На правах рукописи



Балябин Артём Алексеевич

Метод обеспечения киберустойчивости облачных платформ критической информационной инфраструктуры на основе теории подобия и размерностей

2.3.6. Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Федеральная территория «Сириус»

2026

Работа выполнена в автономной некоммерческой образовательной организации высшего образования «Научно-технологический университет «Сириус»

Научный руководитель:
Петренко Сергей Анатольевич
доктор технических наук, профессор
Автономная некоммерческая образовательная организация высшего образования «Научно-технологический университет «Сириус»

Защита состоится 01 декабря 2026 года в 14:00 на заседании диссертационного совета НТУ.2.3.6.23 на базе АНОО ВО «Университет «Сириус» по адресу 354340, Краснодарский край, федеральная территория «Сириус», Олимпийский пр., д. 1.

С диссертацией можно ознакомиться в библиотеке и на сайте АНОО ВО «Университет «Сириус»: https://siriusuniversity.ru/sveden/science/obyavleniya-o-zashchitakh/.

Автореферат разослан «___» октября 2026 года.

Ученый секретарь
диссертационного совета,
кандидат физико-математических наук,
доцент  Кузнецов Сергей Борисович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. В рамках реализации национального проекта Российской Федерации «Экономика данных» ведется активная разработка и внедрение современных цифровых технологий, направленных на обеспечение конкурентоспособности экономики, достижение цифровой трансформации, технологического суверенитета и лидерства. К таким технологиям относятся, в частности, облачные вычисления.

Облачные платформы упрощают разработку, тестирование, развертывание, масштабирование и управление типовыми программными решениями, а также обеспечивают бесшовное взаимодействие федеральных и региональных органов власти посредством сети Интернет. Примером отечественных облачных платформ является Единая цифровая платформа (ЕЦП) «ГосТех», позволяющая создавать цифровые сервисы и государственные информационные системы (ГИС), которые в силу своей значимости могут быть отнесены к критической информационной инфраструктуре (КИИ). К облачным платформам КИИ могут предъявляться повышенные требования в части безопасности и киберустойчивости.

Вместе с тем наблюдается тенденция постоянного роста количества и сложности компьютерных атак на информационные ресурсы как в Российской Федерации, так и в мире в целом. Кибератаки все чаще приобретают комплексный и целенаправленный характер, при этом большую их часть составляют новые, ранее неизвестные атаки, которые зачастую не могут быть своевременно обнаружены и предотвращены существующими классическими методами и средствами защиты. Реализация таких атак на облачные платформы КИИ может привести к катастрофическим последствиям.

Таким образом, рост количества и сложности киберугроз, а также высокая критичность нарушений делает задачу обеспечения киберустойчивости облачных платформ КИИ в условиях компьютерных атак актуальной.

Степень разработанности темы исследования. Обеспечению безопасности и устойчивости объектов КИИ в условиях компьютерных атак посвящены работы С.И. Макаренко, А.С. Шабурова, А.О. Калашникова, И.В. Котенко, И.Б. Саенко, О.С. Лауты, Р.И. Захарченко, А.А. Корниенко, С.В. Корниенко (Диасамидзе), А.П. Глухова, А.С. Маркова, В.А. Воеводина, В.А. Минаева, Ю.В. Бородакого, А.А. Тарасова.

Существуют также интеллектуальные и биоинспирированные подходы к обеспечению безопасности и устойчивости различных информационно-вычислительных систем (ИВС). Подходы на основе методологии гомеостаза, реконфигурации, фрактальных и спектральных методов рассматривались в работах П.Д. Зегжды, Д.П. Зегжды, Е.Б. Александровой, М.О. Калинина, М.А. Полтавцевой, Д.С. Лавровой, Е.Ю. Павленко, А.А. Штыркиной. Подходы на основе превентивного реагирования, антиципации, самоорганизации и синтеза упреждающего поведения рассматривались в работах А.Г. Ломако, Ю.Г. Ростовцева, Д.Н. Бирюкова, С.А. Петренко. Подходы на основе совершенствования систем обнаружения вторжений (СОВ) с использованием методов искусственного интеллекта и машинного обучения рассматривались в работах О.И. Шелухина, Е.С. Новиковой, И.В. Котенко, А.В. Мелешко, К.Е. Израилова. Подходы на основе создания искусственных иммунных систем и сетей, адаптации алгоритмов иммунного ответа рассматривались в работах М.Е. Бурлакова, Р.Р. Шамсутдинова, М.Ю. Ваганова, В.И. Васильева, А.М. Вульфина, А.А. Браницкого, В.А. Головко, С.В. Безобразова, И.В. Котенко, А.О. Тараканова, Ю.М. Туманова, В.Д. Котова, С. Хофмейр, С. Форрест, Т. Стибор, Дж. Тиммис, К. Эккерт, У. Айкелин, Д. Дасгупта. Подходы на основе организации самовосстанавливающихся вычислений и кибериммунитета рассматривались в работах С.А. Петренко и В.А. Новикова.

Известен ряд диссертационных работ, посвященных обеспечению информационной безопасности и устойчивости различных ИВС, в том числе облачных. Среди них можно выделить диссертационные работы А.А. Станкевичуса, Ю.М. Туманова, В.Л. Платоновой, М.Ю. Ваганова, А.С. Молякова, М.Е. Бурлакова, А.А. Браницкого, Д.С. Лавровой, М.А. Полтавцевой, В.М. Крундышева, Р.Р. Шамсутдинова, А.А. Штыркиной, Е.Ю. Павленко.

Среди прикладных разработок можно выделить решения, предназначенные для резервного копирования, защиты публично доступных сервисов, контейнерных сред, виртуальных машин и рабочих нагрузок, операционных систем, сред виртуализации и гипервизоров. Среди решений, реализующих механизмы кибериммунитета, наиболее известна кибериммунная операционная система KasperskyOS, а также прототипы кибериммунных СОВ, такие как ARTIS, HiDE-IDS и DarkTrace.

Современные исследования посвящены решению актуальных проблем и задач обеспечения безопасности и устойчивости ИВС, однако они не в полной мере учитывают особенности облачных платформ КИИ, а именно, их многоуровневую иерархическую структуру, функционирование в условиях компьютерных атак, направленных на нарушение целостности вычислений, и необходимость оперативного восстановления штатного функционирования. Существующие классические средства защиты зачастую не обладают способностью к адаптации и самообучению, вследствие чего они оказываются неэффективными в условиях ранее неизвестных компьютерных атак.

Объектом исследования являются облачные платформы КИИ в условиях роста угроз безопасности информации.

Предметом исследования являются модели, методы и методики обеспечения киберустойчивости облачных платформ КИИ в условиях компьютерных атак.

Цель исследования состоит в обеспечении киберустойчивости облачных платформ КИИ в условиях компьютерных атак, направленных на нарушение целостности вычислений.

Гипотеза исследования состоит в том, что достижение цели исследования возможно за счет применения метода и методики обеспечения киберустойчивости облачных платформ КИИ на основе теории подобия и размерностей.

Для достижения цели исследования сформулирована **научная задача** организации самовосстанавливающихся вычислительных процессов облачных платформ КИИ на основе теории подобия и размерностей.

В данной постановке цель исследования и научная задача формулируются впервые. Цель и научная задача **соответствуют специальности** 2.3.6. Методы и системы защиты информации, информационная безопасность по следующим пунктам паспорта:

п. 6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях;

п. 9. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем, позволяющие получать оценки показателей информационной безопасности;

п. 18. Модели и методы управления информационной безопасностью, непрерывным функционированием и восстановлением систем, противодействия отказам в обслуживании.

В процессе исследования выполнена декомпозиция **научной задачи на следующую совокупность частных научных и прикладных задач**:

1) разработка 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 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 обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей, позволяющей наделять их способностью обнаруживать известные и новые, ранее неизвестные атаки, направленные на нарушение целостности вычислений, восстанавливать штатное функционирование и самообучаться;
4) проектирование архитектуры и разработка прототипа программного комплекса обеспечения киберустойчивости облачных платформ КИИ в условиях роста угроз безопасности информации для экспериментального исследования предложенной модели, метода и методики.

Положения, выносимые на защиту, соответствуют результатам решения вышеуказанных частных научных и прикладных задач:

1) модель киберустойчивой облачной платформы КИИ с самовосстановлением на основе теории подобия [1, 2, 3, 9, 11, 16-18];
2) метод обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением за счет варьирования коэффициента покрытия облачных вычислительных программ проверками подобия [4, 5, 19-22];
3) методика обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей [6, 12, 23, 24];
4) архитектура программного комплекса обеспечения киберустойчивости облачных платформ КИИ в условиях роста угроз безопасности информации [11-15].

Научная новизна полученных результатов:

1) Разработанная модель киберустойчивой облачной платформы КИИ с самовосстановлением впервые учитывает обнаружение нарушений целостности вычислений и восстановление штатного функционирования облачных платформ на основе 3-й теоремы подобия Кирпичева-Гухмана. Кроме того, впервые предложен варьируемый коэффициент покрытия облачных вычислительных программ проверками подобия, позволяющий осуществлять оценивание и управление киберустойчивостью облачных платформ КИИ с учетом их самовосстановления.

2) В разработанном методе обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением для нахождения необходимого значения коэффициента покрытия облачных вычислительных программ проверками подобия впервые применен модифицированный метод бисекции. Кроме того, для проверки возможности обеспечения требуемой вероятности достижения цели и времени выполнения программ сформулирован и доказан соответствующий критерий устойчивости облачных платформ КИИ.

3) Разработанная методика обеспечения требуемой киберустойчивости облачных платформ КИИ отличается тем, что для синтеза моделей штатного функционирования программ применен аппарат теории подобия и размерностей, что позволяет обнаруживать нарушения целостности вычислений по отклонению инвариантов размерностей в контрольных точках

вычислительных процессов от штатных и восстанавливать функционирование программ, возвращая их в состояние, удовлетворяющее условиям подобия. При этом для формирования подмножества контролируемых линейных блоков используется необходимое и достаточное значение коэффициента покрытия программ проверками подобия, определяемое с учетом требований к показателям киберустойчивости.

4) Впервые предложена архитектура программного комплекса обеспечения киберустойчивости облачных платформ КИИ, включающая отдельные программные модули трансляции с внедрением избыточности для контроля целостности вычислений, оценивания и управления киберустойчивостью, обнаружения нарушений и восстановления на основе теории подобия и размерностей, а также базу данных образцов вредоносных входных данных.

Теоретическая значимость работы заключается:

- в расширении научно-методического инструментария оценивания и управления киберустойчивостью облачных платформ КИИ за счет разработки новых модели, метода и методики, учитывающих операции самовосстановления на основе теории подобия и размерностей;
- в развитии подходов к организации самовосстанавливающихся вычислений и кибериммунитета, позволяющих противодействовать известным и новым, ранее неизвестным угрозам, обнаруживать нарушения целостности вычислений, оперативно восстанавливать штатное функционирование систем, а также самообучаться для предотвращения повторных нарушений;
- в формулировании и доказательстве утверждений, связывающих целостность облачных вычислений со свойствами подобия вычислительных процессов, а также описывающих зависимости показателей киберустойчивости от полноты проверок подобия и обосновывающих критерий устойчивости облачных платформ КИИ.

