На правах рукописи

Русаков Алексей Михайлович

ОЦЕНКА ВЛИЯНИЯ ЭФФЕКТОВ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ИНФРАСТРУКТУРНОГО ГЕНЕЗА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

2.3.6. Методы и системы защиты информации,
информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Москва – 2026

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «МИРЭА – Российский технологический университет» на кафедре КБ-2 «Информационно-аналитические системы кибербезопасности» Института кибербезопасности и цифровых технологий.

Научный руководитель: доктор технических наук, доцент
Максимова Елена Александровна

Официальные оппоненты: **Стародубцев Юрий Иванович**,
доктор военных наук, профессор,
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации, кафедра безопасности инфокоммуникационных систем специального назначения, профессор

Тебуева Фариза Биляловна,
доктор физико-математических наук, доцент,
Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», кафедра вычислительной математики и кибернетики, доцент

Ведущая организация: Акционерное общество «Научно-производственное объединение «Эшелон», г. Москва

Защита состоится 15 апреля 2026 года в 14:00 на заседании объединенного диссертационного совета 99.2.038.03, созданного на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Балтийский государственный технический университет «ВОЕНМЕХ» им. Д.Ф. Устинова», Федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет аэрокосмического приборостроения», Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» по адресу: Санкт-Петербург, пр. Большевиков, д. 22, корп. 1, ауд. 554/1.

С диссертацией можно ознакомиться в библиотеке СПбГУТ по адресу Санкт-Петербург, пр. Большевиков, д. 22, корп. 1 и на сайте www.sut.ru.

Автореферат разослан 10 февраля 2026 года.

Ученый секретарь
диссертационного совета 99.2.038.03,
канд. техн. наук, доцент А.Г. Владыко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В настоящее время растущие объемы данных и потребность в их обработке в реальном времени усиливают требования к производительности и эффективности функционирования распределенных информационных систем организаций (далее – РИС). Растущая сложность РИС, при этом, значительно усиливает риски информационной безопасности (далее – ИБ).

В настоящее время устойчивое функционирование РИС приобретает особую значимость в рамках национального проекта «Экономика данных и цифровая трансформация государства», что подтверждается рядом документов, принятых на уровне Президента и Правительства Российской Федерации. Так, в Паспорте данного национального проекта обозначены федеральные проекты: «Цифровые платформы в отраслях социальной сферы», «Искусственный интеллект», «Цифровое государственное управление», «Отечественные решения», «Инфраструктура кибербезопасности» и другие. Для обозначенных проектов РИС служат фундаментальной основой при создании ключевых компонентов цифровой инфраструктуры. Кроме того, согласно Федерального закона от 23 июля 2025 г. № 248-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в целях внедрения цифрового рубля», для проекта «Национальная система цифрового рубля», устойчивое и безотказное функционирование РИС является основополагающим.

Безопасность РИС традиционно достигается реализацией комплекса мер, связанных с резервированием, связанных с резервированием, мониторингом, управлением ресурсами и др. При этом рост нагрузки на РИС выступает основным триггером перехода ее в неустойчивое состояние, сопровождающееся деградацией качества обслуживания и отказами ее компонентов. Классические методы теорий надёжности, отказоустойчивости, протоколов консенсуса и др., зачастую недостаточно эффективны для обеспечения отказоустойчивости РИС. Это объясняется усложнением и облачной интеграцией РИС, на фоне эволюционирования угроз ИБ в интеллектуальные, а также автоматизацией ботнетов и адаптивностью тактик их реализации на базе искусственного интеллекта.

Сегодня появляются новые типы угроз ИБ для РИС: многовекторные, на поддомены и программные интерфейсы, с массовыми WebSocket-соединениями, «ковровыми бомбардировками» и фрагментацией IP-пакетов и др., что свидетельствует об их возрастающей сложности, интеллектуальности и непредсказуемости. Одним из источников возникновения данных угроз является инфраструктурный деструктивизм (далее – ИД), то есть саморазрушение инфраструктуры, приводящий, в том числе, к деградации качества функционирования РИС.

Современные исследователи характеризуют эффекты ИД как феномен, возникающий в РИС, в результате деструктивных воздействий инфраструктурного генеза (далее – ДВ ИГ), приводящих к системным изменениям, связанным с нарушением отказоустойчивости, безопасности и управляемости системы. В данном случае, можно говорить о наличии эффектов ИД, способных привести к серьезным аномалиям в работе РИС с одной стороны, и отсутствии методов и технологий, позволяющих их оценивать и использовать при построении эффективной системы защиты информации – с другой.

В отличие от традиционных угроз, ДВ ИГ проявляются не как следствие внешних атак, а как результат внутренних процессов: ошибок проектирования, несовершенства архитектуры, неучтённых взаимосвязей и изменений состава или функций объектов на всех этапах жизненного цикла РИС. Эти процессы могут привести к нарушению

инфраструктурных связей, снижению управляемости, а также к саморазрушению инфраструктуры в целом.

Угрозы ИД становятся новым классом имманентных угроз ИБ, источники и последствия которых обусловлены самой природой и эволюцией инфраструктуры РИС. Однако, их проявления могут носить как разрушительный, так и обеспечивающий самозащиту, характер.

Таким образом, недостаточное исследование угроз ИД с одной стороны, а также отсутствие готовых решений в сфере ИБ– с другой, подчёркивают актуальность вопросов разработки моделей и методов, позволяющих выявлять, анализировать и количественно оценивать эффекты инфраструктурного деструктивизма в РИС для обеспечения их ИБ.

Степень разработанности темы. Общие вопросы обеспечения ИБ в РИС нашли отражение в трудах П.Д. Зегжды, Н.Г. Милославской, А.И. Толстого, Ф.Б. Тебуевой, А.В. Царегородцева, А.А. Малюка, Е.К. Барановой, Е.А. Басыни, А.А. Шелупанова, К.З. Билятдинова, С.Л. Зефирова, В.С. Аткиной, P.W. Singer, M. Whitman, H. Mattord и др. Анализируемые исследования освещают актуальные проблемы и методы управления ИБ. Однако влияние деструктивных воздействий инфраструктурного генеза в них учитывается косвенно.

Методологические подходы к моделированию систем и технологий при решении вопросов ИБ обозначены в работах Г.А. Остапенко, Ю.И. Стародубцева, М.А. Полтавцевой, О.С. Лауты, Б.А. Швырева, В.В. Баранова, А.Г., А.С. Маркова, А.Г. Владыко, Ю.Ю. Громова, A. Shostack, J. Holt и др. Эти исследования позволяют повысить уровень ИБ, но нуждаются в дальнейшем развитии для анализа угроз инфраструктурного генеза.

Поведенческие модели и искусственный интеллект признаны перспективными направлениями в ИБ и исследованы в работах В.И. Городецкого, И.И. Виксина, И.С. Лебедева, И.А. Зикратова, Т.В. Зикратовой, Н.А. Дородникова, A. Enberg и др. Предложенные в исследованиях модели позволяют описывать особенности взаимодействий элементов систем. Однако антропоморфные характеристики межобъектных взаимодействий на уровне объектов защиты в этих работах не анализируются. Развитие методов защиты от нарушения доступности информации в РИС в настоящий момент – актуальное направление в сфере ИБ.

Среди работ в области оценки эффектов инфраструктурного деструктивизма следует выделить работы Е.А. Максимовой, М.В. Буйневича, К.Е. Израилова, С.И. Макаренко. В работах данных ученых рассматриваются межобъектные взаимодействия в системе критической информационной инфраструктуры и предложенные ими модели и методы в РИС возможны только при проведении дополнительных исследований. Также стоит отметить исследования И.В. Котенко, М.А. Еремеева, Е.Б. Саенко, О.И. Шелухина, где задачи оценки эффектов инфраструктурного деструктивизма решаются косвенно, без учета специфики этого явления.

Таким образом, решение вопросов, связанных с выявлением и оценкой эффектов деструктивного воздействия инфраструктурного генеза при обеспечении информационной безопасности распределенных информационных системах, требует дальнейшего развития.

Объект исследования – эффекты деструктивного воздействия инфраструктурного генеза в распределенных информационных системах.

Предмет исследования – модели и методы оценки влияния эффектов деструктивного воздействия инфраструктурного генеза.

С учетом вышеизложенного, **целью исследования** является повышение оперативности и точности выявления эффектов деструктивного воздействия инфраструктурного генеза в распределенных информационных системах.

Для достижения цели исследования, в соответствии с п. 9 Постановления Правительства РФ «О порядке присуждения ученых степеней», сформулирована научная (научно-техническая) задача: разработка моделей и методов, позволяющих выявлять, анализировать и количественно оценивать эффекты деструктивного воздействия инфраструктурного генеза в сервис-ориентированных информационных системах в условиях инфраструктурного деструктивизма.

Для решения данной научной задачи необходимо решение следующих (частных) **задач:**

1) исследовать проблемы обеспечения безопасности в распределенных информационных системах;

2) разработать комплекс моделей взаимодействия сервисов информационных систем для обнаружения эффектов деструктивного воздействия инфраструктурного генеза;

3) разработать методы оценки эффектов деструктивного воздействия инфраструктурного генеза;

4) разработать методику выявления угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах.

Научная новизна работы состоит в том, что:

1) разработан оригинальный комплекс моделей, впервые учитывающий антропоморфические особенности взаимодействия сервисов в распределенных информационных системах, а также позволяющий выявлять и оценивать угрозы инфраструктурного генеза;

2) впервые разработан метод оценки эффектов деструктивного воздействия инфраструктурного генеза, состоящий в поэтапном анализе шаблонов последовательностей запросов и их структурирования на основе антропоморфических типов межсервисных взаимодействий;

3) в отличие от существующих, предложенная методика выявления угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах, учитывает антропоморфические свойства и межсервисные взаимодействия.

