МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ (МИНОБРНАУКИ РОССИИ)
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«МИРЭА – Российский технологический университет»

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

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель:
доктор технических наук, доцент
Максимова Елена Александровна

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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 комплексом мер, 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, 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, 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.

Достижение поставленной цели потребовало решение следующих **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, учитывающий антропоморфические особенности взаимодействия сервисов в распределенных информационных системах;

2) впервые разработан метод оценки эффектов деструктивного воздействия инфраструктурного генеза, основанный на антропоморфическом подходе, к исследованию 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.

1 ИССЛЕДОВАНИЕ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Принципы построения, проектирования и эксплуатации распределенных информационных систем

В современном мире распределённые информационные системы (РИС) приобретают всё большую значимость, где рост объёмов данных и потребности в высокой производительности требуют новых подходов к их обработке и хранению. Такие системы обеспечивают масштабируемость, отказоустойчивость и гибкость, позволяя эффективно распределять вычислительные задачи и ресурсы между различными физически разнесёнными узлами. Благодаря этому, они способны поддерживать непрерывность работы и отказоустойчивость, быстро адаптироваться к изменениям и обеспечивать устойчивый доступ (доступность) к информации.

Важным аспектом функционирования РИС является обеспечение их безопасности. В условиях распределённой архитектуры предъявляются высокие требования к защите данных, контролю доступа, целостности и доступности информации, так как уязвимости в одной части системы могут повлиять на всю её ИТ-инфраструктуру [95]. Надёжная система безопасности в РИС становится краеугольным камнем доверия пользователей и гарантирует сохранность конфиденциальных и критически важных данных при одновременном сохранении высокого уровня доступности и производительности. Таким образом, безопасность и эффективность РИС являются ключевыми факторами успешного внедрения и эксплуатации современных ИТ-инфраструктур.

Определение. Распределённая информационная система (РИС) — это информационная система, объекты данных и/или процессы которой физически распределены на две или более компьютерные системы и функционируют в составе единой ИТ-инфраструктуры, включающей программно-аппаратные ресурсы, коммуникационные средства и организационные компоненты, обеспечивающие взаимодействие, хранение, обработку и передачу информации для удовлетворения

информационных потребностей пользователей и поддержки деятельности организации.

При введении определения РИС возникли сложности при выборе государственных стандартов, в которых это определение дано наиболее полным образов. В [27] содержится только базовое определение РИС как информационная система (ИС), объекты данных и/или процессы которой физически распределены на две или более компьютерные системы. В [30, 36] описаны стандарты в области мониторинга и безопасности РИС, где рассматриваются РИС в контексте интеграции и управления, но нет описаний архитектур и принципов функционирования РИС. В [40] дан комплекс стандартов на автоматизированные системы, где регламентируются части, связанные с автоматизированными системами и включающие понятия о РИС без акцента на технические особенности.

Понятия микросервисов и микросервисной архитектуры в контексте РИС и облачных вычислений, наиболее полно обозначены в [41, 42], однако также нуждаются в уточнении. В настоящий момент в Российской Федерации РИС используют современные технологические решения с географическим распределением компонентов (так как имеют большую территориальную распределённость), с микросервисной архитектурой и высокими требованиями к отказоустойчивости и масштабируемости. Следует отметить, что, используя предложенное определение РИС, например «компьютерный класс» можно также считать распределённой системой, если его компоненты (компьютеры, сети, серверы, программное обеспечение) физически распределены по разным местам и взаимодействуют друг с другом в рамках единой ИТ-инфраструктуры. В настоящий момент примерами наиболее важных РИС с точки зрения их безопасности являются порталы крупных социальных сетей, единый портал государственных и муниципальных услуг (Госуслуги), единая региональная автоматизированная информационная система поддержки деятельности многофункциональных центров предоставления государственных и муниципальных услуг (ЕРАИС МФЦ) и другие.

Далее определим понятие информационно-технологической (ИТ) инфраструктуры.

Определение. Информационно-технологическая инфраструктура (далее – ИТ-инфраструктура) — это совокупность всех аппаратных, программных, сетевых, коммуникационных и сервисных компонентов (объектов), которые обеспечивают функционирование и поддержку информационных технологий в организации, предприятии, государственной структуре, промышленном производстве, и других областях [34, 208].

Следует отметить, что также часто встречается определение «информационная инфраструктура». Эти два определения не эквивалентны между собой.

Определение. Информационная инфраструктура — это совокупность систем, сетей и сервисов, которые поддерживают сбор, обработку, хранение, передачу и доступ к информации [67].

Таким образом, инфраструктура является одним из ключевых факторов развития общества, без нее нельзя представить осуществление повседневной деятельности, она образует целые информационные пространства сама по себе и играет важнейшую роль в повышении уровня и качества жизни каждого человека [80].

Определение. Инфраструктура — комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и обеспечивающих основу функционирования системы [80].

Данный термин имеет разнообразное значение в зависимости от области его применения. Для предметной области информационной безопасности наиболее применимо определение понятия ИТ инфраструктуры.

Определение ИТ-инфраструктуры является более общим по отношению к определению информационная инфраструктура. Таким образом определение ИТ-инфраструктуры включает в себя также и определение информационной инфраструктуры. В данной работе будем исследовать безопасность информации для РИС и их ИТ-инфраструктур.

На сегодняшний момент устойчивое и безотказное функционирование РИС особенно актуально в рамках национальной проекта «Экономика данных и цифровая трансформация государства» [107, 175], состоящего из федеральных проектов:

1) инфраструктура доступа к информационно-телекоммуникационной сети «Интернет»;

2) цифровые платформы в отраслях социальной сферы;

3) искусственный интеллект;

4) цифровое государственное управление;

5) отечественные решения;

6) прикладные исследования и перспективные разработки;

7) инфраструктура кибербезопасности;

8) кадры для цифровой трансформации;

9) государственная статистика.

В данных проектах РИС выступают в виде базовой основы, на которой строятся компоненты основной системы.

Определение. Сетевая инфраструктура — это совокупность аппаратных, программных и коммуникационных компонентов, которые обеспечивают передачу данных, связь и взаимодействие между устройствами и системами в пределах одной или нескольких сетей [183].

Следует отметить, что определение сетевой инфраструктуры входит в определение ИТ-инфраструктуры и информационной инфраструктуры.

Для проекта «Национальной системы цифрового рубля» (ЦР) безопасность РИС является основополагающей [130]. С 1 июля 2025 года должна появиться РИС для работы с ЦР для крупных кредитных организаций. Предполагается, что в 2025–2027 годах произойдёт тиражирование ЦР [185].

В банковском секторе согласно положению Положение Банка России № 716-П от 08.04.2022 вводится понятие платежной инфраструктуры ИС.

Определение. Платежная инфраструктура ИС — это совокупность организаций и процессов ИС, обеспечивающих обработку и передачу платёжной информации от плательщика к получателю денег [35, 118, 119].

Помимо проекта «Национальной системы цифрового рубля» (ЦР) платежная инфраструктура используется для организации банковской деятельности. Платежная система как инфраструктура финансового рынка обеспечивает клиринг,

расчёты и учёт по денежно-кредитным и другим финансовым операциям, таким как платежи, ценные бумаги и контракты по производным инструментам [172].

Отдельным важным аспектом информационной безопасности РИС является использование их для построения критической информационной инфраструктуры (КИИ).

Определение. Критическая информационная инфраструктура (КИИ) — совокупность ИС и/или телекоммуникационных сетей, критически важных для работы ключевых сфер жизнедеятельности государства и общества: здравоохранения, промышленности, связи, транспорта, энергетики, финансового сектора и городского хозяйства [177].

Объекты критической информационной инфраструктуры (КИИ) — это также ИС, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Безопасность КИИ в основном регламентируется следующими нормативным документом: Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ [177]. Категорирование объектов КИИ осуществляется исходя из требований, которые прописаны в ФЗ-187, ПП РФ № 127 и приказах ФСТЭК № 235, 239 и 236. Нормативно-правовая база обеспечения безопасности КИИ постоянно совершенствуется и предъявляются всё более жесткие требования. Постоянно разрабатываются новые подходы по обеспечению безопасности КИИ [85].

Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие ИС, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА) — информационная система в Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных РИС и иных ИС [128]. Главным оператором системы является Минцифры России [128] при поддержке [124] и [179] РИС имеют главенствующую

роль для обеспечения национальной безопасности Российской Федерации. Также обеспечение безопасности РИС весьма необходимо при поддержке электронных медицинских РИС [123].

На фоне повсеместного продолжающегося импортозамещения особенно важным является обеспечение безопасности РИС промышленного сегмента [121]. Обеспечение безопасности РИС промышленного сегмента требует комплексного подхода, учитывающего специфику технологических процессов, территориальную распределенность, разнообразие устройств и критичность работы систем. Работы в данном направлении ведутся в течении нескольких последних лет. Разрабатываются различные системы защиты отечественных РИС и их внедрения. Как указано в [72], к 2025-2027 планируется полностью заменить зарубежные ИС для критически важных областей на отечественные. Для этого активно развивается отечественный проект «Корпоративная ИТ-инфраструктура 2.0» [72] и др. Создан отдельный Интернет-проект по отечественным ИС и их ИТ-инфраструктур [73]. Все это показывает необходимости уделения особого внимания безопасности РИС и их ИТ-инфраструктур.

1.1.1 Архитектура и типы распределенного программного обеспечения

Архитектура и типы РИС определяются этапами своего развития. На каждом этапе происходили изменения, при этом разработанные технологии используются и сейчас. Опишем основные этапы развития РИС [57, 61, 104, 106] и по каждому этапу отдельно проанализируем особенности информационной безопасности как показано рисунке 1.

Разработанные технологии для каждого этапа развития РИС, приведенные на рисунке 1 до сих пор применяются на практике, но в видоизмененном виде. Например, технологии мейнфреймов получили свое развитие под видом технологии «тонкий клиент», принципы и наработки сохраняются до сих пор.

Под методами построения РИС будем понимать подходы и стратегии, используемые для проектирования, развертывания и управления ИТ-инфраструктурой, которая поддерживает работу организации.

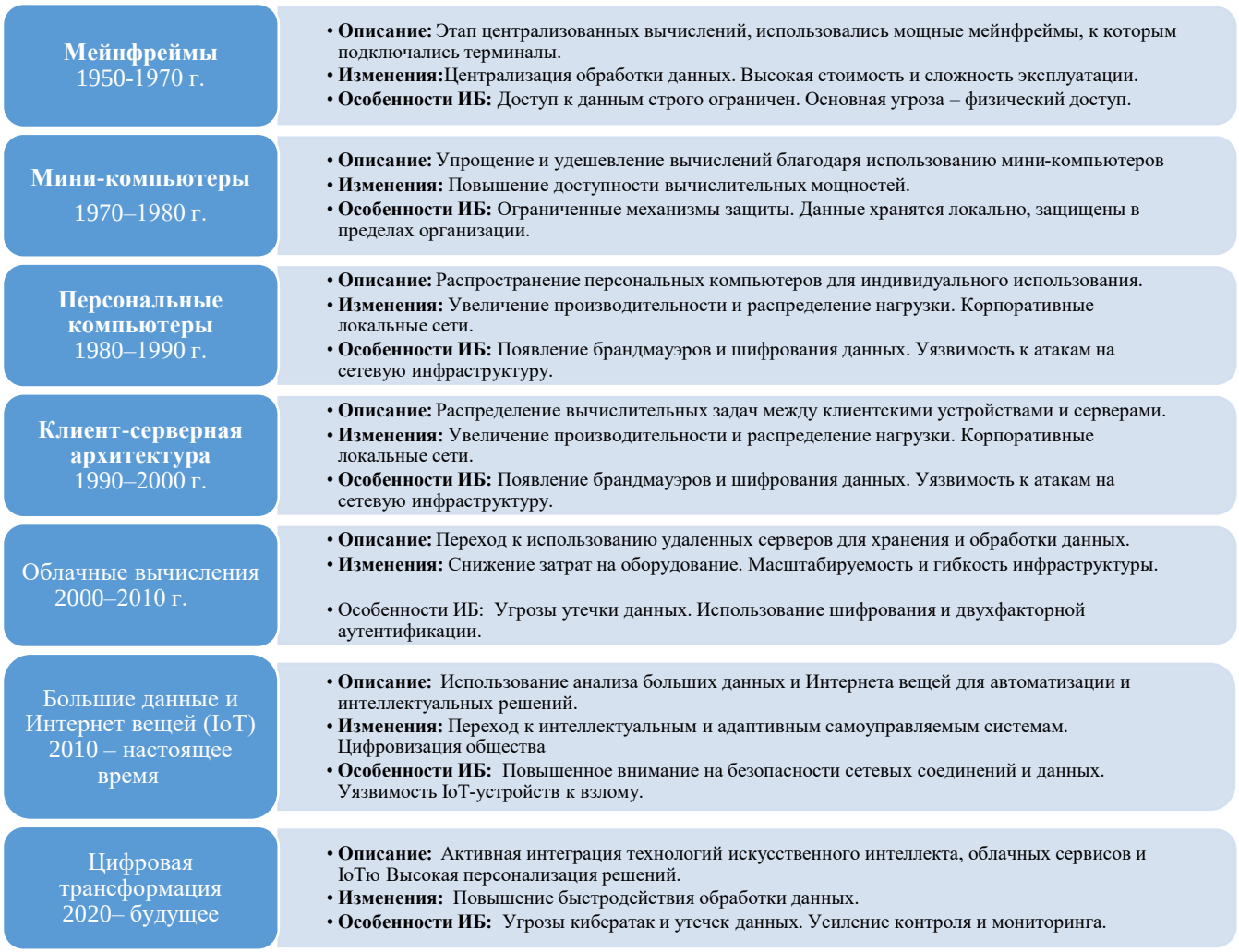

Рисунок 1 – Основные этапы развития распределенных информационных систем

При построении РИС не существует универсального решения [57]. Сценарий создания и проектирования ИС может меняться в зависимости от размеров организации, сферы деятельности, используемого программного обеспечения и приложений, наличия или отсутствия пиковых нагрузок, особенности хранения баз данных и многого другого.

По аналогии со схемой основных этапов развития РИС, представленной на рисунке 1. построим таблицу 1. содержащую основные методы построения РИС с указанием выявленных особенностей ИБ. Представленные методы построения РИС являются основными, но существуют и другие методы мене популярные методы: централизованная архитектура, монолитная архитектура, динамическая архитектура [180] и другие. Данные методы построения РИС, менее распространены и в настоящее время мало используются.

Таблица 1 – Методы построения РИС с указанием выявленных особенностей ИБ

Метод построения РИС	Описание	Преимущества	Недостатки	Примеры использования	Особенности ИБ
Традиционный	Физические серверы, коммутаторы и маршрутизаторы размещаются в дата-центре или офисе.	Простота реализации. Прямой контроль над оборудованием.	Высокие капитальные затраты. Ограниченная гибкость.	Малый бизнес. Небольшие офисы.	Высокая защита физического доступа. Угрозы сбоя оборудования, атаки на локальную сеть.
Виртуализация	Создание нескольких виртуальных машин на одном физическом сервере.	Экономия ресурсов. Простота масштабирования.	Требует мощности физического оборудования. Зависимость от гипервизора.	Облачные платформы. Корпоративные сети.	Уязвимость гипервизоров. Использование сетевых экранов и антивирусов.
Контейнеризация	Использование контейнеров (Docker, Kubernetes) для изоляции приложений и их ресурсов.	Быстрое развертывание. Упрощение разработки и тестирования.	Требует навыков работы с контейнерами. Менее эффективна при ресурсозатратных приложениях.	Разработка микросервисов. DevOps-процессы.	Полная изоляция контейнеров. Угрозы: атаки на внутренние процессы контейнеров.
Инфраструктура как код (IaC)	Использование кода для автоматического развертывания и управления инфраструктурой.	Автоматизация процессов. Минимизация человеческого фактора.	Требует значительных затрат на первоначальную настройку.	Компании с частыми изменениями инфраструктуры.	Безопасность скриптов и конфигураций. Угрозы: уязвимости в программном коде.
Гиперконвергентная	Интеграция вычислений, хранения и сетей в одном устройстве или программной платформе.	Удобство управления. Масштабируемость.	Высокая стоимость. Сложность модернизации.	Компании, разворачивающие частные облака.	Комплексная защита на уровне оборудования и ПО.
Децентрализованная	Инфраструктура, где управление и ресурсы распределены между множеством узлов.	Высокая отказоустойчивость. Независимость от центральных узлов.	Сложность управления. Требует продвинутого планирования.	Системы «Blockchain». Сети «Peer-to-peer».	Риски распределенных атак отказ в обслуживании (DDoS). Сложность обеспечения безопасности распределенных данных.

1.1.2 Анализ взаимодействия активных элементов распределенных информационных систем

Под способом организации РИС будем понимать вариант размещения оборудования, который выбирается в зависимости от размеров организации, сферы деятельности, географической распределённости оборудования, используемого программного обеспечения (далее – ПО), наличия пиковых нагрузок и других факторов. Выбор архитектуры ПО во многом определяет организацию и построение РИС. Различные варианты способов организации РИС представлены в таблице 2.

Таблица 2 – Способы организации РИС

Способ организации РИС	Описание	Преимущества	Недостатки	Примеры использования	Особенности ИБ
Локальная (On-Premises)	Вся инфраструктура находится на территории компании, включая серверы, хранилища и сети.	Полный контроль. Высокий уровень безопасности. Нет зависимости от интернета.	Высокая стоимость реализации и обслуживания. Ограниченная масштабируемость.	Банковский сектор. Государственные учреждения.	Физический контроль за доступом. Возможность внедрения кастомных решений ИБ.
Облачная (Cloud)	Используются удаленные серверы и услуги облачных провайдеров для хранения и обработки данных.	Гибкость. Масштабируемость. Платежи по мере использования.	Зависимость от интернета. Потенциальные риски утечки данных.	Стартапы. Компании с высокой динамикой роста.	Шифрование данных. Двухфакторная аутентификация. Зависимость от уровня безопасности поставщика услуг.
Гибридная (Hybrid)	Сочетание локальной инфраструктуры и облачных ресурсов.	Баланс между безопасностью и гибкостью. Оптимизация затрат.	Сложность управления. Необходимость интеграции двух сред.	Корпорации с распределенными офисами.	Комплексный подход к безопасности. - Шифрование при передаче данных между средами.
Мультиоблачная (Multi-Cloud)	Использование услуг нескольких облачных провайдеров для снижения рисков и увеличения надежности.	Отказоустойчивость. Независимость от одного провайдера.	Сложность интеграции и управления.	Крупные международные компании.	Сложные системы управления доступом. Риск ошибок в конфигурации безопасности.
Виртуальная (Virtualized)	Создание виртуальных серверов и сетей на физических машинах для оптимизации использования ресурсов.	Эффективность использования оборудования. Удобство управления.	Требует мощного оборудования. Может быть уязвима к атакам на гипервизоры.	Центры обработки данных (ЦОДы).	Безопасность зависит от гипервизора. Обязательное использование антивирусных решений.
Программно-определяемая (SDI)	Управление ресурсами через программные интерфейсы, минимизируя роль физического оборудования.	Централизованное управление. Высокая гибкость.	Требует высокой квалификации персонала.	Современные центры обработки данных.	Потребность в защите программных интерфейсов. Риски из-за человеческого фактора.

Под архитектурой ПО будем понимать структуру или высокоуровневый дизайн программной системы, который определяет, как её компоненты взаимодействуют друг с другом, с внешними системами, модулями, подпрограммами и пользователями. Это фундаментальный этап проектирования РИС, на котором принимаются ключевые технические и организационные решения, влияющие на весь жизненный цикл ПО. История развития архитектур ПО демонстрирует движение от простых, централизованных решений к более сложным и распределенным

системам, которые лучше справляются с масштабируемостью, гибкостью и скоростью изменений в современных условиях.

Основные этапы развития архитектур ПО представлены на рисунке 2.

Рисунок 2 – Основные этапы развития архитектур программного обеспечения

Рассмотренные основные типы архитектур ПО, представленные рисунке 2 могут применяться для одной РИС в любой комбинации. Таким образом, на практике часто довольно сложно классифицировать РИС только одним типом архитектуры, в этом случае обычно используют понятие сервис-ориентированной ИС.

Рассмотрим для примера архитектуру РИС представленную в [161] и вместе с ней её ИТ-инфраструктуру, содержащую наиболее часто используемые в настоящее время элементы: шлюз программного интерфейса, балансировщик нагрузки, очереди (брокеры) сообщений, объединение в кластер, технологии кеширования,

системы мониторинга, системы аналитики метрик, реляционные и не реляционные (NoSQL) базы данных. Очереди (брокеры) сообщений содержат элементы, которые принимают – «консумеры» и отправляют – «продюсеры» сообщения в определенном формате. Схема данной архитектуры РИС представлена на рисунке 3. Предложенный пример архитектуры РИС показывает, то, что с возрастанием сложности архитектуры становится также важным и межобъектное (межэлементное) взаимодействие, которое содержит особенности функционирования ИТ-инфраструктуры.

Межобъектное взаимодействие в ИТ-инфраструктуре, РИС предлагается рассматривать на нескольких независимых уровнях. Каждый из рассматриваемых уровней представляет собой различную степень абстракции и масштабируемости для РИС описанный в основном в [68, 97, 181]. Расположим данные уровни в порядке возрастания их сложности реализации.

Уровень низкоуровневого взаимодействия состоит из следующих элементов:

1) Процедурное программирование. Один из вариантов использования процедурного программирования, в которой взаимодействие происходит на уровне вызова различных методов и функций в различных частях программного кода [23, 163]. Также возможно использование в объектно-ориентированной парадигме программирования для выполнения методов взаимодействующих объектов [165].

2) Глобальные переменные и общий доступ к данным. Уровень взаимодействие через глобальные области данных (переменные). Основной целью которого является синхронизация работы при совместном выполнении задач. Например, паттерны программирования (паттерн «Наблюдатель») [181].

3) Обработка событий. Один объект может генерировать события (сигналы), а другие объекты – их обрабатывать [23]. Например, библиотеки и фреймворки событийного типа.

Уровень среднеуровневого взаимодействия состоит из следующих элементов РИС:

1) Модули и библиотеки РИС. Группировка объектов и классов в модули и библиотеки, обеспечивающая организацию кода и управление зависимостями [163, 174].

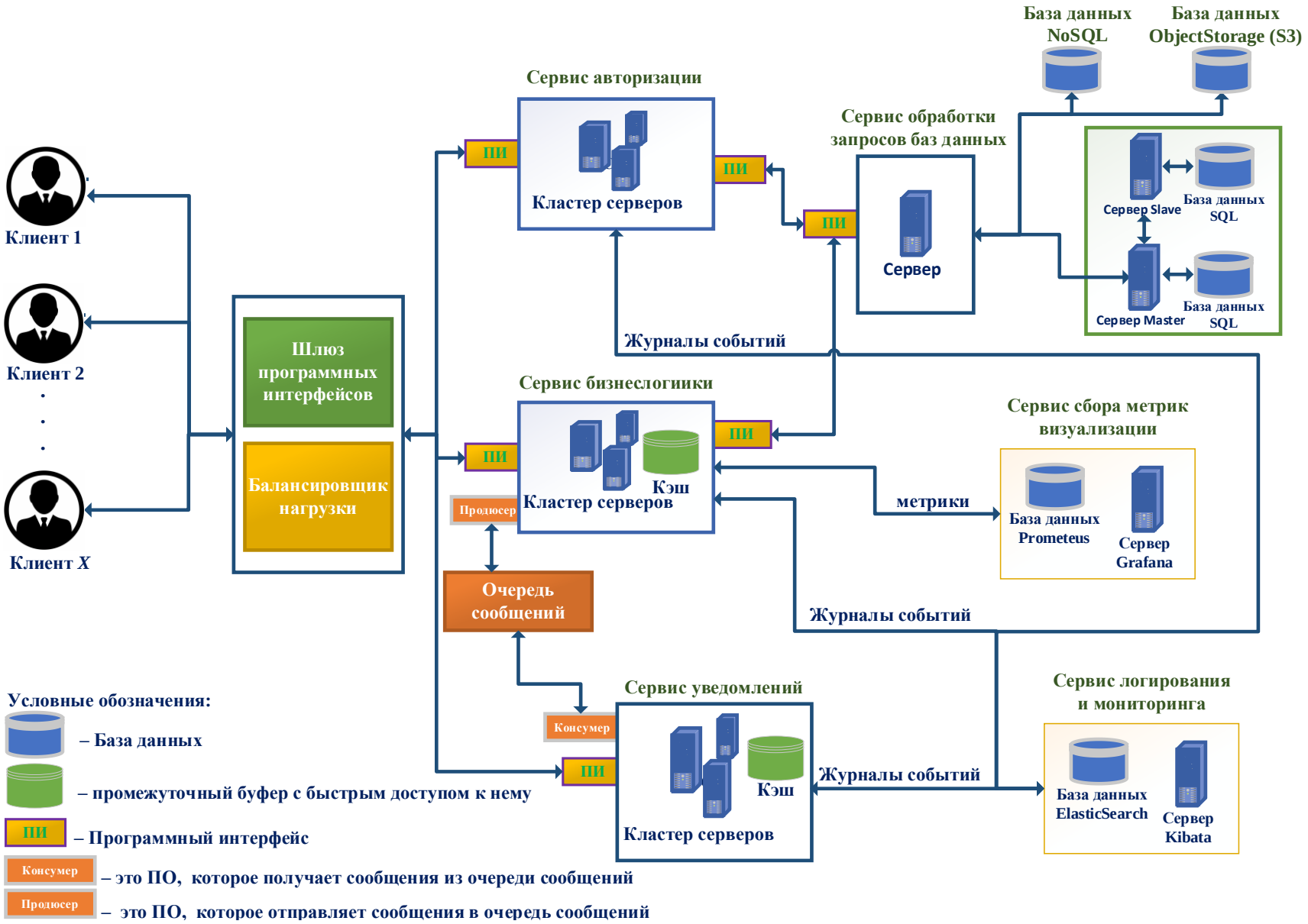

Рисунок 3 – Пример архитектуры распределенных информационной системы

2) Компоненты РИС. Более крупные строительные блоки РИС, которые могут включать несколько объектов и классов. Взаимодействие между компонентами обычно осуществляется через четко определенные интерфейсы [163].

3) Абстрактные классы и интерфейсы. Определяют контракты взаимодействия между объектами, обеспечивая стандартизацию и снижение зависимости от конкретной реализации [165].

Уровень высокоуровневого взаимодействия состоит из следующих элементов:

1) Программные интерфейсы РИС. Интерфейсы для взаимодействия между разными системами и приложениями [148, 211].

2) Сервисы РИС. В микросервисной архитектуре сервисы взаимодействуют друг с другом через сетевые протоколы [76, 108]. Каждый сервис представляет собой независимый компонент, который может быть разработан, развернут и масштабирован отдельно [219].

3) Сервис-ориентированная архитектура (SOA, Service-Oriented Architecture). Объединение сервисов для выполнения бизнес-функций [105]. Взаимодействие обычно осуществляется через ссервисную шину (ESB, Enterprise Service Bus).

Системный уровень состоит из следующих элементов РИС:

1) Интеграция программных систем РИС. Взаимодействие между разными РИС и приложениями в рамках одной организации или между организациями [105].

2) Межсетевое взаимодействие РИС. Взаимодействие между программными системами через интернет или другие сети, включая обмен сообщениями, синхронизацию данных и интеграцию сервисов [93, 108].

3) Оркестрация и управление рабочими процессами РИС. Управление взаимодействием между различными компонентами и системами для достижения бизнес-целей. и оркестрационные инструменты [219].

Межобъектное взаимодействие элементов в ИТ-инфраструктурах РИС предлагается группировать по уровню взаимодействия, способу реализации, типу взаимодействия и абстракции, данная классификация межобъектного взаимодействие элементов в ИТ-инфраструктурах РИС схематично показана на рисунке 4.

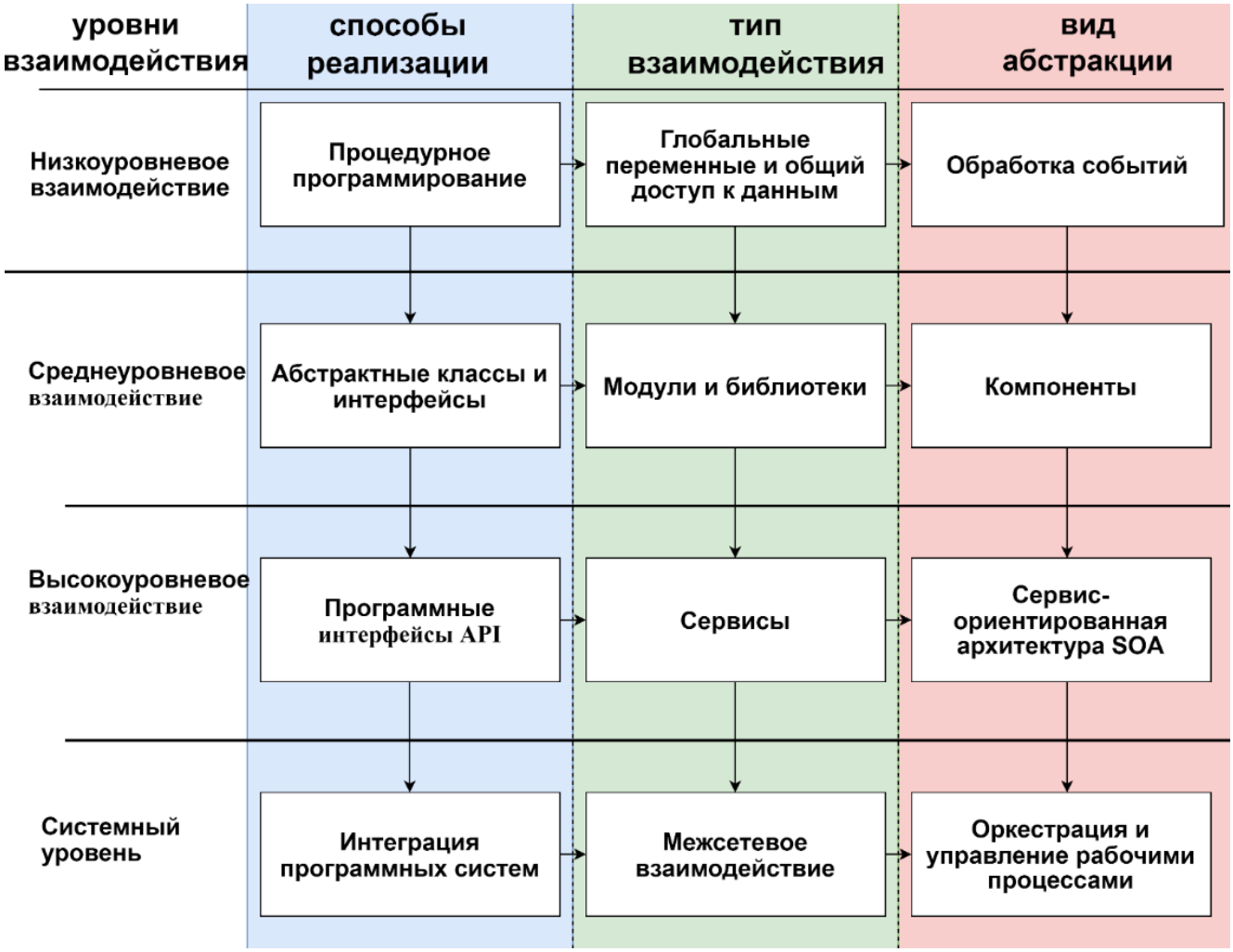

Рисунок 4 – Межобъектное взаимодействие элементов в ИТ-инфраструктурах РИС

В данном пункте не рассматриваются вопросы, связанные с взаимодействием уязвимостей в РИС. Таким образом, проведенный обзор и анализ уровней взаимодействия элементов ИТ-инфраструктур показал, недостаточную проработанность в области ИБ взаимодействия элементов РИС. То есть сами по себе элементы (объекты) РИС могут пройти проверки безопасности, но при этом появятся проблемы безопасности иного характера. В первую очередь, связанные с непредвиденными эффектами при взаимодействии элементов ИТ-инфраструктур РИС [127].

1.1.3 Безопасность программных интерфейсов информационных систем

Рассмотрим программные интерфейсы как точки входа в РИС с позиции обеспечения их ИБ.

Определение. Программный интерфейс (далее – ПИ, API – Application Programming Interface) — интерфейс, с помощью которого приложения, сервисы и программы обмениваются информацией [148, 211].

В таблице 3 показаны основные этапы развития технологий ПИ в РИС отражающая, год их создания, описание и соответствующие механизмы обеспечения информационной безопасности [116, 161, 199, 225].

Таблица 3 – Этапы развития технологий программных интерфейсов в РИС

Год создания	Название технологии	Описание технологии	Информационная безопасность (механизмы защиты)
1990 г.	SOAP (Simple Object Access Protocol)	Протокол для обмена структурированными сообщениями между компьютерами через HTTP или SMTP. Используется для сложных взаимодействий в РИС.	Использует WS-Security для защиты сообщений, шифрование и аутентификацию с помощью XML.
2000 г.	REST (Representational State Transfer)	Архитектурный стиль для построения API, использующий HTTP-методы. REST API стало стандартом для веб-сервисов, предлагая лёгкость и масштабируемость.	Шифрование данных через HTTPS, аутентификация через API-ключи или OAuth.
2010 г.	OAuth 2.0	Стандарт авторизации, позволяющий сторонним сервисам получать ограниченный доступ к защищённым данным без использования паролей.	Использует токены доступа, JWT, проверку подлинности через авторизационные серверы.
2010 г.	JSON-RPC	Протокол удалённого вызова процедур, основанный на JSON. Лёгкий и эффективный механизм для обмена данными между клиентом и сервером.	Механизмы безопасности включают аутентификацию через API-ключи и TLS для защиты передачи данных.
2010 г.	GraphQL	Язык запросов для API, который позволяет клиенту точно запрашивать только нужные данные, делая запросы более гибкими и оптимизированными.	Защита с помощью аутентификации через OAuth или JWT, поддержка HTTPS для защиты данных.
2014 г.	gRPC (Google Remote Procedure Call)	Высокопроизводительный фреймворк для создания API, использующий HTTP/2, поддерживающий двустороннюю потоковую передачу данных. Популярен в микросервисных архитектурах.	Аутентификация с помощью TLS, поддержка шифрования и проверка целостности сообщений.
2017 г.	WebSocket API	Протокол для создания постоянного соединения между клиентом и сервером для обмена данными в реальном времени (например, чат, уведомления).	Шифрование через TLS, защита от атак через механизмы контроля доступа и аутентификацию.
2020 г.	GraphQL Federation	Расширение GraphQL, которое позволяет комбинировать несколько GraphQL-сервисов в одну API-систему, улучшая масштабируемость и управление сложностью.	Защита через интеграцию с OAuth 2.0, использование JWT для защиты доступа и контроля данных между сервисами.
2023 г.	OpenAPI 3.0	Стандарт спецификации для описания REST API, который позволяет разработчикам документировать и тестировать API с удобством и точностью.	Защита с помощью OAuth, использование API-ключей для аутентификации, защита API через WAF (Web Application Firewall).

Отметим, что программный интерфейс (ПИ) — это своего рода язык общения между сервисами (программами). Он включает в себя набор инструкций, правил, способов, инструментов, посредством которых и происходит обмен данными.

Таблица 3 показывает, как развитие технологий реализации ПИ шло в сторону улучшения гибкости, производительности и безопасности для пользователей и разработчиков [197]. В таблице 4 отражены основные проблемы информационной безопасности ПИ в РИС, их описание и возможные решения.

Таблица 4 – Основные проблемы информационной безопасности ПИ в РИС

Проблема информационной безопасности ПИ в РИС	Описание проблемной ситуации	Возможное решение
Недостаточная аутентификация и авторизация	Неэффективные или отсутствующие механизмы аутентификации и авторизации могут позволить злоумышленникам получить доступ к ПИ.	Использование надежных методов аутентификации (OAuth 2.0, JWT), двухфакторная аутентификация, контроль доступа на основе ролей.
Утечка чувствительных данных	Протоколы ПИ могут передавать данные, включая пароли и личную информацию, без должной защиты.	Обязательное использование HTTPS для шифрования данных, шифрование паролей и секретных ключей, безопасное хранение данных.
Перегрузка ПИ (Rate Limiting)	Отсутствие ограничения по количеству запросов от одного клиента в единицу времени может привести к перегрузке системы или DDoS-атаке.	Внедрение механизма «rate limiting», ограничение количества запросов от одного клиента в определенный промежуток времени.
Уязвимости в коде ПИ	Ошибки в программном обеспечении, такие как SQL-инъекции, XSS или CSRF, могут быть использованы для эксплуатации уязвимостей API.	Тестирование на уязвимости (PenTest), использование безопасных библиотек, параметризованные запросы, валидация входных данных и кодирования вывода.
Недостаточная защита от атак на сессии	Уязвимости в управлении сессиями могут позволить злоумышленнику захватить или манипулировать сессиями пользователей.	Использование безопасных токенов, двухфакторной аутентификации, хранение токенов в «HTTPOnly cookies».
Недостаточный аудит и логирование	Отсутствие или недостаточность логирования запросов и действий пользователей затрудняет обнаружение атак.	Внедрение логирования всех запросов ПИ, мониторинг аномальных запросов, хранение логов для расследования инцидентов.
Устаревшие версии ПИ	Использование устаревших версий API, которые больше не поддерживаются, может создать уязвимости в безопасности.	Регулярное обновление ПИ, депрецирование старых версий, использование только актуальных версий ПИ.
Проблемы с межсервисной коммуникацией	В микросервисных архитектурах множество точек взаимодействия увеличивает риски безопасности.	Использование «mutual TLS» (mTLS) для безопасной передачи данных между сервисами, защита межсервисных соединений.
Проблемы с контролем доступа	Неправильное разделение доступа между пользователями и сервисами может позволить злоумышленникам выполнять операции, не предусмотренные их ролями.	Реализация строгого контроля доступа на основе ролей (RBAC), минимизация прав доступа для каждого пользователя и компонента.
Проблемы с безопасностью сторонних библиотек	Использование сторонних библиотек и сервисов может ввести уязвимости, если они не обновляются или имеют известные проблемы безопасности.	Регулярные обновления сторонних библиотек, использование проверенных поставщиков, мониторинг уязвимостей (например, CVE).

Однако, с развитием новых технологий старые технологии продолжают использоваться. Например, технология REST используется более чем в 70% проектах. Этот факт показывает не совершенство информационной безопасности ПИ [211].

Рассмотрим современные технологии обеспечения безопасности ПИ [199]. В таблице 5 представлены описание наиболее популярных современных технологий обеспечения безопасности ПИ с описанием их принципа работы.

Таблица 5 – Технологии для обеспечения безопасности ПИ в РИС

Название технологии для обеспечения безопасности ПИ в РИС	Описание и принцип обеспечения информационной безопасности
WS-Security (SOAP)	В «SOAP» используется стандарт «WS-Security» для обеспечения конфиденциальности и целостности сообщений, а также для управления подписями и шифрованием.
HTTPS	Используется для защиты всех видов ПИ, шифруя передаваемые данные.
OAuth 2.0 и JWT	Токенизированная система авторизации, которая предоставляет доступ к API с использованием токенов доступа, ограничивающих действия пользователей
TLS (Transport Layer Security)	Стандарт шифрования для обеспечения безопасной передачи данных по сети, особенно для «gRPC» и «WebSocket».
WAF (Web Application Firewall)	Защита веб-приложений от распространённых атак, таких как SQL-инъекции или XSS, через фильтрацию API-запросов.

Проведенный общий аналитический обзор уязвимостей ПИ (см. табл. 5) показал не универсальность решений по устранению уязвимостей и не возможность найти одно общее универсальное решение для всех типов архитектур ПО. Таким образом для РИС — ПИ являются одним из основных источников угроз ИБ.

1.2 Анализ безопасности распределенных информационных систем

Проблемы ИБ РИС являются одной из самых серьезных угроз для бизнеса и государственных организаций [103].

В РИС существует множество типов угроз безопасности. Они могут варьироваться от технических до организационных, от внутренних до внешних, и влияют на конфиденциальность, целостность и доступность данных [70, 92, 112, 186].

1.2.1 Угрозы информационной безопасности различного генеза

Рассмотрим угрозы ИБ различного генеза (то есть происхождения). Согласно действующей в настоящее время методики оценки угроз безопасности

информации ФСТЭК [101] сформирован банк угроз [8], в котором большая часть угроз безопасности относятся и к разным уровням ИТ-инфраструктур РИС. Данный факт указывает что безопасность ИТ-инфраструктур РИС особенно важна в настоящее время [5].

В [47] рассмотрены различные угрозы ИБ РИС, связанные с получением несанкционированным доступом, уязвимостями ПО, человеческим фактором и вредоносного программного обеспечения (ВПО).

В [186, 188] дана классификация угроз ИБ для ИТ-инфраструктур по уровням сетевого взаимодействия, ПО, физическая и контроля доступа. Показано, что данные направления нуждаются в разработке соответствующих мер защиты, которые не решают текущие проблемы безопасности ИТ-инфраструктур до конца [188].

В [46, 54, 79, 83, 112] описаны угрозы безопасности ИТ-инфраструктур РИС с позиции сетевых технологий и телекоммуникаций. Подробно рассмотрены типовые средства и способы реализации угроз атак на компьютерные сети, варианты защиты и обеспечения информационной безопасности. Вводится понятия угроз сетевых атак на инфраструктуры РИС и показаны подходы к их защите.

В [120] вводится понятие многоуровневой концепции безопасности систем управления большими данными включающая в себя также задачи по противодействию угрозам безопасности на уровне ИТ-инфраструктур РИС.

В [58] приводится экспериментальное исследование метода обнаружения атак различного генеза на сложные объекты, в том числе и на ИТ-инфраструктур РИС. Показана важность угроз безопасности ИТ-инфраструктур на основе оценки и прогнозирования состояния сложных объектов РИС.

В [45] выполнена разработка методов адаптивного управления доступностью ресурсов геоинформационных систем критического применения в условиях деструктивных воздействий, таких как атаки на доступность.

В [86, 88] и [85, 89, 90] предложен подход по прогнозированию угроз инфраструктурного деструктивизма (ИД) для критической информационной инфраструктуры (КИИ). Данная область является важной и перспективной.

Определение. Инфраструктурный деструктивизм – не способность информационной инфраструктуры реализовывать свой функционал в полном объеме под воздействием процессов внутри инфраструктуры [85, 86].