Практическая значимость работы заключается в возможности применения разработанных модели, метода, методики и архитектуры программного комплекса как на этапе проектирования, так и на этапе эксплуатации облачных платформ КИИ для обеспечения требуемой их киберустойчивости. Исследование киберустойчивости облачных платформ КИИ показало, что применение разработанного метода и методики обеспечивает прирост: до 17,10% по показателю вероятности достижения цели на *i*-ом уровне; до 88,02% по показателю общей вероятности достижения цели; до 3,75% по показателю полноты обнаружения и противодействия атакам. Разработан прототип программного комплекса, позволяющий наделять облачные платформы КИИ способностью противодействовать известным и ранее неизвестным атакам, самовосстанавливаться и самообучаться, для компонентов которого получены свидетельства о государственной регистрации программ для ЭВМ.

Достоверность научных результатов подтверждается: использованием основных принципов системного подхода при постановке научной задачи; корректным применением апробированных математических методов при решении научной задачи; строгим аналитическим выводом математических зависимостей, используемых в модели, методе и методике; соответствием экспериментальных результатов теоретическим выводам; непротиворечивостью полученных результатов с научными работами в данной предметной области; апробацией полученных результатов в научно-рецензируемых изданиях и их публичным представлением на научно-практических конференциях.

Методы исследования включают в себя методы теории системного анализа, теории многоуровневых иерархических систем, теории вероятностей и математической статистики, теории подобия и размерностей, методы оптимизации.

Публикация результатов исследования. По теме диссертационного исследования всего опубликовано 27 работ, из них:

- 8 статей в рецензируемых изданиях, рекомендованных ВАК для публикации диссертационных исследований по защищаемой специальности и отрасли наук [1-8], из них статьи [2, 4, 6] опубликованы в российских журналах К-1 перечня ВАК, входящих также в единый государственный перечень научных изданий – «Белый список», что соответствует требованиям пп. 2.4–2.6 Положения о присуждении ученых степеней АНОО ВО «Научно-технологический университет «Сириус» (в действующей редакции);
- 5 свидетельств о государственной регистрации программ для ЭВМ [11-15];
- 2 работы в изданиях, индексируемых международными базами Scopus и Web of Science (сборники материалов конференций) [9, 10];
- 12 работ в иных сборниках материалов конференций [16-27].

Личный вклад соискателя. Из вышеуказанных 27 работ 10 работ [1, 4, 9, 10, 16, 17, 19, 20, 23, 25] выполнены автором единолично, что подтверждает самостоятельность выполнения исследования и личное получение основных результатов работы. В 9 работах [2, 3, 5, 6, 8, 18, 21, 24, 26], выполненных в соавторстве с научным руководителем – С.А. Петренко, которому принадлежит руководящая роль в формировании замысла и общего направления исследований, автору диссертации принадлежит основная роль в конкретизации целей и задач, непосредственном получении и верификации результатов исследований, формировании итоговых выводов. В 3 работах [7, 22, 27], выполненных в соавторстве как с научным руководителем – С.А. Петренко, так и с другими учеными, автору диссертации также принадлежит основная роль в конкретизации целей и задач, непосредственном получении и верификации результатов исследований, формировании итоговых выводов. В 5 программах для ЭВМ [11-15], разработанных авторскими коллективами, автору диссертации принадлежит ведущая роль в разработке и программной реализации алгоритмов их функционирования.

Апробация результатов исследования. Результаты исследования апробировались и обсуждались на 8 всероссийских и международных научно-практических конференциях: на 3-х Всероссийских конференциях «Методы и технические средства обеспечения безопасности информации» (г. Санкт-Петербург, 2022, 2024, 2025); на XXVII Международной конференции по мягким вычислениям и измерениям «2024 XXVII International Conference on Soft Computing and Measurements SCM» (г. Санкт-Петербург, 2024); на 3-х Международных научно-технических конференциях «The Symposium on Cybersecurity of the Digital Economy – CDE» (г. Иннополис, 2023, 2025; г. Казань, 2024); на IX Всероссийском молодежном научном форуме «Наука будущего – наука молодых» (г. Самара, 2024) – по результатам отбора в финал IX Всероссийского конкурса научно-исследовательских работ студентов и аспирантов.

Реализация, внедрение и использование результатов исследования. Исследование получило государственную поддержку в виде гранта Российского научного фонда № 25-11-20037, а также Проекта ФТС-2024-2.3-VY-1160-5744 «Технологии противодействия ранее неизвестным квантовым киберугрозам» в рамках реализации мероприятия 2.3 государственной программы федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус». Полученные основные научные результаты диссертационного исследования

использованы: в научно-производственной деятельности АО «Технологии радиоконтроля» при выполнении опытно-конструкторской работы по разработке программного комплекса «Диадема»; в Научно-технологическом университете «Сириус» при выполнении I и II Этапов научного Проекта «Технологии противодействия ранее неизвестным квантовым киберугрозам», реализуемого в рамках государственной программы развития федеральной территории «Сириус» «Научно-технологическое развитие федеральной территории «Сириус» (Соглашение № 23-03 от 27.09.2024 г.), а также в учебном процессе ФГАОУ ВО «СПбГЭТУ «ЛЭТИ» им. В.И. Ульянова (Ленина)» при проведении учебных занятий по дисциплинам «Методы защиты информации» и «Информационная безопасность облачных платформ цифровой экономики РФ», что подтверждается соответствующими актами о внедрении и использовании.

Структура и объем диссертации. Диссертационная работа состоит из введения, пяти глав, заключения, списка литературы из 153 наименований и 2 приложений. Общий объем работы составляет 183 страницы, в том числе 37 рисунков и 14 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении приведено обоснование актуальности темы диссертационного исследования, сформулирована цель и поставлена основная научная задача. Выполнена декомпозиция научной задачи на совокупность частных научных и прикладных задач. Представлены положения, выносимые на защиту, соответствующие результатам решения частных научных и прикладных задач, сведения об их научной новизне, теоретической и практической значимости.

В первой главе представлены результаты анализа общих характеристик и отличительных особенностей облачных платформ КИИ. Обоснованы причины возникновения новых, ранее неизвестных угроз, связанных с нарушением целостности вычислений. Сформирована модель угроз и нарушителей безопасности облачных платформ КИИ. Проведен анализ моделей, методов и методик обеспечения безопасности и киберустойчивости облачных платформ КИИ. Выполнена декомпозиция и формализация научной задачи.

Выделены такие уровни типовых облачных платформ, как: гипервизоры; операционные системы (ОС); промежуточные среды выполнения; прикладные облачные сервисы.

К общим характеристикам типовых облачных платформ относятся: архитектура с изолированными независимыми модулями; наличие нескольких уровней, имеющих доступные посредством сети Интернет интерфейсы управления; вложенный иерархический характер программного обеспечения и наличие вертикальных (логических) связей между компонентами.

К отличительным особенностям облачных платформ КИИ можно отнести следующее:

- возможность реализации мульти-облачной и гибридной архитектуры, позволяющей охарактеризовать такие платформы как многоуровневые иерархические системы с вертикальными (логическими) и горизонтальными (информационными) связями;
- потенциальное наличие уязвимостей вследствие ускоренного замещения иностранных технологий и недостаточного тестирования программного обеспечения;
- повышенные требования к безопасности и киберустойчивости;
- высокая критичность нарушений и необходимость оперативного восстановления.

Иерархию уровней облачной платформы КИИ можно представить в виде совокупности взаимодействующих вычислительных программ, каждая из которых реализует некоторую вычислимую по Тьюрингу функцию (аналог универсальной машины Тьюринга большой вложенности) $f : X \to Y$, так, что $\forall x \in X, \exists y \in Y : f(x) = y$, где: X – множество входных данных; Y – множество выходных данных.

Если вычислительная программа содержит ошибку (недостаток), то множество ее входных данных X содержит непустое подмножество вредоносных входных данных $X^- \subset X$, $X^- \neq \varnothing$, обработка которых приводит к нарушениям. Такие ошибки являются причиной возникновения уязвимостей «нулевого дня», создающих угрозу реализации новых, ранее неизвестных компьютерных атак, направленных на нарушение целостности вычислений.

Под *нарушением целостности вычислений* будем понимать нарушение корректности вычислений, сопровождающееся модификацией вычислительных структур, свойств или действий (возникновение аномальных состояний программ, отличающихся от ожидаемых).

Тогда под *киберустойчивостью* будем понимать способность системы корректно функционировать в условиях компьютерных атак и самовосстанавливаться при возникновении нарушений.

Определены актуальные угрозы безопасности и устойчивости функционирования облачных платформ КИИ, к которым относятся, в частности, угрозы перехвата потока управления и внедрения кода. К вероятным нарушителям отнесены, в частности, специальные службы иностранных государств, обладающие достаточным потенциалом для выявления ранее неизвестных уязвимостей и разработки средств целенаправленного воздействия.

Анализ исследований, посвященных разработке моделей и методов обеспечения безопасности и киберустойчивости различных ИВС показал, что они не позволяют в полной мере одновременно учесть многоуровневый характер облачных платформ КИИ, необходимость противодействия как известным, так и ранее неизвестным атакам, направленным на нарушение целостности вычислений, а также необходимость оперативного самовосстановления и самообучения для предотвращения повторных нарушений. Анализ прикладных решений показал, что они также зачастую не обладают способностью к адаптации и самообучению, вследствие чего они оказываются неэффективными в условиях ранее неизвестных атак.

Для контроля целостности облачных вычислений и обеспечения киберустойчивости облачных платформ КИИ предложено применять теорию подобия и размерностей. В соответствии с данной теорией необходимым и достаточным условием подобия физических процессов является их однородность и равенство критериев подобия (инвариантов). Применительно к вычислительным процессам под инвариантами подобия понимаются некоторые характеристики, метрики или соотношения, одинаковые для штатных реализаций вычислительных программ, но отличающиеся в случае нарушения. Одним из таких инвариантов являются размерности вычислительных операндов. Классические размерности устанавливают связи между физическими величинами (например, сила есть произведение массы на ускорение). Абстрактные размерности вычислительных операндов учитывают семантические связи между переменными и инвариантны по отношению к их значениям и маршрутам выполнения программ, что позволяет контролировать и восстанавливать целостность вычислений, абстрагируясь от конкретных сигнатур атак.

Любая вычислительная программа представима управляющим графом $\Gamma(B,T)$, где $B = \{b_i \mid i \in [1,k]\}$ – множество линейных блоков, состоящих из последовательностей вычислительных операций; k – количество линейных блоков; $T = \{B \times B\}$ – множество связей по управлению между блоками. Тогда возможны два типа нарушений: нарушение состояния и нарушение перехода.

Для контроля целостности облачных вычислений предложено осуществлять отображение управляющего графа $\Gamma(B,T)$ в модель штатного функционирования программы $M(ST,TR)$, где $ST = \{st_i \mid i \in [1,k]\}$ – множество состояний программы в линейных блоках в терминах инвариантов

подобия и размерностей; $TR = \{ST \times ST\}$ – переходы между состояниями, а также внедрять в линейные блоки программы элементы структурно-функциональной избыточности. Это увеличит время ее выполнения, что может быть недопустимо. Тогда можно ввести коэффициент покрытия $k_{\text{покр}}$, определяющий долю наиболее критичных линейных блоков, подлежащих контролю, однако это приведет к пропуску некоторых нарушений, приходящихся на участки управляющего графа, для которых не осуществляется контроль целостности вычислений.