Теоретическая значимость научных положений, состоит в следующем:

1) установлено соответствие между поведенческими особенностями сервисов и возможностью возникновения эффектов деструктивного воздействия инфраструктурного генеза в распределенных информационных системах;

2) расширена теория инфраструктурного деструктивизма в части понятийного аппарата и методологии управления динамикой рисков инфраструктурного генеза в части научно-методического аппарата прогнозирования;

3) доказана возможность выявления угроз ИБ инфраструктурного генеза в сервис-ориентированных информационных системах.

Практическая значимость полученных результатов состоит в следующем:

1) комплекс антропоморфических моделей позволяет выявлять и анализировать угрозы ИБ инфраструктурного генеза, приводящие к отказу в обслуживании и формировать стратегии их предотвращения на основе анализа поведенческих особенностей сервисов и их взаимодействий;

2) разработанный метод оценки эффектов деструктивного воздействия инфраструктурного генеза позволяет повысить точность выявления скрытых синергетических эффектов, приводящих к неконтролируемому саморазрушению инфраструктуры РИС, более чем на 10 %;

3) разработанная методика выявления угроз ИБ инфраструктурного генеза позволяет оперативно выявлять эффекты инфраструктурного деструктивизма в сервис-ориентированных РИС на ранних этапах его возникновения за счет автоматизации процедур.

Методология и методы исследования. Для решения поставленных задач использовались методы построения агентных систем, теория инфраструктурного деструктивизма, теории надежности, математической логики, математического моделирования, элементы методологии программирования и теории принятия решений, антропоморфический и регулятивный подходы.

Положения, выносимые на защиту. Соискателем лично получены следующие основные научные результаты, выносимые на защиту:

1) комплекс антропоморфических моделей взаимодействия сервисов информационных систем (п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса» паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»);

2) метод оценки эффектов деструктивного воздействия инфраструктурного генеза (п. 10 «Модели и методы оценки защищенности информации и информационной безопасности объекта» паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»);

3) методика выявления угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах (п. 3 «Методы, модели и средства выявления, идентификации, классификации и анализа угроз нарушения информационной безопасности объектов различного вида и класса» паспорта научной специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»).

Степень достоверности основных полученных результатов обеспечивается корректностью постановки научно-технической задачи исследования; представительным библиографическим материалом, опирающимся на современную научную базу; корректным применением апробированных общенаучных и специальных методов исследования; подтверждается непротиворечивостью полученных результатов известным и достоверно подтвержденным результатам исследований других авторов, а также их широкой апробацией и обсуждением результатов на международных научных конференциях, рецензированием и экспертизой научных статей, опубликованных в ведущих научных изданиях, а также получением государственной регистрации на программы для ЭВМ по результатам исследования.

Апробация результатов. Основные положения и результаты диссертации докладывались, обсуждались и получили одобрение на Всероссийских научно-технических конференциях «Новые информационные технологии» (г. Москва в 2013-2014 гг.), третьей Международной конференции молодых ученых, студентов и магистрантов «Прикладные исследования и технологии» ART2016 (г. Москва, 14 сентября 2016 г.), второй Всероссийской междисциплинарной конференции Института проблем управления им. В.А. Трапезникова РАН (г. Москва, 2019 г.), Всероссийской научно-практической конференции «Проблемы обеспечения безопасности (Безопасность-2021)» (г.

Уфа, 11 марта 2021 г.), второй Всероссийской научно-практической конференции «Теория и практика обеспечения информационной безопасности» (г. Москва, 2022 г.), Национальных научно-практических конференциях «Цифровизация техносферы: научный подход» (г. Москва, 2022-2025 гг.), Всероссийских научных школах-семинарах «Современные тенденции развития методов и технологий защиты информации» (г. Москва, 2023-2024 гг.), XIX Всероссийской научно-теоретической конференции «Информационная безопасность цифровой экономики» (г. Улан-Удэ, 2023 г.), Всероссийских научно-технических конференциях «Кибернетика и информационная безопасность» (г. Москва, 2023-2025 гг.), Международной научной конференции «Актуальные проблемы прикладной математики, информатики и механики» (г. Воронеж, 2024 г.).

Публикации. Основные результаты диссертационного исследования опубликованы в 28-ми научных трудах, из них: 9 – в рецензируемых научных изданиях из Перечня ВАК; 2 – в изданиях, входящих в международную систему цитирования Scopus; 9 – свидетельств о государственной регистрации программы для ЭВМ; 3 – статьи в научных журналах; 5 – в сборниках научных статей, трудов, тезисов докладов и материалах конференций. Результаты диссертационной работы отражены в публикациях.

Реализация результатов исследования. Диссертационная работа выполнялась при поддержке Министерства образования и науки РФ (Грант аспирантам, ученым, соискателям на исследования, направленные на обеспечение информационной безопасности, Проект № 40469-25/2022-К).

Практическое использование полученных научных результатов в профильных организациях ИБ-отрасли: АО «Национальный Инновационный Центр» (г. Москва), ФГАНУ Центр информационных технологий и систем органов исполнительной власти (г. Москва), ФГБОУ ВО «Санкт-Петербургский университет Государственной противопожарной службы МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева» (г. Санкт-Петербург, НИР «Кибермониторинг», рег. №НИОКТР125031703734-4), а также в учебном процессе ФГБОУ ВО «МИРЭА – Российский технологический университет» (г. Москва), – подтверждается соответствующими актами внедрения.

Структура и объем работы. Диссертационная работа состоит из введения, основной части (содержащей 4 раздела), заключения, списка литературы и 4 приложений. Общий объем работы – 257 страниц, из них основного текста – 200 страниц. Работа содержит 86 рисунков и 62 таблицы. Список литературы включает 228 библиографических источников.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе, в качестве объекта исследовались РИС на предмет обнаружения угроз ИБ, связанных, в том числе, с эффектами ИД.

Проведён анализ принципов создания, проектирования и эксплуатации РИС с упором на обеспечение их ИБ. Выполнен системный анализ различного вида и класса архитектур ИС, включающий анализ моделей их развёртывания (On-Premises, Cloud, Hybrid, Multi-Cloud), микросервисную парадигму, средства контейнеризации (Docker, Kubernetes) и эволюцию протоколов программных интерфейсов (SOAP, gRPC, OpenAPI). Идентифицирован и охарактеризован класс угроз ИБ, связанных с межсервисным взаимодействием в РИС.

Выполнен систематический анализ современных моделей киберугроз и методик их нейтрализации в РИС. Описаны ключевые инструменты обнаружения и реагирования на инциденты ИБ, включая центры SOC, платформы SIEM, XDR, SOAR, а также системы мониторинга (Prometheus и Grafana). Обоснована недостаточная оперативность и точность по выявлению и оценке эффектов деструктивного воздействия инфраструктурного генеза у существующих решений.

Проанализированы методы оценки и управления рисками ИБ. Обоснована возможность использования антропоморфического подхода к моделированию межсервисных взаимодействий в РИС. Установлена необходимость разработки автоматизированных систем мониторинга и реагирования для предиктивной аналитики угроз ИБ инфраструктурного генеза в сервис-ориентированных РИС.

Основное содержание раздела и изложенных в нем научных результатов опубликовано в работах автора [2, 7, 13, 15, 25, 26].

Во втором разделе в качестве объекта исследовались эффекты ИД в РИС на предмет оценки влияния ДВ ИГ. Введены определения базовых категорий.

Определение. Инфраструктурный деструктивизм — это феномен, возникающий в РИС, когда в результате деструктивных воздействий инфраструктурного генеза происходят системные изменения, ведущие к нарушению устойчивости, целостности, доступности, функциональности и управляемости системы.

Эти воздействия могут быть как внутренними (ошибки проектирования, внедрения, сопровождения, эксплуатации и др.), так и внешними (атаки, изменения среды функционирования и др.) воздействиями, и реализуются преимущественно через сложные межобъектные взаимодействия внутри ИТ-инфраструктуры.

Определение. Под деструктивным воздействием инфраструктурного генеза будем понимать воздействие, в результате которого проявляется непредвиденное и (или) нежелательное событие, вызванное совокупностью факторов и условий инфраструктурного генеза, создающих опасность нарушения ИБ РИС.

Проявление эффектов ИД во многом зависит от внутренних состояний, внутренних целей, сценариев работы и взаимодействия объектов РИС. Обозначенное необходимо рассматривать на уровне сервисов, так как в основе современных РИС заложены сервисные архитектуры.

Для оценки устойчивости сервисов к эффектам ИД предложены адаптивные алгоритмы генерации нагрузочных последовательностей запросов, максимизирующие воздействие на РИС. В качестве одной из возможных метрик измерения деструктивных возможностей предлагается вычислять дисперсию времени отклика, определяемую как разность между максимальными и минимальными значениями задержек запросов.

В качестве возможных источников возникновения эффектов ИД (угроз инфраструктурного генеза) выявлены компоненты сервисных архитектур РИС: планировщики и оптимизаторы запросов, кэширующие сервисы, обратные прокси-сервера, балансировщики нагрузки, брокеры сообщений. Наличие их в сервисной архитектуре РИС является необходимым условием для проявления эффектов ИД. Данные компоненты обеспечивают масштабируемость РИС при высоких нагрузках, одновременно создавая предпосылки для реализации эффектов ИД.

Для формализации множественных взаимодействий сервисов и клиентов (объектов) в РИС рассотрим следующую схему их организации (рисунок 1).