Расширим данное определение и для оценки угроз инфраструктурного деструктивизма и для ИТ-инфраструктур РИС.

Определение. Инфраструктурный деструктивизм – не способность ИТ–инфраструктуры РИС реализовывать свой функционал в полном объеме под воздействием процессов внутри инфраструктуры.

Определение. Под деструктивным воздействием инфраструктурного генеза (т. е. происхождения) будем понимать воздействие, в результате которого проявляется непредвиденное и(или) нежелательное событие, вызванное совокупностью факторов и условий инфраструктурного генеза, создающих опасность нарушения ИБ ИТ-инфраструктуры РИС[85, 88].

По уже имеющейся классификации угрозе ИБ ИГ наиболее соответствует угроза УБИ.140: «Угроза приведения системы в состояние – отказ в обслуживании» [8], а также тактике T1499: «Точечный отказ в обслуживании» [216].

Определение. Угроза ИБ ИГ— это угроза, возникающая не из-за злонамеренных действий человека, а из самой природы и ИТ-инфраструктуры РИС.

Отметим, что источником угрозы ИБ ИГ является не нарушитель, а структурные особенности, взаимодействия и зависимости между компонентами РИС. Деструктивное воздействие ИГ это разрушительное влияние, которое самопроизвольно возникает в результате функционирования сложной РИС, без внешнего злонамеренного вмешательства [10]. Таким образом, угроза ИБ ИГ является внутренней угрозой РИС и заменить понятие угрозы ИБ ИГ понятием «внутренней угрозы» не представляется возможным.

Также отметим, что угроза ИБ ИГ может проявляться как усиление деградации в РИС, приводящее к отказам в обслуживании из-за накопившихся архитектурных особенностей, без воздействия внутреннего злоумышленника. Например, для системы распознавания лиц входящей в состав контроля и управления доступа угроза ИБ ИГ способна привести к отключению контроля периметра.

Государственный стандарт по разработке безопасного программного обеспечения [31] не содержит конкретного перечня угроз безопасности РИС. Вместо этого он устанавливает общие требования к процессам моделирования угроз и анализа поверхности атаки. Исходя из общих принципов безопасности ПО, изложенных в стандарте [31], классифицированы наиболее важные категории угроз для РИС:

1) Угрозы архитектурного уровня: уязвимости в ПИ взаимодействия между компонентами РИС, недостаточная сегментация сетевых соединений, уязвимости в протоколах обмена данными.

2) Угрозы уровня компонентов: использование уязвимых заимствованных компонентов (композиционный анализ), нарушение целостности при передаче данных между узлами, компрометация секретов и ключей подписи.

3) Угрозы инфраструктурного уровня: атаки на цепочки поставок компонентов ПО, нарушение безопасности ИТ-инфраструктуры разработки, внедрение вредоносного кода через уязвимые зависимости.

В данном пункте с точки зрения автора приведены наиболее важные угрозы безопасности ИТ-инфраструктур РИС, другие возможные угрозы и проблемы безопасности классифицированы и описаны в приложении В: «Результаты сравнительного анализа методик повышения уровня ИБ в РИС».

1.2.2 Поведенческие модели и искусственный интеллект в информационной безопасности

Поведенческие модели в ИБ описывают стадии, паттерны (шаблоны) и особенности поведения как злоумышленников, так и пользователей и систем с целью выявления угроз и построения эффективной защиты [204].

Рассмотрим основные наиболее популярные в настоящий момент поведенческие модели в ИБ как показано в классификации в [49, 216]:

1) Модель Cyber Kill Chain — показывает этапы атак злоумышленника (разведка, вооружение, доставка, эксплуатация и т.д.) для построения многоуровневой поведенческой защиты.

2) Модель матрицы MITRE ATT&CK — модель тактик и техник атак с фокусом на поведенческом аспекте злоумышленников, используемая для обнаружения и анализа инцидентов.

3) Модель доказательств (Evidence Intention) — разделение доказательств вредоносной активности на намеренные и ненамеренные, что важно для приоритезации и достоверности расследований.

4) Вероятностные поведенческие модели — на основе вероятностных деревьев атак позволяют предсказывать вероятности реализации угроз и оценивать риски системы.

Определение. Поведенческий интеллект — это применение методов машинного обучения и искусственного интеллекта для анализа поведения пользователей, систем и сетей с целью обнаружения аномалий и угроз в режиме реального времени.

Рассмотрим основные особенности применения поведенческого интеллекта, в ИБ в настоящий момент [129]:

1) Формирование профиля нормального поведения пользователя, устройства или системы на основе широкого набора параметров (трафик, использование приложений, шаблоны работы).

2) Обнаружение аномалий, отклоняющихся от норм, которые могут свидетельствовать о кибератаках, инсайдерских угрозах или эксплуатации уязвимостей.

3) Использование поведенческого интеллекта для выявления неизвестных угроз, включая атаки нулевого дня и маскировку вредоносных действий.

4) Автоматизация реакции на угрозы, например, отключение подозрительных устройств или блокировка подозрительных действий.

Таким образом, поведенческие модели создают концептуальную основу для понимания и структурирования угроз, а поведенческий интеллект реализует эти модели через алгоритмы анализа и прогнозирования поведения в ИТ-инфраструктурах РИС.

Вместе они повышают эффективность выявления и предотвращения угроз, обеспечивая более адаптивную и проактивную защиту.

Так, например, в [26] рассматривается построение многоагентной системы комплексной защиты информации в компьютерных сетях, направленной на предотвращение утечек данных и повышение уровня ИБ.

Представленный подход направлен на повышение эффективности защиты информации за счёт интеграции многоагентных технологий и методов искусственного интеллекта с учётом динамики поведения нарушителей и особенностей технических каналов утечки.

Исследование [26] вносит значимый вклад в развитие методов защиты информации с использованием многоагентных систем и формирует основу для дальнейших исследований и практических реализаций в области ИБ компьютерных сетей.

В [126] рассматривается подход к обнаружению вредоносного программного обеспечения с использованием алгоритмов машинного обучения, включая анализ признаков исполняемых файлов и сравнение эффективности различных моделей классификации.

Полученные результаты подтверждают перспективность искусственного интеллекта для задач кибербезопасности в условиях роста сложности вредоносного ПО.

Таким образом, поведенческие модели и поведенческий интеллект в ИБ, являются перспективным направлением позволяющим повысить уровень ИБ для РИС.

1.2.3 Современные комплексы средств защиты информационных систем

Современные системы ИБ используют комплексы средств защиты информационных систем, которые защищают ИТ-инфраструктуры РИС и обрабатываемую в ней информацию от взлома, кибератак, утечек и других угроз [83, 112, 186].

Они помогают сохранить конфиденциальность обрабатываемых персональных данных, медицинских сведений, детализации транзакций банковского сектора, корпоративной информации, параметров сетевой инфраструктуры и других важных данных [96].

В коммерческом и в государственном секторе организаций повсеместно создаются специализированные центры обеспечения безопасности или просто центры обеспечения ИБ [55, 170, 224]. Опишем основные системы, подсистемы и инструментальные средства, которые в настоящий момент встречаются в системах по обеспечению ИБ.

Определение. Центр обеспечения безопасности SOC (Security Operations Center) — это центр, который занимается мониторингом и анализом событий ИБ в организации [170, 224].

Определение. Система управляемого обнаружения и реагирования MDR (Managed Detection and Response) — это служба ИБ, которая помогает активно защищать организации от киберугроз с помощью расширенных возможностей обнаружения и быстрого реагирования на инциденты ИБ [170].

Определение. Система расширенного обнаружения и реагирования XDR (Extended Detection and Response) — это технология, которая объединяет различные методы обнаружения и реагирования на угрозы ИБ. Она позволяет организациям получать более полную картину угроз и принимать более обоснованные решения о реагировании [170].

Определение. Система EDR (Endpoint Detection and Response) — технология, предназначенная для обнаружения и реагирования на инциденты безопасности на конечных точках сети. EDR-системы собирают данные с конечных точек и анализируют их на предмет подозрительной активности [170].

Определение. Система SOAR (Security Orchestration, Automation and Response) — платформа, которая автоматизирует процессы обеспечения ИБ, такие как обнаружение угроз, реагирование на инциденты и управление уязвимостями. SOAR-платформы позволяют организациям быстрее реагировать на угрозы и снижать нагрузку на специалистов по безопасности [170].

Определение. Система SIEM (Security Information and Event Management) — система, которая собирает, анализирует и коррелирует события ИБ из различных источников. SIEM-системы помогают организациям выявлять аномалии и потенциальные угрозы, а также отслеживать активность пользователей [170, 224].

Схема соприкосновения систем сбора, анализа и реагирования на события ИБ по взаимодействию описанных систем представлена на рисунке 5.

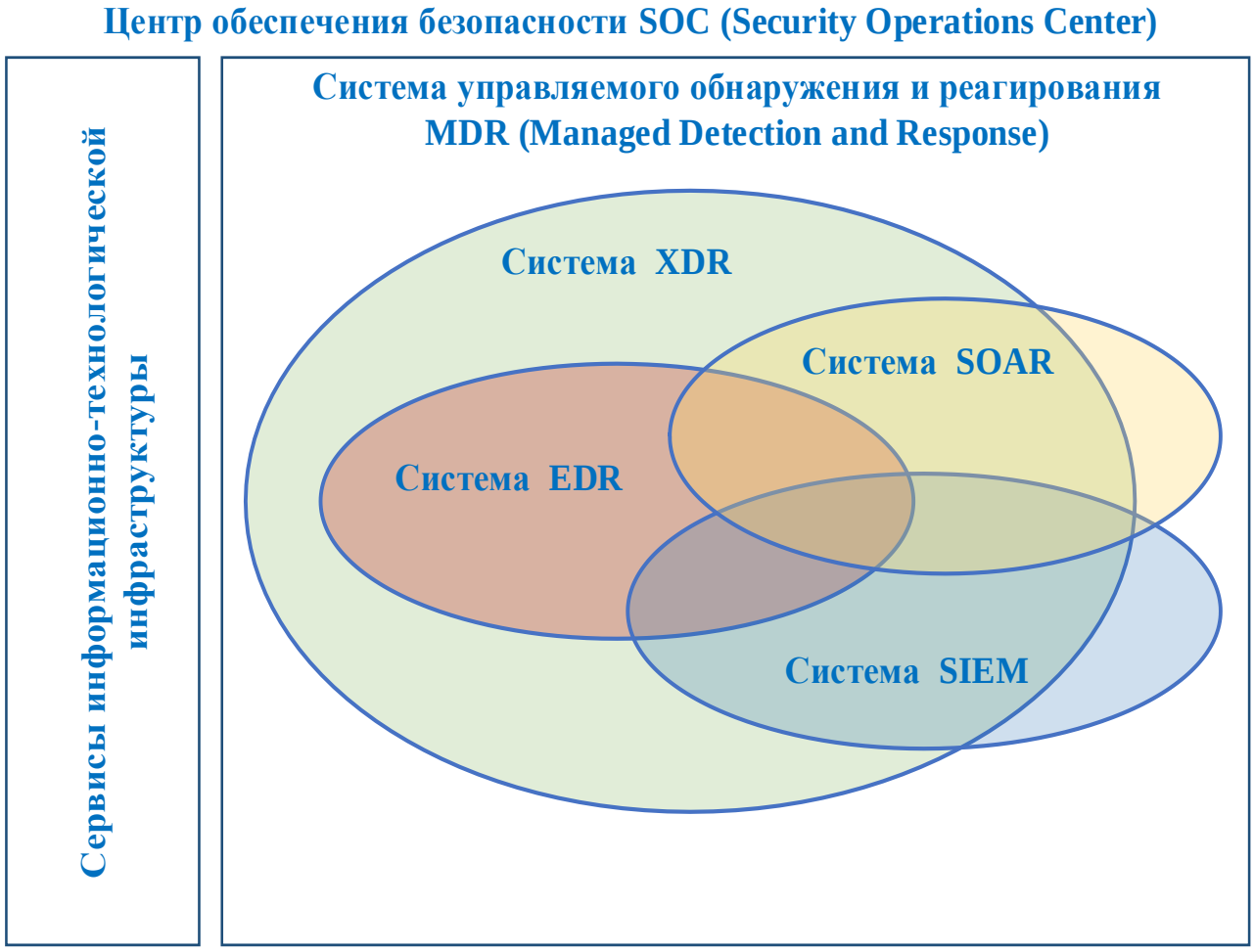

Рисунок 5 – Схема соприкосновения систем сбора, анализа и реагирования на события информационной безопасности

Отметим, что на схеме, представленной на рисунке 5, представлены подсистемы обеспечения информационной безопасность верхнего уровня РИС.

Также существуют и другие системы защиты такие как системы предотвращения атак на веб-приложения WAF (Web Application Firewall), межсетевой экран нового поколения NGFW (Next Generation Firewall) и другие.

В современных системах ИБ, защита данных приобретает критическое значение. Целевые продолжительные угрозы (APT — Advanced Persistent Threats) являются одним из самых сложных видов кибератак, с которыми сталкиваются организации по всему миру [173].

В работе [74] рассматриваются основные понятия — целевые атаки, продвинутые постоянные угрозы (APT), атрибуция кибернарушителей, а также ключевые проблемы построения эффективных систем атрибуции. Детально анализируются такие модели, как классическая и унифицированная цепочка кибервторжений (kill chain), Diamond Model, а также модель MITRE ATT&CK.

Приводятся примеры методик атрибуции: аргументированное рассуждение с техническими и социальными доказательствами, использование технических артефактов для выявления ложных флагов.

Особое внимание уделено тенденциям применения современных решений на базе искусственного интеллекта и машинного обучения для автоматизированной и интеллектуальной атрибуции атак и нарушителей.

В отличие от большинства кибератак, которые стремятся быстро достигнуть своих целей, APT-атаки характеризуются долгосрочным присутствием в зараженной системе. Отмечается недостаток квалифицированных специалистов в данной области [184].

Современные APT-группировки без труда обходят штатные средства защиты — антивирусы, системы обнаружения и предотвращения вторжений. Атакующий может находиться в сети месяцы или даже годы, постепенно расширяя свое влияние и избегая обнаружения [173, 196]. Наличие APT группировок требует использования более совершенных мер защиты.

Непрерывный мониторинг и анализ поведения системы с применением последних достижений в области технологий безопасности, включая искусственный интеллект и машинное обучение является неотъемлемым для большинства современных систем безопасности [195].

Как известно, целевые атаки постоянная серьёзная угроза APT происходят, используя вполне определенную последовательность этапов [196]: разведка; получение первичного доступа; закрепление в инфраструктуре; перемещение внутри периметра; повышение привилегий; компрометация и получение доступа к искомым данным; эксфильтрация (вывод из системы) данных и деструктивные воздействия.

Отметим, что угроза инфраструктурного деструктивизма охватывает все этапы реализации целевых атак постоянной серьёзной угрозы APT и способна повлиять как в положительную, так и в отрицательную сторону [86, 132].

Рассмотрим существующие средства обеспечения работоспособности и наблюдения за инфраструктурами с позиции выявления угрозы инфраструктурного деструктивизма.

1.2.4 Инструменты наблюдаемости, трассировки и мониторинга в информационных системах

Суть работы средств обеспечения работоспособности и наблюдения за инфраструктурами состоит в использование программных средств, которые формируют журналы событий (лог-файлы) и специализированные программы, которые анализируют полученные данные и определяют ключевые параметры функционирования ИТ-инфраструктур РИС.

Выделяют два типа анализируемых данных [161]: журналы событий и метрики. Интеллектуальный анализ журналов событий (логов) ИТ-инфраструктур РИС представляет собой процесс использования современных методов и технологий для выявления, изучения и предотвращения угроз, инцидентов и аномалий на основе данных логов.

Этот подход основан на обработке больших объёмов данных, поступающих от различных систем, приложений и устройств. Обычно для этих целей используются мощные поисковые системы «OpenSearch» (Elasticsearch) с различными системами визуализации данных, например Kibana. С другой стороны, используют подход обработки данных событий в РИС на основе метрик.

Определение. Метрика — это количественный или качественный показатель работы подсистем РИС.

Подход на основе метрик эффективно применяется на практике и обычно является основным способом оценить процессы, происходящие в ИТ-инфраструктур РИС [65, 161].

Для РИС одним из популярных средств мониторинга являются система «Prometheus» и средство визуализации данных «Grafana». Метрики и журналы событий позволяют строить панели мониторинга (дашборды), в которых отображается полезная информация о функционировании всех систем ИТ-инфраструктур РИС.

По своей сути данные подходы похожи на те же самые алгоритмы анализа данных, которые применяются в системах мониторинга информационной безопасности SIEM. То есть анализ событий безопасности также использует данные журналов событий и рассчитывает метрики.

Как правило ландшафт современных атак на любую информационную систему состоит из 3-х основных этапов [214, 216]: разведка, атака и закрепление. Данные этапы с описанием возможных деструктивных воздействий показаны на рисунке 6.

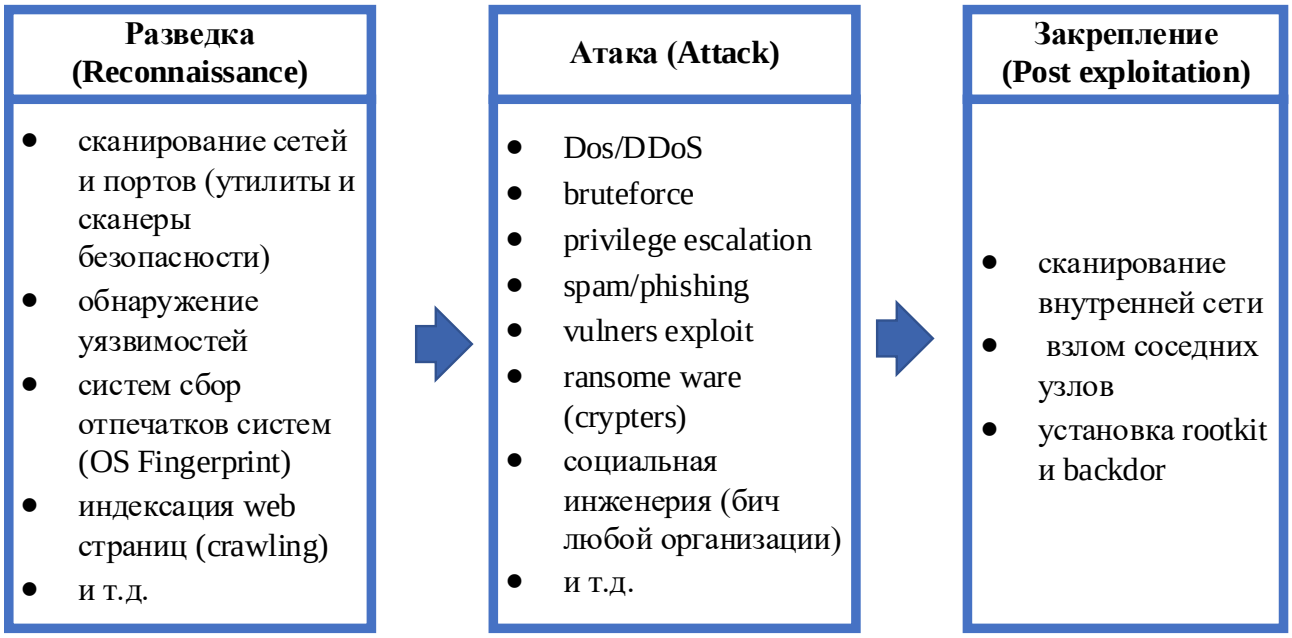

Рисунок 6 – Типовой ландшафт атак на РИС

В противовес ландшафту атак, инженеры ИБ со своей стороны выстраивают следующие защитные мероприятия: превентивные, детективные и корректирующие, как показано на рисунке 7. Следует отметить, что матрице MITRE ATT&CK есть

другие тактики для анализа. Но на практике используются не все, а только те, которые соответствуют специфике защищаемой организации.

Превентивные	Детективные	Коррективные
Управление активами • сбор информации об активе — HW, OS, ПО, адреса, порты — методами аудита и pentest • сбор информации о взаимодействии между активами (в т.ч. построение матрицы доступности) • сбор и управление учетными записями Управление уязвимостями • сбор данных об уязвимостях в активах системы • управление патчами и обновление • работа с пользователями - инструкции и обучение (привет социальной инженерии)	Сбор событий ИБ с активов нормализация событий агрегирование событий анализ и корреляция событий • корреляции событие 1 — событие 2 • корреляция событие — актив • корреляция внутри актива хранение событий	Расследование (forensics) результатов атаки В результате расследования: • мероприятия по изменению политики ИБ • изменение настроек безопасности активов

Рисунок 7 – Типовой ландшафт защиты и мероприятия повышения уровня ИБ в РИС

Таким образом интеллектуальный анализ журналов событий является неотъемлемой частью при организации и работе SIEM систем.

Общая последовательность обработки событий в системах управления информационной безопасностью представлена на рисунке 8.

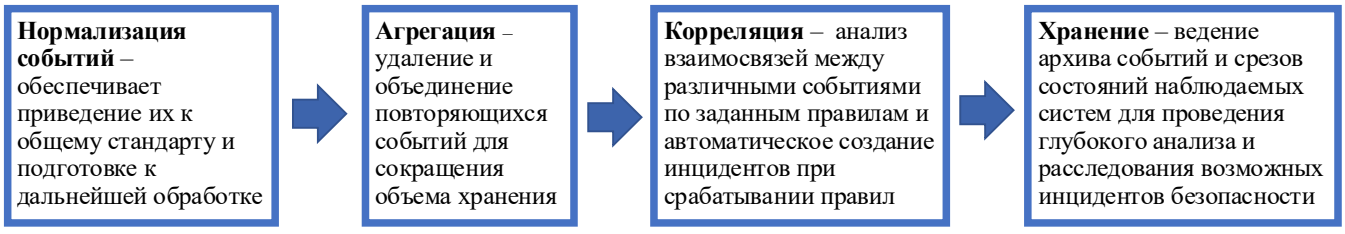

Рисунок 8 – Основные этапы обработки событий в системах управления информационной безопасностью РИС

Суть процесса обработки событий в системах информационной безопасности сводится к последовательному выполнению этапов: нормализация, агрегация, корреляция и хранения данных событий.

Анализ корреляций представляет собой процесс нахождения некоторых закономерностей в данных и событиях систем [194]. Проблемам анализа данных событий в журналах РИС уже посвящено достаточно большое количество исследований [194]. Многие крупные вендоры занимаются интеллектуальным анализом журналов событий с целью обнаружения аномальных значений, а также повышения производительности работы РИС [201].

Существуют открытые соревнованию по анализу данных в данной области. В [205] описан датасет трассировки программного обеспечения систем управления кластером компании «Google». Объем выборки составляет порядка 29 дней за 2011 год около 41 ГБ и порядка 29 дней за 2019 год, что составляет около 2.4 Тебибайт данных. Отслеживание рабочих нагрузок, выполняемых в вычислительных кластерах «Google Borg».

В трассировке описываются все отправленные задания, решения по планированию и данные об использовании ресурсов для заданий, которые выполнялись в этих кластерах. В [198] описан датасет трассировки программного обеспечения систем управления кластером компании «Alibaba». Объем выборки составляет порядка 2 месяцев с 6500 компьютерных серверов.

Отслеживание рабочих нагрузок вычислений с использованием микросервисов и вычислений на графических процессорах (GPU). В [215] содержится четыре общедоступных набора данных трассировок «Microsoft Azure» (трассировки виртуальных машин, трассировки функций) для использования исследовательским и академическим сообществом.

Трассировки представляют собой очищенные подмножества рабочей нагрузки виртуальных машин первой линии в одном из географических регионов. Открытые данные «DeepTraLog» [203] из лаборатории разработки программного обеспечения университета Фудань (Китай, Шанхай). Данные «DeepTraLog» использовались для проведения соревнований по обнаружению аномалий в журналах

событий для ИТ-Инфраструктуры ИС, построенных на сервисах с использованием облачной платформы OpenStack.

На основе анализа [198, 201, 203, 205, 215] синтезирована следующая классификация математических методов применяемых для интеллектуального анализа журналов событий РИС, которая представлена на рисунке 9.

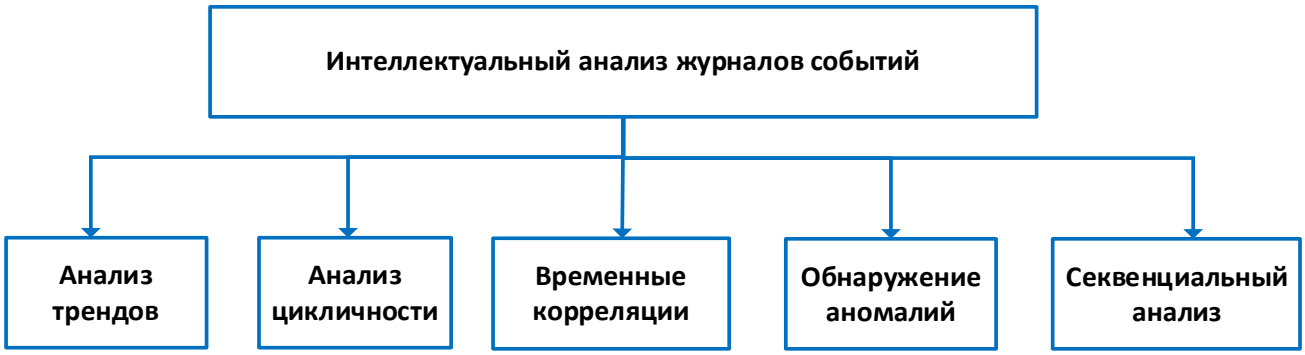

Рисунок 9 – Классификация математических методов применяемых для интеллектуального анализа журналов событий РИС

Следует отметить, что в сфере ИБ особое распространение получили методы для обнаружения аномалий средствами интеллектуального анализа данных.

Так в работах [190, 191] показан метод мониторинга аномальных состояний компьютерных систем, позволяющий эффективно решать задачи по обнаружению подозрительной активности в системных журналах.

Отдельно отметим подход связанный с секвенциальным анализом последовательностных паттернов содержащихся в журналах событий систем [189]. Данный подход позволяет диагностировать «здоровье» компьютерной сети.

Помимо интеллектуального анализа журналов событий (logging) для сервисных систем используются подходы связанные с мониторингом (monitoring) с трассировкой работы систем (tracing), вычислением метрик (metrics), а также мониторингом производительности (application performance monitoring) [68, 181].

Все эти подходы комбинируются и используются в том числе и в сферах информационной безопасности.

1.2.5 Применение антропоморфического подхода в технических системах для повышения уровня информационной безопасности

Антропоморфическое поведение в технических системах — это явление, при котором системы, устройства или программное обеспечение проявляют черты или модели поведения, напоминающие человеческие. Это может быть сознательное внедрение элементов, имитирующих человеческие действия, эмоции или мышление, с целью повышения качества функционирования технических систем.

В [17] рассматриваются вопросы, как взаимодействие уязвимостей систем. В этом случае антропоморфический подход является полностью оправданным. Особенности различных типов взаимодействий уязвимостей программного кода говорят о том, что последние могут быть достаточно сложными и иметь непредсказуемые эффекты. Таким образом, данный аспект информационной безопасности является не только малоизученной, но и крайне актуальной темой для исследования. Применение антропоморфизма для понимания взаимодействий уязвимостей оказалось достаточно удачным – как для типизации, так и для их интерпретации человеком. Предложенная формализация [17] показала свою жизнеспособность, хотя для полноценного математического аппарата необходимы дополнительные исследования и подходы, выходящие за рамки одной лишь сферы информационной безопасности.

С позиций данного подхода описан жизненный цикл программного кода и эволюция ее уязвимостей. В [18] выделены девять антропоморфических типов взаимодействий уязвимостей в программе: облигативный и факультативный симбиоз, комменсализм, паразитизм, комменсализм, паразитизм, хищничество, нейтрализм, аменсализм, аллелопатия и конкуренция. Обосновано использование данного подхода для описания взаимодействия уязвимостей программного кода и показан результат моделирования.

В [90] с использованием антропоморфного подхода определен деструктивнообразующие виды межобъектных связей и методы их идентификации. Также установлены зависимости источников происхождения деструктивных воздействий от сфер функционирования взаимодействующих субъектов и антропоморфизма

межобъектных связей. В результате данного подхода позволяет рассмотреть возникающий на субъекте синергетический эффект и определить момент появления точки бифуркации – точки саморазрушения системы. Данный эффект в работе [90] назван эффектом инфраструктурного деструктивизма и описан подход по его оценки для критических информационных инфраструктур.

В [83] в результате исследования модели антропоморфического взаимодействия конфликтующих сторон выявлены типовые состояния конфликта, а также бифуркации конфликта – такие значения параметров конфликтующих сторон, при которых качественно меняются траектории развития конфликта и возможности выигрыша той или иной стороны.

На основе этих исследований предложены сценарии действий одной из сторон по изменению ее параметров для достижения выигрыша в конфликте. Проведен подробный анализ типовых сценариев действий для одной из сторон, в интересах обоснования наиболее «сильных» параметров этой стороны и направлений их изменения для обеспечения выигрыша.

В [189] представлен подход, который позволяет диагностировать «здоровье» компьютерной сети. Предложено характеризовать «состояние здоровья» компьютерной сети с помощью «Зеленого», «Желтого» и «Красного» уровней аномальности.

В качестве системных показателей, характеризующих «здоровье компьютерной сети» используется уровень обслуживания (Service Level Objectives, SLO), и соглашение об уровне предоставляемого сервиса (Service Level Agreement, SLA).

На конкретном примере [189] рассмотрена визуализация процесса кластеризации состояний компьютерной сети с использованием алгоритма «k-means» и алгоритма понижения размерности «TSNE».

Предложено оценивать «здоровье сети» по близости текущей оценки прогноза состояния компьютерной сети к сформированной в результате кластеризации области аномальных состояний в виде расстояния до ближайших центров кластеров, на порядковой шкале от 1 до 5.

В [102] предложены метрики здоровья РИС, которые основываются на определении пороговых значений метрик, соответствующих комфортной работе пользователей сервисов.

В [74] предлагается использование имитационного моделирования на уровне сетевых пакетов для исследования механизма защиты «нервная система сети». Описывается архитектура системы защиты, реализующей данный механизм защиты, и алгоритмы его работы, представляются результаты экспериментов.

На основе полученных экспериментальных данных проводится анализ эффективности предлагаемого механизма защиты. Данный подход дает качественно новые возможности защиты компьютерных сетей.

В [109] предложен кибериммунный подход к защите промышленного интернета вещей (IoT). Данные механизмы позволяют более точнее самооргонизавать процесс защиты конечных устройств.

В [9] разработана методика контроля и восстановления целостности вычислительных процессов в информационных системах, позволяющая на основе положений теории подобия и размерностей формировать цифровой паспорт вычислительного процесса в терминах размерностей, осуществлять динамический контроль целостности вычислительных процессов, выявлять признаки наличия нарушений целостности вычислений, осуществлять их восстановление, а также осуществлять самообучение и накопление новых знаний приобретаемого кибериммунитета.

Киберимунный подход описан как один из перспективных механизмов по самонастройке сложных систем.

В исследовании [69] описаны возможности использования защищенной, киберимунной операционной системы «Kaspersky OS» для дистанционного управления мобильным роботом устойчивым к внешним атакам, приводящим к потере связи с координационным центром.

Таким образом применение антропоморфического подхода в технических системах во многом помогает по-новому взглянуть на проблемы безопасности РИС и получить качественно лучшие результаты.

1.2.6 Анализ результатов проявления эффектов инфраструктурного деструктивизма в информационных системах

В данном пункте рассмотрим анализ результатов проявления инфраструктурного деструктивизма.

Определение. Инфраструктурный деструктивизм (ИД) — это намеренное или случайное разрушение ИС, её компонентов или зависимых систем [85].

Такой деструктивизм может проявляться через кибератаки, саботаж, неправильное управление ресурсами или несанкционированные действия.

Анализ результатов проявления позволяет выявить признаки подобных действий и предотвратить дальнейшие угрозы.

Определение. Проявления эффектов инфраструктурного деструктивизма — это информация, оставленная действиями пользователей, систем или злоумышленников в ИС, приводящей к ИД. Например: журналы событий; сетевые потоки; изменения конфигураций; аномалии в данных или процессах.

Автором исследования выдвигается гипотеза о том, что в качестве возможных результатов проявления ИД могут выступать следующие основные ситуации: состояние гонки ресурсов, нарушение идемпотентности и взаимная блокировка ресурсов**.**

Определение. Гонка ресурсов (race condition) в ИС — это состояние, при котором два или более процесса или потока одновременно пытаются получить доступ к общим ресурсам (например, файлам, переменным, базам данных), и результат их взаимодействия зависит от порядка выполнения [167, 193]. Такие состояния могут приводить к ошибкам, нестабильности ИС и уязвимостям безопасности.

Определение. Идемпотентность — это свойство операции, при котором повторное выполнение этой операции с одинаковыми входными данными не изменяет результат [167]. В контексте РИС идемпотентность особенно важна для обеспечения надёжности, предсказуемости и устойчивости систем, таких как ПИ, базы данных, облачные сервисы и системы управления конфигурацией.

Определение. Взаимная блокировка (deadlock) в контексте ИБ — это состояние, при котором два или более процесса или компонента системы блокируют

доступ друг другу к необходимым ресурсам, в результате чего ни один из них не может продолжить выполнение [167].

Такое состояние может угрожать ИБ и стабильности системы, особенно если оно возникает в критических процессах или службах и может привести к возникновению эффектов ИД.

1.3 Анализ методик оценки рисков информационной безопасности информационных систем

Методики анализа и оценки рисков ИБ позволяют идентифицировать риски, ранжировать их по степени опасности и вероятности возникновения, а также выработать метод обработки этих рисков [11].

В данной работе предлагается разделить методы оценки рисков ИБ на методы инфраструктурного и не инфраструктурного генеза (то есть происхождения).

1.3.1 Оценка рисков информационной безопасности инфраструктурного генеза

Оценка рисков информационной безопасности инфраструктурного генеза предполагает систематический анализ угроз, уязвимостей и последствий для компонентов РИС. Этот процесс помогает определить вероятности реализации угроз и их влияние на бизнес, что способствует формированию стратегий защиты.

Для оценки рисков ИБ инфраструктурного генеза на практике используются различные инструменты для расчёта состояния здоровья сервисов ИТ-инфраструктуры ИС, каждый из которых обладает своими особенностями и областями применения.

Программные комплексы для расчёта состояния «здоровья» сервисов ИТ-инфраструктуры РИС приведены в таблице 6.

Таблица 6 – Программные комплексы для расчёта состояния «здоровья» сервисов ИТ-инфраструктуры РИС

Инструментарий (Платформа)	Основное назначение и особенности
C-VIEW	Централизованное управление и мониторинг цифровых сертификатов (PKI), контроль их жизненного цикла, автоматизация процессов выдачи, продления и отзыва. Позволяет снижать риски, связанные с просроченными или недействительными сертификатами, а также обеспечивать непрерывность бизнес-сервисов [202].
Monq	Универсальная платформа для мониторинга ИТ-инфраструктуры РИС и бизнес-сервисов. Охватывает все аспекты мониторинга: инфраструктура, сервисы, события, метрики, логи. Поддерживает автоматизацию процессов, предоставляет единую панель для управления состоянием сервисов, автоматически строит карты здоровья ИТ-среды и помогает быстро выявлять причины инцидентов [221].
Monitoring by Service Operation Status (NOC)	Набор инструментов и решений для мониторинга состояния сервисов и инфраструктуры в центрах сетевых операций (NOC). Включает системы для отслеживания работоспособности, производительности и доступности сервисов, генерации оповещений, анализа метрик и событий в реальном времени [218].

Оценка рисков ИБ инфраструктурного генеза (ИГ) может быть описана в виде процесса управления компьютерными инцидентами ИБ.

Процесс управления компьютерными инцидентами ИБ — это система взаимосвязанных этапов, направленных на быстрое и эффективное реагирование на сбои, атаки и иные нештатные ситуации в информационных системах организации. Цель — минимизировать ущерб, восстановить нормальную работу и не допустить повторения инцидентов в будущем [37, 38, 220].

Основные этапы процесса управления компьютерными инцидентами ИБ:

Этап 1. Обнаружение и регистрация инцидента ИБ. На этом этапе осуществляется мониторинг ИБ, сбор информации о событиях и регистрация инцидентов. Важно своевременно выявлять подозрительные события и фиксировать их для дальнейшего анализа [37 ,39].

Этап 2. Анализ и идентификация инцидента ИБ. Проводится предварительный анализ инцидента ИБ для подтверждения его наличия и оценки масштабов. Определяется, какие элементы инфраструктуры затронуты, и выявляются признаки компрометации [39].

Этап 3. Локализация (сдерживание). Локализация инцидента ИБ направлена на ограничение его распространения и предотвращение дальнейшего ущерба.

Затронутые системы могут быть изолированы от сети, доступ к ним ограничен [37, 176].

Этап 4. Ликвидация последствий и восстановление. После локализации устраняются причины инцидента ИБ (удаляются вредоносные программы, устраняются уязвимости), восстанавливается работоспособность систем и данных из резервных копий [38].

Этап 5. Изучение и фиксация материалов инцидента ИБ. Собирается и сохраняется информация об инциденте ИБ, включая доказательства, данные журналов событий, временные метки и другие данные, необходимые для расследования и его анализа [37, 176].

Этап 6. Определение причин и условий возникновения инцидента ИБ. Проводится анализ причин возникновения инцидента, выявляются условия, способствовавшие его реализации, и разрабатываются рекомендации по предотвращению подобных ситуаций в будущем [38, 176].

Этап 7. Закрытие инцидента ИБ и анализ результатов. После устранения последствий и реализации рекомендаций инцидент закрывается. Проводится анализ эффективности реагирования, накапливается опыт, вносятся изменения в процессы и документы [176].

Таким образом управление компьютерными инцидентами ИБ — это циклический процесс, включающий обнаружение, анализ, локализацию, восстановление, анализ причин и внедрение улучшений. Чёткое следование руководству по реагированию позволяет минимизировать ущерб, быстро восстановить работу систем и повысить уровень ИБ ИГ организации.

Оценка рисков ИБ инфраструктурного генеза (ИГ) может быть также осуществлена на основе подхода UEBA (User and Entity Behavior Analytics) [66]. Подход UEBA — это современный подход к повышению уровня кибербезопасности, основанный на анализе поведения пользователей и различных сущностей (устройств, приложений, сетевого трафика и т.д.) с помощью машинного обучения и расширенной аналитики в том числе и для ИТ-инфраструктур РИС организаций.

Системы безопасности UEBA выявляют шаблоны обычного поведения и автоматически обнаруживают аномалии, которые могут указывать на угрозы, такие как компрометация учетных записей, внутренние нарушения или сложные атаки.

UEBA анализирует данные из множества источников (журналы событий, сетевой трафик) и помогает обнаруживать угрозы, которые не видны классическим средствам защиты информации [66].

В [77] рассматривается системный подход к оценке рисков в компьютерных сетях критически важных инфраструктур (КИИ), направленный на упреждающее выявление и предотвращение киберугроз. Акцент делается на раннем обнаружении признаков подготовки атак, использовании автоматизированных механизмов корреляции событий ИБ из различных источников, а также внедрении технологий искусственного интеллекта и анализа больших данных для повышения эффективности защиты информации. Отмечена важность интеграции предлагаемых решений с нормативными требованиями и критикует ограниченность традиционных методов предупреждения атак. В итоге подход способствует повышению уровня безопасности КИИ за счёт адаптивных и прогнозных технологий, соответствующих современным проблемам ИБ.

В [78] представлен комплексный подход к повышению устойчивости объектов КИИ к сложным целевым компьютерным атакам. Подход основан на комбинированном анализе угроз ИБ с применением сигнатурных и эвристических методов, а также математическом моделировании процессов воздействия и состояния систем. Автором разработана методология автоматизированного тестирования безопасности, реализованы механизмы динамического контроля, резервирования критически важных компонентов и оперативного восстановления.

Предложенная схема позволяет адаптироваться к изменяющимся условиям атак, автоматизировать принятие решений и значительно сократить время восстановления систем. Методология апробирована на объектах энергетики и промышленности, что подтвердило её эффективность и практическую значимость.

В [6] рассматриваются методы оценки рисков ИБ для экономических информационных систем (ЭИС), учитывающие их специфику: высокую ценность финансовых данных, нормативные требования (например, PCI DSS) и уязвимости, связанные с транзакционными операциями.

Предлагается адаптированные подходы к идентификации угроз ИБ (мошенничество, хищение данных, DDoS-атаки на платёжные шлюзы) и анализу уязвимостей в контексте экономических процессов. Особое внимание уделяется интеграции методов количественной и качественной оценки рисков для ИТ-инфраструктур ЭИС, а также разработке мер защиты, соответствующих отраслевым стандартам и бизнес-процессам.

В [82] рассматривается применение методов нечеткой логики для анализа рисков ИБ, что позволяет эффективно работать с неопределённостью и субъективностью оценки угроз, уязвимостей и последствий в условиях динамичной ИТ-инфраструктуры РИС.

Предлагается поэтапную реализацию анализа: формализацию параметров риска через лингвистические переменные, построение функций принадлежности, разработку правил нечеткого вывода и дефаззификацию результатов для получения количественных оценок ИБ.

Методология продемонстрирована на примере анализа DDoS-атак и показала эффективность при обработке экспертных данных, а также при интеграции с традиционными методами машинного обучения.

Подход рекомендован для использования в системах поддержки принятия решений при аудите безопасности, повышая точность и объективность оценки рисков в условиях неполноты информации.

В [65, 22, 166] рассматривается системный подход к разработке и применению метрик ИБ как инструмента для объективной оценки рисков ИБ в организации. Выделены основные категории метрик: эффективности, результативности и соответствия, приводят примеры их использования и подчеркивают важность увязки показателей с бизнес-целями.

Предлагаются практические рекомендации по автоматизации сбора данных, регулярному пересмотру метрик и их интеграции с процессами управления ИБ. Акцентируется роль метрик в обосновании инвестиций в безопасность и демонстрации результативности руководству, а также необходимость баланса между

техническими и бизнес-ориентированными показателями ИБ инфраструктурного генеза.

1.3.2 Оценка рисков информационной безопасности не инфраструктурного генеза

Типовой процесс оценки рисков ИБ состоит из последовательности взаимосвязанных этапов, направленных на выявление, анализ и управление угрозами для информационных активов организации, как показано на рисунке 10.