Для формализации научной задачи введены обозначения:

N – количество уровней облачной платформы КИИ;

$L = \{L_i \mid i \in [1, N]\}$ – облачная платформа КИИ, функционирующая на N уровнях;

$F = \{f_i \mid i \in [1, N]\}$ – множество вычислительных программ облачной платформы КИИ, где f_i – вычислительная программа i-го уровня;

$X = \{X_i \mid i \in [1, N]\}$ – множество входных данных облачной платформы КИИ, где X_i – входные данные вычислительных программ i-го уровня;

$Y = \{Y_i \mid i \in [1, N]\}$ – множество выходных данных облачной платформы КИИ, где Y_i – выходные данные вычислительных программ i-го уровня;

$I = \{I_i \mid i \in [1, N]\}$ – множество обнаруженных вредоносных входных данных, где $I_i = \{x \mid x \in X_i^-\}$ – вредоносные входные данные i-го уровня;

O – отображение проверки корректности (подобия) вычислений;

V – отображение синтеза восстанавливающего воздействия;

$k_{\text{вред}i}$ – доля входных данных, являющихся вредоносными, на i-ом уровне;

$k_{\text{изв}i}$ – доля известных вредоносных входных данных на i-ом уровне;

$A = \{A_i \mid i \in [1, N]\}$ – параметры интенсивности и повторяемости атак на облачную платформу КИИ, где $A_i = \{k_{\text{вред}i}, k_{\text{изв}i}\}$ – параметры i-го уровня;

$k_{\text{покр}i}$ – коэффициент покрытия вычислительных программ проверками подобия i-го уровня, определяющий долю линейных блоков программы f_i, для которых выполняется контроль целостности вычислений на основе теории подобия;

$D = \{D_i \mid i \in [1, N]\}$ – управляемые параметры облачной платформы КИИ, где $D_i = \{k_{\text{покр}i}\}$ – управляемые параметры i-го уровня;

$P_{\text{цели}i}$ – вероятность достижения цели облачной платформы КИИ на i-ом уровне;

$P_{\text{цели}i}^{\text{тр}}$ – требуемая вероятность достижения цели на i-ом уровне;

$R = \{R_i \mid i \in [1, N]\}$ – множество основных вероятностных показателей киберустойчивости облачной платформы КИИ, где $R_i = \{P_{\text{цели}i}\}$ – показатели киберустойчивости i-го уровня;

$T_{\text{вып}i}$ – время выполнения программного цикла на i-ом уровне;

$T_{\text{вып}i}^{\text{тр}}$ – требуемое время выполнения программного цикла на i-ом уровне;

$T = \{T_i \mid i \in [1, N]\}$ – множество временных показателей функционирования облачной платформы КИИ, где $T_i = \{T_{\text{вып}i}\}$ – временные показатели i-го уровня.

Выполнена формальная постановка научной задачи организации самовосстанавливающихся вычислительных процессов облачных платформ КИИ на основе теории подобия и размерностей, для решения которой необходимо разработать модель M_1 киберустойчивой облачной платформы КИИ L с самовосстановлением, устанавливающей на каждом i-ом уровне закономерность изменения показателей киберустойчивости $R_i \subset R$ и временных показателей функционирования $T_i \subset T$ от значений параметров интенсивности и повторяемости компьютерных атак $A_i \subset A$ и управляемых параметров $D_i \subset D$:

$$M_1 :< L, F, I, O, V, A, D > \rightarrow < R, T >,$$

метод M_2 обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением L, обеспечивающий на каждом i-ом уровне требуемое значение $P^{\text{тр}}_{\text{цели}i}$ вероятности достижения цели $P_{\text{цели}i} \in R_i \subset R$ при ограничении $T^{\text{тр}}_{\text{вып}i}$ на максимально допустимое время выполнения программного цикла $T_{\text{вып}i} \in T_i \subset T$, в условиях компьютерных атак $A_i \subset A$ за счет варьирования значений управляемых параметров $D_i \subset D$:

$$M_2 :< L, F, A, D, R, T > \rightarrow < P_{\text{цели}i}, T_{\text{вып}i} > \Big| \begin{cases} \forall P_{\text{цели}i} \geq P^{\text{тр}}_{\text{цели}i}, P_{\text{цели}i} \in R_i \subset R \\ \forall T_{\text{вып}i} \leq T^{\text{тр}}_{\text{вып}i}, T_{\text{вып}i} \in T_i \subset T \end{cases}, i \in [1, N],$$

а также методику M_3 обеспечения требуемой киберустойчивости облачных платформ КИИ L с использованием теории подобия и размерностей, обеспечивающую на каждом i-ом уровне требуемое значение $P^{\text{тр}}_{\text{цели}i}$ вероятности достижения цели $P_{\text{цели}i} \in R_i \subset R$ при ограничении $T^{\text{тр}}_{\text{вып}i}$ на максимально допустимое время выполнения программного цикла $T_{\text{вып}i} \in T_i \subset T$, в условиях компьютерных атак $A_i \subset A$, за счет варьирования значений управляемых параметров $D_i \subset D$:

$$M_3 :< L, F, A, D, R, T > \rightarrow < P_{\text{цели}i}, T_{\text{вып}i} > \Big| \begin{cases} \forall P_{\text{цели}i} \geq P^{\text{тр}}_{\text{цели}i}, P_{\text{цели}i} \in R_i \subset R \\ \forall T_{\text{вып}i} \leq T^{\text{тр}}_{\text{вып}i}, T_{\text{вып}i} \in T_i \subset T \end{cases}, i \in [1, N].$$

Во второй главе предложена модель киберустойчивой облачной платформы КИИ с самовосстановлением на основе теории подобия, позволяющая исследовать устойчивость ее функционирования в условиях компьютерных атак, направленных на нарушение целостности вычислений. Проведены теоретическое и экспериментальное исследования модели.

Частная научная задача разработки модели в формализованном виде выглядит следующим образом. Необходимо разработать модель M киберустойчивой облачной платформы КИИ L с самовосстановлением, устанавливающую на каждом i-ом уровне закономерность изменения показателей киберустойчивости $R_i \subset R$, а именно вероятности достижения цели $P_{\text{цели}i} \in R_i$, и временных показателей функционирования $T_i \subset T$, а именно полного времени выполнения программного цикла $T_{\text{вып}i} \in T_i$, от значений параметров интенсивности и повторяемости компьютерных атак $A_i \subset A$, представленных долей входных данных, являющихся вредоносными, $k_{\text{вред}i} \in A_i$ и долей известных вредоносных входных данных в общем их количестве $k_{\text{изв}i} \in A_i$, и значений управляемых параметров $D_i \subset D$, представленных коэффициентом покрытия вычислительных программ проверками подобия $k_{\text{покр}i} \in D_i$:

$$M :< L, F, I, O, V, A, D > \rightarrow\!\!\!\prec < R, T >,$$

при допустимых значения параметров: $\forall k_{\text{изв}i} \in A_i \subset A, k_{\text{изв}i} \in [0,1]$; $\forall k_{\text{покр}i} \in D_i \subset D, k_{\text{покр}i} \in [0,1]$; $\forall k_{\text{вред}i} \in A_i \subset A, k_{\text{вред}i} \in [0,1]$.

Для формализации модели введены дополнительные обозначения:

$f_i = \{k_i, m_i, n_i\}$, где k_i – количество линейных блоков программы i-го уровня; m_i – количество инструкций в линейном блоке; n_i – количество параметров в инструкции;

O_i – отображение проверки корректности (подобия) вычислений на i-ом уровне;

V_i – отображение синтеза восстанавливающего воздействия на i-ом уровне;

$P_{\text{мод}i}$ – вероятность модификации вычислительных структур (обнаруживаемой и необнаруживаемой) вследствие атак (известных и неизвестных) на i-ом уровне. Считается, что известные атаки приводят к обнаруживаемым нарушениям, а неизвестные – могут приводить как к обнаруживаемым, так и к необнаруживаемым нарушениям;

$P_{\text{обн}i}$ – вероятность обнаружения нарушений, вызванных известными и ранее неизвестными атаками на i-й уровень;

p_i – вероятность обнаружения нарушения, возникшего вследствие ранее неизвестной атаки на i-й уровень;

$P_{\text{прот}i}$ – вероятность успешного противодействия атакам на i-ом уровне;

$T_{\text{ср.атак}i}$ – среднее время между пропусками атак на i-ом уровне;

$N_{\text{проп.атак}i}$ – количество пропусков атак за $n_{\text{ц}}$ циклов вычислений на i-ом уровне;

$P_{\text{восст}i}$ – вероятность успешного восстановления после атаки на i-ом уровне;

$T_{\text{ср.восст}i}$ – среднее время восстановления после атаки на i-ом уровне;

$N_{\text{восст}i}$ – количество успешных восстановлений за $n_{\text{ц}}$ циклов вычислений на i-ом уровне;

$P_{\text{раб}i}$ – вероятность нахождения облачной платформы КИИ на i-ом уровне в работоспособном состоянии в произвольный момент времени;

$T_{\text{выч}i}$ – время непосредственно вычислений на i-ом уровне;

$t_{\text{обн}i}$ – время проверки вычислений на предмет наличия нарушений на i-ом уровне (время обнаружения нарушений) без учета $k_{\text{покр}i}$;

$T_{\text{обн}i}$ – время обнаружения нарушений на i-ом уровне с учетом $k_{\text{покр}i}$ ($T_{\text{обн}i} = k_{\text{покр}i} t_{\text{обн}i}$);

$T_{\text{восст}i}$ – время восстановления штатного функционирования i-го уровня;

t_0 – время выполнения элементарной операции (при расчетах $t_0 = 1$ ед. времени).

Сформулированы ряд допущений. Облачная платформа представляет собой многоуровневую иерархическую систему (по М. Месаровичу). Положено, что множество вычислительных программ на каждом i-ом уровне облачной платформы можно представить эквивалентной единственной программой f_i. Все программы функционируют циклически и обрабатывают входные данные последовательно в порядке их поступления. Нарушения возникают вследствие обработки вредоносных входных данных, при этом одновременное возникновение нескольких нарушений невозможно. Восстановление штатного функционирования возможно путем маскирования, возврата к предыдущему состоянию, вызова исключения, перезапуска или останова.