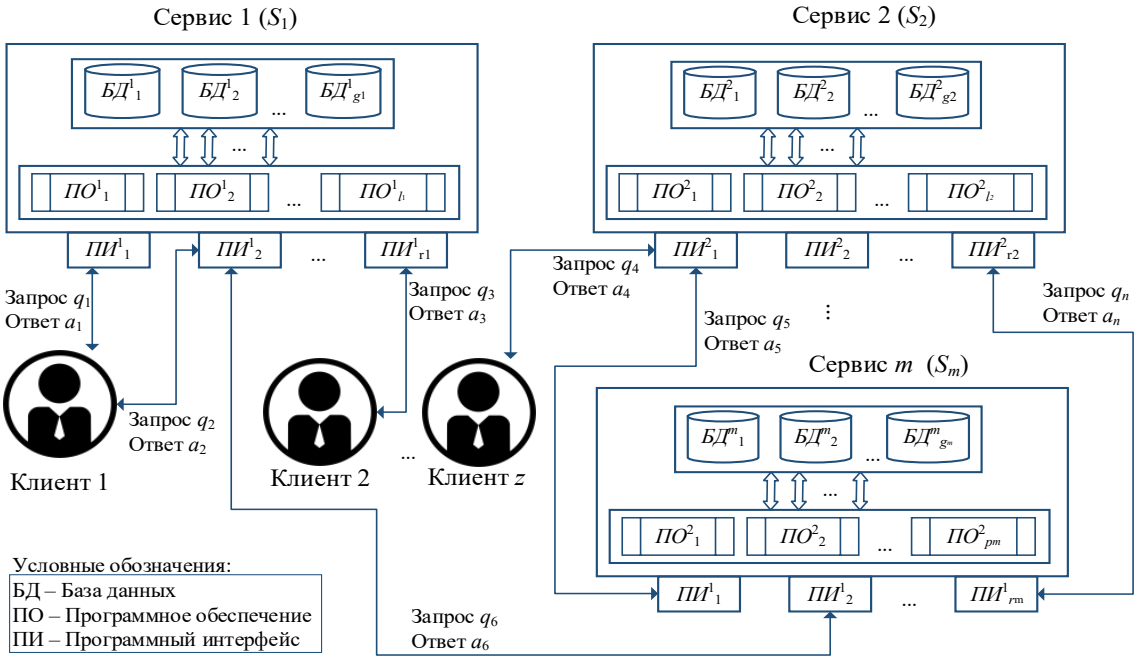


Рисунок 1 – Схема организации взаимодействия сервисов и клиентов в РИС

Пусть $S=\{S_1,S_2\dots S_m\}$ – множество взаимодействующих сервисов в РИС. $C=\{C_1,C_2\dots C_z\}$ – множество клиентов в РИС.

Система взаимодействия сервисов и клиентов в РИС описывается композицией отображения множеств сервисов $S=\{S_j\}_{j=1}^{|S|}$ и клиентов $C=\{C_k\}_{k=1}^{|C|}$, где взаимодействие описывается декартовым произведением множеств $S\times C$ с отображением $\varphi: S\times C\to Proc(Q)$. Внутри каждого сервиса j, $j=\overline{1,m}$ находится комплект программного обеспечения (КПО): $КПО_j=\{ПО_1^j,ПО_2^j\dots ПО_{l^j}^j\}$ и комплект баз данных $КБД_j=\{БД_1^j,БД_2^j\dots БД_g^j\}$. Элементы множеств $КПО_j$ и $КБД_j$ между собой взаимодействуют. Сервисы S_j, также взаимодействуют между собой и с клиентами через наборы программных интерфейсов (НПИ): $НПИ_j=\{ПИ_1^j,ПИ_2^j\dots ПИ_{r^j}^j\}$, где r – количество программных интерфейсов для каждого сервиса j. Общее число программных интерфейсов в РИС – множество $R=\{r_1,r_2,\dots r_m\}$. На каждый из программных интерфейсов поступает последовательность запросов $Q_i^j=q_1^i,q_2^i\dots q_{n_i}^i$, где $j=\overline{1,m}$,

$i = \overline{1, r_j}$. Каждый запрос q_i инициирует процесс его обработки $Proc_i$, выполняемый сервисом РИС, по завершении которого формируется и отправляется ответ a_i.

Таким образом, каждый сервис S_J содержит комплекты $КПО_j$, $КБД_j$, взаимодействуя через наборы $НПИ_j$, формируя полную композицию отображения множеств $\oplus_{j=1}^{|S|}(S_j, КПО_j, КБД_j, НПИ_j)$. Результат композиции отображения множеств запросов и процессов обеспечивает динамику взаимодействия сервисов, *НПИ*, запросов и процессов: $\oplus_{j=1}^{|S|}, НПИ, Q, Proc$.

На рисунке 2 представлена временная диаграмма работы запроса q_i, реализуемого процессом $Proc_i$, с определённой длительностью выполнения Tq_i.

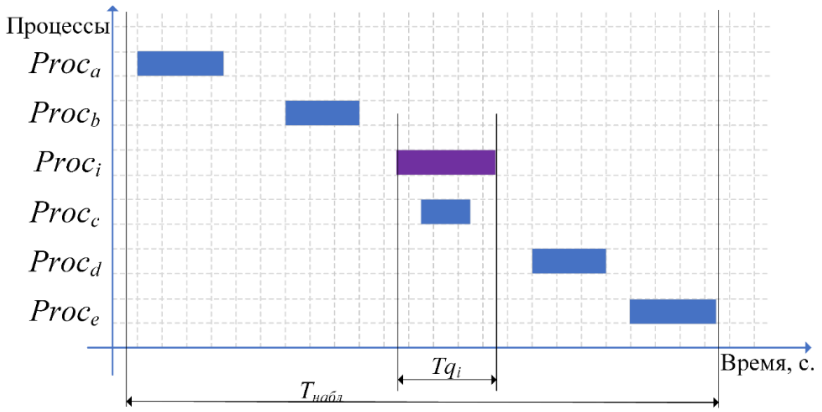
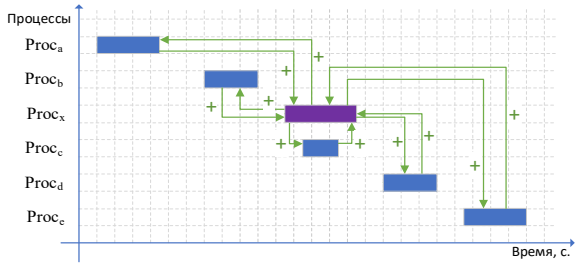
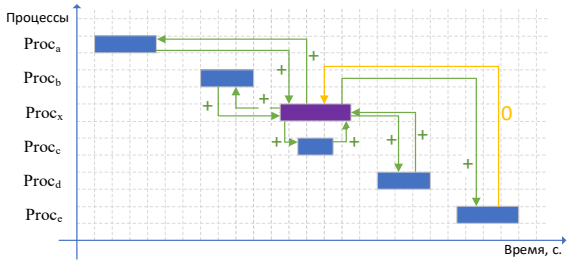


Рисунок 2 – Временная диаграмма работы взаимодействующих процессов

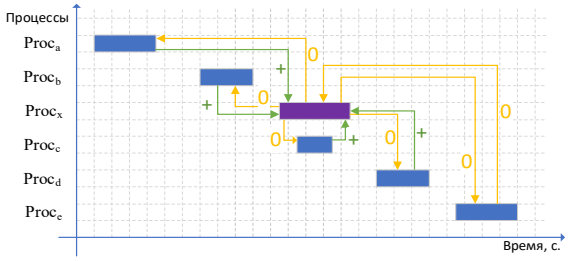
На рисунке 3 представлены временные диаграммы, иллюстрирующие взаимное влияние процессов по основные антропоморфическим типам их взаимодействий в РИС.



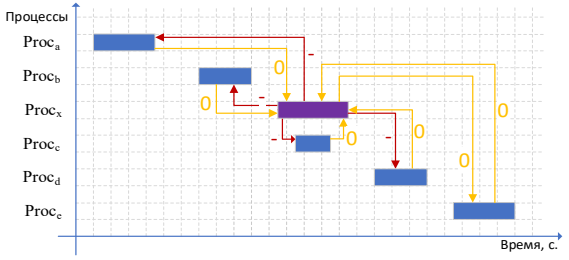
Тип 1 – «Облигатный симбиоз» (+|+). Данный тип характеризуется необходимостью совместного сосуществования организмов



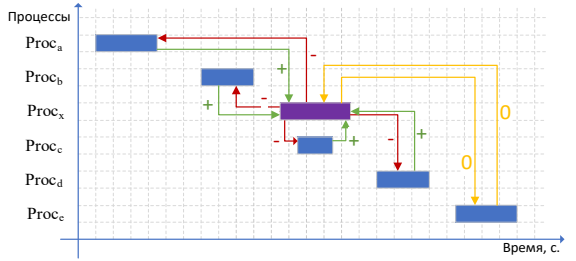
Тип 2 – «Факультативный симбиоз» (+|+) – характеризуется взаимной выгодой от совместного сосуществования организмов, но без необходимости как таковой



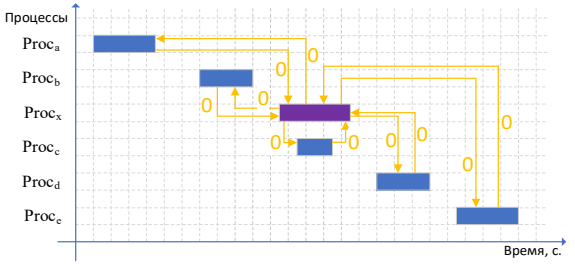
Тип 3 – «Комменсализм» (+|0). Данный тип характеризуется выгодой от существования одного организма при отсутствии какого-либо эффекта для другого



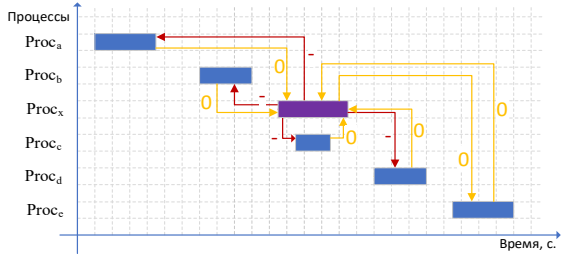
Тип 4 – «Паразитизм» (+|–) – характеризуется извлечением выгоды от сосуществования одним организмом, используя при этом другого как источник питания, среду обитания и т.п., возлагая на него часть своих отношений с внешней средой.