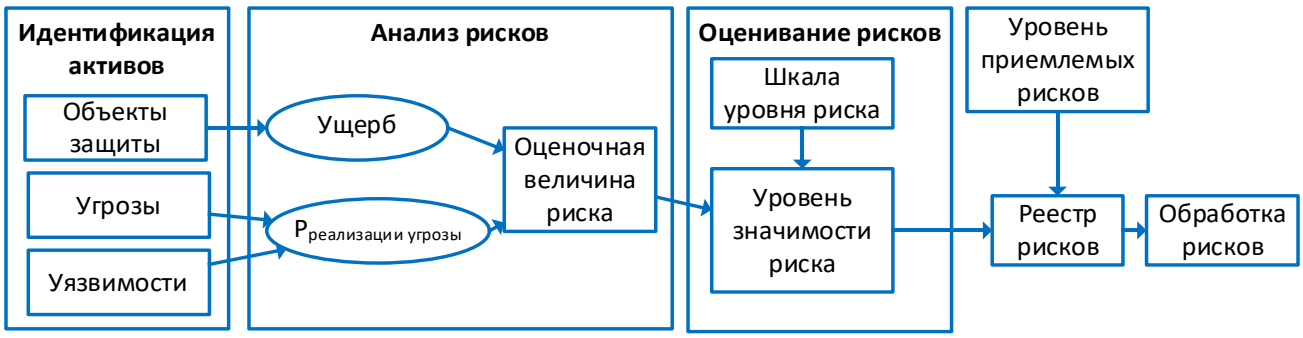

Рисунок 10 –Процесс оценки рисков ИБ

Этапы типового процесса оценки рисков ИБ:

1) Идентификация и определение приоритетов активов. Сначала выявляются все информационные активы, которые требуют защиты (данные, системы, оборудование, персонал), и определяется их ценность для бизнеса [11, 33, 131].

2) Определение угроз и уязвимостей. Анализируются возможные угрозы (например, кибератаки, сбои оборудования, человеческие ошибки) и уязвимости, которые могут быть использованы для реализации этих угроз [33, 131].

3) Анализ существующих средств контроля. Оценивается эффективность уже внедрённых мер защиты и контроля, выявляются пробелы в системе ИБ [33].

4) Определение вероятности реализации угроз. Рассчитывается вероятность того, что выявленные угрозы смогут быть реализованы с учётом имеющихся уязвимостей и средств контроля [131].

5) Оценка возможного воздействия угрозы. Определяется потенциальный ущерб для организации в случае реализации угрозы (финансовые потери, ущерб репутации, простои, утечка данных) [11, 131].

6) Расчёт и ранжирование рисков. Риск определяется как комбинация вероятности и возможного ущерба, после чего риски ранжируются по степени их значимости для организации [11, 131].

7) Составление рекомендаций и выбор стратегии управления рисками ИБ. Для каждого значимого риска разрабатываются рекомендации по его снижению, передаче, принятию или избеганию [33].

8) Документирование результатов. Все этапы, результаты и принятые решения фиксируются для дальнейшего мониторинга и пересмотра процесса управления рисками [11, 131].

Современные методики оценки рисков ИБ отличаются разнообразием подходов — от простых качественных методик до сложных количественных моделей и имитационных систем.

Выбор метода зависит от специфики организации, сложности ИС, требований регуляторов и доступных ресурсов [114].

В условиях роста сложности и масштаба киберугроз особую актуальность приобретают гибридные и имитационные методы, позволяющие учитывать как технические, так и организационные аспекты безопасности, а также прогнозировать возникновение новых классов угроз, в том числе и угроз ИД.

Они различаются по уровню детализации, поддерживаемым стандартам, сложности внедрения и требованиям к квалификации пользователей.

В таблице 7 приведены наиболее известные и используемые в настоящий момент программные комплексы и методологии, широко применяемые для оценки и управления рисками ИБ [11, 12].

Таблица 7 – Программные комплексы для оценки рисков ИБ

Программный комплекс, наименование методологии	Разработчик, страна	Основные особенности и применение
CRAMM	Insight Consulting, UK	Комплексная качественная оценка рисков, поддержка стандартов, выбор контрмер, высокая квалификация аудитора
RiskWatch	RiskWatch Inc., USA	Количественная и качественная оценка рисков, обширная база угроз и уязвимостей, гибкость
vsRisk	IT Governance, UK	Оценка рисков по ISO 27001, удобство использования, поддержка международных стандартов
MSAT (Microsoft Security Assessment Tool)	Microsoft, USA	Предварительная оценка рисков, простота, рекомендации по улучшению ИБ
Ra2	Отечественная разработка	Оценка рисков по российским стандартам, поддержка ГОСТ, гибкость функционала.
CORAS	Международный проект	Открытая методология, визуализация рисков, поддержка международных стандартов
ГРИФ	Российская разработка	Отечественная разработка, поддержка российских стандартов, интеграция с ИС
OCTAVE	Carnegie Mellon University, USA	Открытая методология, крупные организации, качественная оценка

На рисунке 11 приведен процесс управления риском ИБ согласно ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска» [33]. Существуют и более общие подходы к оценке рисков ИБ, например [44].

До принятия решения о внедрении той или иной методики управления рисками ИБ следует убедиться, что она достаточно полно учитывает бизнес-потребности компании, ее масштабы, а также соответствует лучшим мировым практикам и имеет достаточно подробное описание процессов и требуемых действий [15].

Для повышения адекватности оценок рисков ИБ не инфраструктурного генеза применяются следующие методы.

Использование экспертных опросов с обеспечением согласованности мнений [19, 48]. Привлечение нескольких экспертов позволяет минимизировать субъективность оценок. Для повышения согласованности применяется коэффициент конкордации, который измеряет степень согласия экспертов.

Чем ближе значение коэффициента к единице, тем выше уровень согласованности. Минимально допустимое значение обычно составляет 0,4.

Если согласованность недостаточна, проводятся дополнительные обсуждения или используются методы исключения крайних оценок.

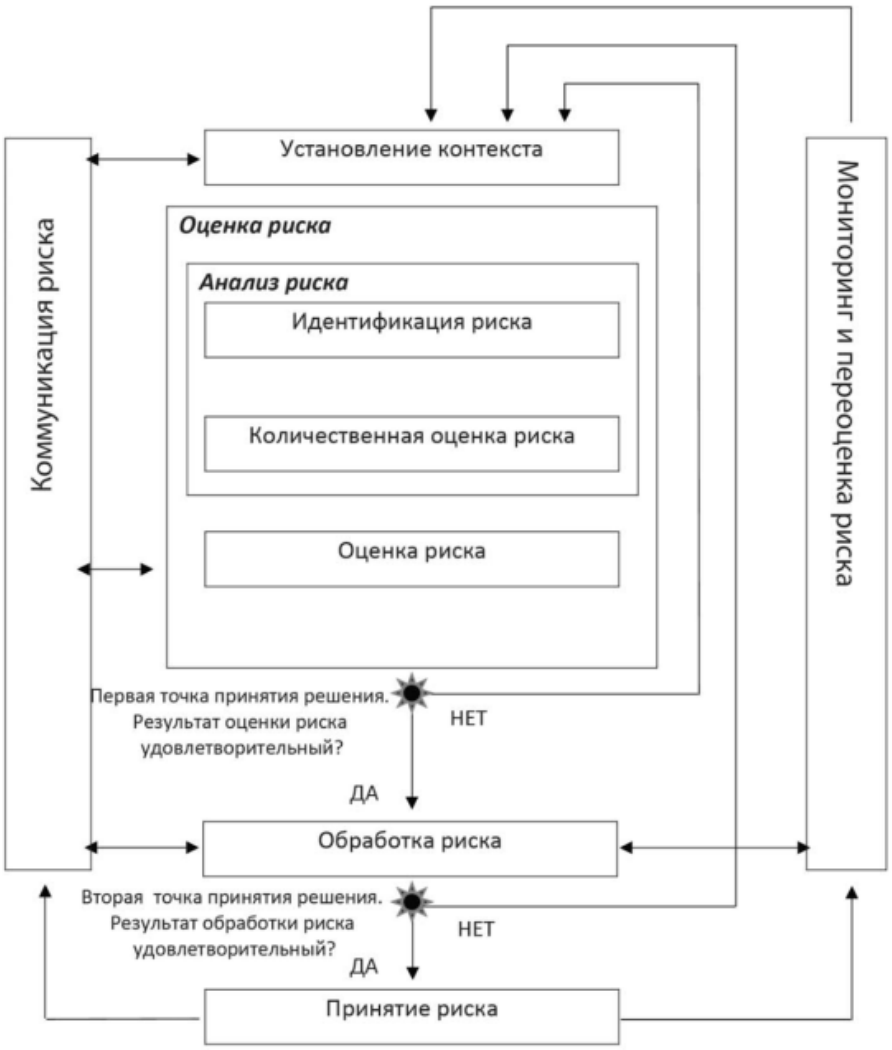

Рисунок 11 –Процесс управления риском информационной безопасности

Применение вербально-числовых шкал и математических моделей [19]. Для формализации оценок используются шкалы (например, шкалы Марголина и Харрингтона), а также математические модели, такие как линейное программирование (симплекс-метод), позволяющие учитывать влияние как наиболее критичных, так и менее значимых факторов риска.

Использование когнитивных карт [87] и автоматизированных инструментов [113, 48]. Когнитивные карты помогают визуализировать и структурировать знания экспертов, что способствует более точной оценке факторов риска.

Автоматизированные инструменты, включая платформы на основе искусственного интеллекта, позволяют анализировать большие объёмы данных, выявлять закономерности и минимизировать человеческую предвзятость.

Интеграция количественных и качественных подходов [100, 56]. Комбинированное применение количественных (числовых) и качественных (описательных) методов оценки рисков позволяет получить более объективную и комплексную картину угроз и уязвимостей.

В работе [168] раскрываются основные понятия и определения, связанные с идентификацией, анализом, оценкой и минимизацией рисков в проектной деятельности. Показана необходимость управления рисками ИБ в том числе и на уровне проектов.

Регулярное обновление и переоценка рисков [48]. Использование ПО, интегрированного с источниками данных в реальном времени, помогает поддерживать актуальность оценок и своевременно реагировать на изменения в информационной среде.

1.3.3 Анализ устойчивости распределённых информационных систем

Устойчивость РИС обеспечивается комплексом организационных и технических мероприятий: резервирование, мониторинг, оптимальное управление компонентами и ресурсами, обеспечение безопасности, а также учёт человеческого фактора [94]. Только интегрированный подход позволяет сохранить целостность и работоспособность РИС в условиях деструктивных воздействий, роста масштабов системы и наличия ИД [114].

Изменение нагрузки, особенно её рост, является одним из основных факторов, влияющих на критическую устойчивость РИС [7]. Критическая устойчивость определяется способностью системы сохранять функционирование при достижении определённых пределов ресурсов, после чего она становится неустойчивой и может перейти в состояние отказа. Отказ системы часто развивается не мгновенно, а по мере накопления перегрузки: происходит постепенное снижение качества работы, возрастают задержки, пропадает доступ к отдельным функциям [111].

В [52] рассматриваются методы оптимизации процессов хранения и обработки данных в РИС с целью повышения их устойчивости к деструктивным воздействиям в том числе и инфраструктурного генеза. Автор разрабатывает комплекс

математических моделей, позволяющих эффективно распределять функциональные задачи, программные элементы и информационные ресурсы между узлами и центрами обработки данных. Предлагаются дискретные методы оптимизации — метод ветвей и границ и генетические алгоритмы, а также экспериментально проверяется их практическая эффективность, выявляются оптимальные стратегии ветвления переменных и способы инициализации популяции для эволюционных методов.

В [110] рассматривается проблема повышения устойчивости функционирования РИС технологического управления инфокоммуникационной сетью специального назначения, подверженной воздействию дестабилизирующих факторов, включая целенаправленные атаки и экстремальные условия эксплуатации. Авторы предлагают метод оптимизации времени активной работы станций РИС, обеспечивающих как централизованное, так и децентрализованное управление с использованием накопительных станций.

Реализация разработанного подхода позволяет смоделировать и эффективно решать задачи, максимально приближенные к условиям реального боевого и террористического воздействия, что способствует устойчивому функционированию критически важных РИС специального назначения.

В [3] представлен методологический подход к моделированию надежности крупных территориально-распределённых ИС, в которых взаимодействуют программно-технические средства и обслуживающий персонал. Основное внимание уделено созданию и применению схем надежности, позволяющих рассматривать систему не как совокупность отдельных компонентов, но как единое целое. Предлагается представлять архитектуру РИС в виде графа, где учитываются все узлы, каналы связи и их взаимодействия, что позволяет формализовать и количественно оценить показатели надежности с учётом отказов критических компонентов и человеческого фактора.

В [6] представлена разработка метода, алгоритмов и программного обеспечения для анализа катастрофоустойчивости РИС. Исследование направлено на количественную оценку способности РИС сохранять работоспособность и быстро

восстанавливаться после аварийных и катастрофических воздействий. Формализовано понятие катастрофоустойчивости как интегрального свойства надежности и безопасности РИС, предложены вероятностные модели для описания процессов отказов и восстановления, а также оригинальные алгоритмы оценки устойчивости с учетом структурных особенностей и критичности компонентов системы.

В [164] анализируются ключевые особенности построения и эксплуатации РИС в современных условиях. Автор выделяет основные архитектурные принципы РИС, такие как клиент-серверная модель, использование распределённых баз данных, поддержка масштабируемости и отказоустойчивости, организация надёжной коммуникации между компонентами и обеспечение ИБ. Подчеркивается роль оптимального распределения функций, структурирования бизнес-процессов и согласования жизненного цикла компонентов системы для максимального соответствия потребностям бизнеса. Особое внимание уделяется вопросам формирования архитектуры с высокой функциональной связностью, распределения сервисов между узлами сети с учётом производительности, памяти и автономности компонентов.

В [182] исследуется проблема влияния человеческого фактора на устойчивость функционирования корпоративных РИС. Рассмотрены причины деструктивного воздействия пользователей (инсайдеров), значимость профессионализма и индивидуальных психологических особенностей персонала. Авторы проводят статистический анализ и формулируют математическую модель компетентности, связывающую уровень прав доступа к информационным ресурсам РИС с профессиональными качествами пользователей. Предложена методика оптимального распределения функций между человеком и машиной для повышения устойчивости системы. Особое внимание уделено построению матрицы доступа к РИС и динамическому управлению пользователями на основе их компетентности и образовательной характеристики. Использование этих подходов позволяет снижать риски, связанные с человеческим фактором, и способствует повышению надежности и устойчивого функционирования РИС в современных условиях.

В [16] рассматриваются организационные и технические процессы, обеспечивающие устойчивое функционирование РИС в условиях внутренних и внешних

деструктивных воздействий в том числе и инфраструктурного генеза. Авторы осуществляют систематизацию процессов по основным компонентам РИС: базы данных, информационные технологии, технические и программные средства. Особое внимание уделено влиянию ИТ-инфраструктуры, поддерживающей работу РИС. Ключевым аспектом становится предотвращение нарушений функционирования и своевременное восстановление отказавших компонентов для сохранения целостности РИС. Процессы описываются как комплекс научно и практически обоснованных операций эксплуатации, технического обеспечения, резервирования и ремонта, необходимых для устойчивости работы системы.

Для устойчивости РИС имеет важное значение теория надежности [171]. Теории надёжности оперируют графовыми, вероятностными и статистическими моделями, охватывают структурную и функциональную надёжность, и являются основой выбора технических и организационных решений для построения отказоустойчивых решений в современных РИС. В настоящий момент существует основной стандарт для теории надежности [27]. В стандарте систематизировано и унифицировано понятия, которые рекомендованы для применения во всех видах технической документации и научных работ, связанных с надёжностью. Однако современные исследования по устойчивости РИС в основном направлены в сторону киберустойчивости.

Киберустойчивость РИС — это способность организаций и их информационных ресурсов сохранять функциональность, противостоять кибератакам и сбоям, а также быстро восстанавливаться после инцидентов, обеспечивая непрерывность операций и защиту данных [1]. В отличие от классической ИБ, акцент делается не только на предотвращении угроз, но и на способности системы функционировать в условиях реализованных рисков, инцидентов ИБ и внешних дестабилизирующих факторов.

В [98] подробно рассматриваются основные концепции и принципы обеспечения киберустойчивости систем, основанных на технологиях машинного обучения и искусственного интеллекта (ИИ). Авторы акцентируют внимание на невозможности достижения абсолютной защиты, что требует перехода к

обеспечению устойчивости к атакам и быстрому восстановлению систем после компрометаций. Пособие содержит практические задания, тесты и вопросы для самопроверки, а также описывает характерные векторы угроз ИБ для ИИ-систем, уязвимости и современные методы защиты РИС.

В [162] рассматриваются ключевые стратегии и методы повышения киберустойчивости корпоративной ИТ-инфраструктуры РИС в условиях возрастающих цифровых угроз. Авторы анализируют современные подходы к обеспечению непрерывности бизнес-процессов, устойчивого функционирования критически важных систем и минимизации ущерба от киберинцидентов. Основными направлениями повышения устойчивости определены регулярная оценка рисков ИБ, своевременное обновление ПО, проведение аудита, тестирования на проникновение и комплексного мониторинга, внедрение принципов минимальных привилегий и многофакторной аутентификации. Авторский анализ подтверждает, что интеграция организационных, технических и образовательных мер способствует существенному повышению киберустойчивости организаций в условиях цифровой трансформации.

В [206] представлен проактивный подход к обеспечению отказоустойчивости РИС с использованием предиктивных моделей машинного обучения. Предложенная методика направлена на раннее прогнозирование потенциальных отказов и своевременное принятие мер по их предотвращению. В работе применены современные алгоритмы машинного обучения, для анализа больших объёмов оперативных данных ИБ в реальном времени. Экспериментальная проверка показала высокую точность предсказаний и значительное увеличение времени предупреждения о сбоях. Предложенный подход позволяет повысить надёжность и доступность РИС, сокращая время простоев и повышая эффективность восстановления после отказов. Адаптивность и масштабируемость метода обеспечивают его применение в различных динамичных распределённых средах и облачной инфраструктуре, что актуально для критически важных отраслей и сервисов РИС.

В [226] представлен метод прогнозирования отказов в распределённых системах на основе обучения временным рядам с использованием глубоких нейронных

структур. Предложенный подход интегрирует модель Gated Recurrent Unit (GRU) для анализа динамики состояния системы с механизмом внимания (attention), что позволяет выделять ключевые временные сегменты, важные для раннего обнаружения потенциальных сбоев. Итоговый классификатор реализован через полносвязную нейронную сеть, обеспечивая высокоточное предупреждение о возможных отказах. Экспериментальная проверка на реальных данных крупномасштабной облачной системы Microsoft Azure показала превосходство предложенной модели над популярными временными моделями (Transformer, Informer, Autoformer, FEDformer) по точности (Accuracy), сбалансированности (F1-Score) и общему качеству классификации (AUC). Данный метод демонстрирует устойчивость, стабильность обучения и способность эффективно выявлять скрытые паттерны системного поведения РИС.

В статье [213] предложен лёгкий и точный подход для прогнозирования отказов и локализации соответствующих неисправностей в многоуровневых РИС. Метод «PreMiSE» совмещает методы обнаружения аномалий и сигнатурные техники для идентификации отказов, влияющих на показатели производительности, с высокой точностью и низким уровнем ложных срабатываний. Эксперименты, проведённые на облачной системе «IP Multimedia Subsystem», показали, что «PreMiSE» эффективно предсказывает потенциальные отказы и локализует их источники с минимальными накладными расходами по ресурсам. Предложенный метод способствует заблаговременному принятию корректирующих мер и повышению надёжности РИС.

Отметим, что существует так называемая теорема CAP (Consistency, Availability, Partition Tolerance), которая играет ключевую роль в устойчивости РИС, поскольку формулирует фундаментальное ограничение: в условиях сетевых разделений система может выбрать только два из трёх свойств — согласованность (Consistency), доступность (Availability) и устойчивость к разделению (Partition Tolerance) [201].

Теорема CAP заставляет архитекторов и инженеров распределённых систем делать осознанный выбор и идти на компромиссы между консистентностью,

доступностью и устойчивостью к разделению, исходя из конкретных требований и бизнес-рисков информационной системы.

Например, NoSQL-системы для Big Data часто жертвуют консистентностью ради высокой доступности и устойчивости, тогда как финансовые сервисы ставят в приоритет консистентность и устойчивость к разделению, иногда жертвуя доступностью в короткие моменты сетевых проблем теорема CAP служит основой для анализа архитектурных решений, оценки надёжности и отказоустойчивости современных РИС и позволяет гибко управлять рисками ИБ, обеспечивая максимальную устойчивость под заданные требования [50].

Таким образом устойчивость РИС обеспечивается совокупностью организационно-технических мер: резервированием, мониторингом, управлением ресурсами, безопасностью и учётом человеческого фактора. Рост нагрузки является ключевым фактором, способствующим переходу РИС в неустойчивое состояние с постепенным снижением качества работы и отказами. Кроме того, теория надёжности и используемые статистические методы не всегда способны адекватно описать и прогнозировать отказы в современных РИС из-за их возрастающей сложности, интеграции с облачными и гибридными структурами, а также применения новых технологических решений, что требует постоянного обновления и модернизации моделей. Современные методы повышения устойчивости включают оптимизацию распределения задач и ресурсов, применение математических моделей и алгоритмов, а также разработку подходов к управлению специализированными инфокоммуникационными системами в сложных условиях и требуют в том числе выявления и оценки эффектов ИД.

1.4 Постановка цели и задач, решаемых в диссертационном исследовании

Анализ текущего состояния современных подходов к прогнозированию и оценке эффектов ИД в РИС показывает, что возможности существующих научно-методических разработок и решений не удовлетворяют требованиям практики.

Целью работы является повышение оперативности и точности выявления эффектов деструктивного воздействия инфраструктурного генеза в распределенных информационных системах.

Для достижения цели необходимо решить следующие задачи:

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 ИБ инфраструктурного генеза в распределенных информационных системах.

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

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

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.

Таким образом, тема диссертации «Оценка влияния эффектов деструктивного воздействия инфраструктурного генеза на информационную безопасность распределённых информационных систем» в целом соответствует направлению информационной безопасности и специальности, связанной с защитой РИС.

Тематика сфокусирована на исследовании влияния особого класса угроз ИБ — ДВ ИГ (например, сбои оборудования, сетевые отказы, внешние физические воздействия) — что соответствует задачам оценки рисков и обеспечения надёжности РИС, ключевым в ИБ РИС.

Полное исключение или нейтрализация таких угроз часто невозможны или экономически нецелесообразны, так как инфраструктурные риски связаны с техническими и физическими аспектами, находящимися вне прямого управленческого контроля.

Оценка воздействия позволяет выявить степень риска и потенциальные последствия для ИБ, что важно для планирования профилактических мер, резервирования, устойчивости и восстановления работы систем. Анализ позволяет оптимизировать стратегии защиты, сосредоточив ресурсы на наиболее критичных и вероятных сценариях ДВ ИГ.

Кроме того, оценка обеспечивает понимание взаимосвязей между инфраструктурными сбоями и их каскадным влиянием на ИБ, что необходимо для комплексного управления рисками и повышения устойчивости систем.

Таким образом, работа важна, так как направлена не на простое устранение угроз, а на системное понимание их влияния и формирование эффективных мер по снижению рисков ИБ и обеспечению непрерывности работы РИС, что обосновано текущей научной практикой в современными исследованиями по ИБ.

1.5 Выводы разделу 1

В качестве объекта исследовались распределенные информационные системы (РИС) на предмет обнаружения угроз информационной безопасности, связанных с том числе и с эффектами ИД.

В ходе исследования:

1) Проанализированы типы и методы построения РИС и показаны их особенности ИБ. Сформулирован понятийный аппарат для формализации процессов в РИС в контексте ИБ. Сформулированы общие подходы к обеспечению ИБ, а именно: безопасность элементов (объектов) ИТ-инфраструктур РИС, так и как структуры межобъектного взаимодействия. Показана недостаточная проработка по обеспечению ИБ межобъектного взаимодействия в ИТ-инфраструктурах РИС.

2) Рассмотрены и проанализированы методы обеспечения ИБ в ИТ-инфраструктурах РИС. Рассмотрены угрозы ИБ различного генеза для ИТ-инфраструктур. Установлена зависимость увеличения рисков сбоев в работе ИТ-инфраструктур от их взаимозависимостей. Определен конвейер интеллектуального анализа журналов событий. Отмечен перспективный подход к повышению безопасности межобъектного взаимодействия ИТ-инфраструктурах РИС на основе поведенческого анализа (UEBA), в том числе и на основе антропоморфического поведения в технических системах.

3) Проанализированы различные методы для оценки рисков ИБ как инфраструктурного, так и не инфраструктурного генеза. Определен феномен наличия эффектов инфраструктурного деструктивизма (ИД) в РИС. Приведены примеры возникновения эффектов ИД. Выполнен анализ цифровых результатов проявления ИД в РИС, а также и определены закономерности их появления.

4) Выявлено противоречие предметной области: наличие феномена инфраструктурного деструктивизма при ИБ ИТ-инфраструктурах РИС происходит на фоне отсутствия регулятивных методов и готовых методик для их оценивания и выявления.

5) Сформулирована научно-техническая задача исследования, разработка моделей и методов, позволяющих выявлять, анализировать и количественно оценивать эффекты деструктивного воздействия (ДВ) инфраструктурного генеза (ИГ) в сервис-ориентированных информационных системах в условиях инфраструктурного деструктивизма.

Данные результаты непосредственно использованы для формулировки научно-технической задачи – разработка моделей и методов, позволяющих выявлять, анализировать и количественно оценивать эффекты. деструктивного воздействия инфраструктурного генеза в сервис-ориентированных информационных системах в условиях инфраструктурного деструктивизма.

Основное содержание раздела и изложенных в нем научных результатов опубликовано в работах автора [136, 134, 149, 150, 142, 138].

2 КОМПЛЕКС МОДЕЛЕЙ ВЗАИМОДЕЙСТВИЯ СЕРВИСОВ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ ЭФФЕКТОВ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ИНФРАСТРУКТУРНОГО ГЕНЕЗА

2.1 Формальное описание феномена инфраструктурного деструктивизма в распределенных информационных системах

Введем необходимые определения и понятия для описания проявлений эффектов ИД, а также угроз ИБ ДВ ИГ и других смежных областей.

Определение. Инфраструктурный деструктивизм (ИД) — это феномен, возникающий в ИС, когда в результате деструктивных воздействий (ДВ) инфраструктурного генеза (ИГ) происходят системные изменения, ведущие к нарушению устойчивости, целостности, доступности, функциональности и управляемости информационной системы (ИС).

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

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

Сформулируем и опишем основные характеристики феномена ИД:

1) Генезис ИД. ИД возникает не только как следствие целенаправленных атак, но и как результат внутренних процессов, ошибок, несовершенства архитектуры, неучтённых взаимосвязей и изменений состава или функций объектов ИТ-инфраструктуры ИС на протяжении всего жизненного цикла её функционирования.

2) Механизм проявления ИД. ДВ ИГ реализуются через инфраструктурные связи между объектами, что приводит к возникновению новых уязвимостей и разрушению ранее устойчивых связей, зачастую без прямого внешнего вмешательства.

3) Системная деструкция. ИД проявляется как системная деструкция — разрушение структуры, организационных и функциональных связей, приводящее к снижению или потере управляемости, устойчивости, отказу или деградации ИС в целом.

4) Динамический характер ИД. Мера опасности ИД носит динамический характер и зависит от этапа жизненного цикла ИС, режима функционирования, состояния межобъектных связей и других факторов.

5) Имманентная (внутренняя) угроза ИД. ДВ ИГ рассматриваются как новый класс имманентных угроз, отличающихся от традиционных внешних угроз тем, что их источники и последствия обусловлены самой природой и эволюцией ИТ-инфраструктуры ИС.

6) Синергетический эффект. В ряде случаев ИД приводит к синергетическим эффектам, когда разрушительные последствия одного воздействия многократно усиливаются за счёт цепных реакций во взаимодействующих объектах.

7) Доброкачественный и злокачественный ИД. Помимо разрушительных «злокачественных» проявлений, деструктивизм может выполнять и защитную «доброкачественную» функцию, например, локализуя сбои и предотвращая распространение ущерба по инфраструктуре.

Определение. «Деструктивный мусор» – программный код, внесенный в ИС после устранения уязвимостей ИБ и ошибок программного кода, реализованный не оптимальным образом.

Накопление «деструктивного мусора» является не контролируемым процессом и приводит к необратимым процессам на объектах ИС. Данное явление отмечено во многих исследованиях посещённых устойчивости ИС [1, 19, 52]. С целью описания основных процессов, влияющих на развитие ИТ-инфраструктуры, рассмотрим концептуальную модель предметной области. ИТ-Инфраструктуру можно

представить через систему взаимодействующих объектов. Особый интерес представляет межобъектное взаимодействие в инфраструктуры, реализуемое через сервисы. Таким образом на каждом из объектов можно выделить множества ошибок и уязвимостей программного кода, а также множество особенностей межобъектного взаимодействия.

В настоящее время уже рассматриваются проблемы устойчивости ИТ-инфраструктуры. В работах [59,86, 89, 127,186, 188,225] к ним отнесены проблемы сервисов ИТ-инфраструктуры ИС в контексте: координации межобъектного взаимодействия; развертывание инфраструктуры; сетевое взаимодействие сервисов; управление данными; отладка и мониторинг процессов; безопасность; архитектурные особенности.

В качестве источников «конфликтов интересов» в ИТ-инфраструктуре ИС обозначены [186, 188,225]: данные; сетевое взаимодействие; ресурсы; конфигурации. На практике феномен ИД может проявляться в виде событий ИБ, приводящих к необратимым последствиям. Например, «совокупность случайных факторов» проявление «непредвиденных событий», «закономерных случайностей» и др. Данные ситуации, возникшие на одном из объектов ИТ-инфраструктуры в итоге, влияют на её работу в целом. Данные события, ситуационно, предлагается классифицировать следующим образом.

Ситуация 1. Возникновение ИД при условии наличия внешних ДВ. Это могут быть различные кибератаки, вирусные атаки и другие возможные злонамеренные воздействия на объекты ИТ-инфраструктуры из вне. В данной ситуации генез ДВ не конкретизирован.

Ситуация 2. Возникновение ИД при изменении самой инфраструктуры. Данная ситуация возможна при добавлении, удалении, изменении объектов (узлов) и связей информационной инфраструктуры, а также может быть вызвано необратимыми изменениями и прекращением процесса нормального функционирования ИТ-инфраструктуры.

Ситуация 3. Возникновение ИД при отсутствии влияния внешних факторов и изменений в ИТ-инфраструктуре ИС. Данная ситуация возникает за счет

факторов, не зависящих от инфраструктуры и внешних ДВ. Это возможно, например, при наличии скрытых особенностей и ошибок программного кода. Ситуация 3 проявляется не явным образом. При этом сказываются эффекты накопления «деструктивного мусора», который появляется, в том числе, в результате лечения активного заражения и последствий ликвидации кибератак [1].

Накопление «деструктивного мусора» является не контролируемым процессом и приводит к необратимым процессам на объектах. Эффект инфраструктурного деструктивизма для ситуации 3 также может возникнуть и при изменении поведения объектов инфраструктуры.

Например, один сервис замедляет работу другого сервиса, используя общие ресурсы. Или при добавлении одного из объектов в инфраструктуре повышается её производительность в целом. Следует отметить, что возможно одновременное проявление нескольких ситуаций. Тем не менее, в ходе исследования будем рассматривать их локально. На основании вышеизложенного можно утверждать, что появление эффектов ИД, во многом зависит от внутренних состояний, внутренних целей и сценариев работы объектов ИС (рисунок 12).

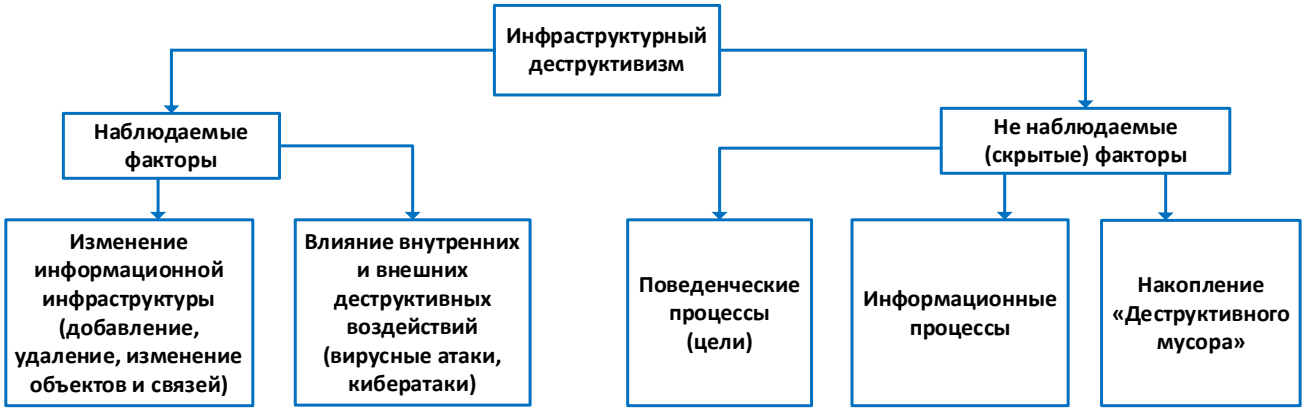

Рисунок 12 – Структурная схема факторов, влияющих на ИД

Обозначенное необходимо рассматривать на уровне сервисов, так как в основе современных ИС заложены сервисно-ориентированные архитектуры. Одним из приоритетных вопросов является вопрос, связанный с обнаружением эффектов ИД сервисов ИС, что предлагается решить на основе разных подходов [1].

2.2 Модель обнаружения эффектов деструктивного воздействия инфраструктурного генеза в сервис-ориентированных информационных системах

2.2.1 Формализация межсервисного взаимодействия в распределенных информационных системах

Для обнаружения эффектов ИД сервисов в РИС рассмотрим и формализируем их принципы работы. Как правило в ИТ-инфраструктуре взаимодействуют несколько сервисов.

Определение. Сервис — это компонент приложения в сервисной архитектуре РИС, который можно разрабатывать, развёртывать, эксплуатировать, изменять и развёртывать повторно, не нарушая работу других сервисов и целостность приложения [42, 186].

На рисунке 13 представлен пример обработки запросов сервисом в ИТ-инфраструктуре. Каждому сервису направляется последовательность запросов в доступные программные интерфейсы (ПИ). Иногда ответ на запрос не приходит. В общем случае у одного сервиса, может быть, несколько разных интерфейсов для обработки запросов. Запросы могут отправлять как пользователи сервиса, так и другие сервисы.

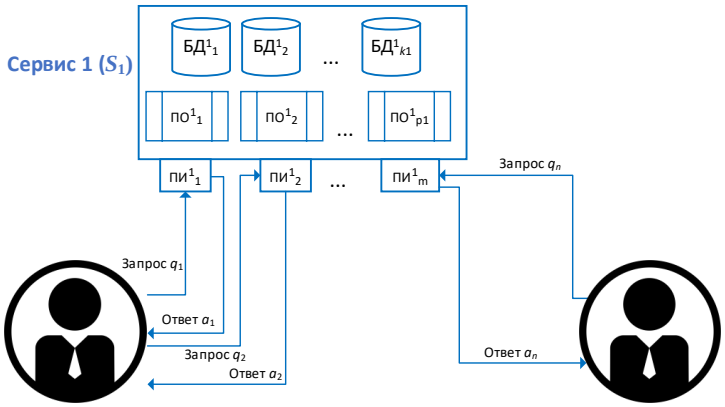

Рисунок 13 – Пример выполнения запросов сервисом ИС через его ПИ

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

клиентов в РИС описывается композицией 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): $КПО_j = \{ПО_1^j, ПО_2^j \ldots ПО_{l^j}^j\}$ и комплект баз данных $КБД_j = \{БД_1^j, БД_2^j \ldots БД_g^j\}$. 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): $НПИ_j = \{ПИ_1^j, ПИ_2^j \ldots ПИ_{r^j}^j\}$, где r – количество программных интерфейсов для каждого сервиса j. Общее число программных интерфейсов в РИС – множество $R = \{r_1, r_2, \ldots r_m\}$. На каждый из программных интерфейсов поступает последовательность запросов $Q_i^j = q_1^i, q_2^i \ldots q_{n_i}^i$, 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 $\oplus_{j=1}^{|S|}(S_j, КПО_j, КБД_j, НПИ_j)$. Композиция запросов и процессов задается отображением $\psi : Q \to Proc$, обеспечивая динамику $(\oplus_{j=1}^{|S|}, НПИ, Q, Proc)$.

Таким образом, сервис S_j, обрабатывая запросы, запускает процессы их обработки и отсылает ответы. Типовая структура запроса к сервису с учетом различных архитектур их взаимодействия представлена на рисунке 14.

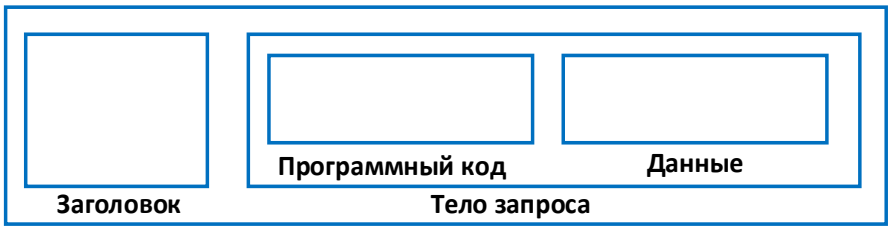

Рисунок 14 – Типовая структура запроса к сервису

Технологический каждый запрос к сервису РИС включает в себя заголовок, тело запроса. В теле запроса передается программная часть и часть с данными. Для каждого сервиса существует набор доступных программных интерфейсов (ПИ), через которое происходит взаимодействие. Таким образом обозначенные выше составные части запроса: заголовок и тело запроса (см. рис. 14) могут содержать

угрозы ИБ. Данные угрозы ИБ в ПИ могут приводить РИС в состояния отказа в обслуживании. Данный факт подтверждает существование эффектов ИД, который вызывают определенные последовательностей запросов. Для упрощения управления конфигурацией и контроля ИБ достаточно часто используется понятие шлюз программных интерфейсов.

Определение. Шлюз программных интерфейсов (API Gateway) – это серверный прокси, который предоставляет интерфейс для клиентов (приложений, устройств, пользователей) для доступа к сервисам инфраструктуры [42,186].

Определение. Конечные точка входа программного интерфейса (точка входа программного интерфейса) – это точка входа в программную часть сервиса, через которую осуществляется взаимодействие [43, 186].

Определение. Параметры запроса – это параметры, передаваемые запросу (опции), которые можно передать вместе с конечной точкой, чтобы повлиять на ответ. Они похожи на фильтры поиска и выделяют данные, которые нужно получить от программного интерфейса.

Пусть последовательность запросов к сервису представлена в виде множества:

$$Q_i^j = q_1^i, q_2^i \dots q_{n_i}^i, \tag{1}$$

где $j = \overline{1,m}$, $i = \overline{1,r_j}$.

Тогда в ответ на запросы Q_i^j, сервис отправляет последовательность ответов:

$$Ack_i^j = \{a_1, a_2, \dots a_n\}, \tag{2}$$

где $j = \overline{1,m}$, $i = \overline{1,r_j}$.

Как запросы Q_i^j, так и ответы Ack_i^j фиксируются в системах регистрации журналов событий. Для сервисных архитектур РИС существуют отдельные программные инструменты, которые позволяют не только собирать данные о работе сервисов, но и их визуализировать. Такой процесс сохранения «следов» запросов к сервисам называется управление журналами событий.

Определение. Управление журналами событий (log management) — это процесс сбора, хранения и анализа данных, которые отслеживают каждое действие или событие в программном обеспечении, приложениях и ИТ-инфраструктуре [43, 38].

2.2.2 Оценка эффектов инфраструктурного деструктивизма

На первом этапе положим, что каждый из запросов Q и ответов Ack к сервису в РИС фиксируется в журнале событий. При этом детализация процессов обработки запросов зависит от конкретных технических реализаций РИС. Для обнаружения эффектов ИД будем анализировать два типа параметров: базовые и дополнительные.

Базовые параметры представлены параметрами из журналов событий: начало выполнения запроса, время окончания выполнения запроса, конечные точка входа программного интерфейса, параметры выполнения запроса. Необходимы для обнаружения эффектов ИД.

Дополнительные параметры представлены параметрами из журнала событий такими как: точный адрес вызова, затраты ресурсов, дополнительные параметры, отчет о возникших ошибках, траектория выполнения и др. Необходимы для расширения представления об исходных данных для описания существующего уровня оценки эффектов ИД.

В работах [25, 99, 81] представлены подходы, связанные с интеллектуальным анализом журналов событий для нахождения аномалий работы сервисов.

Однако данные работы рассматривают аномалии как явление для обнаружения кибератак и не учитывают ДВ инфраструктурного генеза (ИГ), которые также описаны в этих работах.

Деструктивные воздействия ИГ могут привести к изменению времени работы сервиса. Данная ситуация, объясняется наличием общих ресурсов, также особенностью архитектур РИС.

С целью нахождения аномалий – эффектов (показателей) ИД в журналах событий на первом этапе время обработки запросов Q представляется в виде

временной диаграммы. На втором этапе рассматривается зависимость времени обработки запроса от количества потраченных ресурсов.

При обработке каждого запроса затрачивается определённое количество ресурсов каждый из этих ресурсов обозначим переменными:

$$R = \{R_1, R_2, \ldots, R_z\}, \tag{3}$$

где $i = \overline{1,z}$, z – количество анализируемых ресурсов.

Наиболее часто в ИС используются следующие типы ресурсов: процессорное время; использования оперативной памяти; использование долговременной памяти; использование ресурсов видеоадаптера; использование сетевых устройств и другое. Организационная схема обработки последовательности запросов представлена на рисунке 15.