Введена система показателей киберустойчивости облачных платформ КИИ:

- вероятность успешного противодействия атакам, направленным на нарушение целостности облачных вычислений $P_{\text{прот}i}$:
$$P_{\text{прот}i} = 1 - P_{\text{моди}} k_{\text{вред}i} (1 - P_{\text{обн}i})(1 - k_{\text{покр}i} P_{\text{обн}i});$$
- среднее время между пропусками атак $T_{\text{ср.атак}i}$:
$$T_{\text{ср.атак}i} = n_{\text{ц}} (T_{\text{выч}i} + T_{\text{обн}i}) / N_{\text{проп.атак}i};$$
- вероятность успешного восстановления штатного функционирования $P_{\text{восст}i}$:
$$P_{\text{восст}i} = P_{\text{обн}i} P_{\text{восст|обн}i} = k_{\text{изв}i} 1 + (1 - k_{\text{изв}i}) p_i;$$
- среднее время восстановления после нарушения $T_{\text{ср.восст}i}$:
$$T_{\text{ср.восст}i} = n_{\text{ц}} T_{\text{восст}i} / N_{\text{восст}i};$$
- вероятность нахождения облачной платформы КИИ в работоспособном состоянии $P_{\text{раб}i}$, характеризующая вероятность того, что облачная платформа либо успешно противодействует атакам, либо к данному моменту восстановила функционирование:
$$P_{\text{раб}i} = T_{\text{ср.атак}i} / (T_{\text{ср.атак}i} + T_{\text{ср.восст}i});$$
- вероятность достижения цели $P_{\text{цели}i}$, характеризующая в совокупности способность облачной платформы успешно противодействовать атакам и восстанавливать штатное функционирование при возникновении нарушений:
$$P_{\text{цели}i} = P_{\text{цели}i-1} (P_{\text{прот}i} + (1 - P_{\text{прот}i}) P_{\text{восст}i}) P_{\text{раб}i}.$$

– полное время выполнения программного цикла $T_{\text{вып}i}$, включая вычисления, обнаружение нарушений и восстановление:

$$T_{\text{вып}i} = T_{\text{выч}i} + T_{\text{обн}i} + T_{\text{восст}i}.$$

Основными оцениваемыми показателями являются вероятность достижения цели $P_{\text{цели}i}$ и время выполнения программного цикла $T_{\text{вып}i}$.

Формирование модели штатного функционирования программы $M(ST,TR)$ осуществляется следующим образом. Множество линейных блоков программы B отображается в множество состояний ST так, что $\forall b_j \in B, st_j \in ST : st_j = \pi(b_j)$, где π – отображение формирования инварианта подобия. Состояние вычислительного процесса может быть описано матрицей соотношений размерностей операндов вычислительных инструкций линейного блока. Размерности операндов не зависят от обрабатываемых входных данных или реализации вычислительного процесса и являются его постоянной (инвариантной) характеристикой. Множество допустимых переходов между состояниями TR эквивалентно множеству связей по управлению T между линейными блоками.

Теория подобия позволяет представить вычислительный процесс в виде свертки состояний $st_1 \xrightarrow{tr_{12}} st_2 \xrightarrow{tr_{23}} \ldots \xrightarrow{tr_{i-1,i}} st_i$, каждое из которых описывается некоторым инвариантом. В соответствии с 1-й теоремой подобия Ньютона такие инварианты должны быть одинаковы для всех подобных процессов. Тогда для обнаружения нарушений необходимо осуществлять контроль целостности вычислений программы f_i, проверяя принадлежность ее состояния в текущем линейном блоке st_i модели $M_i(ST_i,TR_i)$. Состояние st_i корректно, если оно соответствует одному из допустимых состояний $st_i \in ST_i$ и существует такой переход $tr_{i-1,i} \in TR_i$ из предыдущего корректного состояния st_{i-1}, что $st_{i-1} \xrightarrow{tr_{i-1,i}} st_i$. Тогда отображение $O_i :< ST_i, M_i >\rightarrow \{0,1\}$ в функциональном виде можно записать как:

$$f_O(st_i, M_i) = \begin{cases} 1, \text{если } st_i \in ST_i \text{ и } \exists st_{i-1}, tr_{i-1,i} : st_i \xrightarrow{tr_{i-1,i}} st_{i-1} \\ 0, \text{иначе} \end{cases}.$$

Отличие текущего инварианта подобия st_i' от штатного, свидетельствует о нарушении целостности вычислений. В соответствии с 3-й теоремой подобия Кирпичева-Гухмана для подобия процессов необходимо равенство соответствующих инвариантов в контрольных точках. Отображение $V_i :< ST_i, M_i >\rightarrow TR_i$ представляет собой функцию $tr_{ij} = f_V(st_i', M_i)$, осуществляющую синтез перехода, переводящего вычислительный процесс в одно из корректных состояний, для которого выполняются условия подобия: предыдущее (st_{i-1}), начальное (st_0), конечное (st_{k_i}, останов), за время $T_{\text{восст}i} = 2k_i m_i n_i t_0$ (время выполнения операций чтения-записи памяти), тем самым восстанавливая штатное функционирование облачной платформы КИИ.

Множество I_i состоит из образцов обнаруженных вредоносных входных данных $x \in X_i^-$, обработка которых привела к нарушению, так, что $I_i \subseteq X_i^- \subset X_i$. В ходе последовательного накопления таких образцов происходит самообучение облачной платформы КИИ (формирование так называемого «приобретаемого кибериммунитета»).

В процессе функционирования облачной платформы КИИ в условиях атак осуществляется оценка текущих значений показателей $P_{\text{цели}i}$, $T_{\text{вып}i}$ и варьирование коэффициента покрытия программ проверками подобия $k_{\text{покр}i}$ для обеспечения требуемой киберустойчивости.

Проведено теоретическое исследование разработанной модели. Сформулированы и доказаны Утверждения 1-3 о полноте, непротиворечивости и разрешимости модели, подтверждающие ее адекватность и пригодность.

Сформулировано и доказано Утверждение 4, следующее из 1-й теоремы подобия Ньютона, о том, что вычислительный процесс f' корректен тогда и только тогда, когда для любой i-ой контрольной точки выполняется условие подобия $\pi(f_i') = \pi(f_i)$, где $\pi(f_i)$ – штатный инвариант подобия, $\pi(f_i')$ – фактический инвариант подобия.

Сформулировано и доказано Утверждение 5, следующее из 3-й теоремы подобия Кирпичева-Гухмана, о том, что если f' – вычислительный процесс с нарушением и $\exists i \in [1,k] : \pi(f_i'^*) \neq \pi(f_i)$, то штатное функционирование облачной платформы КИИ может быть восстановлено путем перевода вычислительного процесса в состояние f_j', для которого выполняется условие подобия $\pi(f_j') = \pi(f_j)$.

Также сформулированы и доказаны Утверждения 6-7 о том, что при одновременных атаках на k уровней общая вероятность достижения цели $P_{\text{цели}}$ снижается пропорционально k-ой степени вероятности $P_{\text{цели}i}$ на i-ом уровне – $P_{\text{цели}} \propto P_{\text{цели}i}^k$, а увеличение значения коэффициента покрытия программ проверками подобия $k_{\text{покр}i}$ повышает вероятность достижения цели $P_{\text{цели}i}$.

Проведено экспериментальное исследование зависимостей показателей киберустойчивости облачных платформ КИИ от параметров интенсивности и повторяемости атак ($k_{\text{вред}i}$, $k_{\text{изв}i}$) и коэффициента покрытия программ проверками подобия ($k_{\text{покр}i}$). При отсутствии самовосстановления ($k_{\text{покр}i} = 0$, $p_i = 0$) облачная платформа теряет устойчивость ($P_{\text{цели}} \to 0$). Увеличение же значения $k_{\text{покр}i}$ повышает киберустойчивость облачной платформы по всем введенным показателям и положительно влияет на ее способность достигать цели функционирования, однако при этом не всегда удается одновременно выполнить требования:

$$\begin{cases} P_{\text{цели}i} \geq P_{\text{цели}i}^{\text{тр}} \\ T_{\text{вып}i} \leq T_{\text{вып}i}^{\text{тр}} \end{cases}. \quad (1)$$

Результаты экспериментального исследования согласуются с теоретическими выводами. Сделан вывод о целесообразности выбора значения $k_{\text{покр}i}$, обеспечивающего выполнение требований (1), и о необходимости определения критерия существования решения.

Таким образом, разработанная модель облачной платформы КИИ впервые учитывает свойство самовосстановления, которое обеспечивается за счет обнаружения нарушений целостности и возврата вычислительных процессов в корректное состояние на основе теории подобия и размерностей независимо от конкретных сигнатур атак.

В третьей главе предложен метод обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением за счет варьирования коэффициента покрытия облачных вычислительных программ проверками подобия, позволяющий управлять устойчивостью их функционирования в зависимости от параметров интенсивности и повторяемости компьютерных атак. Проведены теоретическое и экспериментальное исследования метода.

Частная научная задача разработки метода в формализованном виде выглядит следующим образом. Необходимо разработать метод M обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением L, обеспечивающий на каждом i-ом уровне требуемое значение $P_{\text{цели}i}^{\text{тр}}$ вероятности достижения цели $P_{\text{цели}i} \in R_i \subset R$ при ограничении $T_{\text{вып}i}^{\text{тр}}$ на максимально допустимое время выполнения программного цикла $T_{\text{вып}i} \in T_i \subset T$, в условиях атак $A_i \subset A$, интенсивность которых характеризуется долей входных данных, являющихся вредоносными, $k_{\text{вред}i} \in A_i$, а повторяемость – долей известных вредоносных входных данных в общем их количестве $k_{\text{изв}i} \in A_i$, за счет варьирования значений управляемых параметров $D_i \subset D$, а именно коэффициента покрытия вычислительных программ проверками подобия $k_{\text{покр}i} \in D_i$:

$$M :< L, F, A, D, R, T >\rightarrow< P_{\text{цели}i}, T_{\text{вып}i} >\Big|$$
$$\begin{cases} \forall P_{\text{цели}i} \geq P_{\text{цели}i}^{\text{тр}}, P_{\text{цели}i} \in R_i \subset R \\ \forall T_{\text{вып}i} \leq T_{\text{вып}i}^{\text{тр}}, T_{\text{вып}i} \in T_i \subset T \end{cases}, i \in [1, N]'$$

при допустимых значениях параметров: $\forall k_{\text{вред}i} \in A_i \subset A, k_{\text{вред}i} \in [0,1]$, $\forall k_{\text{изв}i} \in A_i \subset A, k_{\text{изв}i} \in [0,1]$ и $\forall k_{\text{покр}i} \in D_i \subset D, k_{\text{покр}i} \in [0,1]$.

Сформулирована гипотеза о возможности обеспечения требуемой киберустойчивости облачных платформ КИИ на основе теории подобия.

Гипотеза 1. Требования к вероятности достижения цели $P_{\text{цели}i}$ и времени выполнения программного цикла $T_{\text{вып}i}$ на каждом i-ом уровне облачной платформы КИИ могут быть одновременно обеспечены за счет варьирования коэффициента покрытия вычислительных программ проверками подобия $k_{\text{покр}i}$ в пределах его необходимого и достаточного значений.

Для формализации метода введены дополнительные обозначения:

$k_{\text{покр}i}^{\text{необх}}$ – необходимое (минимальное) значение коэффициента $k_{\text{покр}i}$ i-го уровня, с учетом требуемой вероятности достижения цели $P_{\text{цели}i} \geq P_{\text{цели}i}^{\text{тр}}$, $k_{\text{покр}i}^{\text{необх}} \in [0,1]$;

$k_{\text{покр}i}^{\text{дост}}$ – достаточное (максимальное) значение коэффициента $k_{\text{покр}i}$ i-го уровня, с учетом требуемого времени выполнения программ $T_{\text{вып}i} \leq T_{\text{вып}i}^{\text{тр}}$, $k_{\text{покр}i}^{\text{дост}} \in [0,1]$;

a_i – левая граница поиска значения $k_{\text{покр}i}^{\text{необх}}$ i-го уровня, $a_i \in [0,1]$;

b_i – правая граница поиска значения $k_{\text{покр}i}^{\text{необх}}$ i-го уровня, $b_i \in [0,1]$;

ε_i – требуемая точность поиска значения $k_{\text{покр}i}^{\text{необх}}$ i-го уровня;

w_i – коэффициент «необходимость-достаточность» i-го уровня, $w_i \in [0,1]$.

