В то же время, надо понимать, что автор несколько сужает значение термина «неизвестных атак», сводя их к атакам, релевантным контролируемым инвариантам подобия и размерностей. В частности, автор предлагает контролировать не шаблон сценария или сигнатуры пакетов кибератаки, а свойства штатного вычислительного процесса. Кстати, такой подход концептуально соответствует известным направлениям поведенческих и аномальных подходов. Получается, что контроль свойств нормального поведения в принципе способен реагировать на ранее не встречавшийся конкретный сценарий кибератаки. Из этого явно не следует способность обнаруживать любую неизвестную кибератаку, так как выявляется только кибератака, которая приводит к наблюдаемому нарушению контролируемого свойства. Однако подобное замечание не снижает теоретической значимости диссертации, а уточняет ее место в научном знании.

Практическая ценность диссертации в явном виде обусловлена четвертым научным результатом и доведением разработанного методического аппарата до программной реализации, что подтверждено свидетельствами Роспатента. В работе автор декларировал возможность применения результатов исследования при проектировании систем защиты национальных облачных вычислительных платформ и привел факты востребованности результатов исследования среди предприятий и научно-исследовательских организаций, ведущих научное сопровождение работ по созданию объектов информатизации КИИ РФ – об эффективности использования результатов исследования имеются акты о внедрении из трех профильных организаций.

**4. Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации**

Достоверность и обоснованность полученных научных результатов обеспечиваются:

- анализом исследований, диссертационных работ и прикладных решений в предметной области;

- корректным применением апробированного математического аппарата;

- наличием доказательств для базовых утверждений;

- согласованностью результатов теоретических и экспериментальных исследований и их непротиворечивостью с известными работами в предметной области;

- апробацией результатов исследования на всероссийских и международных научно-практических конференциях, а также их публикацией в рецензируемых изданиях.

При обосновании полученных результатов автор логично аргументировал использование формализованных моделей вычислительных процессов, аппарата теории подобия и размерностей, проведение аналитических исследований и экспериментальной проверки предложенных решений. При этом автор отметил, что область применимости полученных оценок определяется принятыми вероятностными допущениями, выбранными классами контролируемых вычислений и нарушений, а также условиями проведённых экспериментов.

Следует отметить, что достоверность результатов исследования косвенно подтверждена свидетельствами о регистрации программ, а также актами о внедрении.

**5. Соответствие содержания диссертации и автореферата целям и задачам исследования**

Оглавление и содержание диссертации полно соответствуют целям и задачам исследования.

Содержание автореферата полно соответствует диссертации. Корректно отражены общая характеристика работы, результат решения поставленной научной задачи, итоговые выводы и сведения об опубликованных работах. Автореферат и диссертация соответствуют ГОСТ.

**6. Соответствие паспорту специальности**

Сформулированные в диссертационной работе тема, цель, задачи и научные результаты безусловно соответствуют паспорту специальности 2.3.6, например, в части п. 9 - Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности.

**7. Апробация и публикация основных результатов**

По теме диссертации согласно РИНЦ опубликовано 15 научных статей в изданиях, рекомендованных ВАК, из них по специальности 2.3.6 в журналах К1 – 7. Кроме того, автор имеет две тематические научные статьи в Scopus Q2 и Q1.

Согласно рукописи, основные положения работы прошли апробацию на 8 научных конференциях, тогда как в РИНЦ представлено 32 тезиса тематических конференций, что свидетельствует о высокой научной активности автора.

Анализ публикаций позволяет сделать вывод о самостоятельности научного исследования и личном вкладе автора в науку.

## 8. Замечания и рекомендации по диссертации

Несмотря на научный интерес к исследованию, диссертационная работа, судя по рукописи, не свободна от недостатков и вопросов, к которым, например, могут быть отнесены следующие:

1. На стр. 56 сделано допущение о том, что вероятность возникновения нарушения на каждой *i*-й итерации обработки входных данных зависит только от свойств текущих входных данных и не зависит от свойств на *(i-1)*-й итерации. В то же время, на наш взгляд, возможны многошаговые итерационные кибератаки, использующие накопление состояния и последовательно эксплуатирующие уязвимости (например, атаки с памятью).

2. На стр. 61 обоснование, почему вероятность модификации вычислений при пропуске атаки постоянна, несколько лаконично. Например, не совсем понятно, сохраняются ли выводы о киберустойчивости при изменении вероятности в зависимости от класса кибератаки, состояния системы и истории обработки данных.

3. На наш взгляд, работа бы выиграла, если бы автор более четко уточнил границы применимости семантического контроля, например: конкретные классы нарушений вычислительных процессов, обнаруживаемых посредством контроля инвариантов подобия и размерностей, и нарушения, не приводящие к изменению контролируемых соотношений. Как следствие этого возникают трудности с определением степени полноты обнаружения и ограничения предложенного метода применительно к различным классам «неизвестных» компьютерных атак.

В целом отмеченные замечания и рекомендации не снижают научной значимости работы, так как поставленная в работе цель достигнута. К достоинствам работы необходимо отнести математическую культуру и широкий кругозор автора, актуальность, завершенность, полноту, безусловную инновационность и теоретическую направленность исследований.

## Заключение о соответствии диссертации установленным критериям

Диссертационное исследование Балябина А.А. представляет собой законченную научно-квалификационную работу, выполненную лично соискателем на актуальную тему, которая обладает внутренним единством, отличается новизной, теоретической значимостью и практической ценностью в отрасли информационной безопасности (технические науки).

Автором в диссертации решена научная задача, заключающаяся в разработке методического аппарата обеспечения киберустойчивости облачных платформ КИИ на основе теории подобия и размерностей, имеющая важное значение в обеспечении кибербезопасности и киберустойчивости критически важных информационных ресурсов страны.

Полагаем, диссертационная работа отвечает требованиям Положения о присуждении ученых степеней Автономной некоммерческой образовательной

организацией высшего образования «Научно-технологический университет «Сириус», утвержденного приказом от «02» апреля 2026 г. № 469-ОД-У (в ред. приказа от 29.09.2026 №1524-ОД-У), предъявляемым к диссертациям на соискание ученой степени кандидата наук, а ее автор, Балябин Артём Алексеевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

**Член диссертационного совета НТУ.2.3.6.23**
доктор технических наук, профессор,
президент АО «НПО «Эшелон»

« 2 » ноября 2026 г. Марков Алексей Сергеевич

*Подпись доктора технических наук Маркова Алексея Сергеевича заверяю.*
Начальник отдела кадров АО «НПО «Эшелон» И.С. Грибова

**Сведения:**
Марков Алексей Сергеевич.
Докторская диссертация защищена по специальности 05.13.19 Методы и системы защиты информации, информационная безопасность.
Место работы:
Акционерное общество «Научно-производственное объединение «Эшелон» (АО «НПО «Эшелон»).
Контактная информация:
107023, г. Москва, ул. Электрозаводская, д. 24 стр.1
Телефон: +7 (495) 223-23-92
сайт: https://npo-echelon.ru
эл.почта: a.markov@npo-echelon.ru