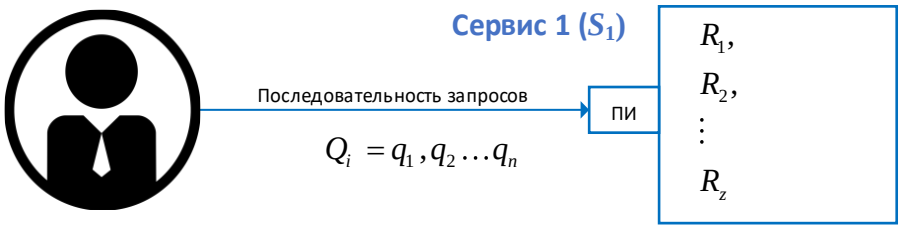

Рисунок 15 – Организационная схема обработки последовательности запросов Q_i

Построим временную диаграмму для отображения затрат ресурсов R для обработки некоторой последовательности запросов Q. Временная диаграмма обработки последовательности запросов Q_i представлена на рисунке *16*.

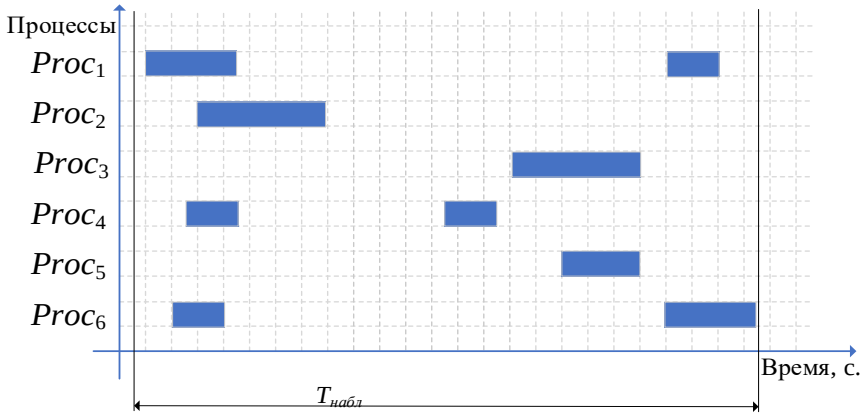

Рисунок 16 – Временная диаграмма обработки последовательности запросов Q

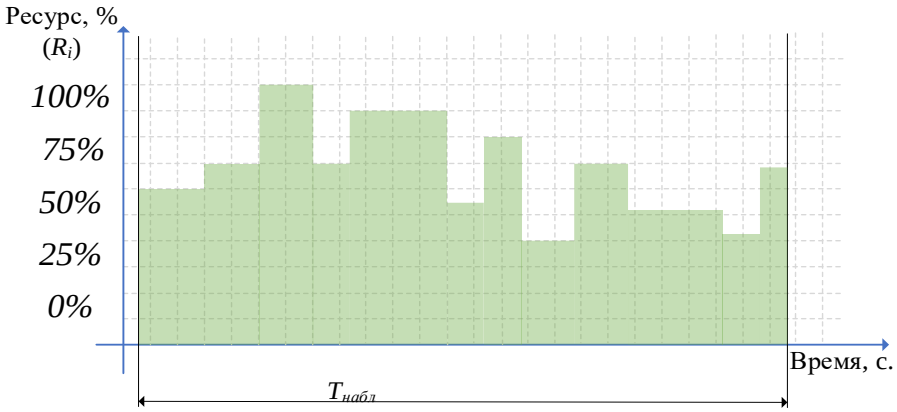

Рисунок 17 – Пример использования ресурсов для обработки последовательности запросов Q

В ситуации, когда ресурсов не хватает для выполнения запросов некоторые запросы выполняются дольше или же возможно приведение РИС в состояние отказ в обслуживании. Для снижения данных эффектов в современных РИС активно применяются инструменты оптимизации, которые используют кэш и другие механизмы позволяющие выполнять запросы параллельно, а также использовать ресурсы для одинаковых задач совместно.

Использование совместных ресурсов позволяет ускорить выполнение запросов. Однако достаточно часто при оптимизации выполнения оптимизатор вместо того, чтобы ускорить процесс обработки запросов – замедляет их обработку. Этот эффект можно объяснить перестройкой внутренних состояний (кеша) оптимизатора. Сама по себе операция перестройки кеша достаточно долгая и может быть в несколько раз дольше чем сам эффект от оптимизации запросов.

Вместо оценки ресурсов, таких как оперативная память и процессорное время, часто используют понятие «O-символики» [71]. «O-символика» (или O-нотация, Big O notation) — это формальное математическое обозначение, используемое для оценки сложности алгоритма. Она показывает, как изменяются временные или пространственные затраты алгоритма (количество шагов, операций или потребляемой памяти) при увеличении размера входных данных. Это стандарт в анализе алгоритмов, поскольку позволяет сравнивать их эффективность и предсказать поведение решений при больших объемах данных, игнорируя конкретную реализацию и скорость каждой отдельной операции. Такой подход позволяет интегрально оценивать использование ресурсов для конкретной алгоритмической

реализации и устанавливает взаимосвязь между временем выполнения программного обеспечения и затрачиваемыми ресурсами [71]. Не нарушая общности, далее в работе будем оценивать потребления ресурсов в РИС для последовательности запросов Q использую время в секундах.

Всё это вместе с тем, что процесс оптимизации запросов часто не предсказуемый, является источником угроз деструктивных воздействий (ДВ) инфраструктурного генеза (ИГ). Рассмотрим по отдельности возможные подходы для нахождения запросов, которые приводят к появлению эффектов ИД.

Рисунок 18 – Структурная схема подходов исследования последовательностей запросов для определения эффектов инфраструктурного деструктивизма

Одно из действий на данном этапе связано с нахождением долгих или аномальных запросов, которые приводят РИС к отказу в обслуживании. Нахождение долгих запросов можно осуществить путём простого анализа последовательности запросов хранящихся в журнале событий системы для нахождения самых долгих из них. Однако гораздо важнее является не только найти эти запросы, но и понять почему они являются долгими, то есть это можно объяснить используя, а описанную выше ситуации обработки запросов, то есть в какой-то момент в РИС запросы исчерпывают ресурсы и работает дольше. Также возможно оптимизатор настроен таким образом, что вместо того, чтобы ускорять выполнение запросов он начинает перестраиваться отмечено, что многие имеющиеся оптимизаторы выполнения запросов работают не оптимально и недостатки способные приводить к ИД. Таким образом выдвигается гипотеза если найти последовательность запросов, которые

являются долгими, и их только посылать в РИС то это может привести к проявлению эффектов Ид и в худшем случае в состояние саморазрушения и отказа в обслуживания

На третьем этапе рассматривается задача прогнозирования времени выполнения запроса. Сформулируем её следующим образом: для заданной последовательности запросов необходимо определить прогнозное время выполнения каждого последующего запроса. В настоящее время существует ряд методов, позволяющих решать данную задачу, среди которых можно выделить: регрессионные модели прогнозирования; авторегрессионные модели (ARIMAX, GARCH, ARDLM); модели экспоненциального сглаживания (ES); модели на основе выборки максимального подобия (MMSP); модели на нейронных сетях (ANN); модели на основе цепей Маркова (Markov Chains); модели классификационно-регрессионных деревьев (CART); модели, основанные на генетических алгоритмах (GA); модели на опорных векторах (SVM); модели на базе передаточных функций (TF); модели, основанные на нечеткой логике (FL). Из рассмотренных методов, с учётом специфики ИТ-инфраструктуры РИС, целесообразно выбрать авторегрессионный подход [2]. Он обеспечивает возможность учитывать прошлые значения временного ряда и одновременно оценивать информационную значимость последующих прогнозов.

Для описания интегрированной модели авторегрессии и скользящего среднего используется классический подход. Таким образом предположим, что для временного ряда y_i который необходимо прогнозировать применяется d-раз операция последовательной разности. В результате чего этот временной ряд становится стационарным рядом который удовлетворяет условие

$$y_t - \varphi_1 \cdot y_{t-1} - ... - \varphi_p \cdot y_{t-p} = \delta + \varepsilon_t - \theta_1 \cdot \varepsilon_{t-1} - ... - \theta_p \cdot \varepsilon_{t-p}, \quad (4)$$

где y_t – прогнозируемое значение; φ_j – параметр авторегрессионной модели $j = \overline{1, t-p}$; θ_i — параметры скользящего среднего; $\varepsilon_t \approx iid(0, \sigma^2)$ – белый шум; p – порядок авторегрессии (AR); d — степень дифференцирования (I); q — порядок скользящего среднего (MA).

Для построения модели ARIMA используется методология Бокса-Джекинса, состоящая из следующих последовательных трех этапов [2].

Шаг 1. Идентификация модели.

1) Процедура получения стационарности ряда. Исходный ряд тестируется на стационарность. Если получается стационарный ряд, то выполняется шаг 1.2, если нет, то применяется процедура взятия последовательной разности и повторяется тестирование.

2) На вход передается стационарный временной ряд, для которого рассчитываются автокорреляционная функция и автокорреляционная функция процесса. Выбранные функции лишь приблизительно соответствуют теоретическим аналогам, но должны быть достаточно приближены.

Шаг 2. Оценивание модели и проверка ее адекватности.

1) Для всего набора выбранных моделей из шага один, строятся оценки их параметров и вычисляются остатки.

2) Каждая из полученных моделей проверяется на соответствие исходным данным. Из тех моделей, которые адекватны данным, отыскивается наиболее простая модель, то есть модель, которая имеет наименьшее количество параметров.

Шаг 3. Прогнозирование временного ряда. После нахождения набора адекватных моделей, выполняется прогноз на несколько шагов по времени с оценкой доверительных границ прогнозных значений.

На четвёртом этапе осуществляется дальнейший анализ, направленный на выявление закономерностей в журналах событий. Эта задача сводится к отысканию частых наборов последовательностей запросов Q в большом наборе данных, содержащемся в журналах событий. Для решения поставленной задачи предлагается применить классические алгоритмы обнаружения частых последовательностей в больших объёмах данных, такие как Apriori (AprioriAll, GSP, SPADE). [117, 192]. Более сложные алгоритмы, основанные на детектировании строго последовательных событий, применяются для идентификации «жёстких» сценариев, например Strict Contiguity (SC). Более гибкий подход, допускающий игнорирование «шумовых» событий между элементами искомого шаблона и особенно актуальный для

анализа реальных журналов событий, реализован в алгоритме Skip-till-next-match (STNM) [192].

Теория последовательных шаблонов во многом основана на теории ассоциативных правил и, по сути, является ее расширением. В частности, базовыми понятиями в ней также являются транзакция, предметный набор, частота набора, поддержка и т.д. Введем ряд определений позволяющих описать процесс обнаружения эффектов ИД на основе частых наборов последовательностей запросов Q в большом наборе данных, содержащемся в журналах событий с учетом имеющейся специфики задачи [117, 192].

Определение. Шаблон последовательности – это последовательность наборов, которая часто встречается в журналах событий и содержит параметры обработки запросов Q.

Определение. Набор последовательности запросов (itemset) $Q^{item} = \{q_a, q_b, ...q_c\}$ – это последовательность наборов цепочек запросов, которая часто встречается в журналах событий вместе и приводит возникновению эффектов ИД.

Определение. Поддержка последовательности (support), приводящая к возникновению эффектов ИД – это отношение количества последовательностей запросов с к общему числу запросов: $\text{supp}(Q^{item}) = \left|Q^{item}\right| / |Q|$.

Пример структуры запросов согласно описанным определениям представлен на рисунке 19.

Определение. Достоверность (confidence), приводящая к возникновению эффектов ИД – показатель того, как часто последовательности запросов встречаются вместе $conf(Q_1^{item} \cup Q_2^{item}) = \text{supp}(Q_1^{item} \cup Q_2^{item}) / \text{supp}(Q_1^{item}) \cdot \text{supp}(Q_2^{item})$.

Определение. Отношение поддержки (lift) – это отношение зависимости набора Q_1^{item} к другому набору Q_2^{item}, которое показывает, насколько наборы зависят друг от друга $lift(Q_1^{item} \cup Q_2^{item}) = \text{supp}(Q_1^{item} \cup Q_2^{item}) / \text{supp}(Q_1^{item}) \cdot \text{supp}(Q_1^{item})$.

Определение. Убедительность (Conviction) – это частота появления набора Q_1^{item} без набора Q_2^{item}: $conv(Q_1^{item} \cup Q_2^{item}) = 1 - \text{supp}(Q_1^{item}) / 1 - conf(Q_1^{item} \cup Q_2^{item})$.

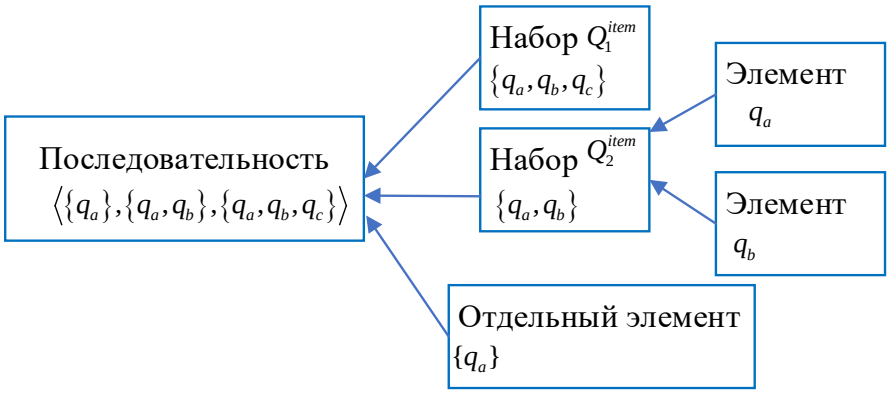

Рисунок 19 – Структурная схема шаблонов последовательностей, наборов и элементов журналов событий для оценки эффектов ИД

Основываясь на принципах работы алгоритмов поиска последовательных шаблонов Apriori (AprioriAll, AprioriSome) [117, 192] введем в следующее утверждение: если $Q_x^{item} \subseteq Q_y^{item}$, то $\text{supp}(Q_x^{item}) \geq \text{supp}(Q_y^{item})$.

Из этого следует следующих два свойства:

1) Если набор запросов Q_y^{item} выполняется долго, то любое подмножество наборов запросов $Q_x^{item} : Q_x^{item} \subseteq Q_y^{item}$.

2) Если набор запросов Q_y^{item} выполняется быстро, то любое подмножество наборов запросов $Q_x^{item} : Q_x^{item} \subseteq Q_y^{item}$.

Обозначенные свойства позволяют подбирать наиболее долгие наборы последовательных запросов, приводящие к проявлению эффектов ИД.

2.2.3 Анализ возможных источников возникновения инфраструктурного деструктивизма

В качестве источников возникновения ИД рассмотрим компоненты сервис-ориентированных архитектур РИС. Это объяснимо тем, что работа сервиса в сервисной архитектуре связана использованием особых компонент, благодаря которым повышается масштабируемость и производительность ИС. Однако эти средства могут как помочь РИС работать быстрее, так и существенно замедлять её работу. Наличие в сервисной архитектуре описанных ниже компонент является

необходимым условием для возникновения эффектов инфраструктурного деструктивизма.

Определение. Планировщик запросов — это компонент сервисных архитектур ИС, который формирует упорядоченный набор шагов, используемых для доступа к данным.

Определение. Оптимизатор запросов — это компонент современных сервисных архитектур, который отвечает за создание плана запроса. Он оценивает несколько альтернативных подходов к решению запроса к базе данных и выбирает наиболее оптимальный план с учётом различных факторов, таких как доступные аппаратные ресурсы, схема базы данных, распределение данных и статистика, сложность запроса и системные настройки.

Определение. Кэширующий сервис — это компонент сервис-ориентированных архитектур, который не является авторитативным ни для одной зоны сервером, но используется для исполнения запросов. Он обслуживает запросы и опрашивает другие сервера, отвечающие за необходимую информацию.

Пример организационной структуры работы кэширующих сервисов РИС представлена на рисунке 20.

Определение. Горизонтальное масштабирование — это подход к обеспечению эффективного роста программных приложений, особенно в контексте сценариев высокой нагрузки и корпоративных сценариев.

Определение. Шлюз программного интерфейса (Gateway API или API-шлюз) — жизненно важный компонент сервисной архитектуры. По сути, это программный компонент (шаблон), размещённый перед программными интерфейсами сервисов или группой микросервисов для облегчения входящих запросов и исходящей доставки данных.

Определение. Балансировщик нагрузки (Load balancer) распределяет входящие клиентские запросы между группой серверов, в каждом случае возвращая ответ от выбранного сервера соответствующему клиенту.

Балансировщики нагрузки могут работать с несколькими протоколами — HTTP, а также протоколом Domain Name System, Simple Message Transfer Protocol

и Internet Message Access Protocol. Балансировщик нагрузки получает и направляет клиентские запросы на данные приложений, текста, изображений или видео на любой сервер в пуле, который способен их выполнить, а затем возвращает ответ сервера клиенту.

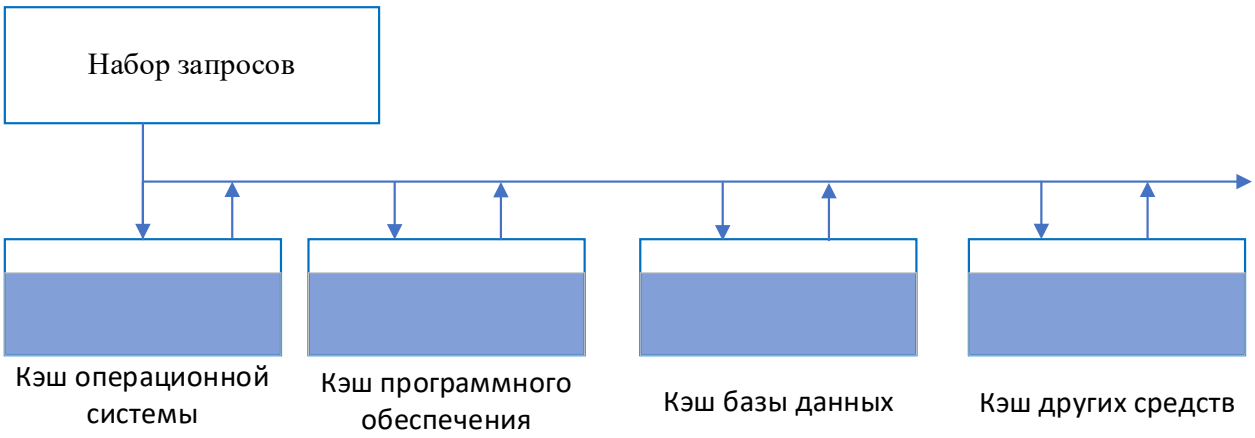

Рисунок 20 – Организационная структура работы кэширующих сервисов РИС

Определение. Обратный прокси-сервер (Reverse Proxy) принимает запрос от клиента, пересылает его на сервер, который может его выполнить, и возвращает ответ сервера клиенту. Другими словами, обратные прокси-серверы действуют как таковые для HTTP-трафика и интерфейсов прикладного программирования

Определение. Брокер сообщений — это архитектурный шаблон в распределённых системах, который выступает посредником в коммуникации между различными частями системы. Обозначенные выше элементы сервис-ориентированных ИС являются возможными источниками возникновения эффектов ИД.

Обозначенные компоненты создают условия для высокоэффективной работы сервисов, однако одновременно являются потенциальными источниками возникновения эффектов ИД, способных существенно снизить скорость функционирования системы при неэффективном взаимодействии или перегрузках. Важно учитывать баланс между внедрением новых архитектурных решений и управлением их взаимодействием для поддержки надёжности, отказоустойчивости и минимизации негативных инфраструктурных эффектов.

Таким образом, архитектурные элементы сервис-ориентированных систем не только способствуют развитию гибкости и масштабируемости РИС, но и требуют комплексного подхода к мониторингу и оптимизации производительности, чтобы эффективно противостоять угрозам инфраструктурного генеза и сохранить устойчивость системы при высокой нагрузке.

2.3 Комплекс антропоморфических моделей взаимодействия сервисов распределенных информационных систем

2.3.1 Модель обработки последовательностей запросов

В пункте 2.2 описана модель оценки эффектов ИД для РИС. Рассмотрим случай, когда несколько сервисов взаимодействуют между собой и на каждый сервис отправляется запросы от клиентов, как представлено на рисунке 21.

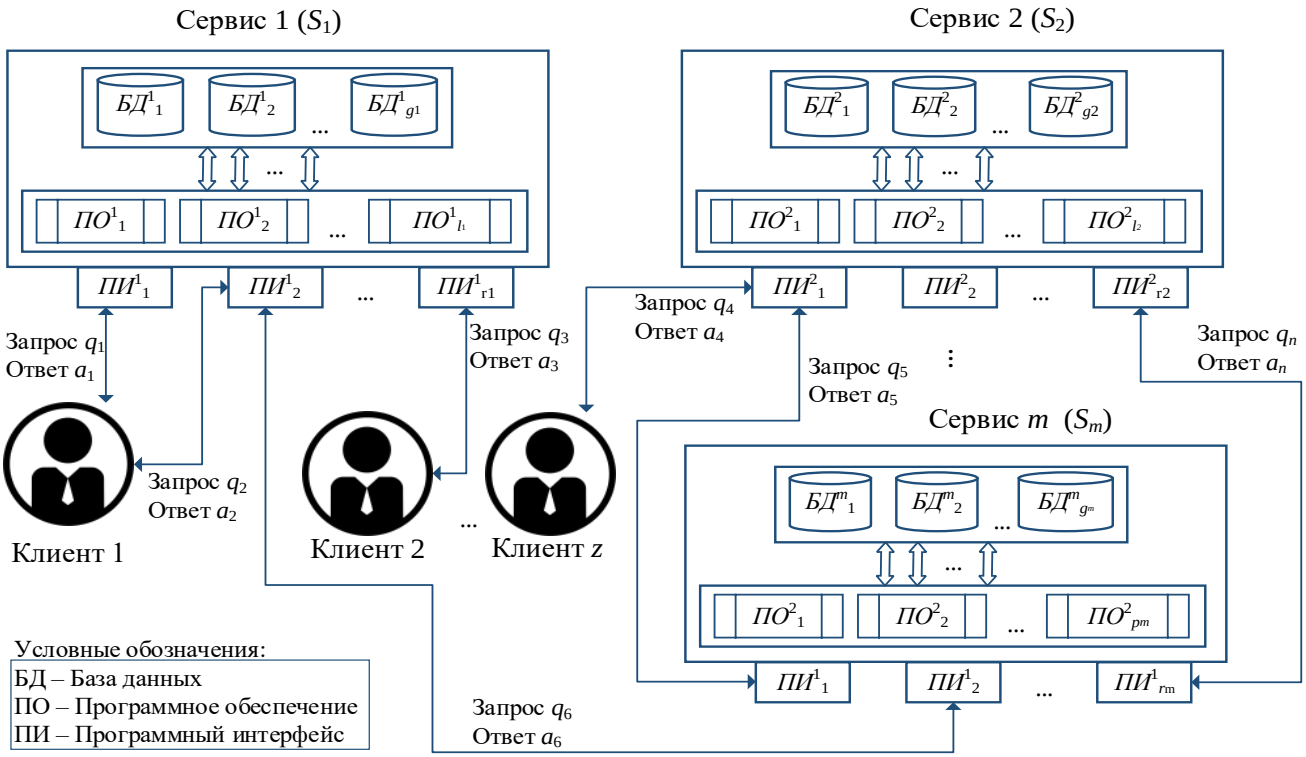

Рисунок 21 – Схема организации взаимодействия сервисов и клиентов в РИС

Каждый запрос в РИС имеет своё время обработки. Для одинаковых запросов время выполнения, может быть разным и зависит от внутреннего состояния и наличия свободных ресурсов РИС.

Обозначим общее количество всех запросов в ИТ-инфраструктуре как $Q_{all} = q_1, q_2, ...q_n$, где n – общее количество запросов РИС.

Каждый из запросов q_i порождает процесс обработки этого запроса $Proc_i$, который обрабатывает сервис РИС, и по окончании обработки высылается ответ a_i.

Обозначим множество всех исследуемых процессов как $Proc_{all} = \{Proc_1, Proc_2, \ldots Proc_n\}$, где n – общее количество анализируемых процессов.

На рисунке 22 представлена временная диаграмма работы запроса q_i, который выполняет процесс $Proc_i$ с длительностью выполнения Tq_i.

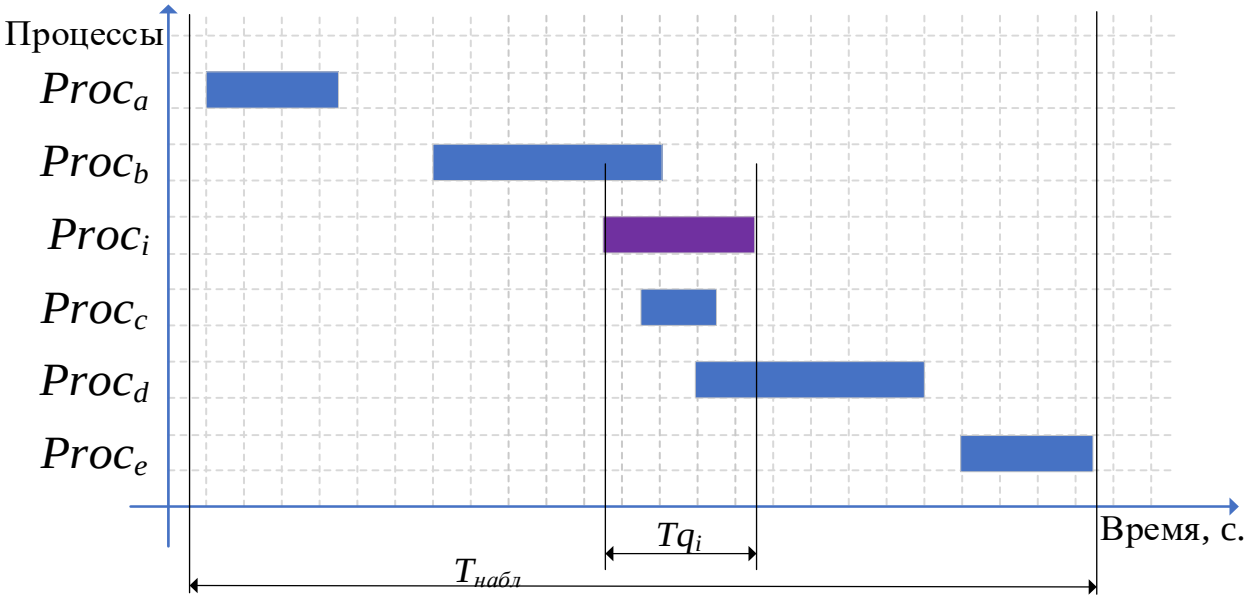

Рисунок 22 – Временная диаграмма взаимодействующих процессов

Для каждого процесса $Proc_i$ существуют процессы, которые выполнялись до его начала, во время его работы и после его работы, а также частично до и после начала и окончания процесса $Proc_i$ за некоторый интервал времени $T_{набл}$.

Обозначим данные процессы по отношению $Proc_i$ как показано на рисунке 23: $Proc_a$, $Proc_b$, $Proc_c$, $Proc_d$ и $Proc_e$.

Указанные процессы $Proc_a$, $Proc_b$, $Proc_c$, $Proc_d$, $Proc_e$ и исследуемый процесс $Proc_i$ могут оказывать взаимное влияние.

2.3.2 Антропоморфические модели взаимодействия сервисов

Для оценки производительности выполнения запросов используется ряд программных решений [152, 154, 159]. В данных средствах используются различные методы поиска и обнаружения аномалий [13]. В отличие от уже имеющихся методов в данной работе предлагается комплекс моделей, описывающих поведенческие особенности функционирования сервисов также как это происходит в микроорганизмах живой природы.

Опишем поведенческие особенности взаимодействий сервисов на основе анализа наблюдаемых процессов. Поведение процессов предлагается оценить с помощью типов взаимодействия организмов живой природы – антропоморфических типов взаимодействия [17, 18, 90].

Согласно широко распространенному в науке делению отношений живых организмов известны следующие типы их взаимодействий: симбиоз (облигатный и факультативный симбиоз, комменсализм, паразитизм, хищничество) – когда хотя бы один из организмов получает выгоду, антибиоз (аменсализм, аллелопатия, конкуренция) – когда один из организмов ограничивает возможности другого, и нейтрализм – сосуществования организмов без взаимного влияния.

Выбор именно 9 типов антропоморфических моделей взаимодействий сервисов в распределенных информационных системах основывается на исследовании ученых [17, 18, 90], которые использовали данный подход для моделирования взаимодействия уязвимостей в программном коде. Это позволило использовать уже имеющиеся наработки в данном направлении, но для другой предметной области – исследование межсервисных взаимодействий в РИС.

На рисунках 24–32 представлены девять временных диаграмм для основных антропоморфических типов взаимодействия процессов в РИС.

Временные диаграммы выполнения процессов (рисунки 24–32) выполнены с использованием элементов описания схем теории автоматического управления [51]. Для рисунков 24–32 введена следующая система обозначений:

1) символ «+» и зеленый цвет стрелочки – процесс оказывает положительное влияние на другой процесс;

2) символ «0» и желтый цвет стрелочки – процесс не оказывает влияние на другой процесс;

3) символ «–» и красный цвет стрелочки – оказывает отрицательное влияние на другой процесс.

Временная последовательность выполнения процессов задается расположением процессов на диаграмме слева направо. Каждый тип взаимодействия процессов можно представить следующим образом.

Тип 1 «Облигатный симбиоз» (+|+). Данный тип характеризуется необходимостью совместного сосуществования организмов (рисунок 24).

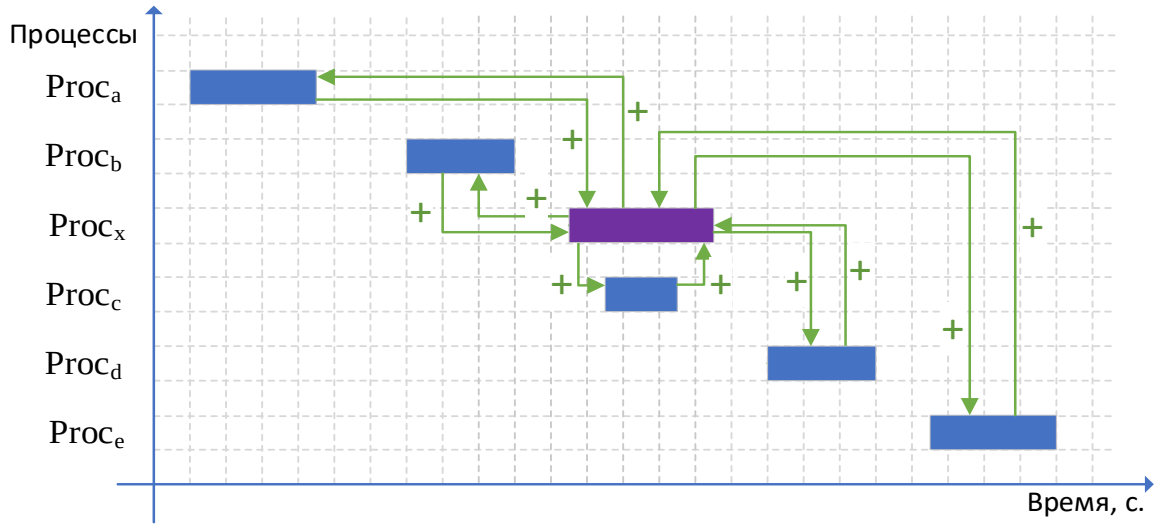

Рисунок 24 – Временная диаграмма выполнения процессов
тип 1 «Облигатный симбиоз»

Тип 2 «Факультативный симбиоз» (+|+) – характеризуется взаимной выгодой от совместного сосуществования организмов, но без необходимости как таковой (рисунок 24).

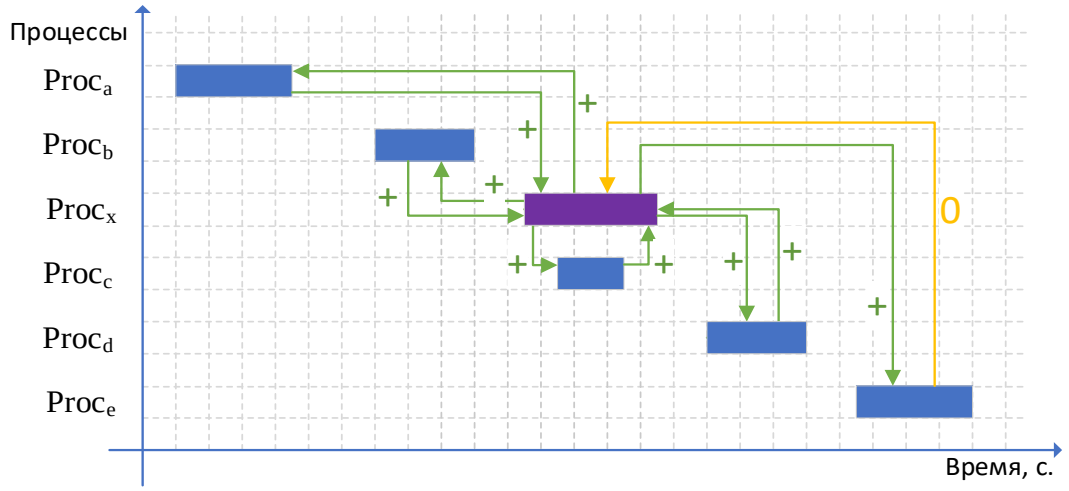

Рисунок 25 – Временная диаграмма выполнения процессов тип 2 «Факультативный симбиоз»

Тип 3 «Комменсализм» (+|0). Данный тип характеризуется выгодой от существования одного организма при отсутствии какого-либо эффекта для другого (рисунок 26).

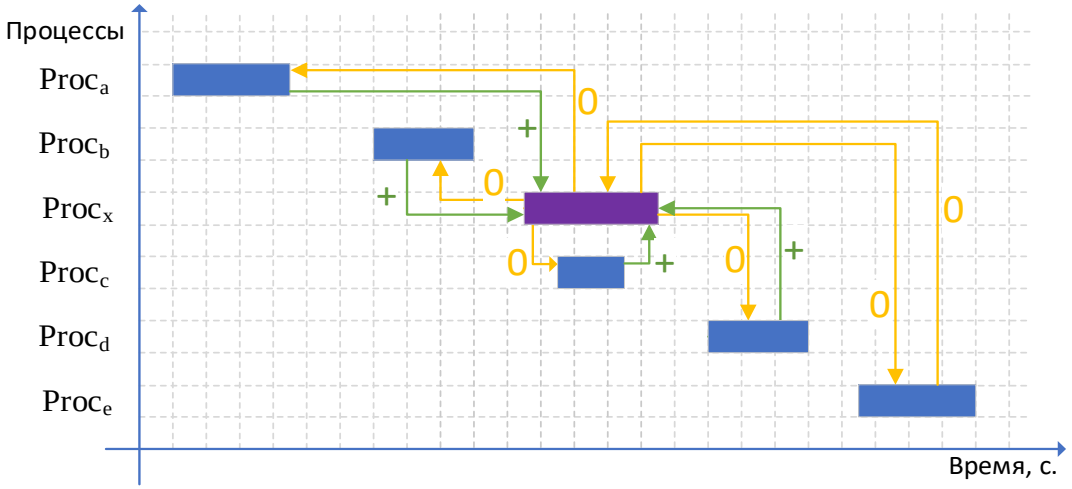

Рисунок 26 – Временная диаграмма выполнения процессов тип 3 «Комменсализм»

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 (рисунок 27).

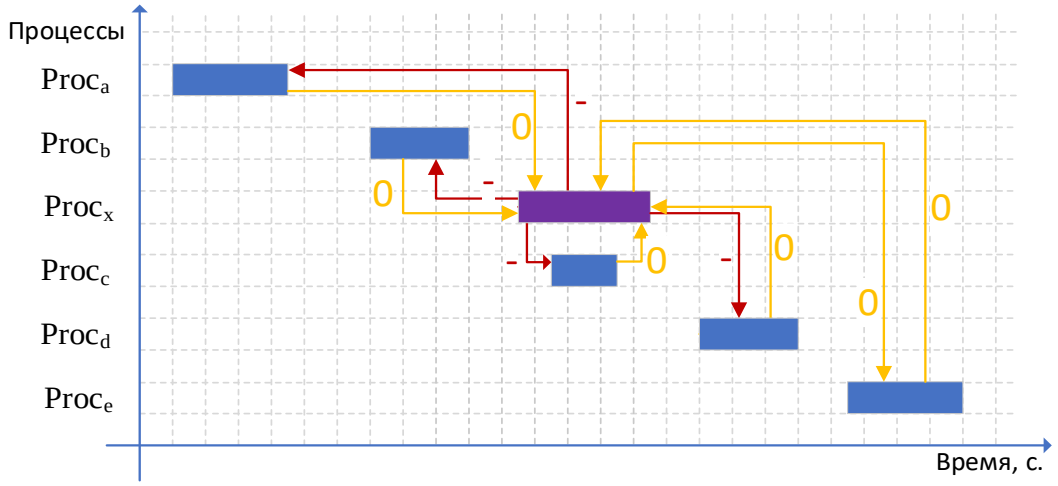

Рисунок 27 – Временная диаграмма выполнения процессов тип 4 «Паразитизм»

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 (рисунок 28).

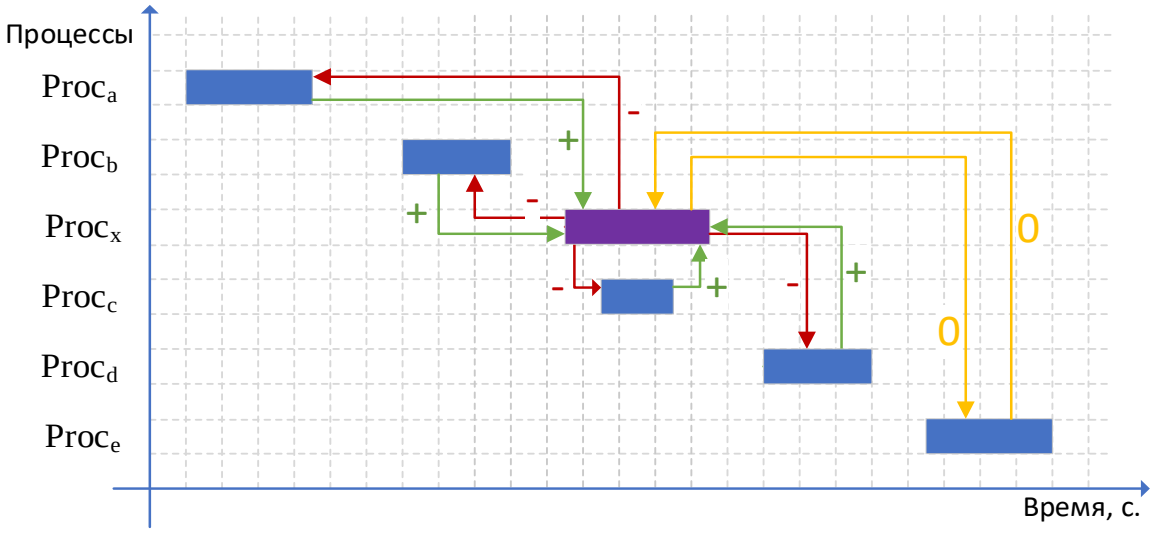

Рисунок 28 – Временная диаграмма выполнения процессов тип 5 «Хищничество»

Тип 6 «Нейтрализм» (0|0) – характеризуется отсутствием каких-либо воздействий друг на друга (рисунок 29).

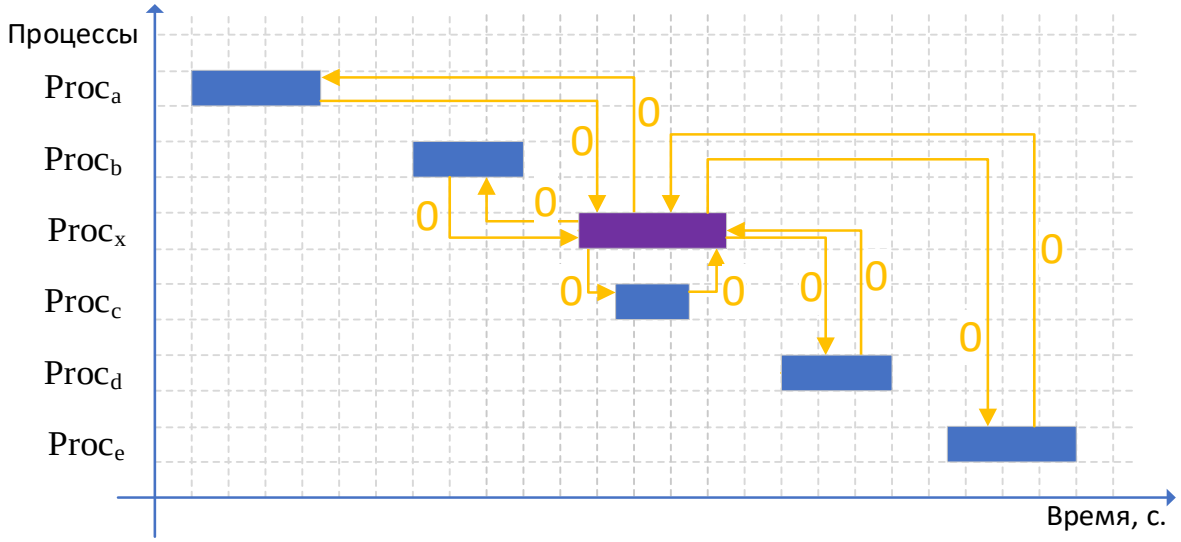

Рисунок 29 – Временная диаграмма выполнения процессов тип 6 «Нейтрализм»

Тип 7 «Аменсализм» (0|–). Данный тип характеризуется отрицательным влиянием одного организма на другого, не испытывая при этом какого-либо обратного влияния (рисунок 30).