Входные данные метода:

- вычислительный процесс облачной платформы КИИ в условиях компьютерных атак;
- инварианты подобия для штатного режима функционирования программы;
- требования $P_{\text{цели}i}^{\text{тр}}$, $T_{\text{вып}i}^{\text{тр}}$.

Выходные данные метода: корректный вычислительный процесс после восстановления штатного функционирования.

Схема работы метода представлена на рисунке 1.

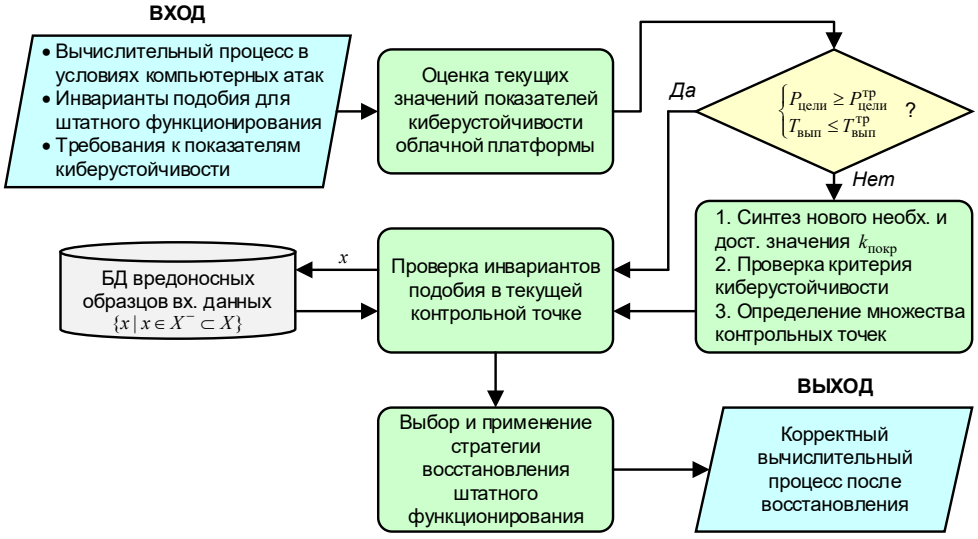


Рисунок 1 – Схема метода обеспечения киберустойчивости облачных платформ КИИ

Во время функционирования облачной платформы КИИ с самовосстановлением в условиях атак на каждом i-ом уровне осуществляется оценка текущих значений показателей

киберустойчивости $P_{\text{цели}i}$, $T_{\text{вып}i}$ и сравнение их с требуемыми значениями $P_{\text{цели}i}^{\text{тр}}$ и $T_{\text{вып}i}^{\text{тр}}$ соответственно. Если не выполняется условие (1), то осуществляется поиск нового значения $k_{\text{покр}i}$ и переконфигурация системы обнаружения нарушений с учетом этого значения.

Сделано предположение о существовании такого необходимого $k_{\text{покр}i}^{\text{необх}}$ и достаточного $k_{\text{покр}i}^{\text{дост}}$ значений коэффициента $k_{\text{покр}i}$, что для любого $k_{\text{покр}i} \in [k_{\text{покр}i}^{\text{необх}}, k_{\text{покр}i}^{\text{дост}}]$ выполняется условие (1).

Достаточное значение $k_{\text{покр}i}^{\text{дост}}$ можно вычислить аналитически, приняв $t_{\text{обн}i} = k_i m_i n_i t_0$:

$$k_{\text{покр}i}^{\text{дост}} = \min\left(1, \max\left(0, \frac{T_{\text{вып}i}^{\text{тр}} - 3k_i m_i n_i t_0}{k_i m_i n_i t_0}\right)\right). \quad (2)$$

Аналитическое вычисление необходимого значения $k_{\text{покр}i}^{\text{необх}}$ затруднительно, поэтому для его нахождения применен модифицированный численный метод бисекции. Данный метод при наличии решения позволяет находить его в заданном промежутке $k_{\text{покр}i} \in [a_i, b_i]$ с требуемой точностью ε_i за конечное число шагов. Кроме того, он не требует вычисления производных и обладает относительно низкой вычислительной сложностью. Модификация состоит во введении шага с проверкой выхода текущего приближения за границы допустимых значений $[0, k_{\text{покр}i}^{\text{дост}}]$.

Модифицированный метод бисекции для поиска $k_{\text{покр}i}^{\text{необх}}$ выглядит следующим образом.

Вход: исследуемая функция $f(k_{\text{покр}i}) = P_{\text{цели}i}(k_{\text{покр}i}) - P_{\text{цели}i}^{\text{тр}} = 0$.

Выход: необходимое значение коэффициента $k_{\text{покр}i}^{\text{необх}}$.

Шаг 1. Инициализация

Выбираются границы поиска ($a_i^0 = 0$ и $b_i^0 = 1$), вычисляется начальное приближение: $k_{\text{покр}i}^0 = (a_i^0 + b_i^0)/2$. Если $f(a_i^0) f(b_i^0) < 0$, то следует перейти шагу 2, иначе решений нет.

Шаг 2. j-ая итерация поиска

Из двух отрезков $[a_i^{j-1}, k_{\text{покр}i}^{j-1}]$ и $[k_{\text{покр}i}^{j-1}, b_i^{j-1}]$ в качестве нового отрезка поиска $[a_i^j, b_i^j]$ выбирается тот, на границах которого исследуемая функция принимает значения разных знаков, и вычисляется *j*-ое приближение $k_{\text{покр}i}^j = (a_i^j + b_i^j)/2$.

Шаг 3. Проверка выхода за границы допустимых значения

Если $k_{\text{покр}i}^{\text{дост}} < a_i^j$, то все значения в отрезке $[a_i^j, b_i^j]$, включая искомое $k_{\text{покр}i}^{\text{необх}}$, превышают $k_{\text{покр}i}^{\text{дост}}$, а значит, решений нет. Иначе необходимо продолжить поиск, перейдя к шагу 4.

Шаг 4. Проверка достижения требуемой точности решения

Выполняется проверка критерия $\left|k_{\text{покр}i}^j - k_{\text{покр}i}^{j-1}\right| \le \varepsilon_i$. Если требуемая точность не достигнута, необходимо продолжить поиск, перейдя к шагу 2, иначе – решение найдено $k_{\text{покр}i}^{\text{необх}} = k_{\text{покр}i}^j$.

После нахождения необходимого $k_{\text{покр}i}^{\text{необх}}$ и достаточного $k_{\text{покр}i}^{\text{дост}}$ значений коэффициента покрытия программ проверками подобия новое значение $k_{\text{покр}i}$ вычисляется с помощью взвешенной суммы:

$$k_{\text{покр}i} = (1 - w_i) k_{\text{покр}i}^{\text{необх}} + w_i k_{\text{покр}i}^{\text{дост}}. \quad (3)$$

Здесь $w_i = 0$ обеспечивает минимальное время $T_{\text{вып}i}$ при минимально допустимой вероятности $P_{\text{цели}i}$, а $w_i = 1$ – максимальную вероятность $P_{\text{цели}i}$ при максимально допустимом времени $T_{\text{вып}i}$.

Далее выполняется определение множества линейных блоков программ, в которых осуществляется контроль целостности вычислений с учетом $k_{\text{покр}i}$. В контрольных точках вычислительного процесса, определяемых множеством контролируемых линейных блоков, выполняется сравнение текущего и штатного инвариантов подобия. При обнаружении нарушения вредоносные входные данные $x \in X^-$ сохраняются в базе данных и более не допускаются.

Восстановление штатного функционирования осуществляется путем перевода вычислительного процесса в состояние, в котором выполняется условие подобия, в соответствии с одной из стратегий: маскирование (замена результата вычислений нейтральным значением,

например, 0, и продолжение выполнения); возврат к предыдущей контрольной точке; вызов исключения (переход в штатный режим обработки ошибок); перезапуск; останов.

Проведено теоретическое исследование метода. Сформулировано и доказано Утверждение 8 о сходимости поиска необходимого значения коэффициента покрытия $k_{\text{покр}i}^{\text{необх}}$ с требуемой точностью ε_i за $N_i = \left\lceil \log_2(10^{\lfloor \log_{10}(k_i) \rfloor + 1}) \right\rceil$ шагов. Сформулировано и доказано Утверждение 9 – критерий устойчивости облачных платформ КИИ, в соответствии с которым одновременное выполнение требований (1) возможно тогда и только тогда, когда:

$$\exists k_{\text{покр}i}^{*} : \begin{cases} P_{\text{цели}i}(k_{\text{покр}i}^{*}) \geq P_{\text{цели}i}^{\text{тр}} \\ T_{\text{вып}i}(k_{\text{покр}i}^{*}) \leq T_{\text{вып}i}^{\text{тр}} \end{cases} \Leftrightarrow 0 \leq k_{\text{покр}i}^{\text{необх}} \leq k_{\text{покр}i}^{\text{дост}} \leq 1 . \quad (4)$$

Проведено экспериментальное исследование зависимостей $k_{\text{покр}i}^{\text{необх}}$ и $k_{\text{покр}i}^{\text{дост}}$ от значений параметров интенсивности и повторяемости атак и требований к показателям киберустойчивости облачных платформ КИИ. Установлено, что при увеличении доли вредоносных входных данных $k_{\text{вред}i}$ увеличивается значение $k_{\text{покр}i}^{\text{необх}}$, необходимое для обеспечения требования $P_{\text{цели}i} \geq P_{\text{цели}i}^{\text{тр}}$, а при увеличении структурной сложности программы, определяемой параметрами k_i, m_i, n_i, уменьшается значение $k_{\text{покр}i}^{\text{дост}}$, максимально допустимое для обеспечения требования $T_{\text{вып}i} \leq T_{\text{вып}i}^{\text{тр}}$. Результаты исследования возможностей обеспечения киберустойчивости облачных платформ КИИ с использованием разработанного метода представлены на рисунке 2.