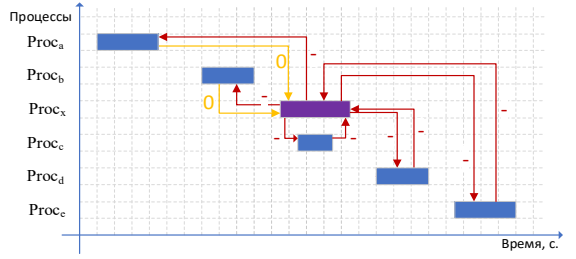
Тип 5 – «Хищничество» (+|–). Данный тип характеризуется тем, что один организм питается частями другого при отсутствии каких-либо симбиотических (то есть взаимовыгодных) отношений и зачастую с умерщвлением первым второго.



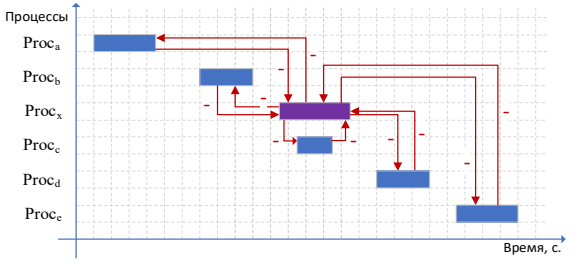
Тип 6 – «Нейтрализм» (0|0) – характеризуется отсутствием каких-либо воздействий друг на друга.



Тип 7 – «Аменсализм» (0|–). Данный тип характеризуется отрицательным влиянием одного организма на другого, не испытывая при этом какого-либо обратного влияния.



Тип 8 – «Аллелопатия» (–|–) – характеризуется взаимновредным влиянием организмов друг на друга.



Тип 9 – Конкуренция (–|–). Данный тип характеризуется косвенным отрицательным влиянием организмов друг на друга по причине борьбы за общие ресурсы.

Рисунок 3 – Временные диаграммы, иллюстрирующие основные антропоморфические типы взаимодействия процессов в РИС

На рисунке 3 используется следующая система обозначений: символ «+» и зелёная стрелка указывают на положительное влияние исследуемого процесса на другой процесс; символ «0» и жёлтая стрелка — на отсутствие воздействия; символ «–» и красная стрелка — на отрицательное воздействие одного процесса на другой.

На основе представленных временных диаграмм сформирован комплекс антропоморфических моделей взаимодействия сервисов РИС. Разработанный комплекс моделей обеспечивает количественную оценку наличия и выраженности определённых антропоморфических типов межсервисных взаимодействий в РИС. Предложенный подход предлагается использовать как индикатор «здоровья» инфраструктуры в системе мониторинга ИБ.

Типы антропоморфического взаимодействия процессов в РИС классифицируются, исходя из динамики их взаимного влияния.

Положительный класс включает: тип 1 – «Облигатный симбиоз», тип 2 – «Факультативный симбиоз», тип 3 – «Комменсализм».

Нейтральный класс включает: тип 4 – «Нейтрализм».

Отрицательный класс включает: тип 5 – «Паразитизм», тип 6 – «Хищничество», тип 7 – «Аменсализм», тип 8 – «Аллелопатия», тип 9 – «Конкуренция».

Использование данной классификации, повышает наблюдаемость процессов в РИС, что особенно важно при прогнозировании развития динамики влияния эффектов ИД.

Данный механизм анализа динамики взаимного влияния процессов в РИС использован для формализации состояний эпидемиологической модели распространения вирусов. Применение представленного подхода обеспечило более точное описание множественного взаимодействия вирусов в рамках эпидемиологической модели.

В исследовании предложена агентная модель для выявления и прогнозирования источников ИД (угроз ИГ) с использованием антропоморфических поведенческих механизмов взаимодействия процессов в РИС.

Основным научным результатом, изложенным во втором разделе, является комплекс моделей для анализа поведенческих особенностей сервисов на основе антропоморфических типов взаимодействия процессов в ИС.

Частными научными результатами, изложенными во втором разделе, являются: формальное описание феномена ИБ в РИС, модель обнаружения эффектов ДВ ИГ сервисов ИС; классификация антропоморфических типов состояний объектов ИС для комплекса эпидемиологических моделей распространения вирусов, агентная модель системы обнаружения и прогнозирования возникновения источников угроз инфраструктурного генеза.

Основное содержание раздела и полученных научных результатов изложено в работах автора [6, 11, 12, 14, 20, 27].

В третьем разделе представлены методы оценки эффектов деструктивного воздействия инфраструктурного генеза.

Взаимное влияние межсервисных процессов представлено в виде временных диаграмм в параметрическом виде. Для каждого сервиса формализованы его поведенческие особенности и представлены в виде множества значений параметров с учетом принадлежности к соответствующему антропоморфическому типу взаимодействия. А именно:

$$Proc_i^{Beh} = \left\{ PB_{T1}, PB_{T2}, PB_{T3}, PB_{T4}, PB_{T5}, PB_{T6}, PB_{T7}, PB_{T8}, PB_{T9} \right\}, \qquad (1)$$

где $PB_{T1}, PB_{T2}, PB_{T3}, PB_{T4}, PB_{T5}, PB_{T6}, PB_{T7}, PB_{T8}, PB_{T9}$ – параметры, определяющие антропоморфические типы поведения исследуемого процесса.

Отмечено, что $Proc_i^{Beh}$, может определять, во-первых, влияние времени работы сервиса на время работы параллельно выполняющихся сервисов (его окружения). Во-вторых, – влияние времени выполнения параллельно выполняющихся сервисов на время исследуемого сервиса.

В разработанной модели, поведенческие особенности сервиса описаны в виде наборов правил для каждого антропоморфического типа взаимодействия. Для этого разработано множество правил для определения антропоморфических типов поведения сервисов на основе продукционной модели представления знаний:

$$Alg_{rules} = \{rul_1, rul_2, ..., rul_{num}\}, \quad (2)$$

где rul_i – продукционное правило, $i = \overline{1, num}$ (num – количество правил) вида:

$$rul_i = \left(sh \wedge W \wedge Pr \wedge A \to B \wedge Ap\right), \quad (3)$$

где sh – идентификатор правила, формируется как $S_h \in$ □ ;

W – сфера применения продукции;

Pr – условие применения ядра продукции (предикат);

$A \to B$ – ядро продукции (если *A,* то *B*);

Ap – постусловие продукции.

Описаны правила поведения сервисов для оценки влияния $Proc_i \to Proc_j$ (таблица 1).

Таблица 1 – Система правил Alg_{rules} для описания поведения сервисов

Идентификатор правила sh	Условие применения ядра продукции *Pr*	Условие правила	Постусловие продукции *Ap*
sh_1	$sh_2 \vee sh_3 \vee sh_4 \vee sh_8 \vee sh_{10} \vee sh_{12} \vee sh_{14} \vee sh_{15} \vee sh_{17}$	Процесс $Proc_i$ работает параллельно процессу $Proc_j$	все
sh_2	$sh_2 \vee sh_3 \vee sh_5 \vee sh_9 \vee sh_{11} \vee sh_{13} \vee sh_{14} \vee sh_{16} \vee sh_{17}$	Процесс $Proc_j$ работает параллельно процессу $Proc_i$	все
...	...	...	...
sh_{17}	$sh_1 \vee sh_2$	$Proc_i$ работает медленнее. $Proc_j$ работает медленнее	Тип 8 или Тип 9

На основе множества правил Alg_{rules} построена система компенсирующих правил для описания поведенческих взаимодействий сервисов:

$$Alg_{ant\_rules} = \{At_1, At_2, At_3, At_4, At_5, At_6, At_7, At_8, At_9\}, \quad (4)$$

где At_i – множество правил для описания i-го антропоморфического типа взаимодействия сервисов, $i = \overline{1,9}$.

Для каждого из процессов $Proc_i$ выполняется его пространственно-временная локация (рисунок 2). При этом:

$$Proc_j \in \{Proc_a, Proc_b, Proc_c, Proc_d, Proc_e\}. \quad (5)$$

Далее выполняется причинно-следственный анализ межсервисного взаимодействия. Если в процессе исследования взаимосвязь процессов $Proc_i \to Proc_j$ подтверждается, то выполняется антропоморфическая оценка межсервисного взаимодействия. Для каждого антропоморфического типа взаимодействия задаётся матрица влияния процессов, что позволяет проанализировать результаты развития сценариев функционирования сервисов в РИС.

На основе проведенного анализа антропоморфических типов взаимодействий процессов в РИС синтезирована система поведенческих правил Alg_{rules} (таблица 2).

Таблица 2 – Система поведенческих правил Alg_{rules}

Идентификатор правила *sh*	Условие применения ядра продукции *Pr*	Условие правила	Постусловие продукции *Ap*
sh_1	$sh_2 \vee sh_3 \vee sh_4 \vee sh_8 \vee sh_{10} \vee sh_{12} \vee sh_{14} \vee sh_{15} \vee sh_{17}$	Процесс $Proc_i$ работает параллельно процессу $Proc_j$	все
sh_2	$sh_2 \vee sh_3 \vee sh_5 \vee sh_9 \vee sh_{11} \vee sh_{13} \vee sh_{14} \vee sh_{16} \vee sh_{17}$	Процесс $Proc_j$ работает параллельно процессу $Proc_i$	все
…	…	…	…
sh_{17}	$sh_1 \vee sh_2$	$Proc_i$ работает медленнее. $Proc_j$ работает медленнее	Тип 8 или Тип 9

Используя правила Alg_{rules}, синтезируются наборы правил Alg_{ant_rules} для описания поведения антропоморфических типов взаимодействия сервисов (таблица 3).