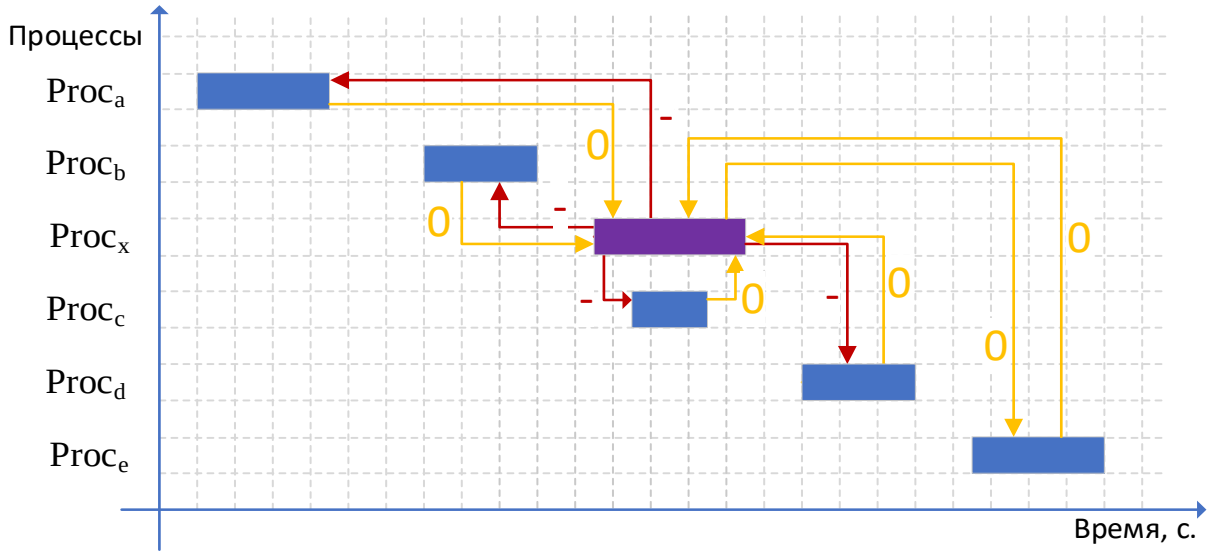

Рисунок 30 – Временная диаграмма выполнения процессов тип 7 – «Аменсализм»

Тип 8 «Аллелопатия» (–|–) – характеризуется взаимно-вредным влиянием организмов друг на друга (рисунок 31).

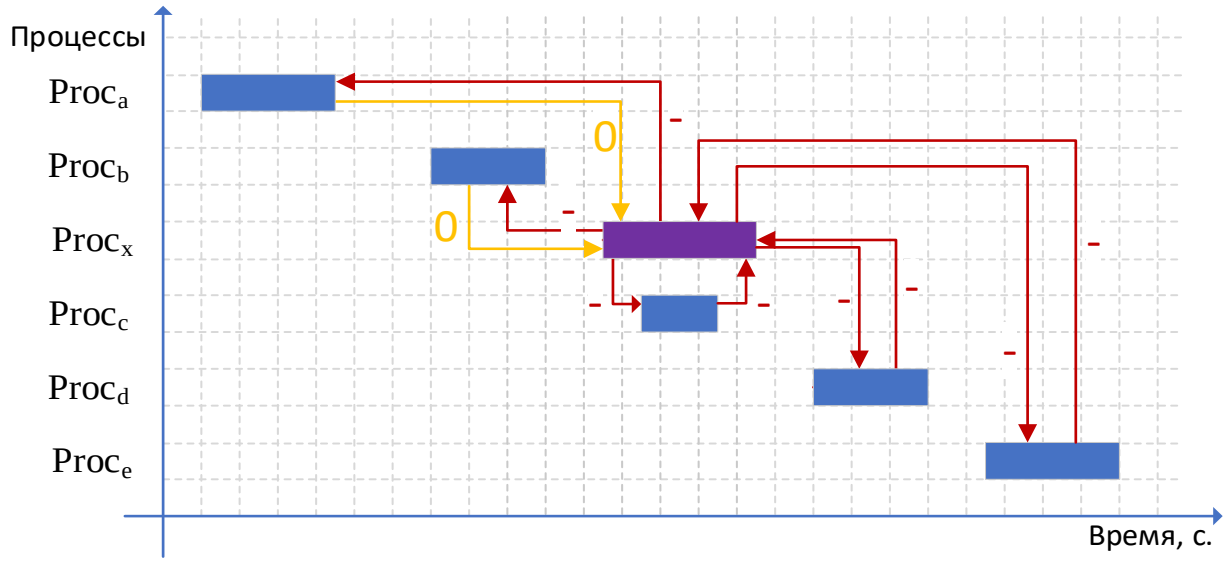

Рисунок 31 – Временная диаграмма выполнения процессов тип 8 «Аллелопатия»

Тип 9 «Конкуренция» (–|–). Данный тип характеризуется косвенным отрицательным влиянием организмов друг на друга по причине борьбы за общие ресурсы (рисунок 32).

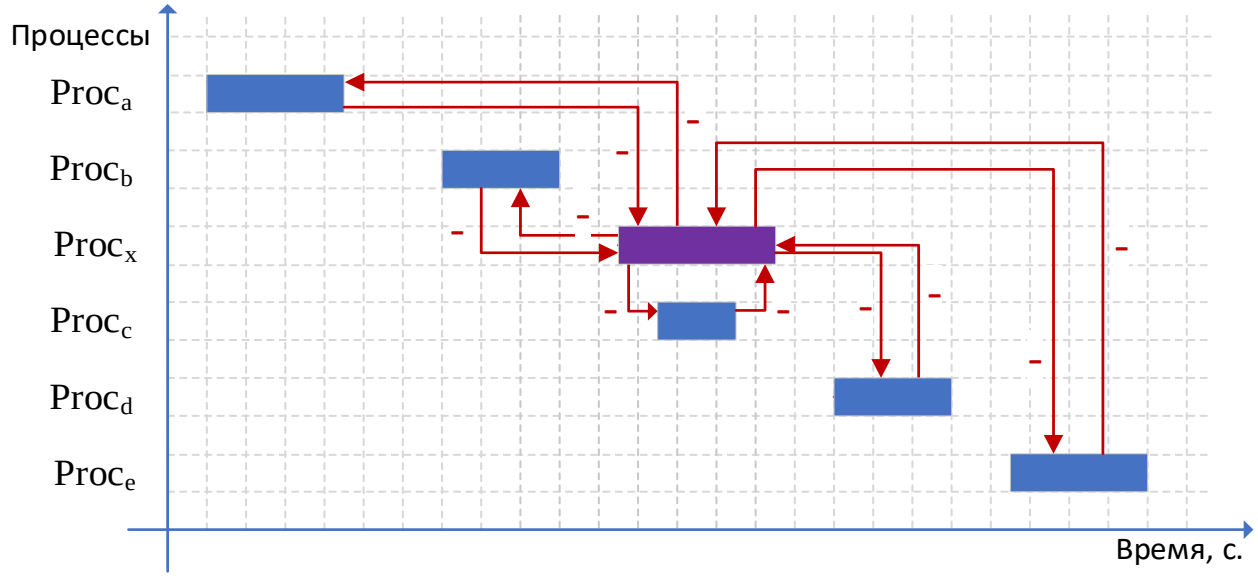

Рисунок 32 – Временная диаграмма выполнения процессов тип 9 «Конкуренция»

На основе временных диаграмм выполнения процессов построен программный комплекс антропоморфических поведенческих моделей [152, 159].

Разработанный комплекс антропоморфических поведенческих моделей процессов позволяет количественно оценить наличие определённых антропоморфических типов сервисов.

Данный подход предлагается использовать как индикатор или метрику «здоровья» в системе мониторинга ИБ. Данный поход поможет для прогнозирования рисков ИД исследуется динамика возникновения и структура негативных поведенческих процессов. Использование такого подхода даёт возможность не просто обнаруживать аномалии, но и анализировать структуру и динамику негативных поведенческих процессов для повышения эффективности мониторинга ИБ. Следует отметить, что использование именно 9 типов взаимодействия не обязательно на практике, в последующих разделах диссертации будут предложены способы синтеза базисов межсервисных взаимодействий. Однако без имеющихся типов взаимодействия обойтись не представляется возможным.

2.4 Модель распространения компьютерных вирусов с антропоморфическими типами эпидемиологических состояний

Данный механизм описания динамики взаимного влияния сервисов ИС применен для описания состояний эпидемиологической модели распространения вредоносного программного обеспечения (ВПО) – вирусов.

Это позволило более точно описать взаимодействие нескольких ВПО в эпидемиологической модели с учетом угрозы инфраструктурного генеза (ИГ):

1) положительное: ВПО помогает друг другу;

2) нейтральное: ВПО не влияет друг на друга;

3) отрицательное: одно ВПО блокирует работу другого ВПО.

Таким образом, разработанный в п. 2.3.2 комплекс антропоморфических моделей предлагается также применить для описания состояний в эпидемиологической модели распространения ВПО.

Среди уже имеющихся моделей эпидемиологических моделей распространения ВПО применение предлагаемого подхода возможно для следующих моделей

[59]: SI-модель, SIR-модель, SEIR модель, PSIDR-модель. Опишем процесс распространения ВПО с учетом антроморфических состояний на примере SEIR-модели. В SEIR-модели учитывается возможность того, что деструктивное воздействие ИГ может иметь некий "латентный период", во время которого оно не наносит какого-либо вреда РИС. Обычно деструктивное воздействие ВПО поражает уязвимую инфраструктуру (S) до входа в свою латентную стадию, в течение латентного периода (Ex, Exposed) элемент инфраструктуры считается заражённым, но не распространяет деструктивные воздействия, через некоторое время он становиться способным к заражению других (I) и далее становиться "вылеченным" (R) [160].

Данное взаимодействие представимо в виде системы дифференциальных уравнений:

$$\begin{cases} \frac{dS}{dt} = OS(t) - SEx(t); \\ \frac{dEx}{dt} = SEx(t) - ExI(t); \\ \frac{dI}{dt} = ExI(t) - IR(t); \\ \frac{dR}{dt} = IR(t); \\ SEx(t) = \frac{b \cdot S(t) \cdot I(t)}{n}; \\ ExI(t) = \frac{Ex(t)}{f}; \\ IR(t) = c \cdot I(t). \end{cases} \quad (5)$$

Системно-динамическая диаграмма распространения ВПО представлена на рисунке 33.

Предложенная модель реализована на основе многоагентной системы моделирования NetLogo [223] и позволяет оценивать динамику рисков ИГ деструктивных воздействий ВПО с учетом антропоморфических состояний.

Для анализа распространения ВПО часто используют подходы, основанные на эпидемиологических моделях, заимствованных из биологии, где устройства или программы представляют собой «организмы», а ВПО **(**вирусы) — «инфекции2.

В этой модели могут быть использованы типы эпидемиологических состояний, аналогичные человеческим заболеваниям. Такой подход позволяет более точно предсказать поведение вируса и возможные меры защиты.

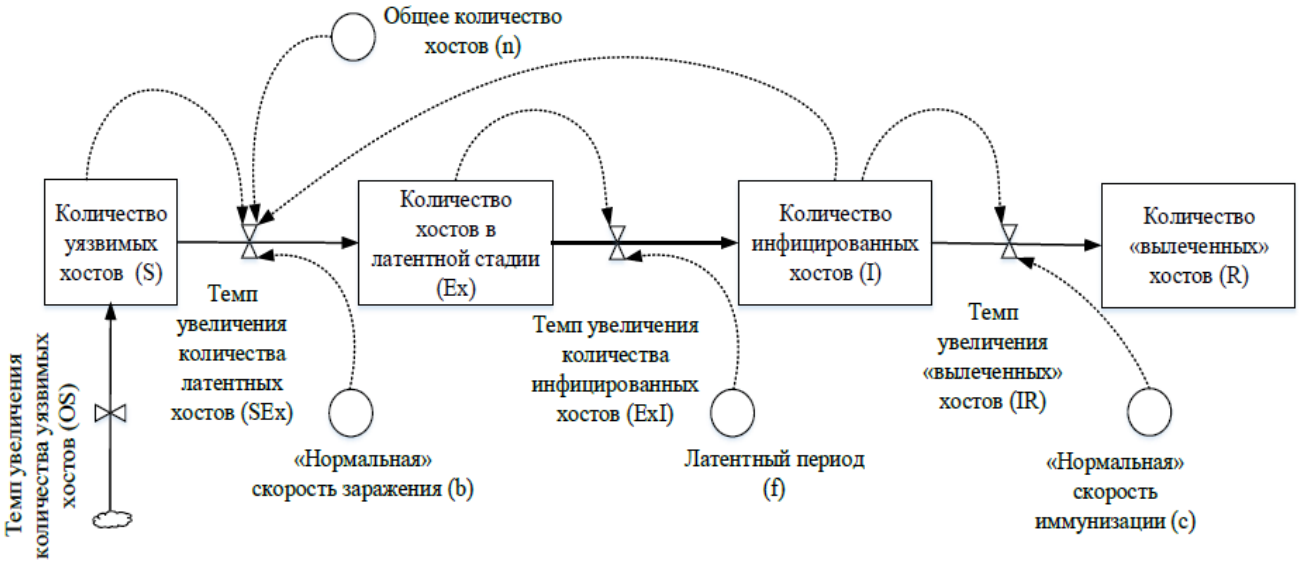

Рисунок 33 – Системно-динамическая диаграмма распространения ВПО

Модели распространения вирусов используют аналогичные биологическим эпидемиям динамические уравнения, которые описывают изменение числа устройств в различных состояниях.

Основные параметры модели.

β — коэффициент передачи вируса, который определяет вероятность того, что инфицированное устройство заразит сенсибилизированное устройство. Этот параметр зависит от множества факторов, таких как уязвимости в ПО, поведение пользователя, степень защиты сети и т. д.

γ — Коэффициент восстановления, который определяет скорость, с которой устройства очищаются от вируса или нейтрализуют его. Это может включать антивирусное программное обеспечение, удаление вирусов, патчи для уязвимостей и другие меры защиты.

δ — Коэффициент повреждения, который определяет скорость, с которой вирус разрушает устройства или программы. Это может зависеть от типа вируса, его агрессивности и возможностей.

Далее опишем, процессы динамики заражения ВПО ИС.

Начальная стадия**.** Вирус распространяется среди сенсибилизированных устройств, заражая их. Количество инфицированных устройств растет экспоненциально, пока значительное число устройств не перейдет в состояние зараженных.

Средняя стадия**.** Зараженные устройства начинают изолировать вирус, либо восстанавливаются от заражения, либо становятся «мертвыми», если вирус слишком агрессивен.

Конечная стадия**.** В идеале вирус либо исчезает, либо его распространение замедляется, так как число доступных для заражения устройств значительно сокращается. Большая часть устройств либо восстанавливается, либо выходит из строя.

Использование антропоморфических состояний в модели распространения вирусов помогает сделать модель более интуитивно понятной и адаптированной к реальному восприятию угроз в ИТ-инфраструктурах РИС:

Сенсибилизированные устройства — это «здоровые» устройства, которые легко могут быть заражены вирусом.

Инфицированные устройства — «больные» устройства, которые могут заразить другие устройства.

Изолированные устройства — устройства, которые изолированы для предотвращения распространения вируса.

Восстановленные устройства — устройства, которые успешно вылечены и больше не могут быть источниками распространения.

Мертвые устройства — устройства, которые разрушены вирусом и больше не могут быть использованы.

Моделирование с антропоморфическими состояниями помогает более точно описать, какие действия необходимо предпринять, чтобы остановить распространение ВПО (например, изоляция зараженных устройств или их восстановление).

2.5 Агентная модель системы обнаружения и прогнозирования возникновения источников угроз инфраструктурного генеза

В ходе моделирования будем рассматривать информационное взаимодействие групп объектов РИС в контексте ИД с учетом структурных и поведенческих особенностей функционирования, исследуемых РИС на основе технологии цифровых двойников. В качестве исходных данных рассматривается по-отдельности формализация агентов РИС и среды их взаимодействия.

Приведем формализацию агентов объектов РИС. Агенты объектов РИС взаимодействуют в некоторой среде, которая определяет все законы взаимодействия. В среде взаимодействия агентов должно быть определено время, расположение и связи взаимодействующих объектов.

$$M_{среды} = \langle T,\ \Sigma,\ Processing,\ Task \rangle, \tag{6}$$

где T – абстрактное линейно упорядоченное множество с отношением порядка «<». Далее под T будем понимать множество моментов моделируемого времени.

Возможны два варианта моделирования времени:

1) Время, определяемое событиями, которые даются в плане вычислений (отображены в журнале событий), измеряется в отсчетах.

2) Время, определяемое временными интервалами с заданным шагом дискретизации, измеряется в секундах. Существуют способы преобразования времени из одной величины в другую.

Σ – Множество событий – множество, для каждого из элементов которого ставится в соответствие временная метка из T (содержимое анализируемых журналов событий). Вообще говоря, элементы множества представляют собой отображения, при которых меняется состояние логического процесса: $\Sigma = \{\delta_t | \delta_t : State \to State\}$.

L – Множество вычислительных процессов – представляется в виде ориентированного графа

$$L = (V; E), \tag{7}$$

где V – вершины графа процессы; E – дуги взаимодействие между процессами.

Следует отметить, что возможно несколько вариантов задания данной структуры модели среды.

При наличии данных о структуре взаимодействия процессов, это множество задается на основе данных о архитектуры РИС. При отсутствии данных строится граф исходя из взаимодействий процессов описанных в журналах событий.

M – множество сообщений, передаваемых между процессами. В общем случае под сообщением будем понимать следующую структуру:

$$Mt = (S, D, \delta_t, \mu, \Theta), \tag{8}$$

где $S \in V$ – процесс отправитель запроса; $D \in V$ – процесс обработчик запроса; δ_t – передаваемое событие с временной меткой t; μ – параметры сообщения.

Θ – Механизм передачи сообщений – совокупность алгоритмов, согласно которым производится передача сообщений между процессами и обеспечивается синхронизация времени.

Приведем формализацию модели агентов ИС. У каждого агента объекта ИС есть множество целей, множество его параметров, множество ресурсов, конечное множество задач, которые может выполнить агент объекта РИС. Каждый агент объекта AO_i ИС имеет следующую формализацию:

$$AO_i = \langle Behaviour, Resource, State, F_{обр}, F_{сред} \rangle, \tag{9}$$

где $Behaviour$ – множество моделей поведения агентов объектов ИС целей при взаимодействии агента объекта ИС;

$Resource$ – множество ресурсов объекта информационной ИС Примеры вычислительных ресурсов: процессорное время, оперативная память, постоянная память, пропускная способность (трафик) сети, время выполнения.

$State$ – текущее состояние агента;

$F_{обр}$ – функции обработки последовательностей запросов, преобразующие состояние агента $F : State \to State$;

$F_{сред}$ – функции высшего порядка, взаимодействующие с внешней средой и через это с другими агентами $F_{сред} = State \times F_{обр} \to F_{обр}$.

2.6 Выводы по разделу 2

В качестве объекта исследовались эффекты деструктивного воздействия инфраструктурного генеза в распределенных информационных системах на предмет оценки влияния эффектов деструктивного воздействия инфраструктурного генеза.

В ходе исследования:

1) Формализована концептуальная модель феномена инфраструктурного деструктивизма. Выявлены и описаны ситуации по возникновению эффектов инфраструктурного деструктивизма для сервис-ориентированной архитектуры ИС. Классифицированы основные признаки возникновения эффектов инфраструктурного деструктивизма. Дано определение и описан механизм появления «деструктивного мусора», который является одним из источников возникновения инфраструктурного деструктивизма.

2) Синтезирована модель обнаружения эффектов инфраструктурного деструктивизма сервиса на основе анализа журналов событий. Введены новые понятие для оценки инфраструктурного деструктивизма: деструктивные возможности инфраструктуры ИС. Получены метрики для оценки уровня инфраструктурного деструктивизма.

3) Синтезирован комплекс антропоморфических моделей для оценки эффектов инфраструктурного деструктивизма сервисов. Сформированы поведенческие последовательные шаблоны для 9 типов антропоморфического поведения сервисов.

4) На основе комплекса антропоморфических моделей для оценки динамики рисков инфраструктурного деструктивизма сервисов построена модель распространения компьютерных вирусов с учетом антропоморфических типов

эпидемиологических состояний. В отличие от базовой эпидемиологической модели SEIR, данная модель учитывает межвирусное взаимодействие.

5) Разработана агентная модель выявления и прогнозирования источников инфраструктурного деструктивизма. На её основе описана идея метод прогнозирования и оценки динамики рисков инфраструктурного деструктивизма для существующих инфраструктур.

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:

1) формальное описание феномена ИБ в РИС;

2) модель обнаружения эффектов ДВ ИГ сервисов ИС;

3) классификация антропоморфических типов состояний объектов ИС для комплекса эпидемиологических моделей распространения вирусов;

4) агентная модель системы обнаружения и прогнозирования возникновения источников угроз инфраструктурного генеза.

Данные результаты непосредственно использованы для получения основного научного результата – разработка комплекса моделей для анализа поведенческих особенностей сервисов на основе антропоморфических типов взаимодействия процессов в ИС.

Основное содержание раздела и изложенных в нем научных результатов опубликовано в работах автора [140, 210, 159, 154, 157, 145].

3 МЕТОДЫ ОЦЕНКИ ЭФФЕКТОВ ДЕСТРУКТИВНОГО ВОЗДЕЙСТВИЯ ИНФРАСТРУКТУРНОГО ГЕНЕЗА

3.1 Общая принципиальная схема работы методов оценки эффектов деструктивного воздействия инфраструктурного генеза

Общая принципиальная схема реализации методов оценки эффектов ДВ ИГ представляет собой универсальную модель, применимую к различным типам РИС. Предлагаемый метод оценки эффектов ДВ ИГ разрабатывался изначально для сервис-ориентированных архитектур, однако так же может быть применен и для других типов архитектур, включая монолитные, микросервисные, событийно-ориентированные и др. Схема реализации методов основана на поэтапном анализе шаблонов последовательностей запросов, их структурировании в соответствии с антропоморфическими типами межсервисных взаимодействий и последующей аналитической оценке характера и степени потенциального ДВ. В развёрнутом виде методологическая схема включает выполнение следующих последовательных этапов.

Этап 1. Сбор и организация данных. На данном этапе осуществляется агрегация и централизация журналов событий РИС, поступающих от различных компонентов и подсистем. Для крупномасштабных систем данная процедура может представлять значительную сложность, поскольку требует обеспечения корректной временной синхронизации и унификации данных, поступающих из разнородных источников.

Этап 2. Сбор и организация данных. Журналы событий РИС собираются с различных устройств и компонентов системы. Для больших и сложных систем это может быть непростой задачей, так как необходимо обеспечить синхронизацию данных с различных источников.

Этап 3. Фильтрация и предварительная обработка данных. Поскольку журналы событий могут содержать избыточные и нерелевантные сведения, осуществляется этап фильтрации и предобработки, направленный на выделение событий,

обладающих аналитической значимостью для последующей оценки эффектов воздействия. Это позволяет существенно сократить объем обрабатываемой информации и повысить эффективность дальнейшего анализа.

Этап 4. Анализ последовательных шаблонов и ассоциативный анализ. На данном этапе осуществляется исследование закономерностей в последовательностях межсервисных взаимодействий с применением методов интеллектуального анализа данных, статистического моделирования и алгоритмов машинного обучения. Результаты анализа служат основой для структурирования паттернов взаимодействий в соответствии с антропоморфическими типами межсервисных взаимодействий (подробно описанными в разделе 2.3). Проведение данного анализа позволяет выявлять регулярные циклы, аномальные отклонения, устойчивые тренды и корреляционные зависимости.

Этап 5. Аналитическая оценка деструктивного воздействия. На основе выявленных закономерностей выполняется визуализация и последующая интерпретация результатов анализа. Использование графических средств представления данных, таких как графики, диаграммы и тепловые карты, обеспечивает наглядное отображение временных зависимостей и динамики изменений в исследуемых процессах. Это способствует повышению точности аналитической оценки интенсивности и направленности ДВ ИГ, а также формированию обоснованных выводов о потенциальных угрозах устойчивости функционирования РИС.

3.1.1 Основные принципы обнаружения эффектов инфраструктурного деструктивизма

Основные принципы обнаружения эффектов ИД базируются на системном анализе взаимодействий между объектами, выявлении аномалий в поведении систем и применении специализированных моделей оценки состояния инфраструктуры. Анализ временных данных в научном контексте включает несколько ключевых направлений, обеспечивающих всестороннее понимание динамики и структуры исследуемых межсервисных взаимодействий. Анализ трендов направлен на выявление долгосрочных тенденций и изменений, позволяя обнаруживать

устойчивые закономерности и направленность развития данных во времени. Анализ цикличности исследует повторяющиеся временные циклы и паттерны, связанные с сезонными изменениями, поведением пользователей или другими периодическими явлениями. Анализ аномалий направлен на идентификацию необычных или отклоняющихся во времени событий, которые могут свидетельствовать о критических инцидентах, таких как аварии или кибератаки. Анализ временных корреляций позволяет определять взаимосвязи и зависимости между переменными, эволюционирующими во времени. Для проведения данного анализа используются методы теории временных рядов, включая статистические модели [2], методы машинного обучения [13] и алгоритмы выявления аномалий [20].

3.1.2 Причинно-следственный анализ взаимодействия сервисов

Оценка межсервисного взаимодействия выполняется в соответствии с подходами, реализованными и описанными в [13]. Таким образом предлагается использовать методы причинно-следственного анализа и наименьших квадратов. Показатель оценки причинно-следственной связи для оценки взаимного влияния сервисов используется подход, описанный в [177].

Суть данного подхода состоит в определении причинное следственной связи на основе метода наименьших квадратов с использованием следующих метрик:

1) $Proc_{ATE}$ (Average Treatment Effect) — средний эффект воздействия;

2) $Proc_{ATC}$ (Average Treatment Effect for Control) — средний эффект воздействия для контроля;

3) $Proc_{ATT}$ (Average Treatment Effect for Treated) — средний эффект воздействия для объекта исследуемого процесса $Proc_x$.

Для оценки эффекта рассчитывают среднее значение зависимой переменной по выборкам наблюдаемой и контрольной групп, затем вычисляют разницу между этими средними. Это позволяет количественно охарактеризовать различия между группами для последующего статистического анализа. Далее оценим, имеет ли воздействие процесса $Proc_x$ $Proc_{ATE}$ по сравнению с эффектом управления этим процессом $Proc_{ATC}$.

Для этого применим метод определения меры склонности [177]. Кроме того, получить информацию о вероятности воздействия в зависимости от независимых переменных.

3.1.3 Алгоритм оценки эффектов инфраструктурного деструктивизма в распределенных информационных системах

Для алгоритмической реализации предложенного в пункте 2.2 подхода к оценке цифровых результатов проявления ИД используется совокупность методов анализа последовательностей, включающая алгоритм обнаружения максимальных последовательных шаблонов и алгоритм выявления последовательных шаблонов фиксированной длины [117]. Важно отметить, что сформированная пошаговая система (см. п. 2.2) позволяет разработать различные варианты алгоритмов зависимости от особенностей РИС. Существует множество алгоритмов обнаружения шаблонов последовательностей, представленных в [117, 192]. На их основе предлагается выполнить следующие общие шаги.

Шаг 1. Фаза сортировки представляет собой этап предварительной обработки, направленный на перегруппировку запросов в соответствии с их временными характеристиками выполнения. Для обеспечения формализованного анализа предлагается использовать качественные категории продолжительности выполнения запросов: долго, умеренно, средне, быстро и очень быстро.

Шаг 2. Фаза отбора кандидатов представляет собой этап первичного анализа исходного набора данных, в ходе которого осуществляется идентификация одноэлементных последовательностей на основании заданного порогового значения минимальной поддержки. В данном исследовании значение минимальной поддержки принято равным 40%, что обеспечивает отбор только статистически значимых шаблонов для дальнейшей обработки.

Шаг 3. Фаза трансформации направлена на преобразование исходных данных путем разложения каждой последовательности запросов на совокупность одноэлементных последовательностей, содержащихся в ней. Если в анализируемой последовательности отсутствуют элементы, отобранные на предыдущем этапе, такая

последовательность исключается из дальнейшего рассмотрения и не включается в результирующую таблицу.

Шаг 4. Фаза генерации последовательностей представляет собой этап построения расширенных шаблонов, формируемых на основе последовательностей, выявленных на предыдущих этапах анализа. На данном этапе осуществляется комбинирование существующих последовательностей с целью формирования более протяженных структур, отражающих закономерности во временных или логических зависимостях между элементами.

Шаг 5. Фаза максимизации направлена на выделение среди множества полученных шаблонов тех последовательностей, которые не являются подмножествами более протяженных шаблонов. На данном этапе осуществляется идентификация максимально длинных последовательностей, обладающих независимой структурой и представляющих завершенные закономерные формы проявления анализируемых процессов.

Анализируя описанный выше алгоритм для обнаружения закономерности выполнения последовательностей запросов к сервису, можно определить следующие основные понятия.

Определение. Последовательный шаблон «маршрут» обозначим как $X_{маршрут}$ — некоторый последовательный шаблон запросов для типичных задач, которые выполняет сервис. При этом некоторые

Определение. Последовательный шаблон «цепь» обозначим как $X_{цепь}$ — это ежедневная последовательность запросов (цепочка), в которой запросы не повторяются, то есть такие запросы, которые выполняет сервис для типичных задач, но без повторений.

Определение. Последовательный шаблон «цикл» обозначим как $X_{цикл}$ — это последовательный шаблон запросов, который повторяется циклично, например несколько раз.

Приведенные выше определения опираются на базовые определения теории графов с выделением особенностей, связанных с обработкой журналов событий. Это позволяет более наглядно показать структуру извлекаемых данных из

журналов событий, а также при необходимости сгенерировать сходные по своей структуре новые последовательность запросов.

Далее представлена обобщенная блок-схема алгоритма обнаружения максимальных последовательных шаблонов (рисунок 34), где F_1 — множество всех частых 1-последовательностей k — длина последовательности, C_k— множество кандидатов длины k, S_i — кандидаты, входящие в C_k, Sup — оператор вычисления поддержки (см. п. 2.2). Рассмотренный выше алгоритм формирует частые последовательности-кандидаты всех возможных длин. На этом принципе основан алгоритм, представленный на рисунке 35. В данном алгоритме используется параметр длины, как параметр последовательностей, анализируемых в алгоритме. Это позволяет вычислять длину частых последовательностей шаблонов.

$$X_{дан}=\{X_1, X_2, \dots X_n\}, \quad (10)$$

где X_n – последовательный шаблон, описывающий структуру данных событий содержащихся в журналах событий системы.

Используя $X_{дан}$ создается план вычислений $P_{выч}$ для запуска в среде симуляции. Таких планов вычислений может быть создано произвольное количество. При их моделирование требуются экспертные оценки. Для создания

Шаг 1. Создаётся начальная выборка из начальных последовательностей — популяция размером N последовательностей – X_{start}, где каждая последовательность шифруется в геном — цепочку, состоящую из генов.

Шаг 2. Происходит скрещивание геномов (кроссинговер). Для этого случайным образом выбираются два генома из популяции, выбирается случайным образом точка деления генома на две или более части, и затем происходит обмен генами между двумя геномами. В результате скрещивания получаются новые геномы — потомки с новым набором генов, а при расшифровке их — новые последовательности запросов $Xnew$.

Шаг 3. Выполняется мутация — выборочное изменение генов в геноме. Мутации подвергается к определенному проценту геномов в популяции. Это означает, что случайным образом выбирается геномов из новой популяции, состоящей из геномов-предков и геномов-потомков, получившихся на предыдущем этапе, и

происходит изменение случайно выбранных генов на противоположные (1 на 0, 0 на 1) с определённой вероятностью. Вероятность мутации выбирается исходя из экспертных данных. В результате мутации появляется новый набор последовательностей X_{mut}, на основе которого формируется некоторый тестовый план вычислений $P_{тест}$.

Шаг 4. Происходит естественный отбор — отсекаются геномы, не удовлетворяющие условиям. Для этого вводится функция выживания, которая вычисляет коэффициент выживания генома в популяции.

В данном случае это функция, которая оценивает, насколько полученный план вычислений $P_{тест}$ соответствует исходным последовательным паттернам.

На этапе отбора оставляется N геномов из новой популяции, максимально удовлетворяющих условиям выживания.

Если в $P_{тест}$ соответствует требуем характеристикам исходных последовательностей шаблонов $X_{дан}$, то данный P_{test} добавляется в итоговый $P_{выч}$.

Иначе происходит кроссинговер, мутация и отбор в новой популяции с переходом на шаг 2,3.

Алгоритм заканчивает работу, если сформирован $P_{выч}$ соответствует заданной длины. То есть в результате работы данного метода формируется один из возможных вариантов работы ИС.

Предлагается также использовать пакетный метод симуляции чтобы оценить возможные сценарии работы ИС: негативный, нейтральный, позитивный сценарии. В этом режиме отображаются найденные источники угроз ИГ и эффекты ИД ИС.

Обобщенная блок-схема алгоритма обнаружения максимальных последовательных шаблонов представлена на рисунке 34.

Пусть t – номер прохода. Тогда $k(t+1)=k(t)+p$ есть представление числа кандидатов на следующем итерационном шаге.

Таким образом можно рассматривать отношение числа частых k-последовательностей к числу всех k-последовательностей-кандидатов в виде её относительной частотной оценки: $h_k = F_k / C_k$ (рисунок 35).

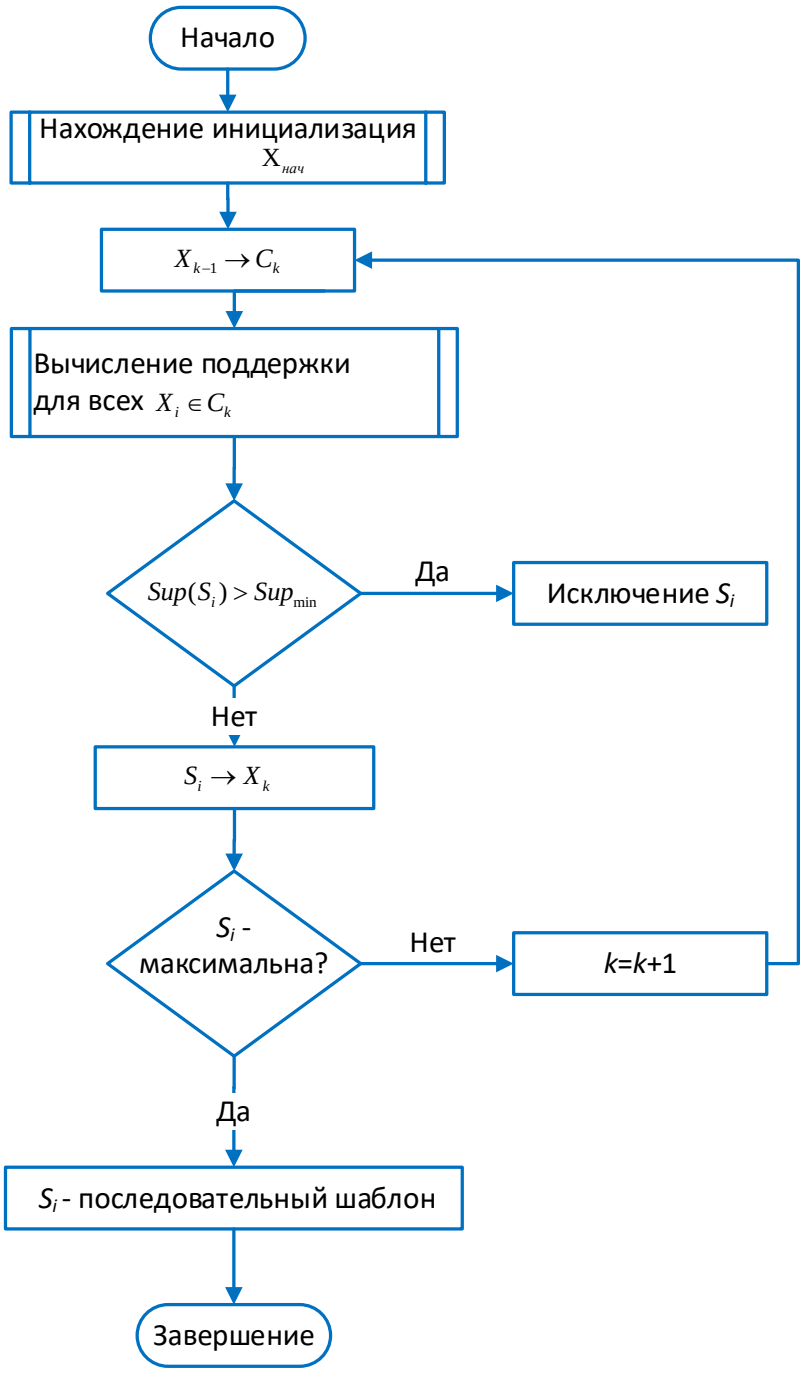

Рисунок 34 –Схема реализации алгоритма обнаружения максимальных последовательных шаблонов

Данные алгоритмы строят последовательные шаблоны, которые отображают общую структуру журналов событий.

Предлагается также использовать основы теории графов и отобрать из найденных шаблонов, те, которые имеют физическую интерпретацию.

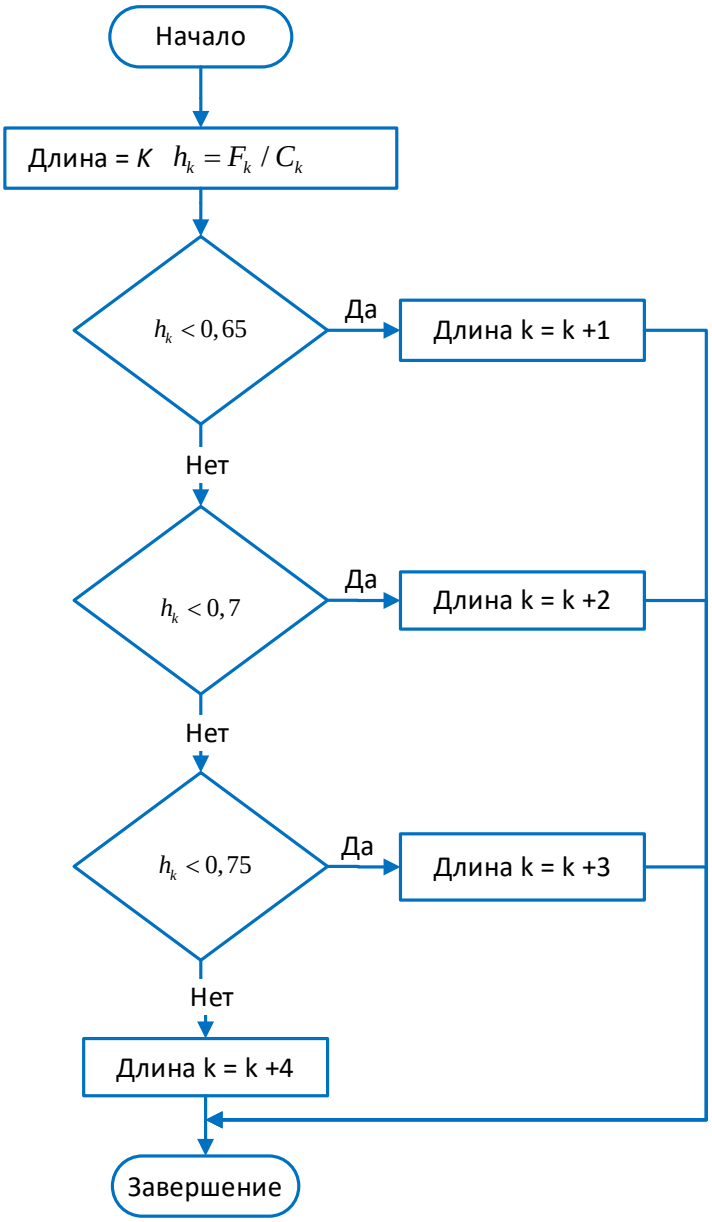

Рисунок 35 – Схема реализации алгоритма обнаружения частых последовательных шаблонов

Обобщенная блок-схема алгоритма обнаружения последовательных шаблонов «маршрут», «цепь» и «цикл» представлена на рисунке 36.

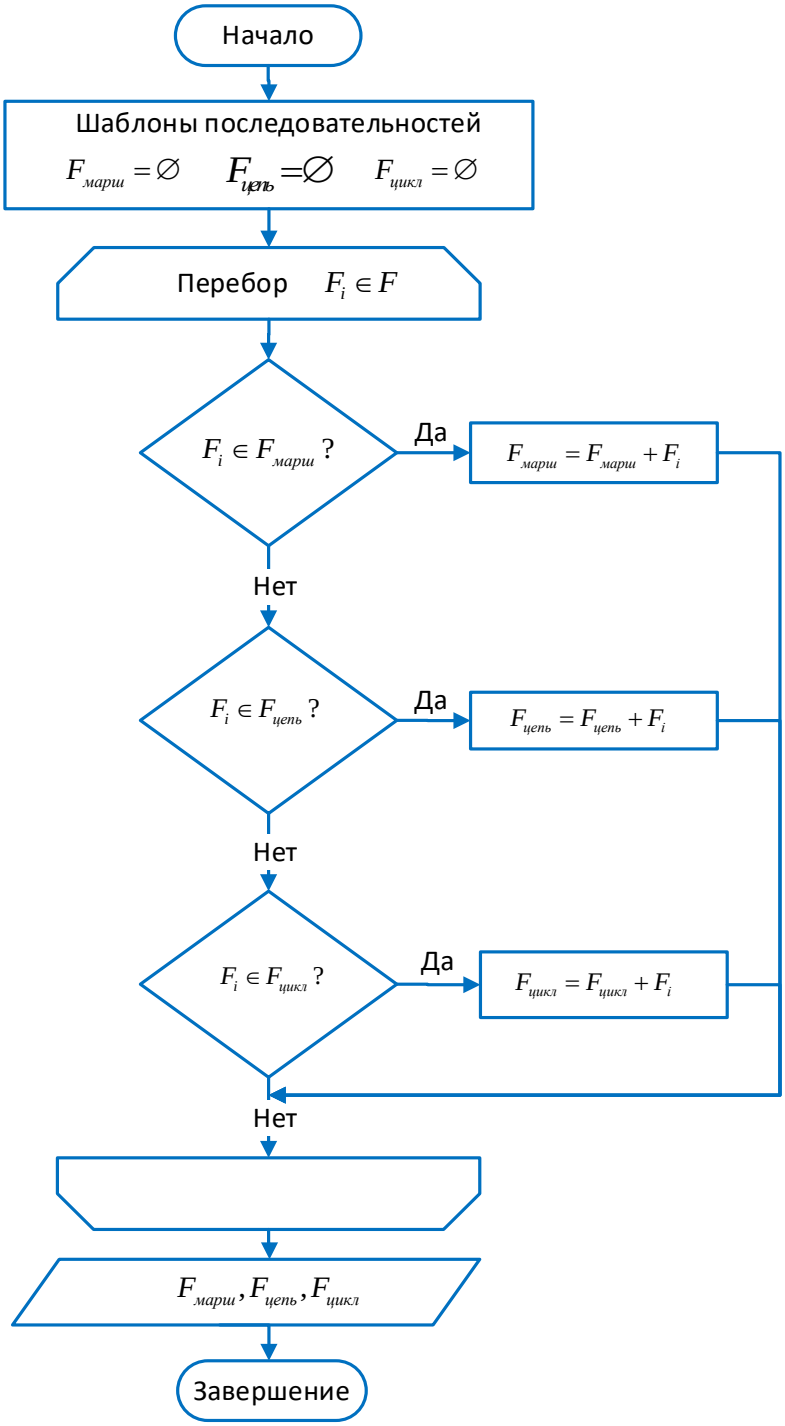

Рисунок 36 – Схема реализации алгоритма обнаружения последовательных шаблонов «маршрут», «цепь» и «цикл».