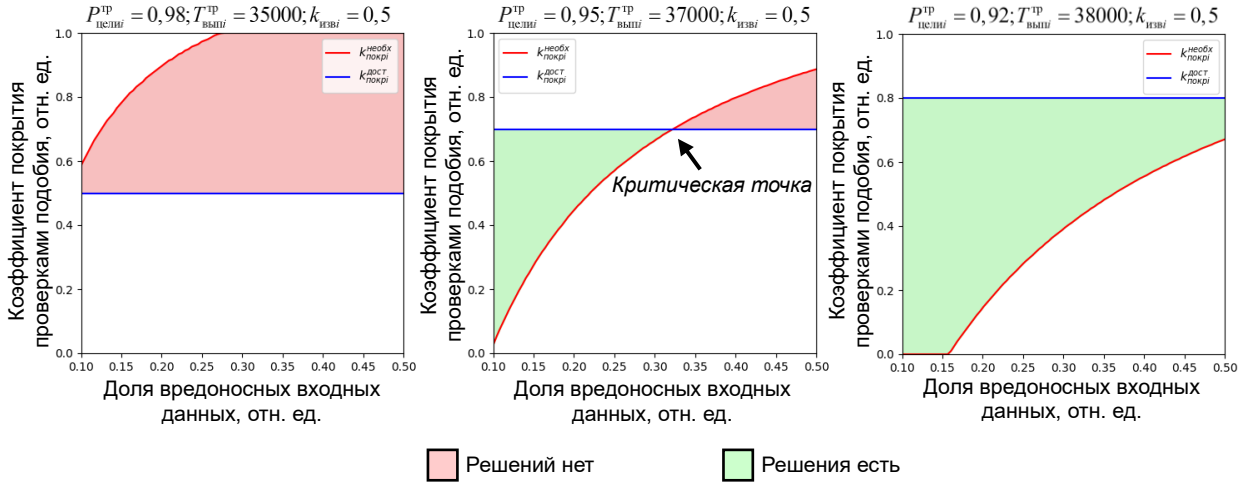


Рисунок 2 – Результаты исследования возможностей обеспечения киберустойчивости облачных платформ КИИ

На графике слева $k_{\text{покр}i}^{\text{необх}} > k_{\text{покр}i}^{\text{дост}}$ при любых значениях $k_{\text{вред}i}$, поэтому в заданных условиях решение отсутствует. На графике по центру существует критическое значение $k_{\text{вред}i}^{*}$, такое, что при $k_{\text{вред}i} \leq k_{\text{вред}i}^{*}$ искомое значение $k_{\text{покр}i}$, в соответствии с критерием (4), лежит в отрезке $[k_{\text{покр}i}^{\text{необх}}, k_{\text{покр}i}^{\text{дост}}]$, а при $k_{\text{вред}i} > k_{\text{вред}i}^{*}$ – решений нет. На графике справа $k_{\text{покр}i}^{\text{необх}} < k_{\text{покр}i}^{\text{дост}}$ при любом значении $k_{\text{вред}i}$ и, в соответствии с критерием (4), решение лежит в отрезке $[k_{\text{покр}i}^{\text{необх}}, k_{\text{покр}i}^{\text{дост}}]$.

Сделан вывод, что для формирования модели штатного функционирования программы и последующего контроля целостности вычислений целесообразно применять математический аппарат, обеспечивающий наибольшую вероятность обнаружения нарушений $P_{\text{обн}i}$ при наименьших дополнительных вычислительных затратах на контроль $t_{\text{обн}i}$.

Результаты проведенных экспериментальных исследований согласуются с теоретическими выводами и подтверждают сформулированную в главе Гипотезу 1.

В четвертой главе проведена оценка применимости существующих технологий защиты и обоснована целесообразность использования теории размерностей для синтеза моделей штатного функционирования вычислительных программ. Разработана методика обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей, позволяющая наделять их способностью обнаруживать известные и новые, ранее неизвестные атаки, направленные на нарушение целостности вычислений, восстанавливать штатное функционирование и самообучаться. Проведены теоретическое и экспериментальное исследования методики.

Частная научная задача разработки методики в формализованном виде выглядит следующим образом. Необходимо разработать методику M обеспечения требуемой киберустойчивости облачных платформ КИИ L с использованием теории подобия и размерностей, обеспечивающую на каждом i-ом уровне требуемое значение $P^{\text{тр}}_{\text{цели}i}$ вероятности достижения цели $P_{\text{цели}i} \in R_i \subset R$ при ограничении $T^{\text{тр}}_{\text{вып}i}$ на максимально допустимое время выполнения программного цикла $T_{\text{вып}i} \in T_i \subset T$, в условиях атак $A_i \subset A$, интенсивность которых характеризуется долей входных данных, являющихся вредоносными, $k_{\text{вред}i} \in A_i$, а повторяемость – долей известных вредоносных входных данных в общем их количестве $k_{\text{изв}i} \in A_i$, за счет варьирования значений управляемых параметров $D_i \subset D$, а именно коэффициента покрытия вычислительных программ проверками подобия $k_{\text{покр}i} \in D_i$:

$$M :\prec L, F, A, D, R, T \succ\rightarrow\prec P_{\text{цели}i}, T_{\text{вып}i} \succ \Big| \begin{cases} \forall P_{\text{цели}i} \geq P^{\text{тр}}_{\text{цели}i}, P_{\text{цели}i} \in R_i \subset R \\ \forall T_{\text{вып}i} \leq T^{\text{тр}}_{\text{вып}i}, T_{\text{вып}i} \in T_i \subset T \end{cases}, i \in [1, N],$$

при $t_{\text{обн}i}$, $P_{\text{мод}i}$ и p_i, определяемых с использованием математического аппарата теории подобия и размерностей, и допустимых значениях параметров: $\forall k_{\text{вред}i} \in A_i \subset A, k_{\text{вред}i} \in [0,1]$, $\forall k_{\text{изв}i} \in A_i \subset A, k_{\text{изв}i} \in [0,1]$, $\forall k_{\text{покр}i} \in D_i \subset D, k_{\text{покр}i} \in [0,1]$.

Сформулирована гипотеза о возможности обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей.

Гипотеза 2. Требуемая киберустойчивость облачной платформы КИИ по показателю вероятности достижения цели $P_{\text{цели}}$ при ограничении на время выполнения программного цикла $T_{\text{вып}}$ может быть обеспечена с использованием теории подобия и размерностей.

Проведен анализ существующих технологий защиты (стековые «канарейки», предотвращение выполнения данных, контроль целостности потока управления, контроль целостности кода в памяти). Установлено, что они эффективны лишь для некоторого подмножества вредоносных входных данных, не позволяют одновременно противодействовать нарушениям состояний и переходов и не позволяют восстанавливать штатное функционирование.

Для синтеза моделей штатного функционирования программ предложено применять аппарат теории размерностей, позволяющий учитывать информационные и управляющие связи между объектами программ и обнаруживать нарушения целостности вычислений с использованием соотношений размерностей операндов вычислительных инструкций в линейных блоках, инвариантных по отношению к различным реализациям программ.

Общая идея предложенной методики заключается в следующем. Необходимо внедрить в линейные блоки исходной программы облачной платформы КИИ специальные метки для контроля маршрутов выполнения, сформировать модель ее штатного функционирования в терминах размерностей, а также определить наиболее критичные линейные блоки, подлежащие контролю. Во время выполнения программы необходимо осуществлять контроль целостности вычислений для подмножества наиболее критичных линейных блоков и оценивать текущие

значения показателей киберустойчивости облачной платформы КИИ. Для управления подмножеством контролируемых линейных блоков с учетом требований к показателям киберустойчивости предлагается использовать необходимое и достаточное значение коэффициента покрытия программ проверками подобия $k_{\text{покр}i}$. При обнаружении нарушений необходимо выполнять возврат программы в устойчивое состояние и сохранять вредоносные входные данные для предотвращения их повторной обработки.

Этап 1. Трансляция с внедрением структурно-функциональной избыточности

Вход: вычислительная программа в виде управляющего графа $\Gamma(B,D)$.

Выход:

- программа с внедренными элементами избыточности;
- модель штатного функционирования программы $M(ST,TR)$;
- ранжированный по убыванию критичности перечень линейных блоков B'.

Шаг 1.1. Каждый из k_i линейных блоков $b_j \in B$ представляется последовательностью m_i арифметических выражений, $b_j = \{b_{j1},...,b_{jm_i}\}$. Каждое арифметическое выражение имеет n_i операндов и представляется деревом разбора, которое в функциональном виде можно записать в виде свертки бинарных операторов $b_{jl} = f_{jl1}(x_{jl1}, f_{jl2}(x_{jl2},...f_{jl,n_i-1}(x_{jl,n_i-1}, x_{jl,n_i})...))$, где f_{jlr} – бинарный оператор из множества $\{+,-,*,/,=\}$.

Шаг 1.2. Выполняется обход дерева разбора линейного блока слева направо, где в каждом узле формируются соотношения абстрактных размерностей операндов с учетом поддеревьев. Совокупность полученных соотношений размерностей приводится к виду системы линейных уравнений, которая путем логарифмирования приводится к виду матрицы st_j, описывающей состояние линейного блока. Совокупность матриц размерностей и переходов между ними составляет модель штатного функционирования программы $M(ST,TR)$.

Шаг 1.3. В линейные блоки программы b_j вносятся метки (контрольные точки) – $b_j = (KT_j^{\text{нач}}, b_{j1},...,b_{jm_i}, KT_j^{\text{кон}})$, где $KT_j^{\text{нач}}$ и $KT_j^{\text{кон}}$ – метки начала и конца линейного блока b_j.

Шаг 1.4. Линейные блоки программы B ранжируется по убыванию критичности нарушений $B' = \{b_1,...,b_{j-1},b_j,...,b_{k_i}\}$, где критичность нарушения в b_{j-1} выше, чем в b_j.

Этап 2. Обнаружение нарушений целостности вычислений, переконфигурация, обеспечение требуемой киберустойчивости

Вход:

- требования к показателям киберустойчивости $P_{\text{цели}i}^{\text{тр}}$ и $T_{\text{вып}i}^{\text{тр}}$;
- ранжированный по степени критичности перечень линейных блоков B';
- модель штатного функционирования программы $M(ST,TR)$.

Выход: вывод о наличии нарушений и необходимости восстановления.

Шаг 2.1. Выполняется оценка текущих значений $P_{\text{цели}i}$ и $T_{\text{вып}i}$. Если $P_{\text{цели}i} < P_{\text{цели}i}^{\text{тр}}$ или $T_{\text{вып}i} > T_{\text{вып}i}^{\text{тр}}$ осуществляется поиск нового значения коэффициента $k_{\text{покр}i}$.

Шаг 2.2. Выполняется поиск $k_{\text{покр}i}^{\text{необх}}$ и $k_{\text{покр}i}^{\text{дост}}$. Существование решения проверяется в соответствии с критерием (4). При наличии решения выбирается новое необходимое и достаточное значение $k_{\text{покр}i}$ в соответствии с (3).

Шаг 2.3. Из B' выбираются первые $l = \lceil k_{\text{покр}i} k_i \rceil$ линейных блоков и формируется подмножество контролируемых линейных блоков $B^* = \{b_1^*,...,b_l^*\}$, для которых осуществляется динамический контроль целостности вычислений в терминах размерностей.

Шаг 2.4. В текущем линейном блоке b_j вычисляется фактическая матрица (инвариант) размерностей st_j', которая проверяется на предмет соответствия модели $M(ST,TR)$. При обнаружении нарушения принимается решение о восстановлении.

Этап 3. Восстановление штатного функционирования

Вход:

- текущее состояние программы st'_j с нарушением;
- образец вредоносных входных данных $x' \in X_i^-$.

Выход: корректное состояние программы.

Шаг 3.1. Для текущего некорректного состояния программы st'_j осуществляется синтез восстанавливающего воздействия tr_{jl} (возврат к предыдущему состоянию, перезапуск, останов), такого, что, $st'_j \xrightarrow{tr_{jl}} st_l$, $st_l \in M(ST,TR)$. Новое состояние st_l характеризуется равенством штатного и фактического инвариантов размерностей, что по 3-й теореме подобия Кирпичева-Гухмана говорит о корректности восстановленного вычислительного процесса.

Шаг 3.2. Вредоносные входные данные $x' \in X_i^-$ сохраняются и более не принимаются.