Таблица 3 – Наборы правил Alg_{ant_rules} для описания антропоморфических типов взаимодействия сервисов

Тип взаимодействия сервисов	Множество наборов правил
Тип 1 – «Облигатный симбиоз» (+|+) At_1	$(sh_1 \wedge sh_3 \wedge sh_4) \vee (sh_2 \wedge sh_3 \wedge sh_5)$
Тип 2 – «Факультативный симбиоз» (+|+) At_2	$(sh_1 \wedge sh_6) \vee (sh_2 \wedge sh_7)$
…	…
Тип 9 – «Конкуренция» (–|–) At_9	$(sh_1 \wedge sh_{17} \wedge sh_{12}) \vee (sh_2 \wedge sh_{17} \wedge sh_{13})$

Для оценки взаимного влияния сервисов в РИС разработан алгоритм оценки антропоморфических типов взаимодействия сервисов.

Основным научным результатом, изложенном в третьем разделе, является метод оценки эффектов деструктивного воздействия инфраструктурного генеза.

Частными научными результатами, изложенными в третьем разделе, являются: оценка старения распределенных информационных систем с позиции ИД (накопление «деструктивного мусора»); расширение рекомендательной системы по профилактике и предотвращению ИД.

Основное содержание раздела и полученных научных результатов изложено в работах автора [3, 4, 5, 17, 18, 24, 28].

В четвертом разделе разработана Методика оценки угроз ИБ ИГ в сервис-ориентированных ИС. Методика строится на комплексном анализе результатов проявления событий РИС, содержащихся в журналах событий; моделировании поведения сервисов с учётом их взаимодействий; использовании агентных и имитационных моделей. Структурный схемы работы с Методикой оценки угроз ИБ ИГ в сервис-ориентированных ИС приведены на рисунках 4 и 5.

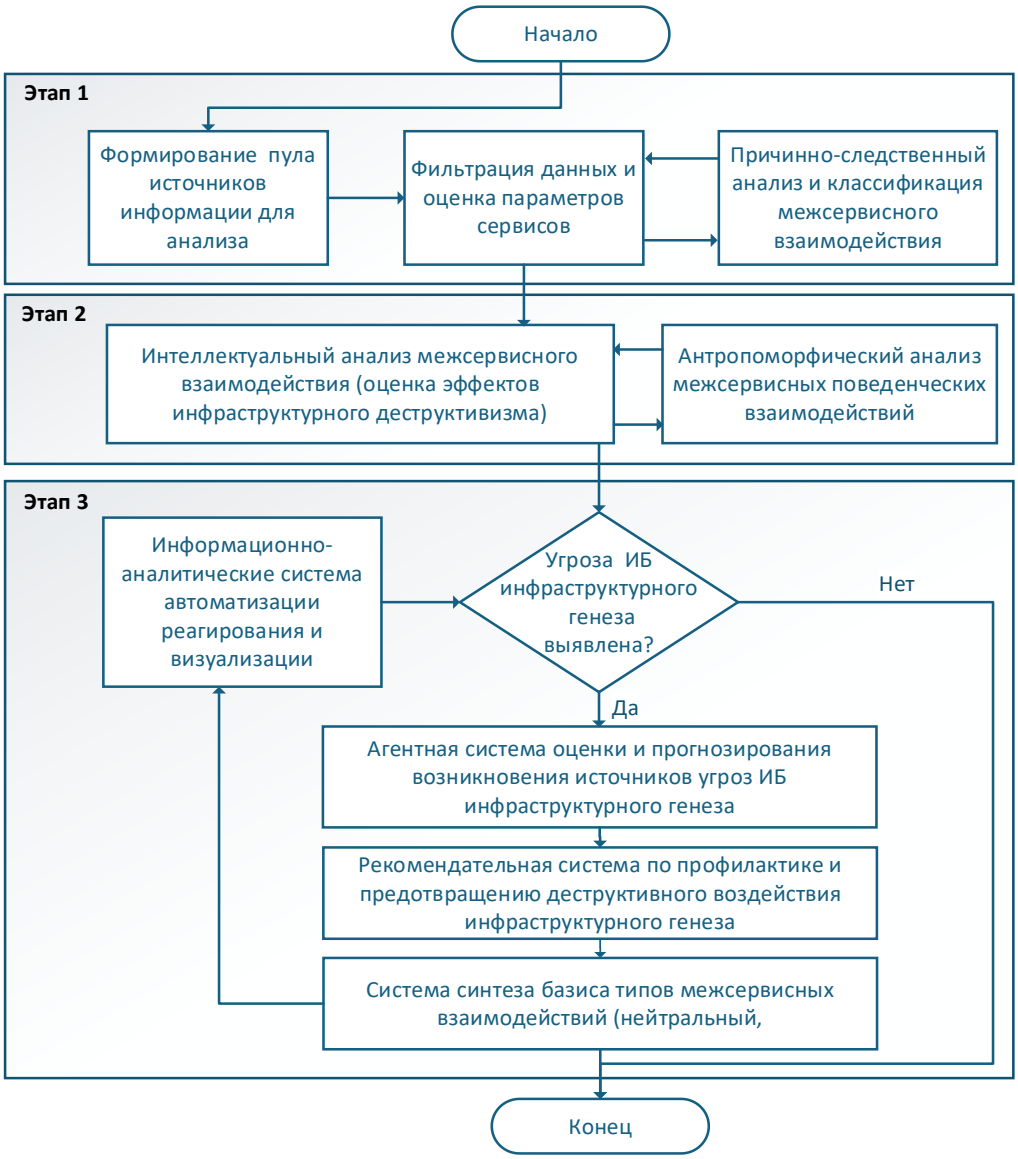


Рисунок 4 – Структурная схема реализации Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС

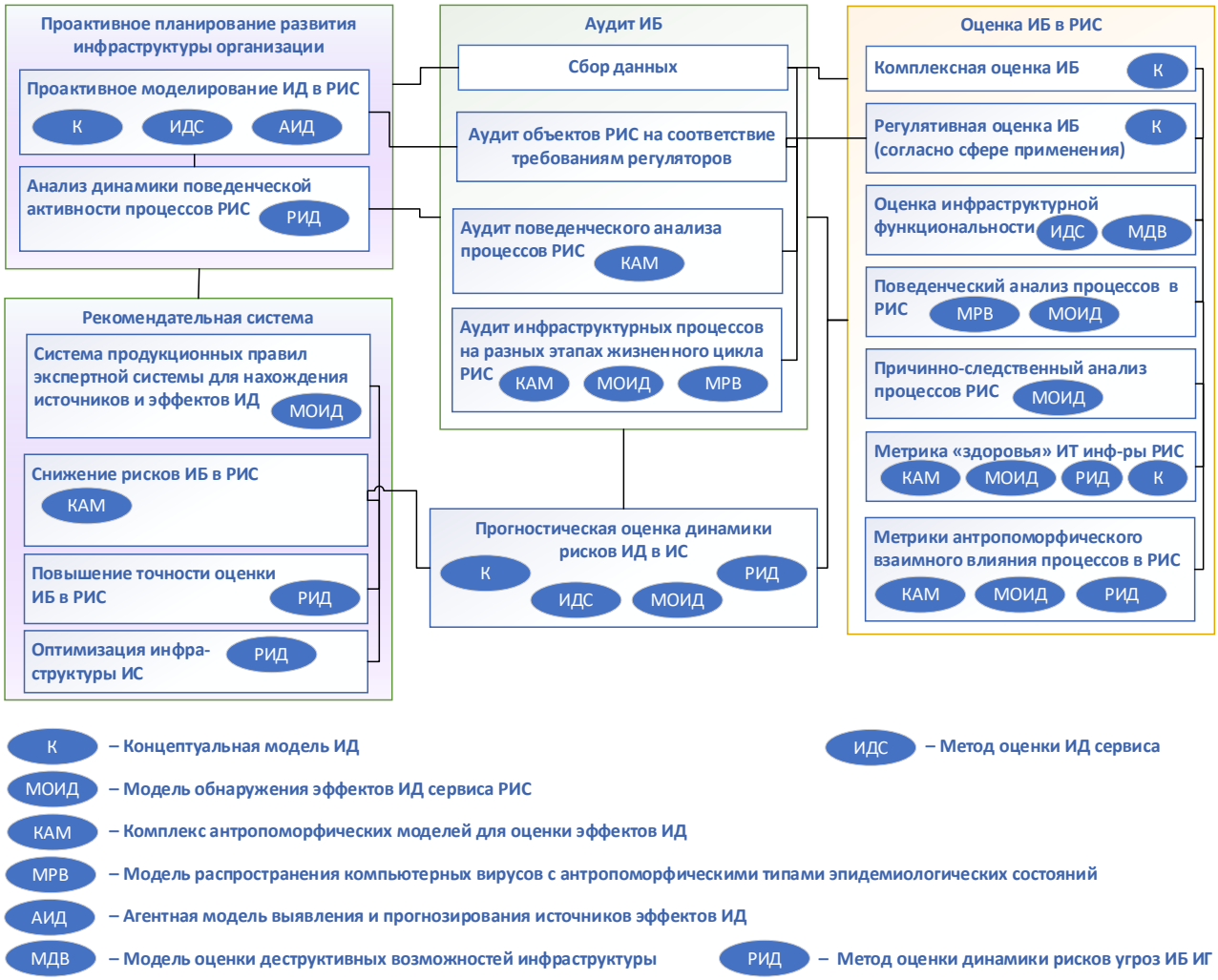


Рисунок 5 – Схема организации Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС

Представленная на рисунке 5 схема, обеспечивает реализацию Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС в режиме реального времени, что позволяет повысить оперативность реагирования на проявление эффектов ИД.