Основываясь на пункте 3.1, приведем алгоритм оценки деструктивных возможностей сервисов (рисунок 37).

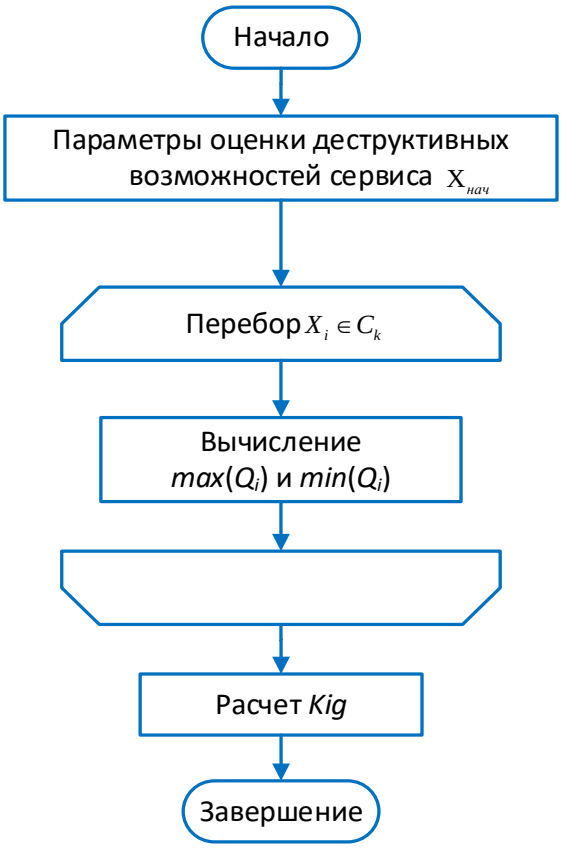

Рисунок 37 – Схема реализации алгоритма оценки деструктивных возможностей сервиса ИС

3.1.4 Ограничения применимости метода

Разработанный метод оценки эффектов ДВ ИГ является эвристическим. Эвристические методы, несмотря на свою практическую ценность и способность точнее решать поставленную задачу, не могут полноценно учитывать все значимые факторы, влияющие на исследуемую РИС. Применение разработанного метода основывается на приближённых правилах и эмпирических наблюдениях, что неизбежно приводит к упрощению модели реальности и исключению некоторых переменных, обладающих потенциальной значимостью. В результате решения, полученные с помощью эвристик, могут оказываться эффективными в типовых случаях, но демонстрировать низкую устойчивость или достоверность при изменении условий, наличии скрытых взаимозависимостей или воздействии нестандартных сценариев.

Метод оценки эффектов ДВ ИГ в РИС обладает свойствами теоретической общности и универсальностью применения.

Теоретическая общность. Введённые формальные определения ИД и ДВ ИГ не зависят от специфики предметной области: они определяют ИД как нарушение устойчивости, целостности, доступности и управляемости ИС под воздействием внутренних или внешних факторов инфраструктуры. Это обеспечивает применимость к любым распределённым техническим и программно-аппаратным комплексам основанных на сервисной архитектуре, вне зависимости от отрасли или сектора применения.

Ключевыми признаками феномена ИД названы динамичность, имманентность (внутренний характер происхождения, а не только внешний), влияние на структуру и динамику системы вне зависимости от типа архитектуры или выбранной платформы. Это доказывает, что метод охватывает любые виды современных сервис-ориентированных ИС. Например: ИС на основе сервис-ориентированной архитектуры (SOA), микросервисные ИС, Веб-сервисные ИС, ИС с сервисным реестром, корпоративные сервисные шины (ESB).

Универсальность применения. Метод оперирует абстрактными характеристиками: анализируются журналы событий ИС, ресурсы, графы взаимодействия, временные параметры исполнения процессов и аномалии без жёсткой привязки к конкретному стеку технологий или видам протоколов.

Универсальность алгоритмических решений и введение метрик, независимо от слоя системы (приложение, база данных, сеть, исполнение сервисов), гарантирует возможность тиражирования подхода на любые масштабы — от малых распределённых систем до территориально-распределённых кластеров и национальных платформ.

Использование антропоморфических моделей взаимодействий (симбиоз, конкуренция, паразитизм и др.), заимствованных из биологии, и последующая стандартизованная группировка типов взаимодействия, позволяет описывать и сравнивать поведенческие особенности сервисов в любой системе независимо от технологической реализации.

В основу метода положена возможность адаптировать пороговые значения, правила идентификации и сценарии для различных бизнес- или технических процессов, а также их эволюционное обновление под требования исследуемой ИС.

Таким образом, разработанный метод является одной из возможных попыток оценки эффектов ДВ ИГ для ИС и нуждается в дальнейших исследованиях и адаптации для конкретной реализации РИС.

3.1.5 Показатели качества работы методов оценки эффектов деструктивного воздействия инфраструктурного генеза

В практике управления качеством информации в ИБ-системах основными показателями являются точность, оперативность, достоверность, актуальность, целостность, доступность; все они имеют утвержденные определения и контрольные процедуры согласно [29, 30].

Оценить полноту, актуальность, целостность, доступность для метода оценки эффектов ДВ ИГ невозможно, потому что для формального нахождения этих показателей требуется знать идеальный или эталонный набор всех релевантных результатов, который фактически недоступен на практике. Таким образом качество работы метода оценки эффектов ДВ ИГ, предлагается оценивать используя оперативность и точность.

Определение. Точность (accuracy) — отсутствие ошибок, искажений или неточностей, позволяющее использовать информацию для принятия решений без дополнительных проверок или коррекции.

Точность является одним из первичных требований к качеству информации и напрямую влияет на ее достоверность и ценность.

Точность описывает долю правильных оценок среди всех сделанных оценок и выражается в виде относительного числа или процента.

Определение. Оперативность (timeliness) — способность информации поступать к потребителю в требуемое время с учетом актуальности задачи и условий ее применения.

В данном исследовании для измерения оперативности предлагается использовать единицы измерения времени (минуты, секунды и др).

Оперативность подразумевает, что данные или сообщения должны быть своевременно представлены, чтобы не терять свою ценность из-за устаревания или задержки в доставке.

Так, например для значимых объектов КИИ нормативно закреплено информирование — не позднее 3 часов с момента обнаружения [125], а внутренние планы реагирования часто устанавливают первичную реакцию на критические инциденты в течение 15 минут и начало активных действий — не позднее 1 часа.

В машинном обучении применяются различные метрики качества, позволяющие оценить эффективность методов при решении задач классификации [20]:

1) Метрика «Accuracy» (Точность) – доля правильно предсказанных объектов от общего числа.

2) Метрика «Precision» (Точность) – доля истинно положительных предсказаний среди всех предсказанных положительных.

3) Метрика «Recall» (Полнота): доля правильно найденных положительных объектов среди всех реальных положительных. Критична, когда важно минимизировать пропущенные положительные.

4) Мера «F1» – гармоническое среднее между метрикой Precision и Recall.

5) Мера ROC-AUC – площадь под ROC-кривой, отражающая способность модели разделять классы при разных порогах.

Для оценки качества работы метода оценки эффектов ДВ ИГ, наиболее востребованным остается предложенное определение оперативности, поскольку на текущий момент для теории ИД формально не существует способов расчёта метрики полноты (Recall).

Таким образом расчёт результативности и меры «F1» в настоящий момент не представляется возможным.

3.2 Метод оценки эффектов деструктивного воздействия инфраструктурного генеза на информационную безопасность распределенных информационных систем

3.2.1 Оценка эффектов инфраструктурного деструктивизма сервиса информационной системы

Для оценки инфраструктурного деструктивизма сервиса ИС предлагается использовать адаптивные механизмы формирования тестовых последовательностей запросов *Q*, которые максимально нагружают ИС. Реализация возможна по любому из предложенных способов.

Способ 1. Предлагается найти самые долгие последовательности выполнения запросов путем перебора всех возможных вариантов из найденных последовательных шаблонов. Каждый из последов

Способ 2. На каждом из этапов предлагается рассматривать лишь те последовательности, которые наиболее проявляют эффект инфраструктурного деструктивизма сервиса. Это можно сделать, используя переборные алгоритмы решения задач. Одним из возможных алгоритмов для генерации необходимых последовательностей запросов является генетический алгоритм.

Способ 3. Суть данного запроса основана на нахождении определенных особенностей в исследуемых закономерностях и определении особых последовательностей, которые приводят к возникновению эффектов инфраструктурного деструктивизма на основе эвристики и экспертных данных.

В качестве одной из возможных метрик измерения деструктивных возможностей ИС предлагается использовать разницу по времени между самыми долгими и самыми быстрыми запросами.

$$K_{ig} = \max(Q) - \min(Q) \tag{11}$$

Для сравнения инфраструктур возможно использовать одинаковые последовательности запросов и соответственно одинаковые исходные данные таким образом можно вычислить именно показатель деструктивных возможностей

инфраструктуры. Сравнить какая информационной инфраструктура будет лучше или хуже по отношению к своим деструктивным возможности. В простом случае, когда значения переменной q_i равномерно заполняют определенный интервал привести данные к форме для сравнения инфраструктур можно с помощью линейного нормирования:

$$K_{ig} = \frac{K_{ig} - \min(Q)}{\max(Q) - \min(Q)} = \frac{\max(Q) - 2\min(Q)}{\max(Q) - \min(Q)} \quad (12)$$

3.2.2 Антропоморфический анализ поведенческих взаимодействий сервисов для оценки деструктивных процессов инфраструктурного генеза

Представим взаимное влияние процессов, используя временные диаграммы процессов виде таблице параметров (см. таблица 9).

Для каждого сервиса формализованы его поведенческие особенности в виде множества значений величин (время в с.) для каждого антропоморфического типа

$$Proc_i^{Beh} = \{PB_{T1}, PB_{T2}, PB_{T3}, PB_{T4}, PB_{T5}, PB_{T6}, PB_{T7}, PB_{T8}, PB_{T9}\}, \quad (13)$$

где $PB_{T1}, PB_{T2}, PB_{T3}, PB_{T4}, PB_{T5}, PB_{T6}, PB_{T7}, PB_{T8}, PB_{T9}$ – величины (время в с.), определяющие антропоморфические типы поведения исследуемого процесса.

Отмечено, что показатель $Proc_i^{Beh}$, может быть, двух видов.

Во-первых, это влияние времени работы сервиса на время работы параллельно выполняющихся сервисов (окружение).

Во-вторых, влияние времени выполнения параллельно выполняющихся сервисов на время исследуемого сервиса.

Поведенческие особенности сервиса описаны в виде наборов правил для каждого антропоморфического типа взаимодействия.

Для этого разработаны правила определения антропоморфических типов поведения сервисов на основе продукционной модели представлений знаний. Рассмотрены множество продукционных правил:

$$Alg_{rules} = \{rul_1, rul_2, ..., rul_{num}\}, \quad (14)$$

где rul_i – продукционное правило $i = \overline{1, num}$ (num – количество правил), которое состоит из

$$\langle sh, W, Pr, A \to B, Ap \rangle, \tag{15}$$

где sh – идентификатор правила, формируется как $S_h \in \mathbb{N}$;

W – сфера применения продукции (для каких сервисов применима данное правило); 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 $Proc_i \to Proc_j$ в словесной форме для последующей алгоритмической реализации в виде таблицы 9.

На основе множества правил $A\text{lg}_{rules}$ построено множество наборов правил для описания поведенческих взаимодействий сервисов

$$A\text{lg}_{ant\_rules} = \{At_1, At_2, At_3, At_4, At_5, At_6, At_7, At_8, At_9\}, \tag{16}$$

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

Для каждого из процессов $Proc_i$ (данные выгружаются из журналов событий) выполняется пространственно-временная локация данного процесса и всех зависимых процессов от данного процесса.

Определяются процессы, выполняющиеся до начала исследуемого процесса $Proc_i$: $Proc_a$, $Proc_b$.

Параллельно вместе с ним: $Proc_b$, $Proc_c$, $Proc_d$ и после: $Proc_e$.

Для оценки типов взаимного антропоморфического влияния сервисов используются данные, представленные в таблице 9.

В таблице 9 обозначения «+1», «-1» и «0» имеют тот же смысл, что и на рисунках 24–32.

Далее используются система поведенческих правил $A\text{lg}_{rules}$ представленная в таблице 8.

Таблица 8 – Правила 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_3	$sh_1 \vee sh_2$	$Proc_i$ работает быстрее. $Proc_j$ работает быстрее	Тип 1 или Тип 2
sh_4	sh_1	$Proc_i$ необходим для работы $Proc_j$. Без параллельного процесса $Proc_i$ процесс $Proc_j$ работает существенно медленнее	Тип 1
sh_5	sh_2	$Proc_j$ необходим для работы $Proc_i$. Без параллельного процесса $Proc_j$ процесс $Proc_i$ работает существенно медленнее	Тип 1
sh_6	sh_1	Без параллельного процесса $Proc_i$ процесс $Proc_j$ работает обычно	Тип 2
sh_7	sh_2	Без параллельного процесса $Proc_j$ процесс $Proc_i$ работает обычно	Тип 2
sh_8	sh_1	$Proc_i$ работает быстрее. $Proc_j$ работает обычно	Тип 3
sh_9	sh_2	$Proc_j$ работает быстрее. $Proc_i$ работает обычно	Тип 3
sh_{10}	sh_1	$Proc_i$ работает быстрее. $Proc_j$ работает медленнее	Тип 4
sh_{11}	sh_2	$Proc_j$ работает быстрее. $Proc_i$ работает медленнее	Тип 4
sh_{12}	sh_1	$Proc_i$ может перестать работать	Тип 5
sh_{13}	sh_2	$Proc_j$ может перестать работать	Тип 5
sh_{14}	$sh_1 \vee sh_2$	$Proc_i$ работает обычно. $Proc_j$ работает обычно	Тип 6
sh_{15}	sh_1	$Proc_i$ работает обычно. $Proc_j$ работает медленнее	Тип 7
sh_{16}	sh_2	$Proc_j$ работает обычно. $Proc_i$ работает медленнее	Тип 7
sh_{17}	$sh_1 \vee sh_2$	$Proc_i$ работает медленнее. $Proc_j$ работает медленнее	Тип 8 или Тип 9

Для каждого из процессов $Proc_j \in \{Proc_a \vee Proc_b \vee Proc_c \vee Proc_d \vee Proc_e\}$ выполняется причинно-следственный анализ их взаимодействия.

Если взаимосвязь процессов $Proc_i \to Proc_j$ подтверждается, то выполняется оценка типов взаимного антропоморфического влияния сервисов.

Таблица 9 – Параметрическое описание взаимного влияния сервисов на основе антропоморфических типов взаимодействия

Тип взаимодействия	Поведенческая особенность процессов	Влияние процесса на его окружение					Влияние окружения на процесс				
		$Proc_a$	$Proc_b$	$Proc_c$	$Proc_d$	$Proc_e$	$Proc_{a'}$	$Proc_{b'}$	$Proc_{c'}$	$Proc_{d'}$	$Proc_{e'}$
Тип 1 – «Облигатный симбиоз» (+|+) PB_{T1}	Сервисы работают быстрее если их процессы работают параллельно. Без совместного выполнения сервисы работают существенно медленнее (вместе лучше, по отдельности плохо)	+1	+1	+1	+1	1+	+1	+1	+1	+1	1+
Тип 2 – «Факультативный симбиоз» (+|+) PB_{T2}	Сервисы работают быстрее если их процессы работают параллельно. Без совместного выполнения сервисы работают обычно (вместе лучше, по отдельности обычно)	+1	+1	+1	+1	+1	+1	+1	+1	+1	0
Тип 3 – «Комменсализм» (+|0) PB_{T3}	Один из сервисов работает быстрее, если их процессы работают параллельно. Другой сервис не имеет выгоды (одному сервису лучше, другому обычно)	+1	+1	+1	+1	0	0	0	0	0	0
Тип 4 – «Паразитизм» (+|–) PB_{T4}	Один из сервисов работает быстрее, если их процессы работают параллельно. Другой сервис работает хуже (одному сервису лучше, другому хуже)	-1	-1	-1	-1	0	0	0	0	0	0
Тип 5 – «Хищничество» (+|–) PB_{T5}	Один из сервисов работает быстрее, если их процессы работают параллельно. Другой сервис работает хуже и может перестать работать (одному сервису лучше, другому хуже или может остановиться)	-1	-1	-1	-1	-1	+1	+1	+1	+1	0
Тип 6 – «Нейтрализм» (0|0) PB_{T6}	Сервисы не влияют друг на друга (одинаково)	0	0	0	0	0	0	0	0	0	0
Тип 7 – «Аменсализм» (0|–) PB_{T7}	Один из сервисов работает обычно, если их процессы работают параллельно. Другой сервис работает хуже (одному сервису обычно, другому хуже)	-1	-1	-1	-1	0	0	0	0	0	0
Тип 8 – «Аллелопатия» (–|–) PB_{T8}	Сервисы работают хуже если их процессы работают параллельно (вместе плохо)	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1
Тип 9 – «Конкуренция» (–|–) PB_{T9}	Сервисы работают хуже если их процессы работают параллельно по причине борьба за общие ресурсы. Один из процессов может перестать работать (вместе плохо)	-1	-1	-1	-1	-1	-1	-1	-1	-1	-1

На основе проведенного анализа антропоморфических типов взаимодействий процессов ИС на основе сервисной архитектуры синтезирована система поведенческих парил Alg_{rules} представленная в таблице 8.На основе таблицы 9 построена таблица 8 содержащая наборы правил Alg_{ant_rules} для описания поведения антропоморфических типов взаимодействия сервисов.

Используя правила Alg_{ant_rules} синтезируются наборы правил Alg_{ant_rules} для описания поведения антропоморфических типов взаимодействия сервисов (таблица 10).

Таблица 10 – Наборы правил Alg_{ant_rules} для описания поведения 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 3 – «Комменсализм» (+|0) At_3	$(sh_1 \wedge sh_8) \vee (sh_2 \wedge sh_9)$
Тип 4 – «Паразитизм» (+|–) At_4	$(sh_1 \wedge sh_{10}) \vee (sh_2 \wedge sh_{11})$
Тип 5 – «Хищничество» (+|–) At_5	$(sh_1 \wedge sh_{10} \wedge sh_{12}) \vee (sh_2 \wedge sh_{11} \wedge sh_{13})$
Тип 6 – «Нейтрализм» (0|0) At_6	$(sh_1 \wedge sh_{14}) \vee (sh_2 \wedge sh_{14})$
Тип 7 – «Аменсализм» (0|–) At_7	$(sh_1 \wedge sh_{15}) \vee (sh_2 \wedge sh_{16})$
Тип 8 – «Аллелопатия» (–|–) At_8	$(sh_1 \wedge sh_{17}) \vee (sh_2 \wedge sh_{17})$
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 ИС разработан алгоритм оценки антропоморфических типов взаимодействия сервисов. В начале работы алгоритма загружается информация о каждом процессе, который работал в ИС.

Для каждого процесса $Proc_i \in Proc_{all}$ формируем множество анализируемых процессов $Proc_j \in \{Proc_a \vee Proc_b \vee Proc_c \vee Proc_d \vee Proc_e\}$. Для каждого $Proc_i$ оцениваем причинно-следственную значимость данного процесса относительно процесса $Proc_i \rightarrow Proc_j$.

Если имеет место зависимость, то формируется множество $Proc_i^{Beh}$ для описания антропоморфического взаимодействия сервиса $Proc_i$ с процессами $Proc_j$.

Таким образом после работы алгоритма классификации поведенческой активности процессов формируется множество $Proc^{Beh}$ для описание всех типов взаимодействия сервисов. Данное множество $Proc^{Beh}$ является индикатором «здоровья». На основе анализа $Proc^{Beh}$ формируется оценка динамики рисков эффектов ИД, исследуемой ИС.

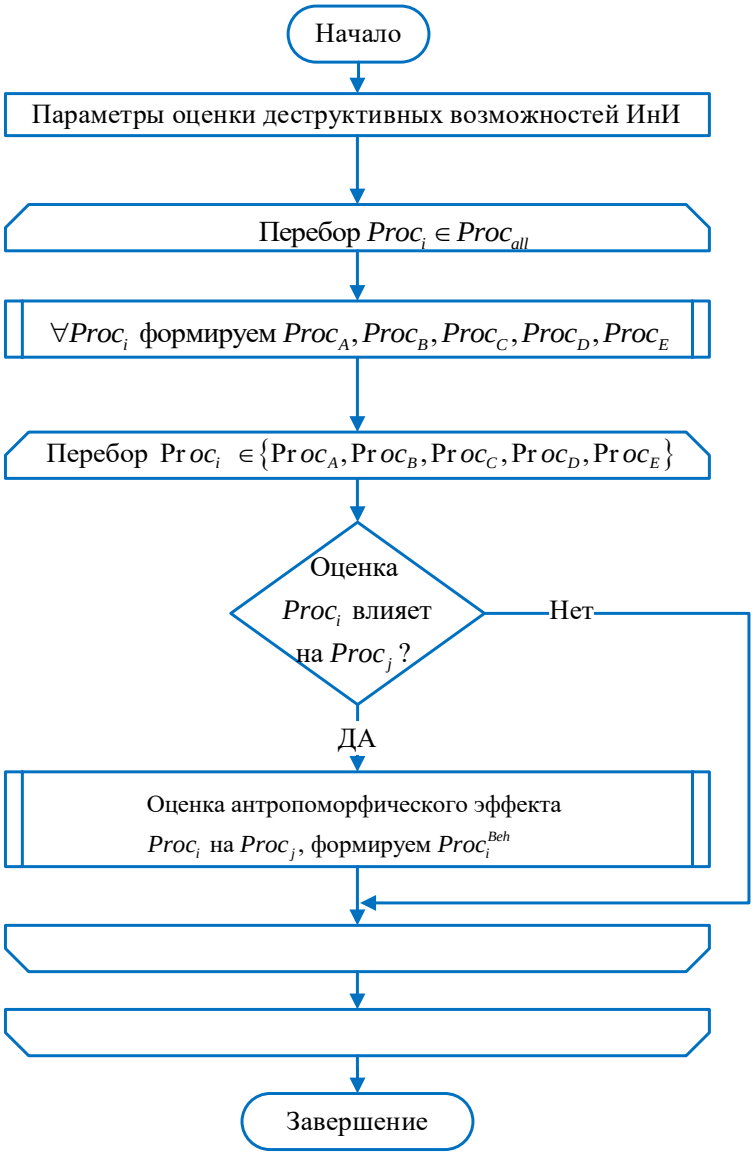

Рисунок 38 – Схема реализации алгоритма оценки антропоморфических типов взаимодействия сервисов РИС

Для удобства отображения результатов предлагается объединить типы антропоморфического взаимодействия процессов в группы и классифицировать динамику взаимного влияния сервисов:

1) положительный класс: тип 1 «Облигатный симбиоз», тип 2 «Факультативный симбиоз», тип 3 «Комменсализм»;

2) нейтральный класс: тип 4 «Нейтрализм»;

3) отрицательный класс: тип 5 «Паразитизм», тип 6 «Хищничество», тип 7 «Аменсализм», тип 8 «Аллелопатия», тип 9 «Конкуренция».

Таким образом применив данную классификацию, повышается наблюдаемость поведенческих процессов сервисов ИС, что особенно необходимо при прогнозировании угроз ИД.

3.3 Архитектура информационно-аналитической системы оценки эффектов инфраструктурного деструктивизма

3.3.1 Схема организации системы оценки инфраструктурного деструктивизма сервиса информационной системы

На основе антропоморфических моделей, представленных в пункте 2.3 и модели оценки деструктивных возможностей, представленной в пункте 3.2.1, разработана схема организации архитектуры системы оценки деструктивных возможностей для двух взаимодействующих сервисов РИС, которая представлена на рисунке 39.

Исходной точкой при организации архитектуры схема организации (рис. 39) является «Модуль 1», который также необходим для работы систем более высокого уровня. Для работы «Модуля 1» используются «Модуль 2» и «Модуль 3» с помощью которых выполняется расчет параметров взаимодействия между объектами ИС. В том числе здесь реализуется информационно аналитическая система анализа антропоморфических свойств — «ИАС 1» состоящая из «Модуля 5» и «Модуля 6». С помощью «ИАС 1» формируется база данных аналитических правил для

моделирования антропоморфических эффектов для двух взаимодействующих сервисов РИС, которая позволяет учитывать антропоморфические свойства сервисного взаимодействия.

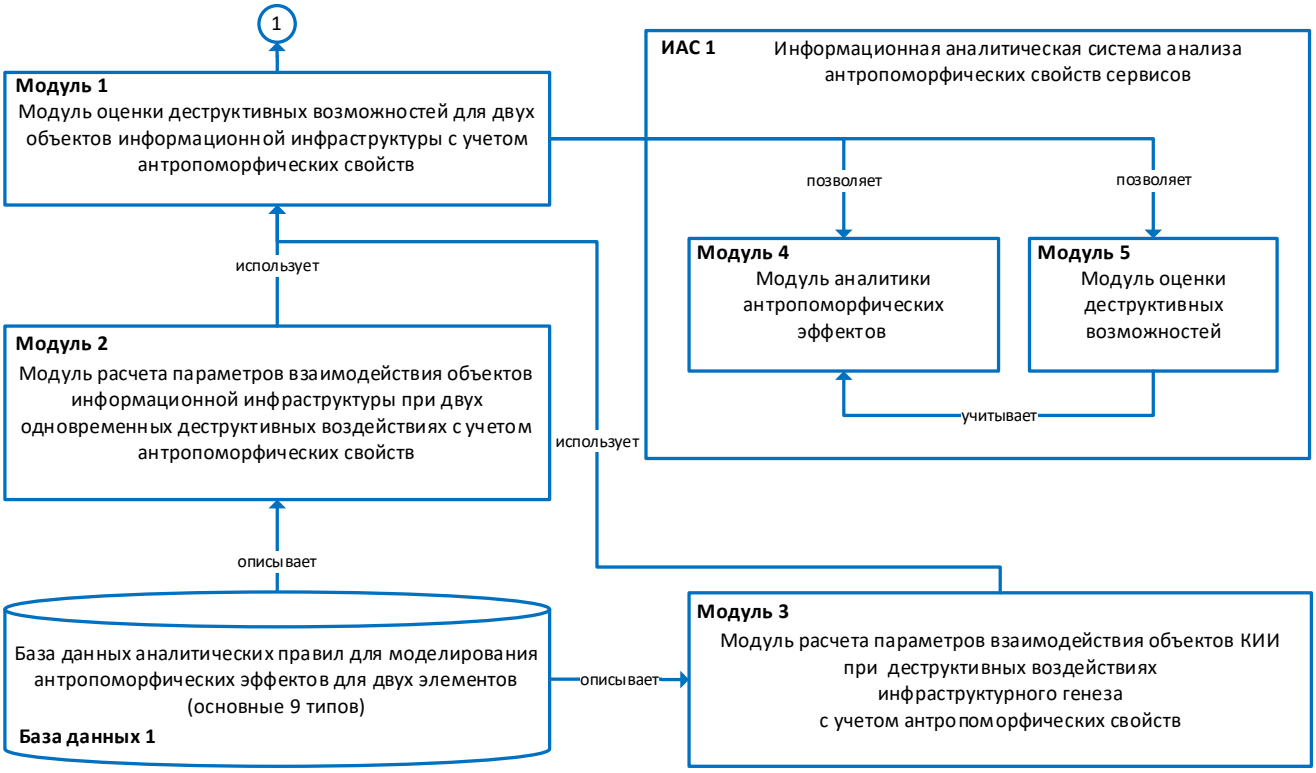

Рисунок 39 – Схема организации архитектуры системы оценки эффектов ИД для двух взаимодействующих сервисов ИС с учетом антропоморфических свойств

3.3.2 Схема организации системы оценки инфраструктурного деструктивизма взаимодействующих сервисов информационной системы

Представленный инструментарий в пункте 3.3.1 является ограниченным в связи с количеством рассматриваемых объектов ИС, а именно рассматривается ситуация, когда количество сервисов равно двум. Для универсализации рассматриваемого решения, опишем каким образом будет выполняться оценка взаимодействия нескольких сервисов. На рисунке 40 представлена схема организации архитектуры системы оценки взаимодействия нескольких сервисов ИС.

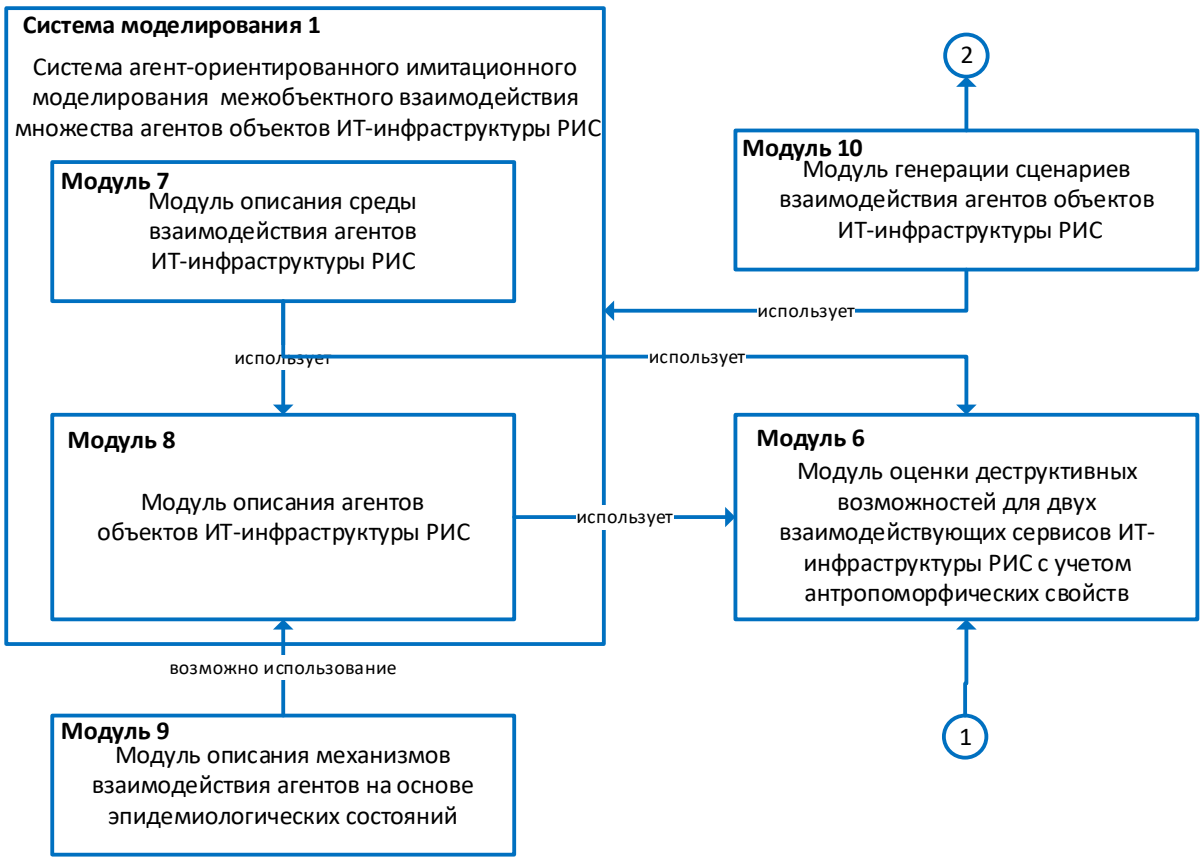

Рисунок 40 – Схема организации архитектуры системы оценки взаимодействия нескольких сервисов РИС

Исходной точкой схемы организации (рис. 40) является «Модуль 10», который генерирует сценарии взаимодействия агентов объектов РИС для «Системы моделирования 1». «Модуль 10» также необходим для работы систем более высокого уровня. Для работы «Системы моделирования 1» используются «Модуль 7» и «Модуль 8» с помощью которых выполняется агент-ориентированное моделирование межобъектного взаимодействия агентов объектов РИС. «Модуль 7» и «Модуль 8» обеспечивают моделирование среды и поведения агентов объектов информационной инфраструктуры с помощью «модуля 6», который является инструментарием описанным в пункте 3.3.1.

Также для «Модуля 8» возможно использование «Модуля 9», который описывает механизмы взаимодействия агентов на основе эпидемиологических состояний которые подробно описаны в пункте 2.5.

Система агент-ориентированного имитационного моделирования межобъектного взаимодействия множества агентов объектов ИС «Система моделирования 1» состоит из двух модулей для описания среды и агентов объектов информационной инфраструктуры, соответственно «Модуль 7» и «Модуль 8». Данная система позволяет моделировать взаимодействие множества агентов объектов РИС с учетом различных сценариев их взаимодействия.

Модуль оценки межобъектного взаимодействия двух объектов информационной инфраструктуры с учетом антроморфических эффектов «Модуль 6». Данный модуль используется в «модуле 8» для описания двух объектов информационной инфраструктуры с учетом антроморфических эффектов и реализует инструментарий, описанный в пункте 3.3.1.

Модуль описания среды взаимодействия агентов информационной инфраструктуры «Модуль 7». Данный модуль описывает процессы взаимодействия в среде агент-ориентированного моделирования, реализует координацию и мониторинг ресурсов среды, отслеживает и фиксирует появление аномального поведения агентов объектов ИТ-инфраструктуры ИС.

Модуль моделирования агентов объектов информационной инфраструктуры «Модуль 8». Данный модуль описывает параметры агентов объектов информационной инфраструктуры и управляет их поведенческой активностью.

Модуль описания механизмов взаимодействия агентов на основе эпидемиологических состояний «Модуль 9». Данный модуль является дополнительным модулем к «Модулю 8» и позволяет использовать состояния эпидемиологических моделей распространения ВПО для описания поведенческой активности агентов объектов ИС.

Модуль генерации сценариев взаимодействия агентов объектов информационной инфраструктуры «Модуль 10». Данный модуль необходим для задания сценариев взаимодействия агентов объектов информационной инфраструктуры согласно сценариям их взаимодействия. Модуль позволяет выполнить оценить ресурсоемкость произвольного сценария взаимодействия агентов объектов ИТ-инфраструктуры РИС и определить: худший, нейтральный и наилучший случай.

Приведем описание алгоритма имитационного моделирования взаимодействия множества объектов информационной инфраструктуры на основе онтологии архитектуры РИС, представленной на рисунке 41.

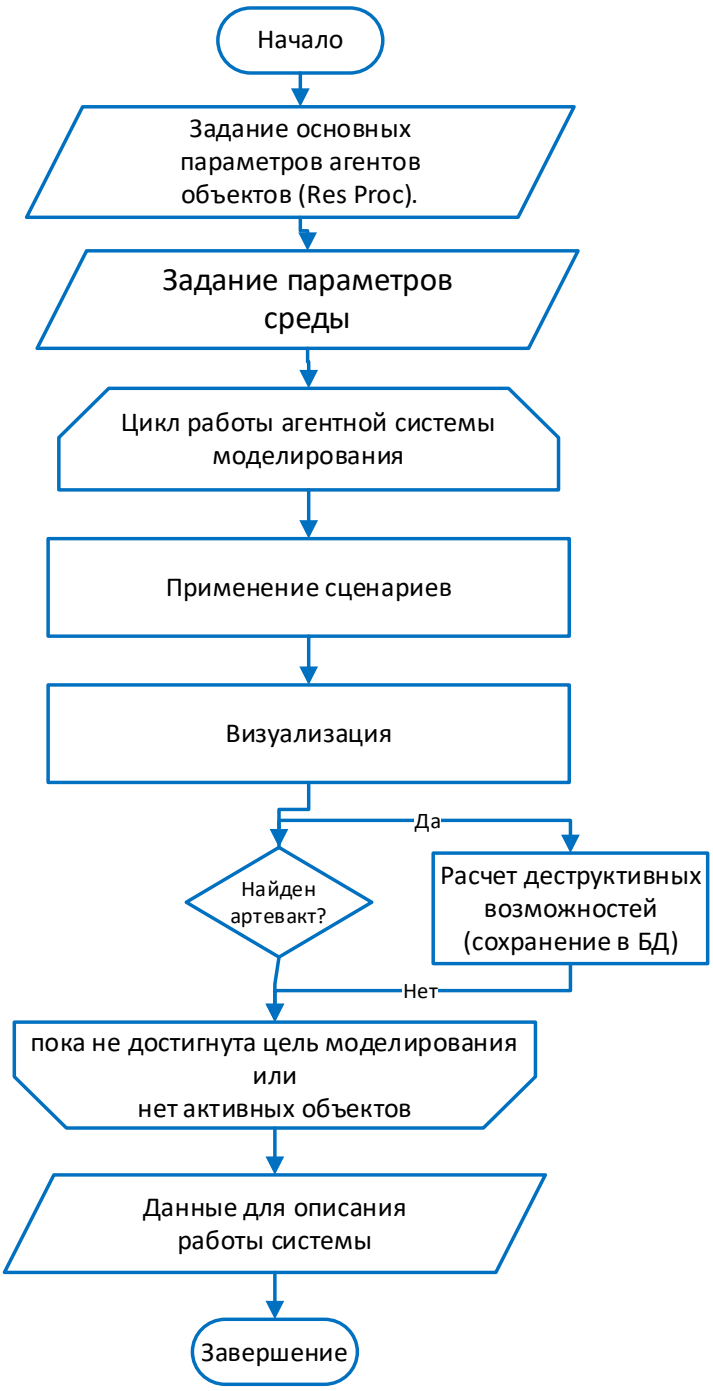

Рисунок 41 – Обобщенная блок-схема системы имитационного моделирования деструктивных возможностей ИТ-инфраструктуры РИС

Формально алгоритм, представленный на рисунке 41 можно также запасать в виде следующих последовательных шагов.

Шаг 1. Начало.

Шаг 2. Ввод параметров для агентов объектов ИТ-инфраструктуры: наборы параметров агентов объектов РИС

Шаг 3. Генерация сценариев взаимодействия агентов объектов РИС.

Шаг 4. Имитационное моделирование сценариев взаимодействия агентов объектов ИТ-инфраструктуры РИС.

Шаг 5. Оценка антропоморфических типов взаимодействия сервисов РИС

Шаг 6. Прогнозирование динамики рисков инфраструктурного генеза на основе оценки антропоморфических типов взаимодействия сервисов РИС.

3.3.3 Схема организации системы оценки взаимодействия нескольких сервисов

Решения описанные в пунктах 3.1-3.3 возможно реализовать с помощью технологий цифровых двойников [32]. Применение технологии цифровых двойников для оценки динамики рисков для существующих РИС на основе анализа журналов событий (рисунок 42).

Рисунок 42 – Онтология архитектуры системы оценки межобъектного взаимодействия множества объектов информационной инфраструктуры

Онтология архитектуры системы оценки межобъектного взаимодействия множества объектов информационной инфраструктуры представленная рисунке 42

позволяет реализовать методы эффектов деструктивного воздействия инфраструктурного генеза на информационную безопасность распределенных информационных систем произвольной архитектуры.

3.3.4 Схема организации системы оценки эффектов инфраструктурного деструктивизма распределенной информационной системы

Онтология архитектуры системы оценки инфраструктурного деструктивизма сервисной ИТ-инфраструктуры РИС представлена на рисунке 43.

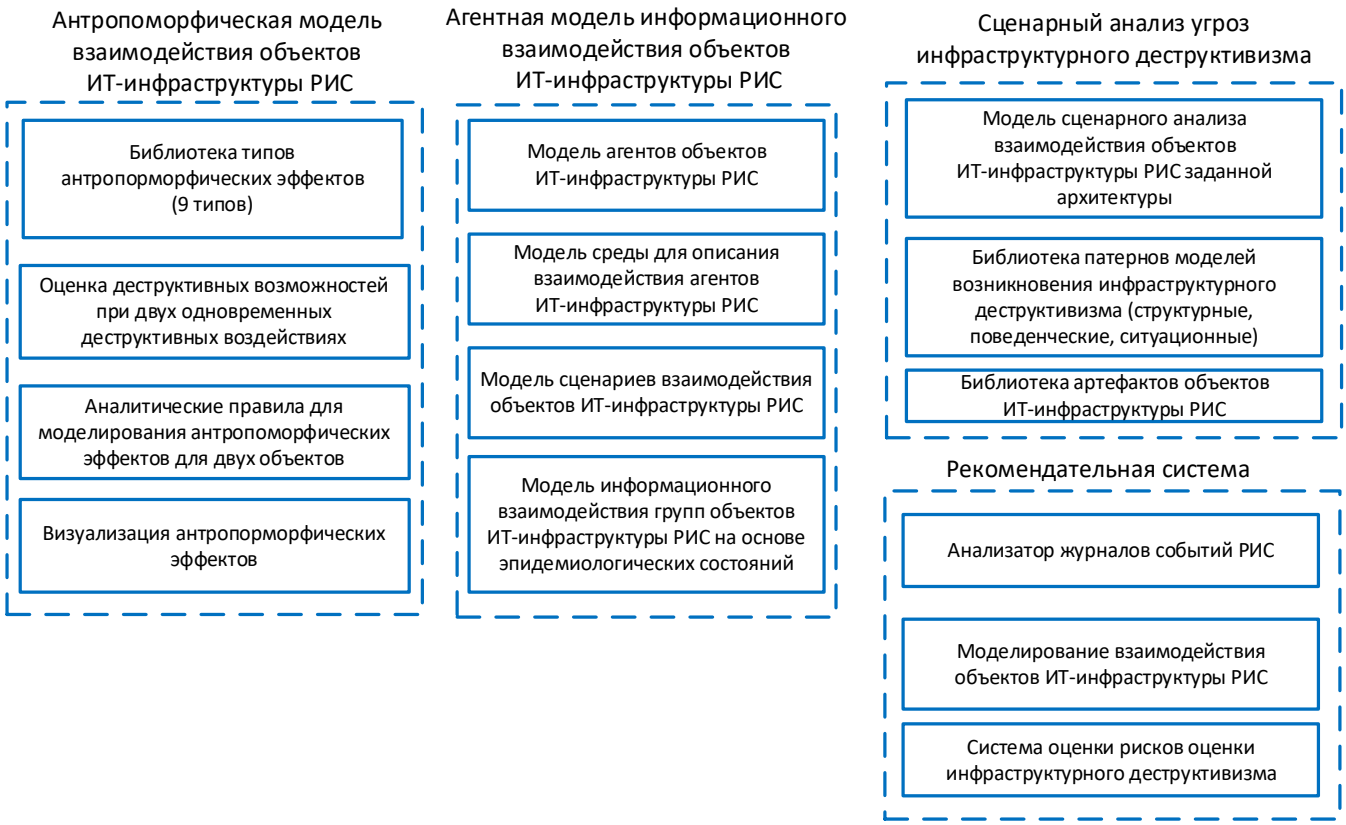

Рисунок 43 – Онтология архитектуры системы оценки инфраструктурного деструктивизма сервисной информационной инфраструктуры

Онтология архитектуры системы оценки инфраструктурного деструктивизма ИТ-инфраструктуры РИС позволяет реализовать методы оценки эффектов деструктивного воздействия инфраструктурного генеза на информационную безопасность РИС.