Проведена оценка времени обнаружения нарушений (формирования и контроля матриц инвариантов размерностей) $t_{\text{обн}i}$, по результатам которой формула (2) была уточнена:

$$k_{\text{покр}i}^{\text{дост}} = \min\left(1, \max\left(0, \frac{T_{\text{вып}i}^{\text{тр}} - 3k_i m_i n_i t_0}{\left(k_i \frac{m_i(m_i-1)}{2}(2n_i-1) + k_i m_i n_i\right) t_0}\right)\right).$$

Проведено теоретическое исследование методики. Сформулировано и доказано Утверждение 10 о том, что вероятность модификации вычислительного оператора вследствие атаки составляет $P_{\text{моди}} = 0,75$, а также Утверждение 11 о том, что вероятность обнаружения модификаций вычислительных операторов, возникших вследствие ранее неизвестных атак, при применении теории подобия и размерностей составляет $p_i = 0,875$. Результаты теоретического исследования свидетельствуют о наличии возможности противодействия как известным, так и ранее неизвестным атакам, направленным на нарушение целостности вычислений, и обеспечения требуемой киберустойчивости облачных платформ КИИ.

Проведено экспериментальное исследование возможностей обеспечения требуемой киберустойчивости облачной платформы КИИ при одновременных атаках на $N = 4$ уровней в соответствии с критерием (4). Для заданных требований $P_{\text{цели}}^{\text{тр}} = 0,995$, $T_{\text{вып}}^{\text{тр}} = 60000$ наибольший эффект от применения методики среди рассмотренных случаев наблюдался при $k_{\text{изв}i} = 0,5$ и $k_{\text{вред}i} = 0,1$. Результаты исследования для данного случая приведены в таблице 1.

Таблица 1 – Результаты применения методики

	Без защиты	С защитой	Прирост
$P_{\text{цели}i}$	0,8533	до 0,9992	до 17,10%
$T_{\text{вып}i}$ ($T_{\text{вып}}$)	30000	до 60000	до 2-х раз
$P_{\text{цели}}$	0,5301	до 0,9967	до 88,02%
Полнота обнаружения атак	0,9625	до 0,9986	до 3,75%
Точность обнаружения атак	1,0	до 1,0	–

Результаты проведенного экспериментального исследования методики согласуются с теоретическими выводами и подтверждают сформулированную в главе Гипотезу 2.

В пятой главе предложена архитектура и разработан прототип программного комплекса обеспечения киберустойчивости облачных платформ КИИ в условиях роста угроз безопасности информации.

В архитектуру программного комплекса (рисунок 3) входят следующие основные компоненты: среда разработки и среда выполнения облачных сервисов; подсистема управления

киберустойчивостью; подсистема обнаружения нарушений и восстановления штатного функционирования.

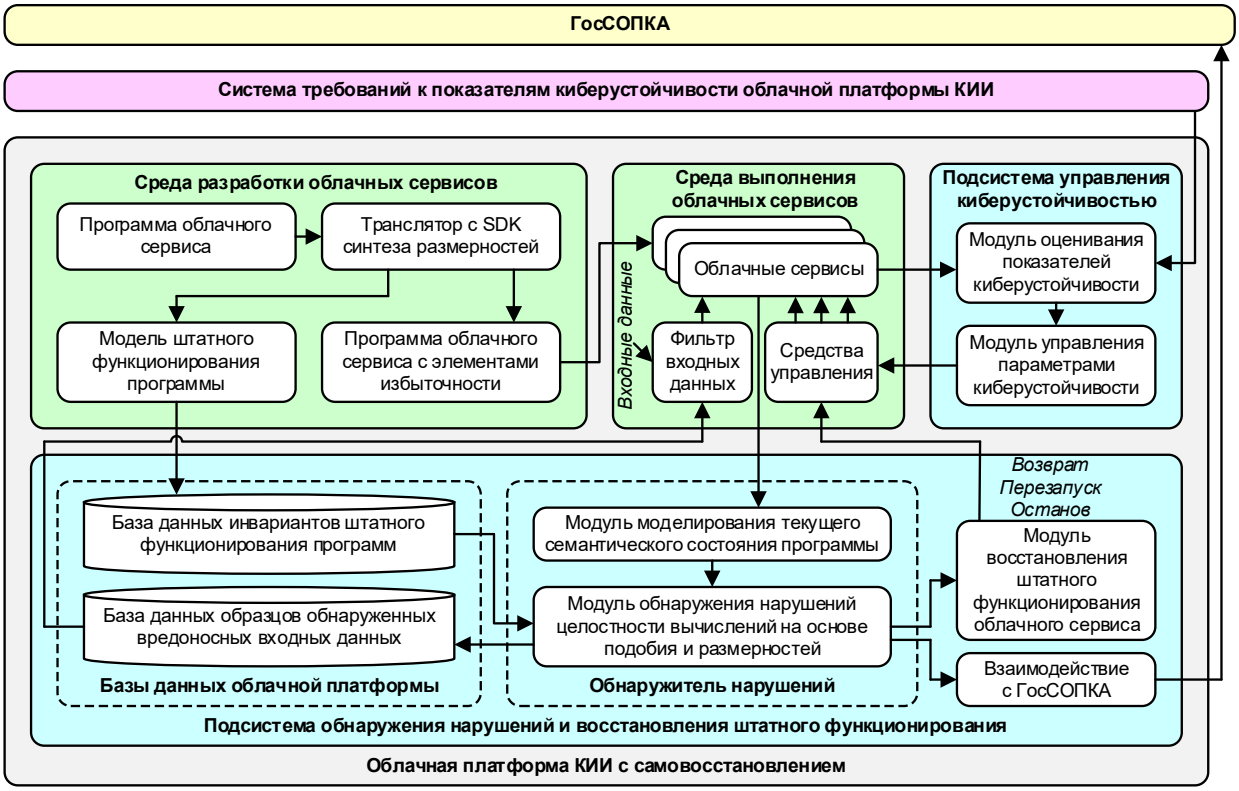


Рисунок 3 – Архитектура программного комплекса обеспечения киберустойчивости облачных платформ КИИ

Предложенная архитектура доведена до прототипа программного комплекса, сформулированы научно-обоснованные рекомендации по его внедрению и эксплуатации на уровне гипервизоров и сред виртуализации, ОС, контейнерных сред, а также прикладных сервисов облачных платформ КИИ. Проведено испытание прототипа на стенде, результаты которого представлены в таблице 2.

Таблица 2 – Результаты испытания до и после применения прототипа программного комплекса

	Входных данных	Из них вредоносных	Коэфф. $k_{\text{покр}}$	Нарушений предотвращено	Перехватов управления	Аварийных завершений
До применения	1000	300	–	0	238	62
После применения	1000	300	0,73	207	34	59

По результатам испытаний продемонстрирована практическая возможность обнаружения нарушений целостности вычислений с использованием инвариантов подобия и размерностей, самовосстановления и самообучения на основе разработанных модели, метода и методики, что подтверждает практическую значимость результатов диссертационного исследования.

В заключении подведены итоги диссертационного исследования, сделаны выводы о достижении цели, сформулированы направления дальнейших исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационном исследовании с целью обеспечения киберустойчивости облачных платформ КИИ в условиях компьютерных атак, направленных на нарушение целостности вычислений, поставлена научная задача организации самовосстанавливающихся вычислительных процессов облачных платформ КИИ на основе теории подобия и размерностей. В процессе исследования выполнена декомпозиция научной задачи на совокупность частных научных и прикладных задач, итогом решения которых являются защищаемые положения, соответствующие частным научным результатам, обладающим научной новизной, теоретической и практической значимостью и являющимся вкладом в развитие соответствующей теоретической формы знаний:

1) модель киберустойчивой облачной платформы КИИ с самовосстановлением на основе теории подобия [1, 2, 3, 9, 11, 16-18];
2) метод обеспечения киберустойчивости облачных платформ КИИ с самовосстановлением за счет варьирования коэффициента покрытия облачных вычислительных программ проверками подобия [4, 5, 19-22];
3) методика обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием теории подобия и размерностей [6, 12, 23, 24];

а также частному прикладному результату, обладающему технической новизной, практической значимостью и являющемуся вкладом в практику технических наук:

4) архитектура программного комплекса обеспечения киберустойчивости облачных платформ КИИ в условиях роста угроз безопасности информации [11-15].

К основным итоговым выводам по результатам диссертационного исследования относится следующее.

1) Анализ исследований в предметной области, диссертационных работ и прикладных решений показал, что они не в полной мере учитывают особенности облачных платформ КИИ, а именно, их многоуровневую иерархическую структуру, функционирование в условиях атак, направленных на нарушение целостности вычислений, повышенные требования к киберустойчивости и необходимость оперативного восстановления штатного функционирования при возникновении нарушений. Известные прикладные решения зачастую не обладают способностью к адаптации, самообучению и оказываются неэффективными в условиях ранее неизвестных атак. Это приводит к невозможности обеспечения требуемой киберустойчивости облачных платформ КИИ с использованием существующих технических и технологических решений, а также невозможности разработки таких научно-обоснованных решений ввиду недостаточности существующего научно-методического аппарата.

2) Для решения общей научной задачи диссертации решены частные задачи разработки модели, метода, методики и архитектуры программного комплекса обеспечения киберустойчивости облачных платформ КИИ. При этом:

- модель киберустойчивой облачной платформы КИИ учитывает свойство самовосстановления, которое обеспечивается за счет обнаружения нарушений целостности вычислений на основе инвариантов подобия и возврата вычислительных процессов в корректное состояние, удовлетворяющее условиям 3-й теоремы подобия Кирпичева-Гухмана. Применение моделей штатного функционирования программ позволяет выявлять нарушения целостности облачных вычислений независимо от конкретных сигнатур атак и вредоносных входных данных, что позволяет противодействовать как известным, так и ранее неизвестным компьютерным атакам;

- разработанный метод направлен на обеспечение киберустойчивости облачных платформ КИИ за счет варьирования доли линейных блоков облачных вычислительных программ, в которых осуществляется контроль целостности вычислений, что позволяет обнаруживать нарушения и восстанавливать штатное функционирование облачных платформ КИИ на основе теории подобия. Для определения возможности обеспечения требуемой киберустойчивости облачных платформ КИИ сформулирован и доказан соответствующий критерий;
- методика обеспечения требуемой киберустойчивости облачных платформ КИИ позволяет внедрять в облачные вычислительные программы элементы избыточности и формировать модели их штатного функционирования в терминах размерностей. Это в свою очередь позволяет обнаруживать нарушения в подмножестве контролируемых линейных блоков, определяемом с учетом коэффициента покрытия программ проверками подобия и требуемых показателей киберустойчивости, а также восстанавливать штатное функционирование облачных платформ КИИ путем возврата вычислительных программ в состояние, удовлетворяющее условиям подобия;
- архитектура программного комплекса включает такие основные компоненты, как среда разработки и среда выполнения облачных сервисов, подсистема управления киберустойчивостью, подсистема обнаружения нарушений и восстановления штатного функционирования. Для внедрения и эксплуатации программного комплекса на различных уровнях облачных платформ КИИ сформулированы соответствующие научно-обоснованные рекомендации.

3) Постановка частных научных задач сопровождалась формулированием гипотез (Гипотезы 1-2), которые были подтверждены теоретически, путем доказательства соответствующих утверждений (Утверждения 1-11), и экспериментально.

4) Исследование киберустойчивости облачных платформ КИИ в условиях атак, направленных на нарушение целостности вычислений, с учетом требований ($P_{\text{цели}}^{\text{тр}} = 0,995$, $T_{\text{вып}}^{\text{тр}} = 60000$) показало, что применение разработанных метода и методики обеспечивает прирост:

- до 17,10% по показателю вероятности достижения цели на *i*-ом уровне;
- до 88,02% по показателю общей вероятности достижения цели;
- до 3,75% по показателю полноты обнаружения и противодействия атакам.