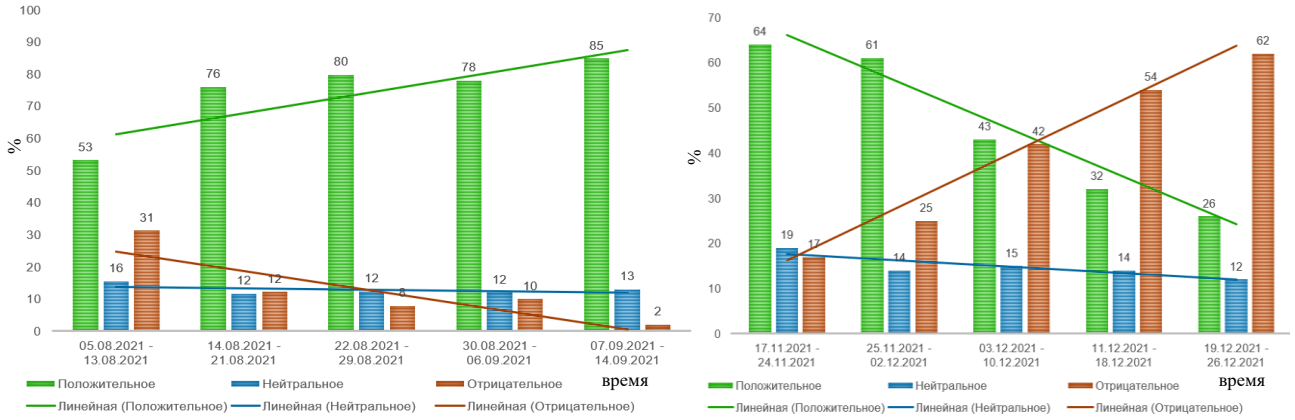
Предложенная Методика оценки угроз ИБ ИГ в сервис-ориентированных ИС, апробирована на базе современных ИС: «GreenPlum», «DeepTraLog», «Alibaba cloud», распределённой системы распознавания лиц «Персона ID».

Исследования сервиса на наличие эффектов ИД на примере открытого набора данных «DVD RENTAL» для базы данных PostgreSql показало, что время обработки запросов определяется внутренними параметрами инфраструктуры СУБД и остаётся постоянным для конкретного экземпляра её функционирования.

Проведён интеллектуальный анализ устойчивости хранилища данных GreenPlum к эффектам ИД, путём обработки журналов событий с использованием авторегрессионной модели ARIMA для прогнозирования времени выполнения запросов. Разработанное решение позволило оперативно оценить динамику рисков возникновения угроз ИБ ИГ в MPP-архитектуре GreenPlum в режиме реального времени. В рамках хакатона «Skolkovo Hack 2022» за данное исследование присуждено 1-е призовое место.

Исследование взаимодействия микросервисов выполнялось с использованием Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС на основе датасета DeepTraLog лаборатории ПО Университета Фудань (Шанхай). Целью являлось обна-

ружение и количественная оценка аномалий функционирования РИС, аналогичных эффектам ИД. Исследована динамика межсервисного взаимного влияния всех видов и типов в РИС (рисунок 5). Выявлено, что эффекты ИД проявятся после 12.12.2021.



а) б)

Рисунок 5 – Результаты исследования динамики межсервисного взаимного влияния всех видов и типов в РИС
а) с 05.08.2021 по 14.09.2021. б) с 17.11.2021 по 26.12.2021.

На рисунке 6 представлены результаты исследования вирусной активности на основе эпидемиологической SEIR модели с учетом антропоморфических эффектов взаимодействия вредоносного программного обеспечения. Использование предложенных решений, экспериментальным путем подтвердило наличие эффектов взаимной компенсации ДВ ИГ при увеличении числа вирусных активностей.

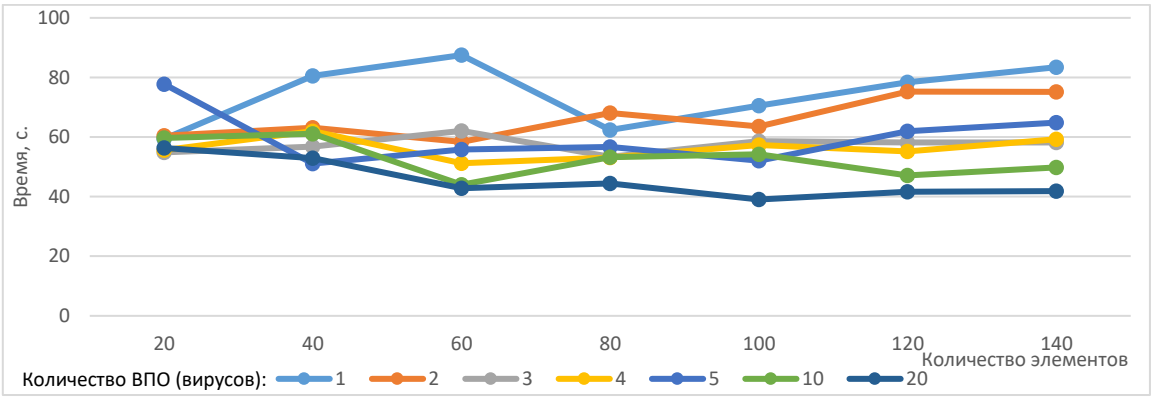


Рисунок 6 – Усреднённые показатели времени реакции и восстановления системы на ДВ ИГ

Таким образом при более 5 одновременных ДВ не имеет смысла в дальнейшем наращивать производительность средств защиты ИС. Система сама справляется с большим количеством деструктивных воздействий вирусов за счет наличия эффектов ИД.

Проанализированы данные журналов событий вычислительного облачного кластера «Alibaba cloud» на предмет оценки угроз ИД. Результаты соответствуют заявленным.

Выполнено исследование распределённой системы распознавания лиц «Персона ID» на основе Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС. Рассмотрены три различных сценария работы системы.

Сценарий 1. Обработка данных в системе происходит с помощью одного сервиса. Недостаточная производительность системы.

Сценарий 2. Обработка данных в системе происходит с помощью трех сервисов. Производительность обработки данных достаточная. Сервисы не мешают друг другу.

Сценарий 3. Обработка данных в системе происходит с помощью семи сервисов. Производительность обработки данных достаточная. В целом система работает не стабильно.

На рисунках 7–8 продемонстрировано ухудшение производительности системы в зависимости от различных сценариев её функционирования. На основании проведённого анализа сделан вывод о причинах, способных инициировать проявление эффектов ИД.

На рисунке 9 представлена диаграмма, из которой следует, что наибольшее значение ДВ ИГ оказывает взаимодействие процессов сервиса обработки распознавания лиц «process.py», являющегося основным источником угрозы возникновения эффектов ДВ ИГ. В целях анализа, оценена динамика рисков ДВ ИГ, для системы распознавания лиц. Для этого выполнены диаграммы, приведённые на рисунках 10–12. Из представленных зависимостей видно, что по мере усиления отрицательного взаимодействия сервисов происходит рост рисков проявления эффектов ДВ ИГ. Это позволяет сделать следующие выводы: эффекты ИД можно прогнозировать, анализируя динамику положительных, нейтральных и отрицательных межсервисных взаимодействий в РИС и их тренды; использование антропоморфических типов для анализа поведенческой активности предоставляет новый взгляд на оценку характеристик РИС; выявление негативных межсервисных взаимодействий на ранних этапах способствует предотвращению реализации тактики «T1499. Отказ в обслуживании» (по классификации MITRE ATT&CK), которая в рассматриваемом случае возникает из-за неправильной настройки системы. Применение метода оценки эффектов ДВ ИГ в составе Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС позволило повысить наблюдаемость поведенческих характеристик процессов РИС, что увеличивает точность выявления скрытых синергетических эффектов, приводящих к неконтролируемому саморазрушению инфраструктуры системы более чем на 11%.

Основным научным результатом, изложенным в четвертом разделе, является разработка методики и реализация программно-аналитического комплекса оценки угроз ИБ ИГ в сервис-ориентированных ИС.

Частными научными результатами, изложенными в четвертом разделе, являются: факторы развития ИД, критерии оценки эффективности работы сервиса ИС с позиции ИД, программно-аналитический комплекс для оценки и прогнозирования эффектов ДВ ИГ.

Основное содержание раздела и полученных научных результатов изложено в работах автора [1, 8, 9, 10, 16, 19, 21, 22, 23].