3.3.5 Схема организации системы имитационного моделирования распространения вирусов на основе эпидемиологической модели с антропоморфическими типами состояний

Схема организации системы имитационного моделирования распространения вирусов на основе эпидемиологической модели с антропоморфическими типами состояний представлена на рисунке 44.

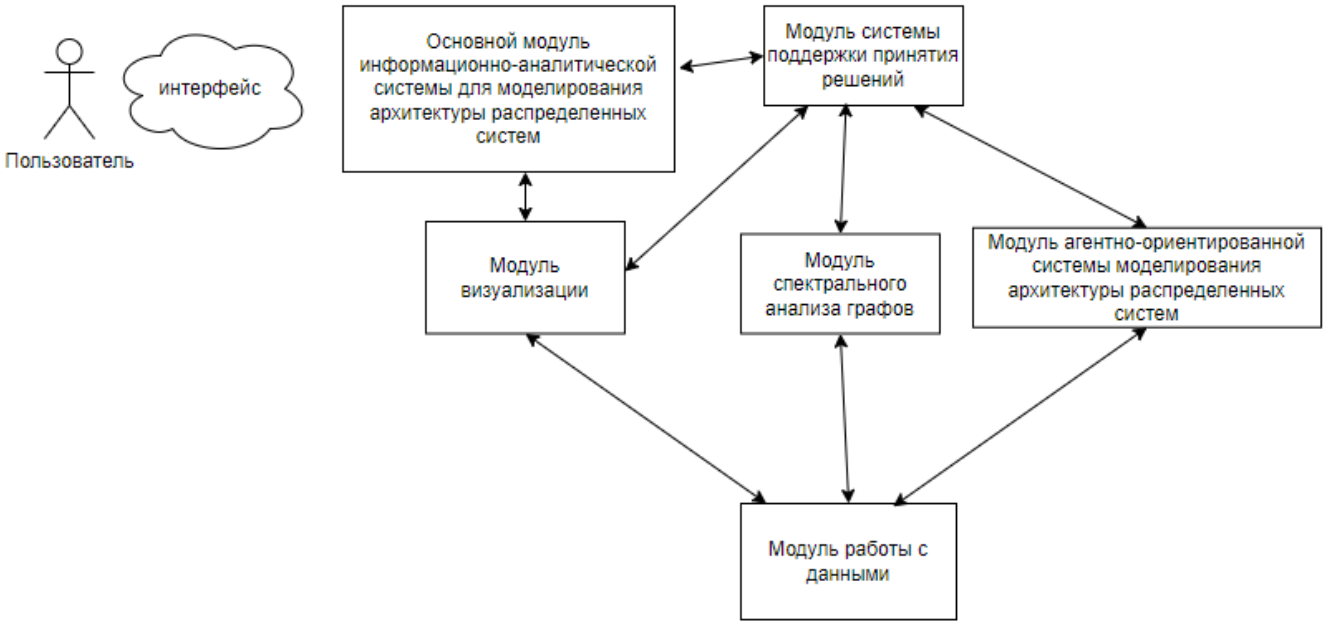

Рисунок 44 – Схема организации системы имитационного моделирования распространения вирусов на основе эпидемиологической модели с антропоморфическими типами состояний

Система имитационного моделирования распространения вирусов, представленная рисунке 44 состоит из следующих компонент:

1) основной модуль;

2) модуль системы поддержки принятия решения;

3) модуль визуализации;

4) модуль агентно-ориентированной системы моделирования основе эпидемиологической модели с антропоморфическими типами состояний;

5) модуль работы с данными.

Приведем детальное описание каждой из описанных компонент системы имитационного моделирования распространения вирусов.

Основной модуль обеспечивает интеграцию всех компонентов системы, а также управляет потоком данных и коммуникацией между модулями. Осуществляет взаимодействие с внешними источниками данных.

Модуль системы поддержки принятия решения проводит анализ результатов моделирования для выявления ключевых трендов и генерирует рекомендации и аналитические выводы для поддержки принятия решений.

Модуль визуализации обеспечивает графическое отображение данных и результатов моделирования, кроме это, предоставляет пользователю интуитивно понятный интерфейс для взаимодействия с системой.

Модуль агентно-ориентированной системы моделирования архитектуры РИС систем реализует многоагентную модель для имитации взаимодействия компонентов распределенной системы при вирусной атаке. Использует эпидемиологические SEIR-модели и другие агентные подходы для описания динамики распространения компьютерных вирусов в сетях.

Модуль работы с данными занимается сбором, хранением и обработкой данных, а также интегрирует средства обеспечения безопасности данных и управления доступом.

В основе системы имитационного моделирования распространения вирусов на основе эпидемиологической модели с антропоморфическими типами состояний лежит алгоритм, представленный на рисунке 45.

Представим основные шаги работы алгоритма системы имитационного моделирования распространения вирусов на основе эпидемиологической модели с антропоморфическими типами.

Шаг 1. Задаются параметры работы системы.

Для работы модуля необходимо задать значения параметрам.

initial-outbreak-size – начальный размер зараженной части сети;

number-of-nodes – общее количество узлов в сети;

average-node-degree – среднее количество связей у каждого узла в сети;

virus-spread-chance1, virus-spread-chance2 и virus-spread-exposed –вероятности распространения вирусов разных типов между узлами;

recovery-chance – вероятность выздоровления зараженных узлов;

gain-resistance-chance – вероятность развития устойчивости к деструктивному воздействию после выздоровления.

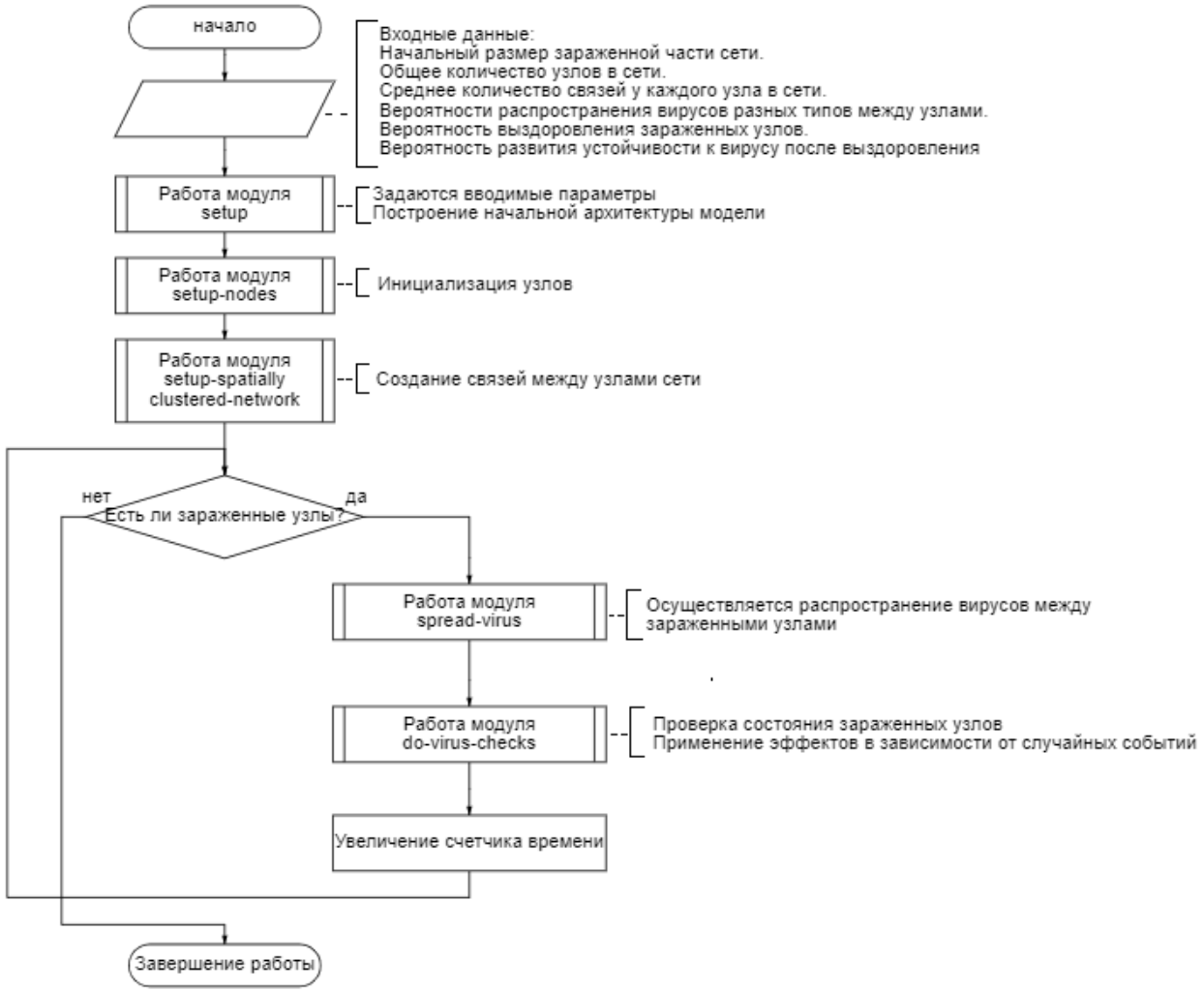

Рисунок 45 – Блок схема алгоритм работы системы имитационного моделирования распространения вирусов на основе эпидемиологической модели с антропоморфическими типами состояний

Шаг 2. Система выполняет действия модуля setup-nodes. Модуль выполняет функцию инициализации узлов в модели. Устанавливается форма по умолчанию для всех узлов в модели в виде круга (circle). Это определяет, как будет выглядеть каждый узел. создается заданное количество узлов (number-of-nodes). Каждый узел создается в соответствии с блоком кода.

Шаг 3. Для каждого создаваемого узла выполняются следующие действия. Задается случайное местоположение каждого узла, при этом координаты выбираются случайным образом в пределах 95% от максимальных координат.

Это делается для визуальных целей, чтобы узлы не находились слишком близко к краям экрана. устанавливается начальное состояние узла как чувствительного к деструктивному воздействию (синий цвет в данной модели).

Таким образом, в результате выполнения данного модуля создаются узлы с случайными координатами, установленной формой и начальным состоянием, делая их чувствительными к деструктивному воздействию.

Шаг 4. Далее вводные данные передаются в модуль setup-spatially-clustered-network. Данный модуль отвечает за создание связей между узлами сети, чтобы моделировать пространственно-кластерную структуру сети. Определяется желаемое количество связей (num-links) в сети на основе средней степени узла (average-node-degree) и общего числа узлов в сети (number-of-nodes);

Шаг 5. Запускается цикл while, который выполняется, пока количество созданных связей (count links) меньше желаемого количества связей (num-links).

Внутри цикла, для каждого прохода, выбирается случайный узел среди всех узлов. Для выбранного узла выполняются следующие действия.

Выбирается соседний узел, который еще не соединен с текущим узлом. min-one-of используется для выбора ближайшего соседа, a distance myself вычисляет расстояние между текущим узлом и потенциальным соседом;

Если найден сосед (choice не равен nobody), создается связь между текущим узлом и выбранным соседом с помощью create-link-with;

Используется функция layout-spring, которая придает сети более аккуратный вид. Это осуществляется путем применения алгоритма пружинной раскладки (spring layout), который рассчитывает координаты узлов в сети так, чтобы связи между узлами подобны пружинам.

Это улучшает визуальное представление структуры сети.

Таким образом, эта процедура создает пространственно-кластерную сеть, соединяя узлы соседними связями и улучшая визуальное представление сети.

Шаг 6. После того, как узлы и связи сформированы, программа начинает свою основную часть работы. Запускается цикл, который проверяет на наличие зараженных узлов. Цикл работает до тех пор, пока не останется ни одного зараженного узла.

Открывает начало работы цикла модуль spread-virus. Здесь осуществляется распространение вирусов между зараженными (или латентными) узлами и их соседями в сети. Выбираются все узлы, которые являются зараженными первым типом вируса (infected1?), зараженными вторым типом вируса (infected2?) или находятся в латентном состоянии (exposed?);

Затем для каждого выбранного узла выполняется следующий блок кода. Он выбирает соседей текущего узла, которые не являются сопротивляемыми деструктивному воздействию (not resistant?) и не находятся в латентном состоянии (not exposed?).

Затем по условию выбирается каким вирусом будет заражен узел, либо же узел переходит в латентное состояние. Этот модуль моделирует случайное взаимодействие между зараженными узлами и их соседями, где вероятность заражения зависит от типа вируса и уровня распространения (virus-spread-chance1, virus-spread-chance2, virus-spread-exposed).

Далее работает модуль do-virus-checks. Модуль отвечает за проверку состояния зараженных узлов и применение эффектов в зависимости от случайных событий. Он моделирует возможность выздоровления зараженных узлов с определенной вероятностью и их последующее приобретение или потерю сопротивляемости к деструктивному воздействию.

Далее идет обновление счетчика на один отсчет. Проверяется условие на наличие зараженных узлов.

Если таковых не имеется – программа завершает свою работу.

3.4 Рекомендательная система по профилактике и предотвращению деструктивного воздействия инфраструктурного генеза в сервис-ориентированных информационных системах

При реализации моделей и методов прогнозирования угроз ИГ и методов оценки эффектов ДВ ИГ в сервис-ориентированных РИС сформирована система правил профилактики и предотвращения ИД, позволяющая:

1) определить наличие эффектов ИД;

2) локализовать источники возникновения угроз ИГ;

3) прогнозировать риски возникновения эффектов ИД;

4) оценивать динамику рисков ИД;

5) предотвратить возникновения ИД в РИС.

В первом случае правила можно рассматривать как профилактические меры обеспечения ИБ РИС

Во всех остальных случаях правила могут рассматриваться как меры снижения (предотвращения) ИД с точки зрения возникновения инцидента ИБ «отказ в обслуживании». В данном случае, под инцидентом ИБ будем рассматривать единственно возможное событие на уровне ИТ-инфраструктуры РИС, связанное с её разрушением. То есть возникновение данного инцидента в ИТ-инфраструктуре РИС как системы будет являться точкой бифуркации в синергетическом развитии инфраструктуры. При этом в ходе расследования данного инцидента предлагаемая система правил позволит определить источник его возникновения.

Классификацию видов правил по профилактике и предотвращению ИД представим, учитывая то, что источниками возникновения угроз ИГ могут быть поведенческие особенности наблюдаемых процессов.

Таким образом, в том числе основываясь на результатах экспериментального исследования представленном в пунктах 4.1-4.6 можем говорить о правилах:

1) определения наличия эффектов ИД (система правил 1);

2) локализация источников возникновения угроз ИГ (система правил 2);

3) прогнозирование рисков возникновения ИД (система правил 3);

4) оценки динамики рисков ИД (система правил 4);

5) предотвращения возникновения ИД в сервисных ИС (система правил 5).

В итоге, на концептуальном уровне сформулирована система продукционные правила.

Система правил 1. Правила определения наличия эффектов ИД:

Правило 1.1. Если существует межсервисное взаимодействие типа 5 «Паразитизм» большой интенсивности, то вероятнее всего проявляются эффекты ИД.

Правило 1.2. Если существует межсервисное взаимодействие тип 6 «Хищничество» большой интенсивности, то вероятнее всего проявляются ИД.

Правило 1.3. Если существует межсервисное взаимодействие тип 7 «Аменсализм» большой интенсивности, то вероятнее всего проявляются эффекты ИД.

Правило 1.4. Если существует межсервисное взаимодействие тип 8 «Аллелопатия» большой интенсивности, то вероятнее всего проявляются эффекты ИД.

Правило 1.5. Если существует межсервисное взаимодействие типа 9 «конкуренция» большой интенсивности, то вероятнее всего проявляются эффекты инфраструктурного деструктивизма.

Правило 1.6. Если уровень «отрицательного» взаимодействия существенно выше, чем уровень «положительного» взаимодействия (описание см. раздел 2.3) то проявляются эффекты инфраструктурного деструктивизма.

Система правил 2. Правила локализация источников возникновения угроз ИГ:

Правило 2.1. Если сервис оказывает межсервисное влияние типа 5 «Паразитизм» большой интенсивности, то вероятнее всего этот сервис является источником угрозы ИГ.

Правило 2.2. Если сервис оказывает межсервисное влияние типа 6 «Хищничество» большой интенсивности, то вероятнее всего этот сервис является источником угрозы ИГ.

Правило 2.3. Если сервис оказывает межсервисное влияние типа 7 «Аменсализм» большой интенсивности, то вероятнее всего этот сервис является источником угрозы ИГ.

Правило 2.4. Если сервис оказывает межсервисное влияние тип 8 «Аллелопатия» большой интенсивности, то вероятнее всего этот сервис является источником угрозы ИГ.

Правило 2.5. Если сервис оказывает межсервисное влияние типа 9 «Конкуренция» большой интенсивности, то вероятнее всего этот сервис является источником угрозы ИГ.

Правило 2.6. Если уровень «отрицательного» взаимодействия сервиса существенно выше, чем уровень «положительного» взаимодействия, то сервис является источником угрозы ИГ.

Система правил 3. Правила прогнозирование рисков возникновения ИД:

Правило 3.1. Если в ИС практически нет (1-4%) сервисов с «отрицательным» уровнем межсервисного взаимодействия, то риск возникновения эффектов ИД «очень низкий» (5-10%).

Правило 3.2. Если в ИС мало (5-10%) сервисов с «отрицательным» уровнем межсервисного взаимодействия, то риск возникновения эффектов ИД «низкий» (11-25%).

Правило 3.3. Если в ИС среднее количество (11-25%) сервисов с «отрицательным» уровнем межсервисного взаимодействия, то риск возникновения эффектов ИД «средний» (26-60%).

Правило 3.4. Если в ИС большое количество (26-35%) сервисов с «отрицательным» уровнем межсервисного взаимодействия, то риск возникновения эффектов ИД «высокий» (61-85%).

Правило 3.5. Если в ИС большое количество (больше 36%) сервисов с «отрицательным» уровнем межсервисного взаимодействия, то риск возникновения эффектов ИД «максимален» (больше 86%).

Система правил 4. Правила оценки динамики рисков ИД:

Для данной системы правил необходимо построить графики оценки динамики рисков ИД как показано на рисунках 81 и 82.

Для каждого из построенных графиков необходимо построить тренды.

Правило 4.1. Если найдена точка пересечения «отрицательного» и «положительного» трендов межсервисного взаимодействия, то данная точка является точкой бифуркцаии и после этой отметки возможно полный отказ исследуемой системы.

Правило 4.2. Если тренд «отрицательного» межсервисного взаимодействия растет по отношению к «положителному», то риск возникновения эффектов ИД «высокий».

Правило 4.3. Если тренд «отрицательного» существенно больше (выше) «положительного» межсервисного взаимодействия, то риск возникновения эффектов ИД «средний».

Правило 4.4. Если тренд «отрицательного» сопоставим с трендом «положительного» межсервисного взаимодействия, то риск возникновения эффектов ИД «низкий».

Правило 4.5. Если тренд «отрицательного» существенно меньше (ниже) чем тренд «положительного» межсервисного взаимодействия, то риск возникновения эффектов ИД «очень низкий».

Правило 4.6. Если тренд «положительного» в межсервисного взаимодействия растет по отношению к «отрицательному», то риск возникновения эффектов ИД «очень низкий».

Система правил 5. Правила предотвращения возникновения ИД в сервисных ИС:

Правило 5.1. Если риск возникновения эффектов ИД «высокий», то необходимо обнаружить источник угрозы и нейтрализовать. Также нужно принять решение стоит ли поддерживать данную систему. Возможно, что экономически целесообразнее провести замену старой системы на новую.

Правило 5.2. Если риск возникновения эффектов инфраструктурного деструктивизма «средний», то необходимо обнаружить источник угрозы и нейтрализовать.

Правило 5.3. Если риск возникновения эффектов ИД «низкий», то необходимо проводить оценку динамики рисков ИД на постоянной основе регулярно.

Правило 5.4. Если риск возникновения эффектов ИД «очень низкий», то необходимо проводить оценку динамики рисков ИД по необходимости.

Важно отметить, что система правил 5 в отличие от систем правил 1 – 4 определяют концептуальные подходы к объекту исследования. Данные правила по форме представления видоизменяемы в зависимости о прикладного назначения защищаемых систем. Данное программное средство, содержащее описанные выше системы правил реализовано в [156].

3.5 Выводы по разделу 3

В качестве объекта исследовался комплекс моделей взаимодействия сервисов информационных систем для обнаружения эффектов инфраструктурного деструктивизма на предмет оценки эффектов деструктивного воздействия инфраструктурного генеза.

В ходе исследования:

1) Реализован алгоритмический метод оценки инфраструктурного деструктивизма сервиса. Определены основные принципы функционирования и установлены ограничения его применения. Предложен подход к вычислению количественного показателя инфраструктурного деструктивизма, основанный на анализе характеристик инфраструктуры.

2) Выполнена алгоритмическая реализация модели оценки деструктивного потенциала ИТ-инфраструктуры распределённой информационной системы для взаимодействующих сервисов. С учётом антропоморфических характеристик поведения элементов инфраструктуры разработано параметрическое представление взаимного влияния сервисов. Сформирован набор правил, описывающих поведение и взаимное воздействие сервисов, а также правила, характеризующие их взаимодействие в соответствии с антропоморфическими типами поведения.

Предложена схема расчёта метрик оценки эффектов инфраструктурного деструктивизма на основе комплекса антропоморфических моделей: положительный класс, тип 1 «Облигатный симбиоз», тип 2 «Факультативный симбиоз», тип 3 «Комменсализм»; нейтральный класс, тип 4 «Нейтрализм»; отрицательный класс, тип 5

«Паразитизм», тип 6 «Хищничество», тип 7 «Аменсализм», тип 8 «Аллелопатия», тип 9 «Конкуренция».

На основе приведенной схемы сформирована метрика для оценки «здоровья» ИТ-инфраструктуры РИС.

3) Разработана архитектура информационно-аналитической системы, предназначенной для оценки эффектов инфраструктурного деструктивизма. Построена схема организации оценки антропоморфических эффектов функционирования сервиса. Сформирована схема организации системы, обеспечивающей оценку взаимодействия множества сервисов информационно-технологической инфраструктуры.

4) На основе совокупности эпидемиологических моделей разработана схема организации системы имитационного моделирования распространения вирусов с учётом антропоморфических типов состояний. Определены и обоснованы оптимальные параметры её функционирования.

5) Расширена функциональность рекомендательной системы, ориентированной на профилактику и предотвращение проявлений инфраструктурного деструктивизма на объектах критической информационной инфраструктуры [90]. Сформирована база знаний и артефактов, предназначенная для прогнозирования и оценки эффектов инфраструктурного деструктивизма.

Основным научным результатом, изложенным в третьем разделе, является алгоритмическая реализация методов оценки эффектов деструктивного воздействия инфраструктурного генеза.

Частными научными результатами, изложенными в четвертом разделе, являются:

1) оценка старения распределенных информационных систем с позиции ИД (накопление деструктивного мусора);

2) расширение рекомендательной системы по профилактике и предотвращению ИД.

Данные результаты непосредственно использованы для получения основного научного результата – разработка методов оценки эффектов деструктивного воздействия инфраструктурного генеза.

Основное содержание раздела и изложенных в нем научных результатов опубликовано в работах автора [143, 132, 139, 156, 155, 147, 145].

4 МЕТОДИКА И РЕАЛИЗАЦИЯ ПРОГРАММНО-АНАЛИТИЧЕСКОГО КОМПЛЕКСА ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФРАСТРУКТУРНОГО ГЕНЕЗА В СЕРВИС-ОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

4.1. Методика оценки угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах

Методика оценки угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах основывается на всестороннем анализе результатов проявления событий, зафиксированных в журналах РИС, моделировании поведения сервисов с учётом их взаимосвязей, а также применении агентных и имитационных моделей.

Как показано на рисунке 46 методика оценки угроз ИБ ИГ в сервис-ориентированных ИС состоит из следующих этапов:

Этап 1. Анализе исходных данных. Формирование набора источников для анализа, включающего журналы событий, из которых извлекается необходимая информация о проявлениях эффектов инфраструктурного деструктивизма. Выполняются фильтрация данных, причинно-следственный анализ и классификация межсервисных взаимодействий с целью оценки ключевых параметров функционирования сервисов РИС.

Этап2. Интеллектуальном анализе на основе антропоморфических типов межсервисных взаимодействий РИС. В крупных и сложных РИС для анализа выбирается не более 15 сервисов, исходя из максимальной глубины причинно-следственного анализа их взаимодействий. При этом исследование проводится не по всем сервисам одновременно, а по кластерам, в пределах которых наблюдается наиболее интенсивное взаимодействие. Это обусловлено тем, что на практике причинно-следственные связи присутствуют лишь между частью сервисов.

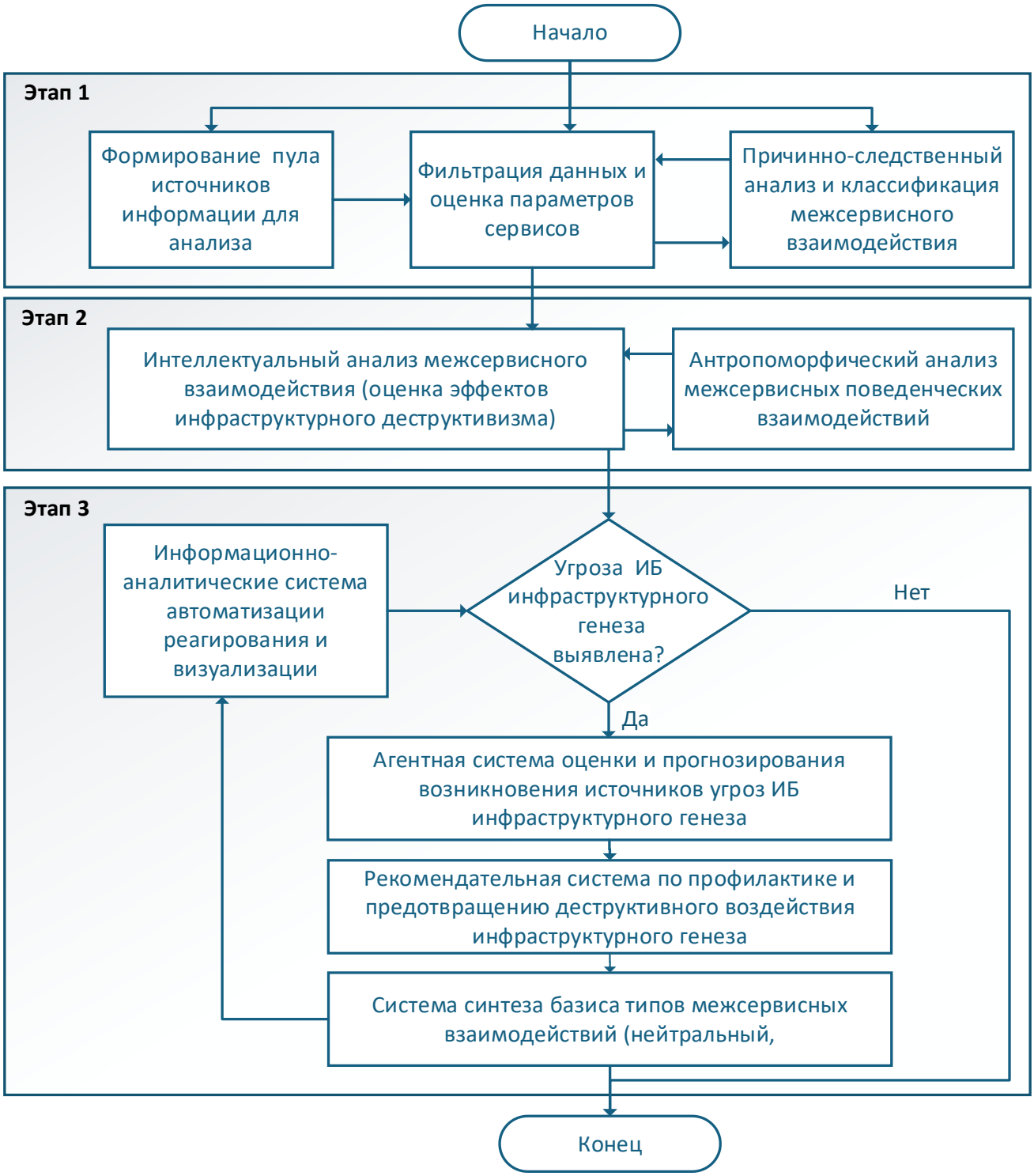

Рисунок 46 – Структурная схема Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС

Этап 3. Оценка угроз ИБ ИГ. На данном этапе осуществляется реализация информационно-аналитической системы автоматизации реагирования и визуализации поведенческих межсервисных взаимодействий на основе антропоморфических типов, обеспечивающей синтез базиса последовательных шаблонов и ассоциативных правил. Алгоритм синтеза базиса типов взаимодействий сервисов

предусматривает классификацию последовательностей по трём категориям (положительная, нейтральная, негативная) согласно метрикам отклика, выделение шаблонов и создание минимального базиса межсервисных взаимодействий для прогнозирования эффектов ИД. Проводится агентное моделирование, направленное на выявление, оценку и прогнозирование возникновения источников угроз ИБ ИГ в РИС. Функционирует рекомендательная подсистема, предназначенная для профилактики и предотвращения ДВ ИГ.

Основные процедуры для применения методики выявления угроз ИБ ИГ в РИС характеризуются следующим.

Шаг 1. Построение ИТ-инфраструктуры РИС.

Шаг 2. Имитация работы РИС. Своевременность доставки информации напрямую зависит от количества серверов и их взаимодействия в аспекте обслуживания пользовательских запросов.

Шаг 3. Сбор данных о работе сетевой инфраструктуры. На данном шаге происходит сбор различной информации (например, журналов событий работы серверов) при обслуживании пользовательских запросов в штатном режиме работы РИС. Шаг выполняется параллельно с Шагом 2.

Шаг 4. Обработка данных о работе сетевой инфраструктуры. Процедура выполняется после завершения имитации работы РИС и предназначена для обработки информации, собранной в процессе с серверов.

Шаг 5. Выявление эффектов ИД. Применяется алгоритмы выявления ИД к информации, собранной на Шаге 3 и обработанной на Шаге 4.

Работа данного шага основана на следующем принципе. Поведенческие особенности для запроса описаны в виде наборов правил антропоморфических типов взаимодействия на основе продукционной модели представлений знаний. Для каждого из запросов (которые выгружаются из журналов событий) выполняется пространственно-временная локация на основе последовательных шаблонов. В начале работы алгоритма загружается информация о запросах, для каждого из которых формируется множество анализируемых взаимодействующих запросов и оценивается причинно-следственная связь. Если зависимость детектируется, то

формируется множество для описания количественных характеристик антропоморфического взаимодействия запросов, что позволяет определить соответствующий тип эффекта. Количественные характеристики рассчитываются на основе фактического времени выполнения запросов по каждому из антропоморфических типов взаимодействия по отношению к общему времени выполнения исследуемых запросов (измеряется в процентах).

Анализ структурной схемы применения Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС позволил определить возможности проактивного прогнозирования рисков ИБ и построить следующую организационную схему её применения для прогнозирования, как показано в таблице 11.

Таблица 11 – Схема применения методики оценки угроз ИД

Наименование этапа	Описание
1. Сбор и анализ результатов проявления ИД содержащихся в журналах событий РИС	Интеллектуальный анализ журналов событий. Выявление аномалий и долгих запросов, фильтрация выбросов.
2. Моделирование взаимодействия сервисов РИС на основе антропоморфических типов взаимодействия	Построение временных диаграмм. Причинно-следственный анализ и классификация взаимодействий сервисов по антропоморфическим типам. Выявление узких мест, обнаружение аномалий, прогнозирование времени выполнения запросов РИС.
3. Имитационное моделирование	Сценарное моделирование (цифровые двойники). Выявление источников ИД
4. Оценка динамики рисков деструктивного воздействия инфраструктурного генеза	Оценка параметров и метрик инфраструктуры РИС: количество долгих запросов, количество аномалий, построение метрики «здоровья» инфраструктуры
5. Автоматизация и визуализация	Интеграция в системы безопасности (SIEM, SOAR). Построение панели мониторинга. Формирование отчётов. Рекомендательная система.

Выявленные особенности в прогностической оценке эффектов ИД в РИС и синтезированная с их учетом схема организации, включающая детализацию представлена на рисунке 47. Схема организации обеспечивает содержит рекомендательную систему по профилактике и предотвращению ДВ ИГ в сервис-ориентированных ИС, продукционные правила для которой приведены в пункте 3.4.

Представленная на рисунке 47 схема организации обеспечивает реализацию Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС в режиме реального времени, что позволяет повысить оперативность реагирования.

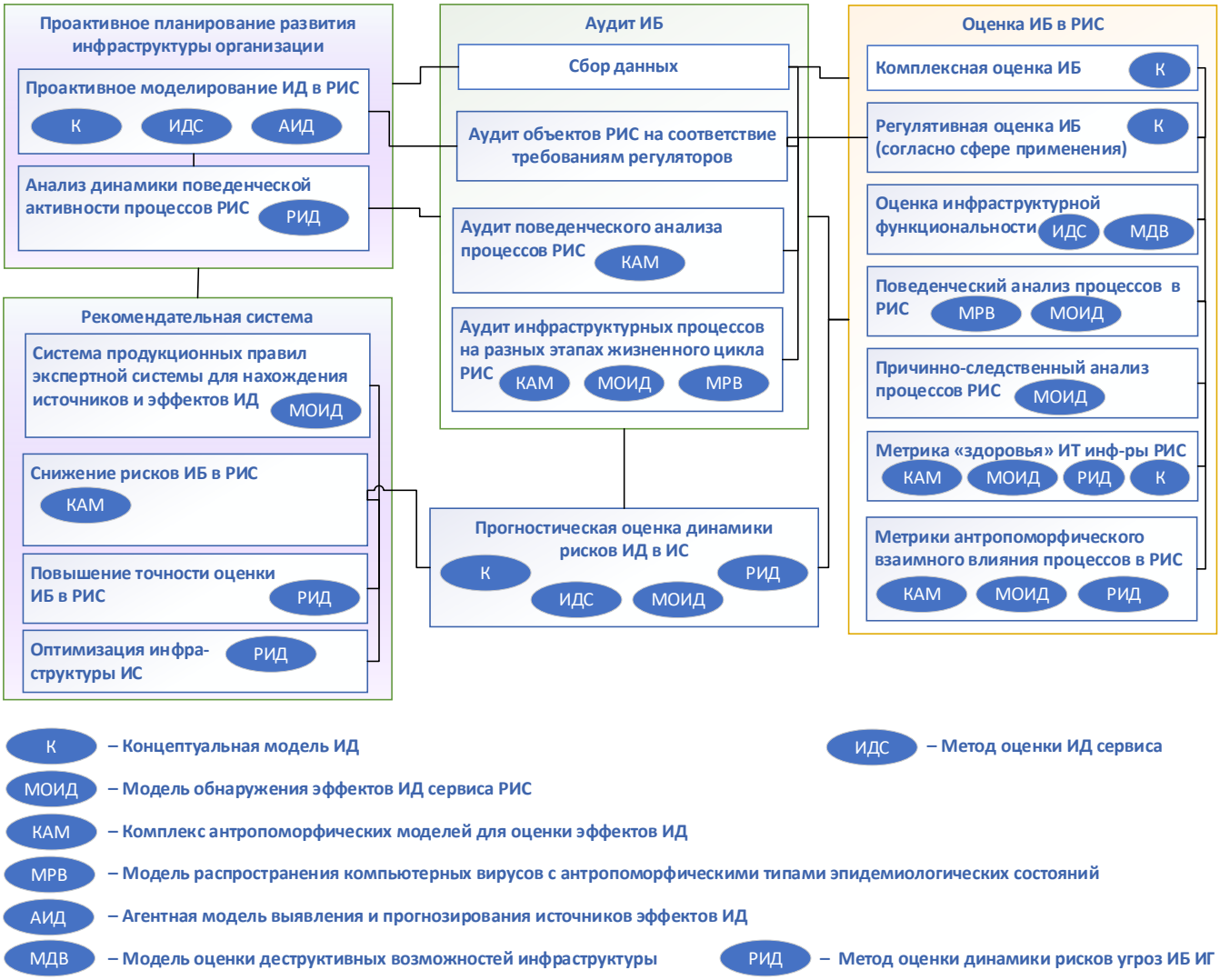

Рисунок 47 – Схема организации Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС

Следует отметить, что для интеграции разработанной методики с другими системами ИБ и распространёнными платформами мониторинга РИС (такими как ELK Stack, Grafana, Prometheus) предлагается использование их программных интерфейсов и стандартных протоколов взаимодействия. Это обеспечивает совместимость и минимизирует сложности при интеграции с существующими программными решениями ИБ.

4.2 Описание плана проведения экспериментального исследования

Экспериментальное исследование разработанных в предыдущем разделе моделей, методов и методик выполняется в несколько последовательных этапов.

На первом этапе основное внимание уделяется выявлению признаков эффектов ИД в РИС и определению момента зарождения его жизненного цикла.

В рамках этого этапа подтверждается наличие эффектов ИД, анализируются возможные способы оценки (выявления) и устанавливается спектр потенциальных деструктивных возможностей.

На втором этапе исследуются антропоморфические модели межсервисных взаимодействий и вычисляются параметры функции зрелости ИТ-инфраструктуры РИС. Анализ журналов событий РИС позволяет описать поведенческие характеристики сервисов и визуализировать внутреннее состояние ИТ-инфраструктуры с точки зрения её динамики и устойчивости.

На третьем этапе формируется имитационная модель межсервисного взаимодействия ИТ-инфраструктуры РИС с применением технологии цифровых двойников, предназначенная для исследования сценариев развития инфраструктурного деструктивизма.

Для проведения моделирования используются параметры, извлекаемые из журналов событий реальных РИС.

Основная цель экспериментального исследования заключается в определении параметров функционирования моделей, методов и методик, применяемых для оценки и выявления эффектов ДВ ИГ на ИБ РИС.

Полный план Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС представлен в таблице 12.

Таблица 12 – План экспериментального исследования Методики оценки угроз ИБ ИГ в сервис-ориентированных ИС

Номер этапа	Номер эксперимента	Название эксперимента	Цель эксперимента	Исходные данные	Варьируемые данные	Прогнозируемый результат
1.	1.	Исследование сервиса на наличие эффекта инфраструктурного деструктивизма.	Формирование данных для постановки задачи по оценке деструктивных возможностей инфраструктуры сервиса.	Тестовая база данных «DVD RENTAL» (15 связанных таблиц, 7 представлений, 13 последовательностей, 1 тригер, 8 функций, 3 Мб тестовых данных).	Последовательность запросов (генерируется программно, 20 запросов SELECT). Версии PostgreSQL: 12, 13, 14.	Определение зависимости последовательностей запросов от времени их выполнения в различных версиях PostgreSQL.
	2.	Интеллектуальный анализ работы хранилища данных GreenPlum на основе обработки лог-файлов в условиях инфраструктурного деструктивизма.	Прогнозирование возникновения точки начала инфраструктурного деструктивизма.	Лог-файлы работы хранилища данных GreenPlum Skolkovo Hack 2022 (выгрузка фалов за 2 недели в разных форматах). Автор участник и призер (1 место)	Выборки из лог-файлов работы хранилища данных GreenPlum. Математические методы прогнозирования временных рядов.	Создание условий для локализации точки возникновения инфраструктурного деструктивизма.
2.	1.	Исследование взаимодействия сервисов на основе антропоморфических моделей	Оценка деструктивных возможностей информационно-технологической инфраструктуры.	Журналы событий работы платформы OpenStack для облачных вычислений. Набор DeepTraLog из 5 датасетов логов бенчмарков тестовой системы бронирования билетов на поезд (41 микросервис)	Выборки из журналов событий систем. Параметры антропоморфических моделей.	Выявление поведенческих особенностей сервисов приводящих к возникновению эффектов инфраструктурного деструктивизма.
	2.	Исследование вирусной активности на основе эпидемиологической SEIR модели с учетом антропоморфических эффектов взаимодействия узлов.	Определение зависимости деструктивных возможностей вирусов от их количества.	Модель распространения вирусов SEIR в системе агентного имитационного моделирования NetLogo.	Структуры узлов в среде моделирования NetLogo. Количество различных распространяющихся вирусов.	Результат оценки деструктивных возможностей вирусов при увеличении их количества.
3.	1.	Реализация системы прогнозирования и оценки эффектов инфраструктурного деструктивизма для существующих систем.	Оценка и прогнозирование эффектов инфраструктурного деструктивизма на основе антропоморфических моделей взаимодействия сервисов в разных режимах	Журналы событий работы интеллектуальной самообучающейся РИС распознавания лиц «Персона ID» в разных тестовых режимах. Журналы событий работы платформы OpenStack. Журналы событий облачных вычислительных кластеров «Alibaba Cloud».	Параметры антропоморфических моделей взаимодействия сервисов Выборки из журналов событий систем	Обнаружение эффектов инфраструктурного деструктивизма.
	2	Реализация системы оценки динамики рисков инфраструктурного деструктивизма для существующих систем.	Обнаружение результатов проявления эффектов ИД для кластера «Alibaba Cloud».		Выборки из лог-файлов. Антропоморфическая матрица параметров процессов системы.	Оценка динамики рисков инфраструктурного деструктивизма.