5) Предложенная архитектура доведена до прототипа программного комплекса, по результатам испытания которого показана практическая возможность обнаружения нарушений целостности вычислений, восстановления штатного функционирования программ и самообучения на основе разработанных модели, метода и методики.

Таким образом, **все поставленные задачи диссертационного исследования выполнены, а цель исследования – достигнута**.

Полученные результаты могут быть использованы университетами, научно-исследовательскими институтами, центрами и подразделениями организаций, ведущими научное сопровождение работ по созданию облачных, киберфизических и иных систем, относящихся к КИИ, и других. Например, такими организациями, как: АНО ВО «Университет Иннополис», АНОО ВО «Университет «Сириус», ФГАОУ ВО «СПбГЭТУ «ЛЭТИ», ФГАОУ ВО «СПбПУ», ФГАОУ ВО «НИЯУ «МИФИ», СПб ФИЦ РАН, ИСП РАН, АО «Лаборатория Касперского», АО «НПО «Эшелон», ООО «СТЦ», АО «Технологии радиоконтроля» и другими.

К направлениям дальнейших исследований можно отнести следующее.

1) Исследование возможностей применения денотационных, аксиоматических и операционных семантик для формирования моделей штатного функционирования программ.

2) Исследование возможностей интеллектуального управления параметрами модели облачной платформы КИИ для обеспечения требуемой ее киберустойчивости с использованием методов искусственного интеллекта и машинного обучения.

3) Исследование возможностей применения полученных результатов для обеспечения безопасности и устойчивости блокчейн-платформ, платформ квантовых вычислений и иных ИВС в условиях новой угрозы осуществления гибридных квантово-классических атак.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ АВТОРОМ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в изданиях из перечня ВАК РФ:

1. **Балябин, А.А.** Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий / А.А. Балябин // Защита информации. Инсайд. – 2024. – № 5(119). – С. 35–44.

2. **Балябин, А.А.** Модель облачной платформы критической информационной инфраструктуры с кибериммунитетом / А.А. Балябин, С.А. Петренко // Информатика и автоматизация. – 2025. – Т. 24. – № 5. – С. 1471–1505. – DOI: 10.15622/ia.24.5.8.

3. **Балябин, А.А.** Модель облачной платформы управления киберфизическими объектами с кибериммунитетом / А.А. Балябин, С.А. Петренко // Защита информации. Инсайд. – 2025. – № 5(125). – С. 32–43.

4. **Балябин, А.А.** Метод защиты облачных платформ критической информационной инфраструктуры на основе кибериммунитета / А.А. Балябин // Прикладная информатика. – 2025. – Т. 20. – № 5(119). – С. 121–143. – DOI: 10.37791/2687-0649-2025-20-5-121-143.

5. **Балябин, А.А.** Метод обеспечения киберустойчивости платформ управления киберфизическими объектами на основе кибериммунитета / А.А. Балябин, С.А. Петренко // Защита информации. Инсайд. – 2025. – № 6(126). – С. 21–29.

6. **Балябин, А.А.** Методика синтеза квантово-устойчивых блокчейн-платформ с кибериммунитетом / А.А. Балябин, С.А. Петренко // Вопросы кибербезопасности. – 2025. – № 4(68). – С. 46–54. – DOI: 10.21681/2311-3456-2025-4-46-54.

7. **Балябин, А.А.** Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ / А.А. Балябин, С.А. Петренко, А.Д. Костюков // Защита информации. Инсайд. – 2024. – № 5(119). – С. 26–34.

8. **Балябин, А.А.** О создании киберустойчивых облачных платформ управления киберфизическими объектами в условиях роста угроз безопасности / А.А. Балябин, С.А. Петренко // Защита информации. Инсайд. – 2025. – № 4(124). – С. 20–30.

Публикации из перечня Scopus и Web of Science:

9. **Balyabin, A.A.** Ensuring the Resilience of Cloud Platforms Based on Cyber Immunity / A.A. Balyabin // 2024 XXVII International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian Federation. – IEEE, 2024. – P. 233–237. – DOI: 10.1109/SCM62608.2024.10554277.

10. **Balyabin, A.A.** Threats to the Resilience of Cloud Platforms / A.A. Balyabin // 2024 XXVII International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russian Federation. – IEEE, 2024. – P. 246–249. – DOI: 10.1109/SCM62608.2024.10554080.

Свидетельства о государственной регистрации программ для ЭВМ:

11. Свидетельство о государственной регистрации программы для ЭВМ № 2024682616 Российская Федерация. Набор инструментов разработки (SDK) для обнаружения и устранения уязвимости универсальной машины Тьюринга CVE-2021-32471 на основе инвариантов подобия и размерностей : № 2024681345 : заявл. 17.09.2024 : опубл. 25.09.2024 / С.А. Петренко, **А.А. Балябин**, Е.Ю. Осетрин, А.С. Петренко, А.Е. Осетрин; заявитель Автономная некоммерческая организация высшего образования «Университет Иннополис».

12. Свидетельство о государственной регистрации программы для ЭВМ № 2024682499 Российская Федерация. Набор инструментов разработки (SDK) для кибериммунной защиты информационных систем на основе теории подобия и размерностей : № 2024681344 : заявл. 17.09.2024 : опубл. 24.09.2024 / С.А. Петренко, **А.А. Балябин**, Е.Ю. Осетрин, А.С. Петренко, А.Е. Осетрин; заявитель Автономная некоммерческая организация высшего образования «Университет Иннополис».

13. Свидетельство о государственной регистрации программы для ЭВМ № 2024682287 Российская Федерация. Набор инструментов разработки (SDK) для обнаружения и устранения уязвимостей информационных систем в среде контейнеризации Docker на основе инвариантов подобия и размерностей : № 2024681395 : заявл. 17.09.2024 : опубл. 20.09.2024 / С.А. Петренко, **А.А. Балябин**, Е.Ю. Осетрин, А.С. Петренко, А.Е. Осетрин; заявитель Автономная некоммерческая организация высшего образования «Университет Иннополис».

14. Свидетельство о государственной регистрации программы для ЭВМ № 2022680528 Российская Федерация. Программный комплекс для моделирования цифровых паспортов приложений под управлением кибериммунной операционной системы KasperskyOS с произвольными выражениями в терминах размерностей : № 2022669913 : заявл. 27.10.2022 : опубл. 02.11.2022 / С.А. Петренко, Е.Ю. Осетрин, А.С. Петренко, А.Е. Осетрин, А.Я. Асадуллин, Я.Я. Асадуллин, **А.А. Балябин** ; заявитель Автономная некоммерческая организация высшего образования «Университет Иннополис».

15. Свидетельство о государственной регистрации программы для ЭВМ № 2022680672 Российская Федерация. Семантический обнаружитель аномалий функционирования программ на C++ под управлением кибериммунной операционной системы KasperskyOS : № 2022669940 : заявл. 27.10.2022 : опубл. 03.11.2022 / С.А. Петренко, Е.Ю. Осетрин, А.С. Петренко, А.Е. Осетрин, А.Я. Асадуллин, Я.Я. Асадуллин, **А.А. Балябин** ; заявитель Автономная некоммерческая организация высшего образования «Университет Иннополис».

Наиболее значимые публикации в других изданиях:

16. **Балябин, А.А.** Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий / А.А. Балябин // The 2023 Symposium on Cybersecurity of the Digital Economy – CDE’23 : Сборник трудов VII международной научно-технической конференции, Иннополис, 11–12 апреля 2023 года. – Иннополис: Университет Иннополис, 2024. – С. 51–63.

17. **Балябин, А.А.** Модель облачной платформы КИИ РФ с кибериммунитетом / А.А. Балябин // The 2024 Symposium on Cybersecurity of the Digital Economy – CDE’24 : Сборник трудов VIII международной научно-технической конференции, Казань, 23–25 сентября 2024 года. – Санкт-Петербург: ООО Издательский Дом «Афина», 2024. – С. 162–171.

18. **Балябин, А.А.** Модель самовосстановление киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета / А.А. Балябин, С.А. Петренко // The 2025 Symposium on Cybersecurity of the Digital Economy – CDE’25 : Сборник трудов IX Международной

научно-технической конференции, Иннополис, 05–06 марта 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью Издательский Дом «Афина», 2025. – С. 76–91.

19. **Балябин, А.А.** Метод защиты государственных информационных систем и цифровых сервисов Единой цифровой платформы Российской Федерации «ГосТех» на основе кибериммунитета / А.А. Балябин // Наука будущего-наука молодых : сборник тезисов докладов участников девятого Всероссийского молодежного научного форума, Самара, 29 октября – 01 2024 года. – Москва: Общество с ограниченной ответственностью «Инконсалт К», 2024. – С. 146.

20. **Балябин, А.А.** Метод защиты облачных платформ критической информационной инфраструктуры на основе кибериммунитета / А.А. Балябин // Методы и технические средства обеспечения безопасности информации. – 2025. – № 34. – С. 97–100.

21. **Балябин, А.А.** Метод самовосстановления киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета / А.А. Балябин, С.А. Петренко // The 2025 Symposium on Cybersecurity of the Digital Economy – CDE’25 : Сборник трудов IX Международной научно-технической конференции, Иннополис, 05–06 марта 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью Издательский Дом «Афина», 2025. – С. 92–102.

22. **Балябин, А.А.** Метод иммунного ответа на ранее неизвестные вредоносные воздействия / А.А. Балябин, В.А. Новиков, С.А. Петренко // Методы и технические средства обеспечения безопасности информации. – 2022. – № 31. – С. 11–13.

23. **Балябин, А.А.** Методика выявления и нейтрализации информационно-технических воздействий для кибериммунных операционных систем / А.А. Балябин // Методы и технические средства обеспечения безопасности информации. – 2024. – № 33. – С. 103–105.

24. **Балябин, А.А.** Методика самовосстановления киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета / А.А. Балябин, С.А. Петренко // The 2025 Symposium on Cybersecurity of the Digital Economy – CDE’25 : Сборник трудов IX Международной научно-технической конференции, Иннополис, 05–06 марта 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью Издательский Дом «Афина», 2025. – С. 103–114.

25. **Балябин, А.А.** Моделирование угроз безопасности для облачных приложений / А.А. Балябин // The 2024 Symposium on Cybersecurity of the Digital Economy – CDE’24 : Сборник трудов VIII международной научно-технической конференции, Казань, 23–25 сентября 2024 года. – Санкт-Петербург: ООО Издательский Дом «Афина», 2024. – С. 144–149.

26. **Балябин, А.А.** О самовосстановлении киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета / А.А. Балябин, С.А. Петренко // The 2025 Symposium on Cybersecurity of the Digital Economy – CDE’25 : Сборник трудов IX Международной научно-технической конференции, Иннополис, 05–06 марта 2025 года. – Санкт-Петербург: Общество с ограниченной ответственностью Издательский Дом «Афина», 2025. – С. 64–75.

27. **Балябин, А.А.** Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ / А.А. Балябин, К.Р. Попова // The 2023 Symposium on Cybersecurity of the Digital Economy – CDE’23 : Сборник трудов VII международной научно-технической конференции, Иннополис, 11–12 апреля 2023 года. – Иннополис: Университет Иннополис, 2024. – С. 31–41.