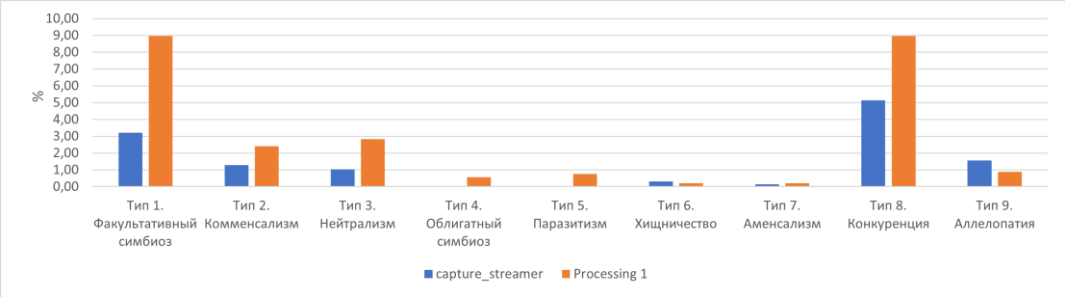


Рисунок 7 – Результат взаимного влияния сервисов системы для сценария 1

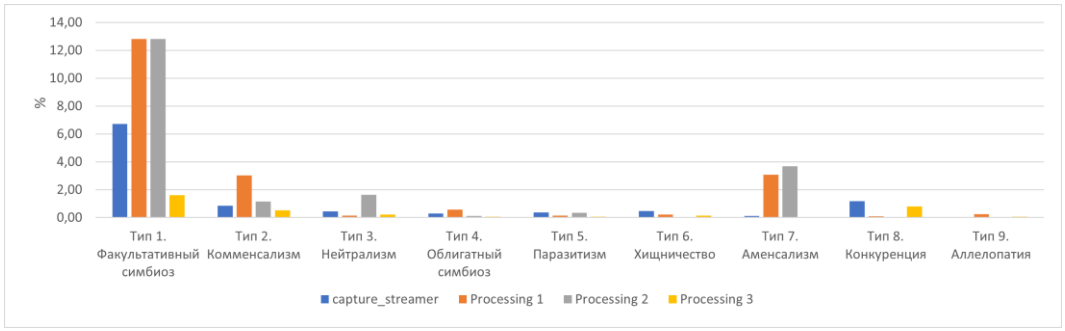


Рисунок 8 – Результат взаимного влияния сервисов системы для сценария 2

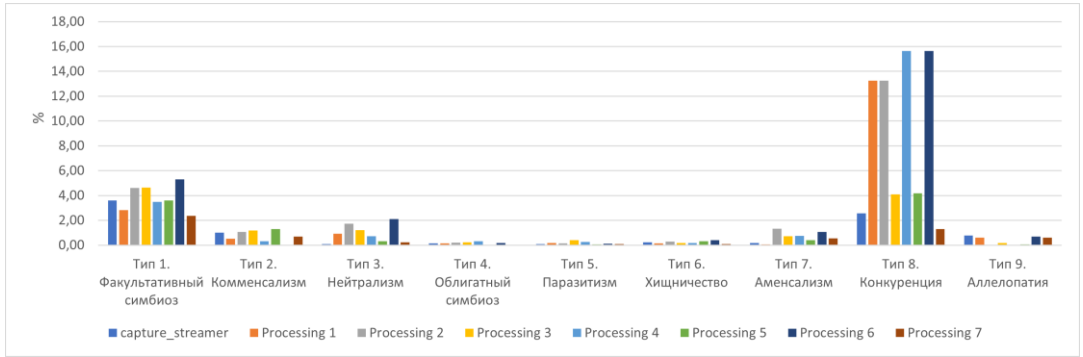


Рисунок 9 – Результат взаимного влияния сервисов системы для сценария 3

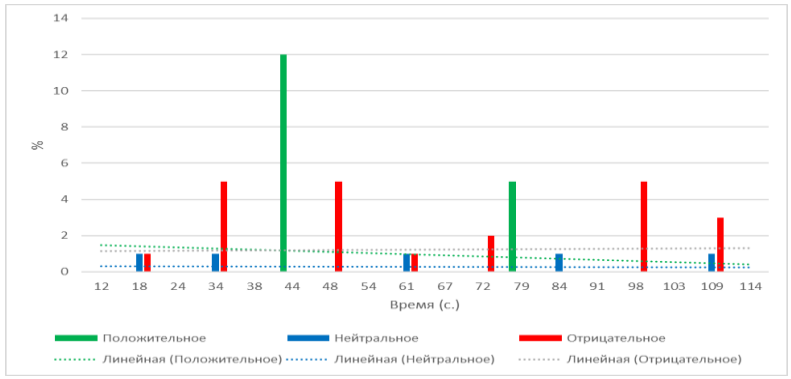


Рисунок 10 – Результат оценки динамики рисков ИД для сценария 1

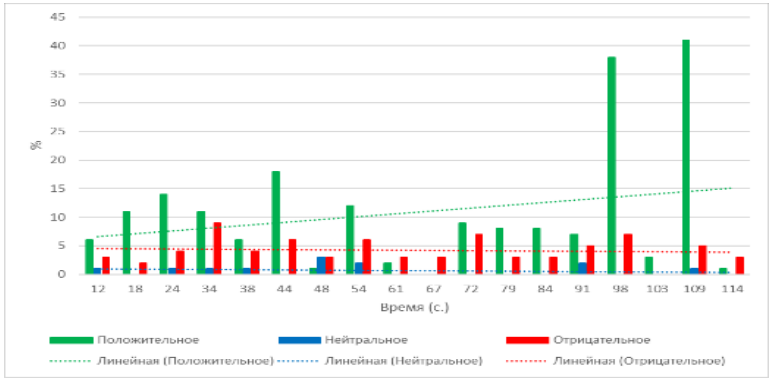


Рисунок 11 – Результат оценки динамики рисков ИД для сценария 2

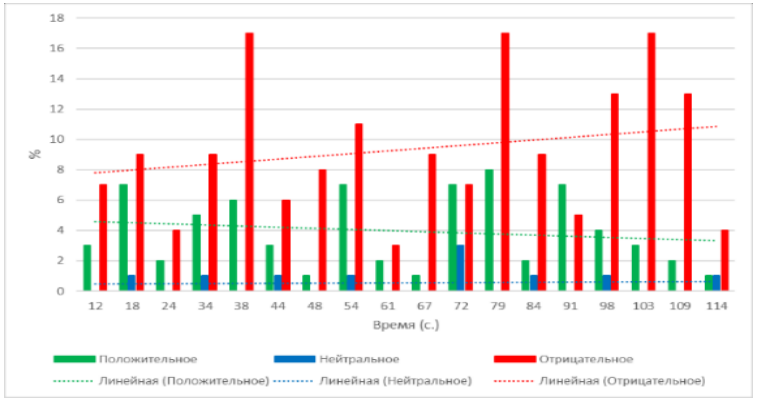


Рисунок 12 – Результат оценки динамики рисков ИД для сценария 3

ЗАКЛЮЧЕНИЕ

В работе исследовались эффекты деструктивного воздействия инфраструктурного генеза в распределенных информационных системах на предмет моделей и методов оценки влияния эффектов деструктивного воздействия инфраструктурного генеза. В соответствии с научной (научно-технической) задачей, связанной с разработкой моделей и методов, позволяющих выявлять, анализировать и количественно оценивать эффекты деструктивного воздействия инфраструктурного генеза в сервис-ориентированных информационных системах в условиях инфраструктурного деструктивизма, а также с целевой установкой решены следующие задачи: исследованы проблемы обеспечения безопасности в распределенных информационных системах; разработан комплекс моделей взаимодействия сервисов информационных систем для обнаружения эффектов деструктивного воздействия инфраструктурного генеза; разработаны методы оценки эффектов деструктивного воздействия инфраструктурного генеза; разработана методика выявления угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах.

В ходе решения указанных задач были получены следующие основные научные результаты, выносимые на защиту:

1) комплекс антропоморфических моделей взаимодействия сервисов ИС;

2) метод оценки эффектов деструктивного воздействия инфраструктурного генеза;

3) методика выявления угроз ИБ инфраструктурного генеза в сервис-ориентированных ИС.

Полученные результаты являются достоверными, обладают необходимой степенью новизны, имеют теоретическую ценность и практическую значимость, апробированы и опубликованы в 28-ми научных трудах.

Кроме того, в работе получен ряд частных научных результатов, а именно: формальное описание феномена инфраструктурного деструктивизма в распределенных информационных системах; модель обнаружения эффектов ДВ ИГ сервисов информационных систем; классификация антропоморфических типов состояний объектов информационных систем для комплекса эпидемиологических моделей распространения вирусов; агентная модель системы обнаружения и прогнозирования возникновения источников угроз инфраструктурного генеза; оценка старения распределенных информационных систем с позиции ИД (накопление «деструктивного мусора»); расширение рекомендательной системы по профилактике и предотвращению ИД; факторы развития ИД; критерии оценки эффективности работы сервиса ИС с позиции ИД; программно-аналитический комплекс для оценки и прогнозирования эффектов ДВ ИГ.

Совокупность полученных результатов свидетельствует о достижении поставленной цели исследования – повышение оперативности и точности выявления эффектов деструктивного воздействия инфраструктурного генеза в распределенных информационных системах.

Полученные научные результаты, по итогам внедрения их на базе профильных организаций, рекомендуются для разработки и реализации системы мероприятий по профилактике и предотвращению инфраструктурного деструктивизма в РИС, в том числе в распределённых системах ситуационного мониторинга. К числу очевидных преимуществ в данном контексте относятся: повышение точности выявления скрытых синергетических эффектов ИД в среднем на 10–15%, автоматизация управления инфраструктурными процессами в условиях деструктивного воздействия инфраструктурного генеза, а также увеличение оперативности обнаружения эффектов инфраструктурного деструктивизма в сервис-ориентированных ИС за счёт автоматизации процедур анализа журналов событий.

Полученные научные результаты по итогам внедрения в образовательный процесс высшего учебного заведения ФГБОУ ВО «МИРЭА – Российский технологический университет» рекомендуются для проактивного развития образовательных траекторий на всех уровнях УГСиНП 10.00.00 и контекстного изменения связей с профессиональными стандартами.

Исследования в данной предметной области могут быть продолжены по следующим направлениям:

Во-первых, разработка моделей киберзащиты РИС с учетом антропоморфизма деструктивных воздействий инфраструктурного генеза представляет инновационный проактивный подход, где уязвимости инфраструктурного генеза и их антропоморфные свойства применяются как механизмы защиты.

Во-вторых, в развитии классификации угроз инфраструктурного генеза заключаются в создании многоуровневой иерархической системы, интегрирующей поведенческий, структурный и временной анализ межсервисных взаимодействий РИС.

В-третьих, возможность адаптации методики выявления угроз ИБ инфраструктурного генеза к различным типам и классам РИС, включая микросервисные, веб-сервисные системы, ИС с сервисным реестром, корпоративные сервисные шины и другие варианты архитектур.

В-четвертых, автоматизированное определение приоритетов критических сервисов по уровню уязвимости к угрозам ИБ инфраструктурного генеза, адаптивное управление показателями качества обслуживания, разработка механизма защитного отключения сервисов, формализация отчётности об инцидентах ИБ с анализом причинно-следственных связей на основе антропоморфических типов взаимодействия, а также масштабирование метода оценки деструктивных воздействий инфраструктурного генеза в кластерных виртуальных (облачных) средах с применением федеративной оценки.

В-пятых, развитие метода оценки эффектов деструктивного воздействия инфраструктурного генеза, направленного на формирование индикаторов компрометации, предполагает агрегирование многомерных метрик, включая метрику оценки «деструктивного мусора», метрику «здоровья» инфраструктуры и ряд других показателей.

В-шестых, развитие метода оценки эффектов деструктивного воздействия направлено на повышение уровня информационной безопасности распределённых информационных систем по количественным показателям, включая полноту выявления источников угроз деструктивного воздействия генеза.

Выполнение перспективных исследований по перечисленным направлениям позволит создать дополнительные возможности для решения задач обеспечения безопасности ИС на уровне межсервисного взаимодействия и по всем аспектам ИБ.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых научных изданиях, рекомендованных ВАК

1. Русаков, А.М. Проактивная оценка динамики рисков инфраструктурного деструктивизма для распределенной системы распознавания лиц / Е.А. Максимова, А.М. Русаков // Защита информации. Инсайд. – 2025. – № 4(124). – С. 66-71.

2. Русаков, А.М. Исследование интеллектуальных методов анализа журналов событий для обеспечения информационной безопасности / А.М. Русаков, А.И. Бобырь-Бухановский // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2025. – №06/2. – С. 180-186.

3. Русаков, А.М. Прогнозирование рисков инфраструктурного деструктивизма с помощью антропоморфического подхода для сервисной архитектуры / А.М. Русаков // Защита информации. Инсайд. – 2025. – № 2(122). – С. 32-37.

4. Русаков, А.М. Алгоритмическая реализация модели оценки эффектов инфраструктурного деструктивизма информационно-технологической инфраструктуры / А.М. Русаков // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2025. – № 1. – С. 121-128.

5. Русаков, А.М. Концептуальная модель и схема организации архитектуры системы прогнозирования эффектов инфраструктурного деструктивизма / А.М. Русаков // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2025. – № 1. – С. 129-137.

6. Русаков, А.М. Комплекс антропоморфических моделей поведенческого анализа процессов для обнаружения эффектов инфраструктурного деструктивизма / А.М. Русаков // Инженерный вестник Дона. – 2024. – № 11(119). – С. 391-404.

7. Русаков, А.М. Анализ современного состояния исследований в области автоматизации мониторинга информационной безопасности сетей промышленного Интернета вещей с использованием технологий искусственного интеллекта / А.М. Русаков, Е.П. Болгар, Е.С. Иванов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2024. – № 12. – С. 114-118.

8. Русаков, А.М. Интеллектуальный анализ работы хранилища данных Greenplum на основе обработки лог-файлов / А.М. Русаков, Д.С. Горин, А.С. Лисютенко [и др.] // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6. – С. 142-149.

9. Разработка анализатора надежности веб-приложения на основе моделирования сетевых атак / А.М. Русаков, В.В. Филатов, С.С. Долженков [и др.] // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 7-2. – С. 105-112.

Публикации в изданиях, входящих в международные базы цитирования

10. Maksimova E.A., Rusakov A.M. Assessment Dynamics Risks Infrastructural Genesis at Critical Information Infrastructure Facilities. In: Lapina, M., Raza, Z., Tchernykh, A., Sajid, M., Zolotarev, V., Babenko, M. (eds) AISMA-2024: International Workshop on Advanced Information Security Management and Applications. AISMA 2024. Lecture Notes in Networks and Systems, – Vol. 863. Springer, Cham. – P. 257–266.

11. Maksimova E.A., Rusakov A.M. Anthropomorphic Model of States of Subjects of Critical Information Infrastructure Under Destructive Influences / E.A. Maksimova, A.M. Rusakov, M.A. Lapina, V.G. Lapin // Lecture Notes in Networks and Systems. – 2022. – Vol. 424. – P. 569-580.

Свидетельства о результатах интеллектуальной деятельности

12. Свидетельство о государственной регистрации программы для ЭВМ № 2025614582 РФ. Интеллектуальная система поведенческого анализа процессов в информационно-технологической инфраструктуре на основе антропоморфических типов взаимодействия: заявл. 12.02.2025: опубл. 24.02.2025 / А.М. Русаков.

13. Свидетельство о государственной регистрации программы для ЭВМ № 2024660851 РФ. «Программное обеспечение для оценки рисков информационной безопасности на основе интеллектуального анализа данных репозитория исходного кода»: № 2024618977: заявл. 18.04.2024: опубл. 14.05.2024 / А.М. Русаков, В.В. Филатов, А.М. Коробкова [и др.].

14. Свидетельство о государственной регистрации программы для ЭВМ № 2023683184 РФ. Антропоморфическая система моделирования деструктивных воздействий инфраструктурного генеза на объектах критической информационной инфраструктуры: № 2023682500: заявл. 24.10.2023: опубл. 03.11.2023 / А.М. Русаков.

15. Свидетельство о государственной регистрации программы для ЭВМ № 2023665252 РФ. Программа для анализа веб-приложения на уязвимости на основе интеллектуального моделирования сетевых атак: № 2023664031: заявл. 30.06.2023: опубл. 13.07.2023 / А.М. Русаков, Д.Д. Голубев, Д.А. Сараев [и др.].

16. Свидетельство о государственной регистрации программы для ЭВМ № 2023684208 РФ. Система оценки рисков деструктивного воздействия инфраструктурного генеза на субъекте критической информационной инфраструктуры: № 2023682379: заявл. 24.10.2023: опубл. 14.11.2023 / А.М. Русаков.

17. Свидетельство о государственной регистрации программы для ЭВМ № 2023683299 РФ. Средство реализации рекомендательной системы для профилактики и предотвращения инфраструктурного деструктивизма на субъекте критической информационной инфраструктуры: №2023682485: заявл. 24.10.2023: опубл. 07.11.2023 / А.М. Русаков.

18. Свидетельство о государственной регистрации программы для ЭВМ № 2023683475 РФ. Эпидемиологическая система моделирования оценки рисков динамики межобъектного влияния в условиях инфраструктурного деструктивизма: №2023682859: заявл. 24.10.2023: опубл. 08.11.2023 / А.М. Русаков.

19. Свидетельство о государственной регистрации программы для ЭВМ № 2022685869 РФ. Программное обеспечение системы моделирования межобъектных системных связей инфраструктурного характера в информационных системах: № 2022685248: заявл. 15.12.2022: опубл. 28.12.2022 / А.М. Русаков.

20. Свидетельство о государственной регистрации программы для ЭВМ № 2022683265 РФ. Программное обеспечение для гарантированного качества обслуживания в программно-конфигурируемых распределенных информационных системах: № 2022682346: заявл. 14.11.2022: опубл. 02.12.2022 / А.М. Русаков, Р.А. Раманцев, Е.К. Джлавян [и др.].

Публикации в других изданиях

21. Русаков, А.М. Прогнозирование рисков инфраструктурного деструктивизма на основе анализа журналов событий облачной платформы Openstack / А.М. Русаков // Актуальные проблемы прикладной математики, информатики и механики: Сборник трудов Международной научной конференции, Воронеж, 02–04 декабря 2024 года. – Воронеж: Научно-исследовательские публикации, 2025. – С. 955-960.

22. Русаков, А.М. Исследование сервиса на наличие эффекта инфраструктурного деструктивизма на примере датасета «DVD RENTAL» для базы данных PostgreSql / А.М. Русаков // Кибернетика и информационная безопасность «КИБ-2024»: Сборник научных трудов Второй Всероссийской научно-технической конференции, Москва,

22–23 октября 2024 года. – Москва: Национальный исследовательский ядерный университет «МИФИ», 2024. – С. 188-189.

23. Русаков, А. М. Анализ динамики рисков деструктивного воздействия инфраструктурного генеза / А. М. Русаков // Кибербезопасность: технические и правовые аспекты защиты информации: Сборник научных трудов I Национальной научно-практической конференции, Москва, 24–26 мая 2023 года. – Москва: МИРЭА – Российский технологический университет, 2023. – С. 85-87.

24. Русаков, А.М. Эпидемиологическая модель оценки динамики рисков информационной безопасности инфраструктурного генеза / А.М. Русаков // Студенческая наука для развития информационного общества: Материалы XV Всероссийской научно-технической конференции с приглашением зарубежных ученых, Ставрополь, 28 ноября 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2023. – С. 257-269.

25. Русаков, А.М. Оценка рисков деструктивных воздействий инфраструктурного генеза на основе спектральной теории графов / А.М. Русаков // Кибернетика и информационная безопасность «КИБ-2023»: Сборник научных трудов Всероссийской научно-технической конференции, Москва, 18–19 октября 2023 года. – Москва: Национальный исследовательский ядерный университет «МИФИ», 2023. – С. 84-85.

26. Русаков, А.М. Исследование структурных свойств информационных систем на основе спектральной теории графов / А.М. Русаков, Н.А. Юшкова // Наукосфера. – 2023. – № 6-1. – С. 192-199.

27. Русаков, А.М. Результаты проекта «Оценка динамики рисков деструктивного воздействия инфраструктурного генеза» / А.М. Русаков // Сборник трудов III Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ, 25-27 октября 2023 г. – М., 2023. – С. 202-208.

28. Русаков, А.М. Разработка модели динамики рисков деструктивного воздействия инфраструктурного генеза / А.М. Русаков // Сборник трудов II Всероссийской научной школы-семинара «Современные тенденции развития методов и технологий защиты информации». Москва, МТУСИ, 22-24 октября 2022 г. – М., 2022. – С. 97-103.

Подписано в печать 05.02.2026. Формат 60×84 1/16.
1,0 а.л. Тираж 100 экз.

Отпечатано в СПбГУТ, 193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1