4.3 Исследование программного интерфейса сервиса информационной системы на наличие эффектов инфраструктурного деструктивизма

В исследовании представлены два подхода к выявлению и прогнозированию источников инфраструктурного деструктивизма. Первый подход основан на анализе откликов на последовательности запросов к сервису и выявлении ситуаций, при которых сервис утрачивает способность корректно выполнять свои функции.

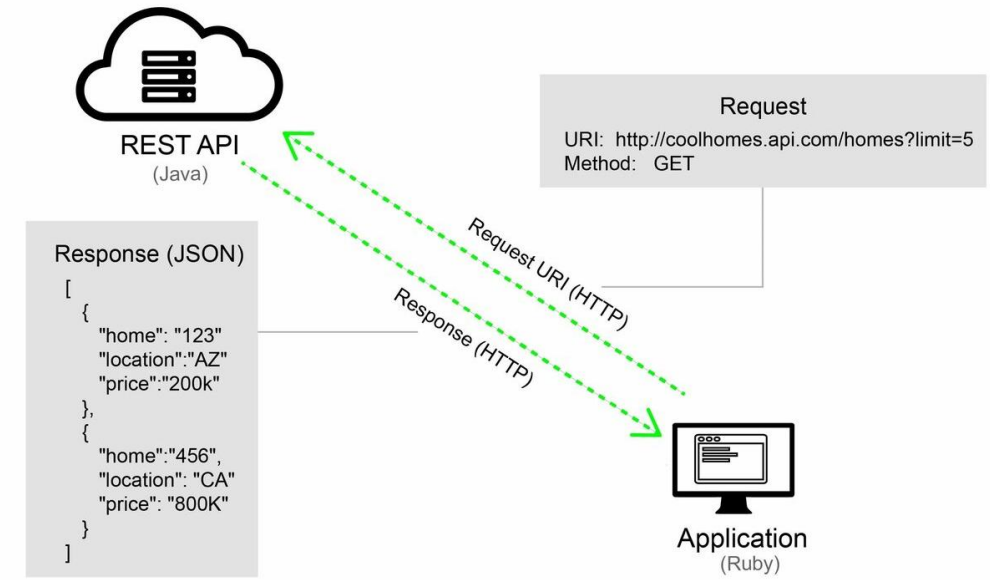

Рисунок 48 – Типовая схема обработки запросов и ответов на основе модели взаимодействия программных интерфейсов REST []

На рисунке 48 изображена схема взаимодействия сервиса и клиента [141]. После направления запроса клиент ожидает получения ответа. Формируя различные последовательности запросов на вход программного интерфейса, фиксируется соответствующая последовательность откликов. Анализ времени обработки таких последовательностей позволяет рассчитать параметры функционирования сервиса в худшем и лучшем сценариях.

Рассммотрим в качестве примера тестовый набор базы данных «DVD RENTAL» для системы управления базами данных PostgreSQL [169]. Данный

набор состоит из 15 таблиц 7 представлений, 13 последовательностей, 1 триггер, 8 функций, 3 Мб тестовых данных.

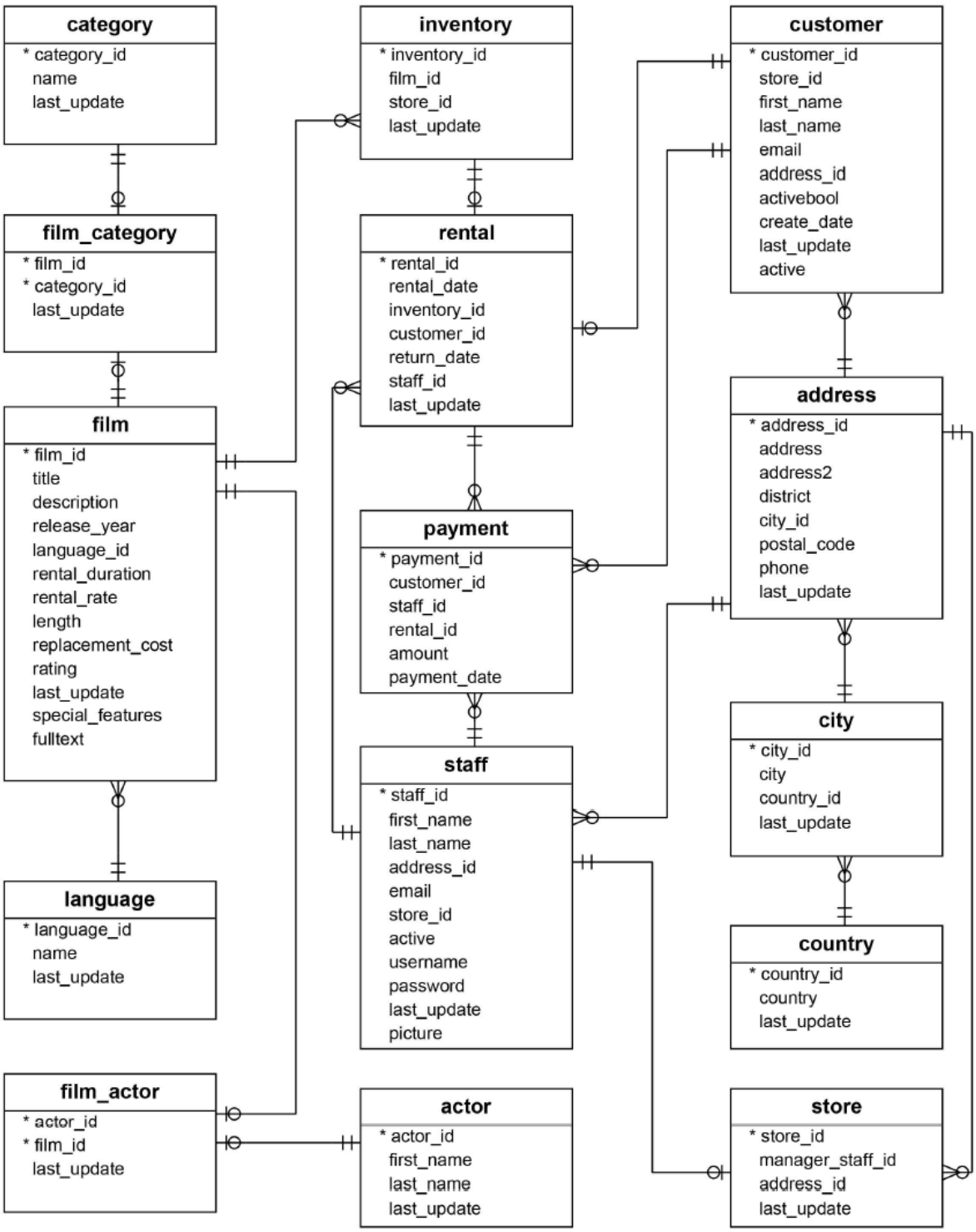

Рисунок 49 – Структура базы данных «DVD RENTAL» в виде ER диаграммы

На рисунке 49 представлена структура базы данных «DVD RENTAL» в виде ER диаграммы состоящая из 15 взаимосвязанных таблиц.

В таблице 13 представлен в качестве примера представлен список из 5 запросов, которые последовательно отправляются в СУБД в разной последовательности. Каждая такая последовательность запросов отправляется в СУБД 100 раз, а результат усреднялся. Всего выполнено 100000 разных последовательностей запросов, для каждой последовательности запросов рассчитано время её выполнения.

Таблица 13 Перечень SQL запросов для тестовой базы данных «DVD RENTAL».

Номер запроса	Исходный код SQL запроса
1	SELECT film.film_id, film.title, inventory.inventory_id FROM film LEFT JOIN inventory ON inventory.film_id = film.film_id ORDER BY film.title;
2	SELECT customer.customer_id, customer.first_name, customer.last_name, payment.amount, payment.payment_date FROM customer INNER JOIN payment ON payment.customer_id = customer.customer_id ORDER BY payment.payment_date;
3	SELECT film.film_id, film.title, inventory.inventory_id FROM inventory RIGHT JOIN film ON film.film_id = inventory.film_id ORDER BY film.title;
4	SELECT last_name, first_name FROM customer WHERE first_name = 'Jamie' AND last_name = 'Rice';
5	SELECT first_name || ' ' || last_name full_name, SUM (amount) amount FROM payment INNER JOIN customer USING (customer_id) GROUP BY full_name ORDER BY amount DESC;

В таблице 14 приведён пример выборки, включающей 10 последовательностей запросов с соответствующими временами выполнения, отсортированных по возрастанию времени обработки. Для наглядности представлены первые 5 последовательностей (с минимальным временем) и последние 5 последовательностей (с максимальным временем).

Таблица 14 – Последовательность запросов и время ответа

п. н.	Последовательность запросов	Время исполнения, с.
1.	4, 3, 10, 5, 13, 6, 12, 7, 11, 9, 1, 14, 15, 0, 8, 2, 16, 17, 19, 18	0,72676
2.	14, 11, 0, 19, 7, 17, 13, 5, 6, 4, 2, 15, 9, 10, 12, 3, 8, 16, 1, 18	0,72991
3.	12, 5, 4, 16, 18, 10, 17, 7, 1, 0, 6, 8, 3, 2, 19, 9, 11, 13, 15, 14	0,74087
4.	2, 9, 17, 11, 3, 18, 6, 8, 0, 1, 4, 14, 5, 16, 15, 7, 12, 10, 13, 19	0,74111
5.	3, 1, 7, 13, 2, 15, 12, 6, 11, 19, 4, 0, 9, 17, 14, 5, 10, 18, 16, 8	0,74566
6.	11, 14, 10, 13, 17, 8, 0, 9, 16, 18, 6, 19, 12, 15, 4, 1, 5, 2, 3, 7	0,84975
7.	6, 10, 2, 18, 13, 15, 14, 12, 0, 17, 8, 5, 3, 1, 9, 7, 11, 19, 16, 4	0,85109
8.	4, 10, 16, 12, 3, 19, 9, 13, 7, 15, 17, 5, 18, 8, 6, 1, 14, 0, 2, 11	0,89897
9.	5, 18, 15, 17, 14, 1, 13, 11, 16, 7, 9, 3, 4, 8, 19, 0, 12, 6, 10, 2	0,92828
10.	5, 8, 13, 3, 9, 19, 4, 16, 17, 18, 11, 1, 12, 14, 6, 15, 7, 10, 0, 2	0,93549

Анализ экспериментальных данных позволяет заключить, что различные последовательности запросов существенно влияют на время их выполнения.

Таким образом, время обработки запросов определяется внутренними параметрами инфраструктуры СУБД и остаётся постоянным для конкретного экземпляра её функционирования. Это утверждение подтверждено экспериментально: в показанных исследованиях применялись три версии PostgreSQL (12.20, 13.16 и 14.12), для каждой из которых были выявлены характерные «медленные» и «быстрые» последовательности запросов.

На основе данного принципа возможно прогнозировать худший и лучший сценарии выполнения запросов, и при переносе сервиса на другую версию СУБД эффект сохраняется.

Анализ последовательностей откликов позволяет количественно оценить степень ИД сервиса, что даёт возможность сравнивать устойчивость различных инфраструктур и прогнозировать риск саморазрушения системы. Предлагается использовать вариабельность времени выполнения как одну из ключевых метрик ИД для оценки деструктивного потенциала инфраструктуры.

4.4. Интеллектуальный анализ журналов событий хранилища данных «GreenPlum» с позиции оценки угроз информационной безопасности инфраструктурного генеза

Одной из ключевых задач анализа журналов событи является оптимизация работы системы GreenPlum. В условиях неполной загрузки ресурсов, когда система простаивает значительную часть времени, выполняется прогнозирование нагрузки для выявления наиболее востребованных таблиц, подлежащих переносу в высокопроизводительные хранилища Hadoop. Это позволяет размещать часто используемые таблицы в альтернативных системах (не обязательно в GreenPlum), высвобождая ресурсы кластера, снижая нагрузку и повышая его экономическую эффективность [57].

На основе предоставленных журналов событий хранилища данных требуется разработать алгоритм обработки информации и прогнозирования критической нагрузки, приводящей к отказам функционирования системы в результате эффекта инфраструктурного деструктивизма. Ключевым компонентом решения выступает выявление, классификация и распределение объектов хранилища по дифференцированным критериям, обеспечивающим эффективное управление ресурсами и предотвращение угрозы ИБ ИГ.

Greenplum — система управления данными, предназначенная для больших проектов из мира Big Data [115]. Система управления базами данных Greenplum сочетает традиционную реляционную модель хранения с горизонтальным масштабированием через кластерные механизмы, аналогичные RAID-массивам, что обеспечивает высокую производительность в распределённых сервис-ориентированных архитектурах.

Полная поддержка реляционной модели гарантирует сохранность целостности и точности данных, делая систему идеальной для обработки структурированных массивов в условиях интенсивных межсервисных взаимодействий, включая финансовые транзакции и журналы событий РИС.

Это позволяет эффективно справляться с эффектами ИД, минимизируя риски его возникновения за счёт оптимизированного распределения ресурсов

На основе предоставленных журналов событий хранилища необходимо разработать алгоритм обработки данных и прогнозирования будущей нагрузки. Важно частью задачи является выявление и распределение объектов хранилища по различным критериям.

В качестве исходных данных предоставлен набор логов, которые содержат запросы к базе данных GreenPlum. Нужно предложить метод быстрой обработки этих данных. Выделению отдельных объектов, к которым чаще всего обращаются пользователи. Выявления самых “тяжелых” и самых “горячих” объектов. Прогнозирование нагрузки на систему в разные временные отрезки.

Особенно важной является задача прогнозирования времени исполнения запроса по предоставленным данным приводящей к отказу системы [57].

Формат хранения данных в журнале событий

В качестве примера приведем фрагмент данных (см. рис. 50)

Rn (bigint)	Loguser (text)	Query (text)
1513	etl_2048	from tbl_142463,join tbl_142465
1361	dev_473	join tbl_33332,join tbl_151403,INTO tbl_385661

```
(format CSV, header, delimiter ',', quote '"', null '', escape '"')
```

Рисунок 50 – Фрагмент хранения данных в журнале событий

На рисунке 4.3 использованы следующие обозначения:

Rn – уникальный номер записи

Loguser – пользователь (dev_* - разработчики, etl_* - загрузчик)

Query – запрос в базу:

- from, join - извлечение данных
- into - запись данных

Пример работы первой части программного средства можно посмотреть на следующих рисунках 51 и 52.

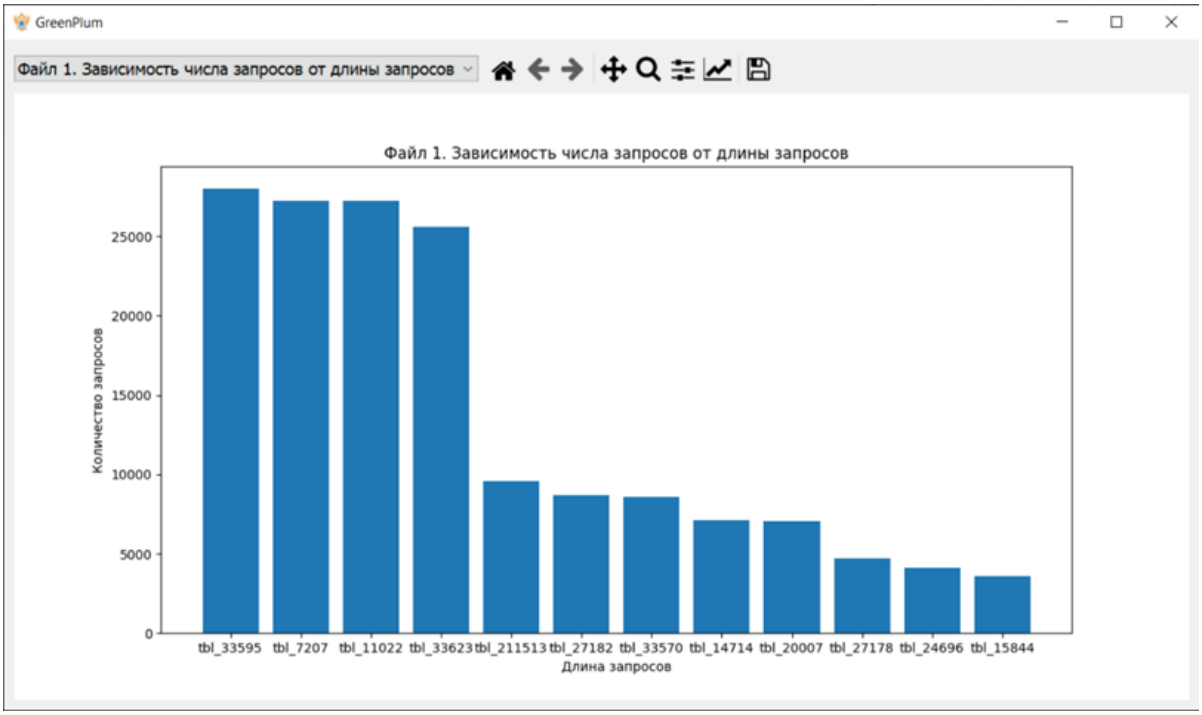

Рисунок 51 – Зависимость числа запросов от длины запросов

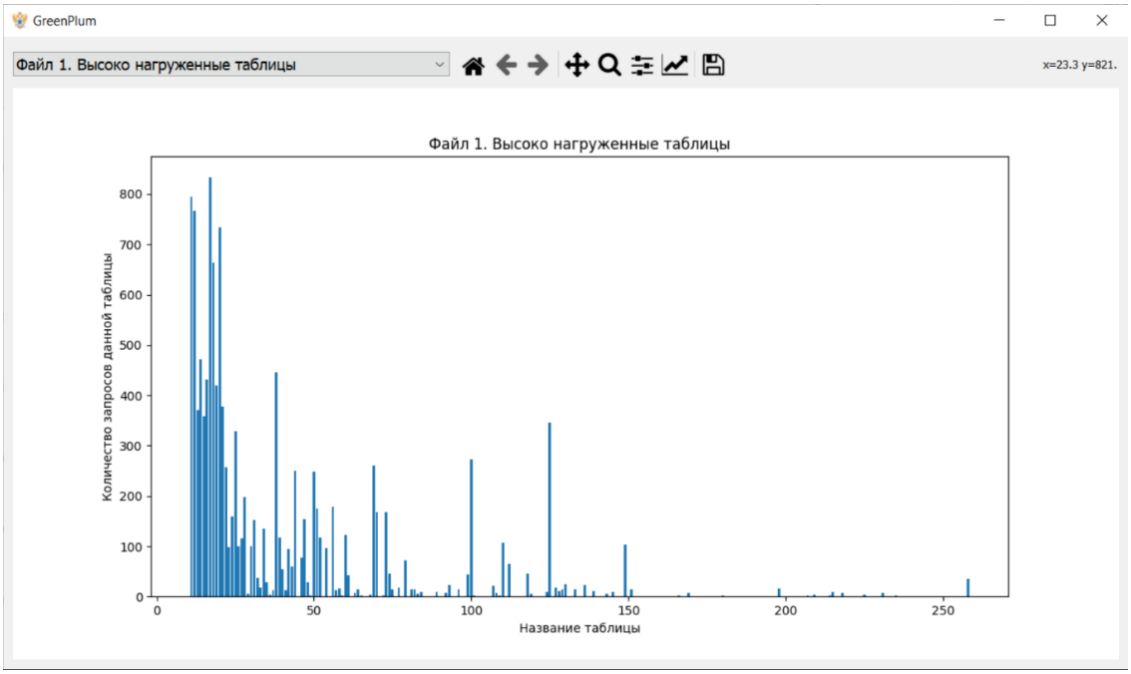

Рисунок 52 – Высоконагруженные таблицы

На рисунках 53 и 54 представлены таблицы с визуализацией в виде столбчатых диаграмм, отражающих интенсивность обращений к самым нагруженным таблицам. Каждый столбец соответствует количеству запросов к конкретной таблице. В ходе анализа данных выявлено четыре таблицы, к которым обращались значительно чаще — среднее число запросов к этим таблицам составляет около 27 000, тогда как для остальных таблиц оно не превышает 10 000.

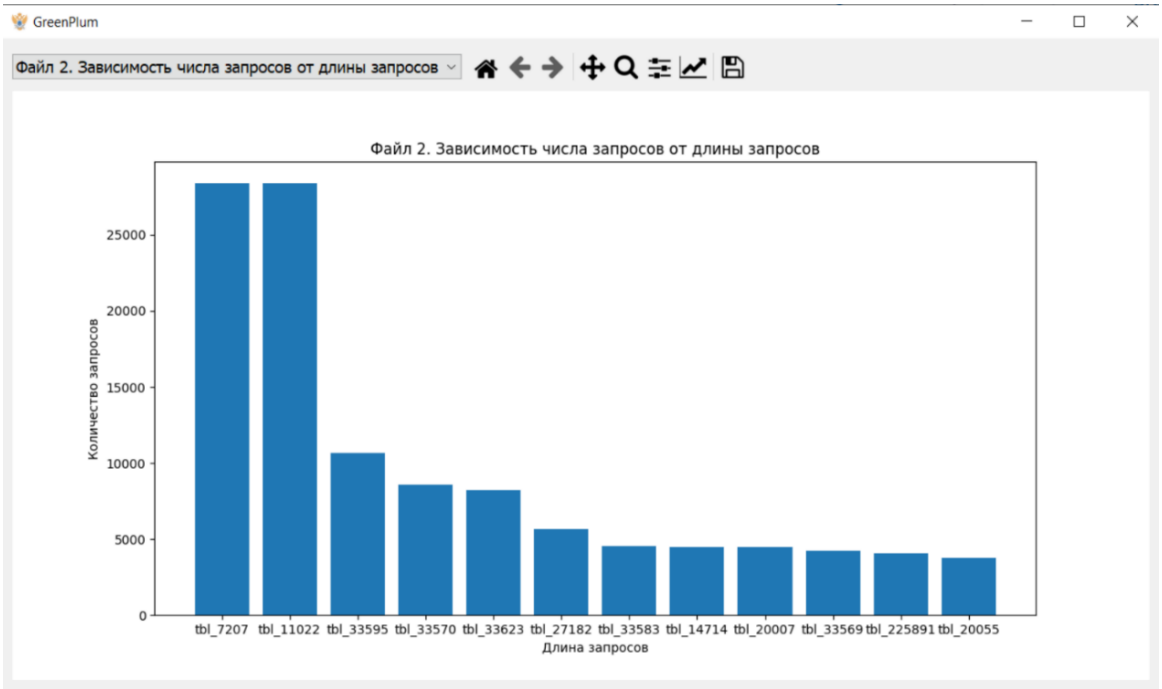

Рисунок 53 – Зависимость числа запросов от длины запросов

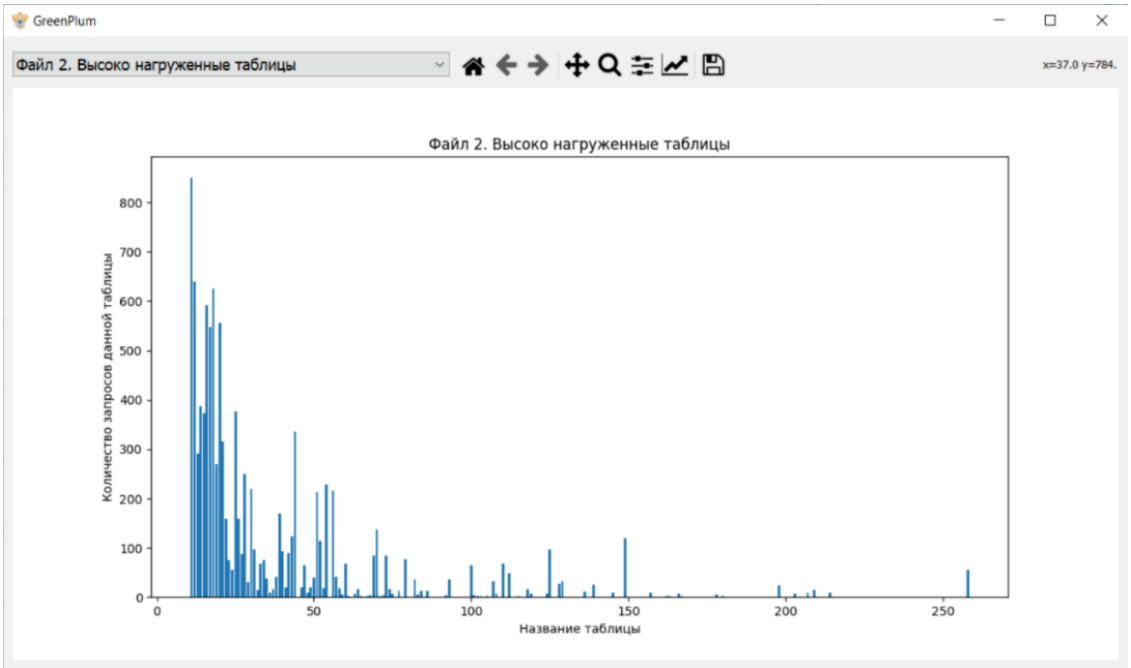

Рисунок 54 – Высоконагруженные таблицы

На этих графиках видно, что зависимость распределения длины запросов от количества запросов подчиняется экспоненциальному закону, это означает, что данное распределение не является нормально-распределенным (Гауссовским). Таким образом можно сделать допущение к данным исследуемым данным можно применить регрессионный анализ.

Далее выполним поиск неиспользуемых таблиц, в которые все записывается и никогда не считывается. Результат показан на рисунке 55.

GreenPlum2

Меню

	table_name	etl_into	etl_join	etl_from	dev_into	dev_join	dev_from	range
1	tbl_27182	475	4718	0	0	0	0	475
2	tbl_29495	468	64	0	0	0	0	468
3	tbl_29497	468	0	0	0	0	0	468
4	tbl_28425	379	0	0	0	0	0	379
5	tbl_27356	379	0	0	0	0	0	379
6	tbl_26783	378	0	0	0	0	0	378
7	tbl_29461	377	0	0	0	0	0	377
8	tbl_29458	373	0	0	0	0	0	373
9	tbl_26784	366	0	0	0	0	0	366
10	tbl_26792	365	0	0	0	0	0	365
11	tbl_28670	365	0	365	0	0	0	365
12	tbl_29481	351	157	0	0	0	0	351
13	tbl_27619	324	0	0	0	0	0	324

Рисунок 55 – Вариант работы второй программы

В данном случае мы отсортировали данные при помощи библиотеки Pandas таким образом, чтобы получились следующие столбцы, изображенные на рисунке 7. Etl_into, etl_join, dev_into, dev_join, dev_from, range (etl_into + dev_into).

Прогнозирование нагрузки на кластер. Для прогнозирования нагрузки на кластер после использования алгоритмов машинного обучения, в частности Байесовский классификатор. Принято решение использование обычной нелинейной регрессионной модели четвертого порядка на основе ARIMA [1].

1) Оценивание параметров модели и вычисление остатков:

$$y_t - \phi_1 \cdot y_{t-1} - \ldots - \phi_p \cdot y_{t-p} = \delta + \varepsilon_t - \theta_1 \cdot \varepsilon_{t-1} - \ldots - \theta_p \cdot \varepsilon_{t-p};$$
$$\varepsilon_t \approx iid(0, \sigma^2) \quad (17)$$

Тогда процесс y_t является *ARIMA*(*p*,*q*,*d*).

Каждая из полученных моделей проверяется на соответствие исходным данным. Из тех моделей, которые адекватны данным, отыскивается наиболее простая модель, то есть модель, которая имеет наименьшее количество параметров [1].

2) Оценивание модели и проверка ее адекватности.

Прогнозирование временного ряда. После поиска ряда моделей, следует выполнить прогнозирование на несколько шагов по времени с оцениванием крайних границ прогнозируемых значений. Благодаря этой модели построена следующее решение, показанное на рисунке 56:

rn	loguser	tbl_nan	duratio	predict_duration	difference
4467	dev_332	from tbl_7	63,108	200	136,892
4512	etl_2048	from tbl_8	31,022	5126,372929	5095,350929
4514	dev_332	from tbl_7	174,179	200	25,821
4522	dev_332	from tbl_2	100987,4	20001,26099	-80986,17801
4530	etl_2048	from tbl_8	146,984	5126,372929	4979,388929
4532	etl_2048	from tbl_8	1491,244	1144,93639	-346,3076098
4543	etl_2048	from tbl_1	339,079	2693,73319	2354,65419
4548	etl_2048	from tbl_8	16,879	1144,93639	1128,05739
4550	etl_2048	from tbl_8	12,398	1144,93639	1132,53839
4552	etl_2048	into tbl_85	3450,567	5326,372929	1875,805929
4554	etl_2048	from tbl_2	808,493	3716,1208	2907,6278
4557	dev_332	from tbl_7	173,476	200	26,524
4561	etl_2048	into tbl_85	8878,601	5326,372929	-3552,228071
4590	etl_2048	from tbl_8	1788,173	1617,775571	-170,3974286
4592	etl_2048	from tbl_8	2279,249	6071,455429	3792,206429

Рисунок 56 – Фрагмент журнала событий для поиска нагруженных таблиц

В результате построена следующая таблица, в которой помимо стандартного лога прописывается два дополнительных поля predict_duration и difference.

Параметр Difference – это разница между значением, которое спрогнозировано и тем, что по факту является. Если система показывает положительный результат, то это говорит о нехватке ресурсов кластера, а если отрицательный, то о нормальной работе системы. Для данного значения difference построены графики на рис. 9 и 10. На рисунке 57 показано, что прогресс доступа к данным показывает о том, что в это время момент простоя, и кластер не нагружен, поскольку присутствует много отрицательных значений. Рисунок 58 показывает график, в котором кластер перегружен и начал давать отказы.

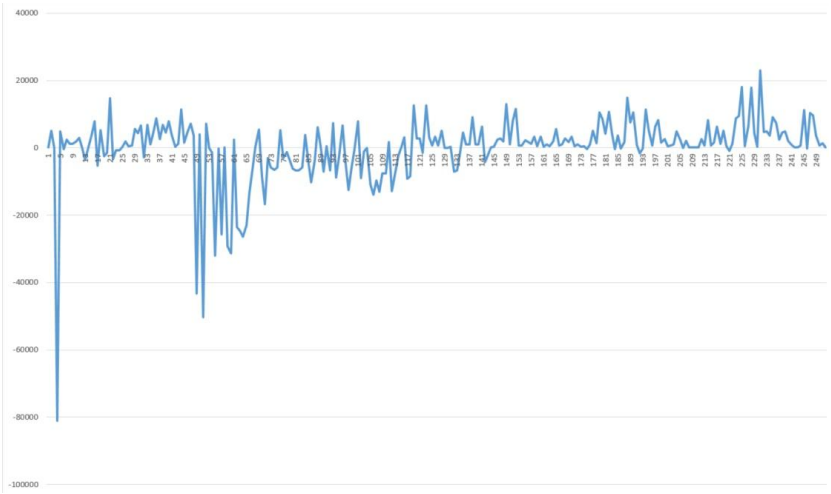

Рисунок 57 – Прогресс доступа к данным

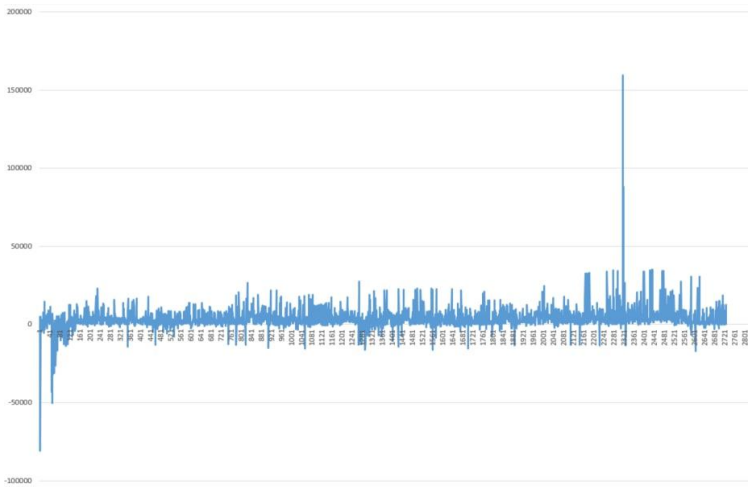

Рисунок 58 – Прогресс доступа к данным

Таким образом используя авторегрессионную модель ARIMA и соответствующие алгоритмы обработки данных из журналов событий системы GreenPlum становиться возможным прогнозировать остаточный ресурс данного кластерного решения и находить нагруженные таблицы. Тем самым повышается эффективность использование системы GreenPlum за счет своевременного прогнозирования и оценки эффектов ИД.

4.5 Исследование взаимодействия сервисов облачной платформы «OpenStack» на основе антропоморфических поведенческих моделей

Для исследования взаимодействия сервисов на основе антропоморфических моделей, разработанных во втором разделе, воспользуемся программным средством разработанным автором в [154, 159].

В качестве данных для анализа использованы данные работы платформы для облачных вычислений OpenStack.

Облачная платформа OpenStack представляет собой комплекс проектов свободного программного обеспечения для создания инфраструктурных облачных сервисов, центров обработки данных, облачных хранилищ, разработки и предоставления приложений.

Облачная платформа OpenStack может использоваться как для публичных, так и частных облачных сервисов.

В данной исследовании используется данные журналов событий системы из открытого набор данных DeepTraLog [203, 227].

В эксперименте использованы открытые данные «DeepTraLog» из лаборатории разработки программного обеспечения университета Фудань (Китай, Шанхай).

Набор данных включает в себя журналы событий трассировки микросервисной распределенной тестовой системы бронирования билетов на поезд (41 микросервис).

Данные «DeepTraLog» использовались для проведения соревнований по обнаружению аномалий в журналах событий для инфраструктур, построенных на сервисах с использованием облачной платформы OpenStack.

В эксперименте использовались данные с 05.08.2021 по 26.12.2021 для 32 сервисов [203]. Из 32 сервисов отобраны 6 наиболее нагруженных сервиса. Проводилась оценка динамики взаимного влияния сервисов на основе антропоморфических моделей поведения.

Фрагмент журнала событий облачной платформы OpenStack представлен на рисунке 59.

StartTime	EndTime	URL	SpanType	Service	SpanId	TraceId	Peer	ParentSpan	Component	IsError
1628884697510	1628884701848	{GET}/api/v1/cancelservice/cancel/{orderId}/{loginId}	Entry	ts-cancel-service	a8ac2bc13e5c423d83743ee2d661482b.42.16288846975100028.0	a8ac2bc13e5c423d83743ee2d661482b.42.16288846975100029	ts-cancel-service	-1	SpringMVC	False
1628884697515	1628884697523	SpringAsync	Local	ts-cancel-service	a8ac2bc13e5c423d83743ee2d661482b.58.16288846975150062.0	a8ac2bc13e5c423d83743ee2d661482b.42.16288846975100029	ts-cancel-service	a8ac2bc13e5c423d83743ee2d661482b.42.16288846975100028.0	SpringAsync	False
1628884697515	1628884697523	/api/v1/inside_pay_service/inside_payment/drawback/4d2a46c7-71cb-4cf1-b5bb-b68406d9da6f/0.00	Exit	ts-cancel-service	a8ac2bc13e5c423d83743ee2d661482b.58.16288846975150062.1	a8ac2bc13e5c423d83743ee2d661482b.42.16288846975100029	ts-inside-payment-service	a8ac2bc13e5c423d83743ee2d661482b.58.16288846975150062.0	SpringRestTemplate	False
1628884697518	1628884697524	{GET}/api/v1/inside_pay_service/inside_payment/drawback/{userId}/{money}	Entry	ts-inside-payment-service	e011366013074feda29701dc14e41305.44.16288846975180094.0	a8ac2bc13e5c423d83743ee2d661482b.42.16288846975100029	ts-inside-payment-service	a8ac2bc13e5c423d83743ee2d661482b.58.16288846975150062.1	SpringMVC	False

Рисунок 59 – Фрагмент журналов событий облачной платформы OpenStack

Разработанное программное обеспечение визуализирует динамику работы процессов как показано на рисунке 60.

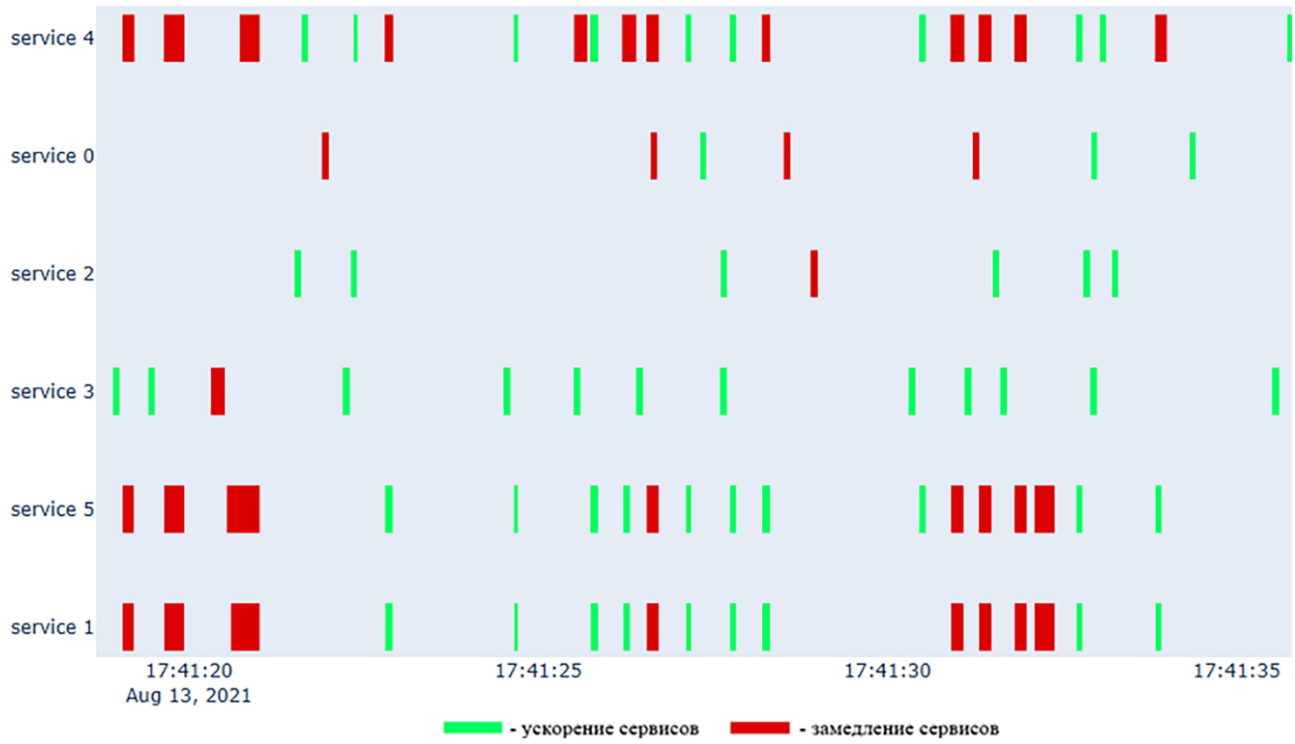

Рисунок 60 – Фрагмент визуализации взаимного влияния процессов для облачной платформы OpenStack

На рисунке 60 красным цветом на временной диаграмме процессов обозначены временные участки, которые выполнялись дольше по отношению к прогнозируемому значению. Зеленым цветом соответственно меньше.

Выполним анализ взаимного влияния сервисов по антропоморфическим типам. Данные расчета взаимного влияния 6 сервисов по 9 антропоморфическим типам за 10 минут 13.08.2021 представлены в таблице 15. Подробное описание взаимного влияние сервисов по антропоморфическим типам взаимодействия представлено разделе 2.

Таблица 15 – Взаимного влияния сервисов за 10 минут 13.08.2021

Типы антропоморфических взаимодействий	Влияние сервиса №1 на сервис №2	Влияние сервиса №1 на сервис №3	Влияние сервиса №1 на сервис №4	Влияние сервиса №1 на сервис №5	Влияние сервиса №1 на сервис №6
Тип 1. Факультативный симбиоз	0,36	1,78	0,25	1,93	2,74
Тип 2. Комменсализм	0,82	14,22	2,00	9,09	1,31
Тип 3. Нейтрализм	0,41	7,11	1,00	7,73	10,97
Тип 4. Облигатный симбиоз	0,46	3,55	0,50	3,86	5,49
Тип 5. Паразитизм	0,31	0,89	0,13	0,97	1,37
Тип 6. Хищничество	0,31	0,44	0,32	0,48	0,69
Тип 7. Аменсализм	0,25	0,25	0,29	1,02	0,34
Тип 8. Конкуренция	1,27	5,68	0,29	15,45	19,16
Тип 9. Аллелопатия	2,54	11,36	0,58	4,55	0,66

В таблице 15 показано процентное отношение длительности каждого процесса, относящееся к определенному типу взаимодействия. Данные из этой удобнее анализировать используя графическое представление в виде столбчатых диаграмм как показано на рисунках 61 – 65.

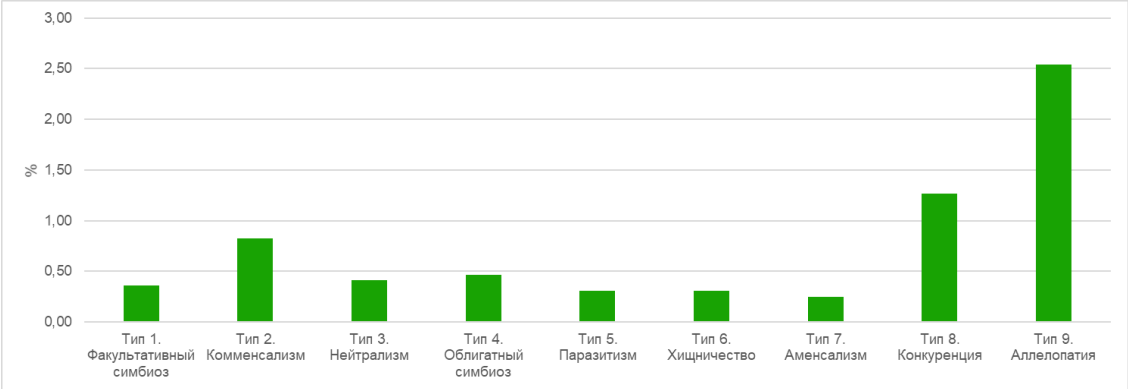

Рисунок 61 – Влияние сервиса №1 на сервис №2

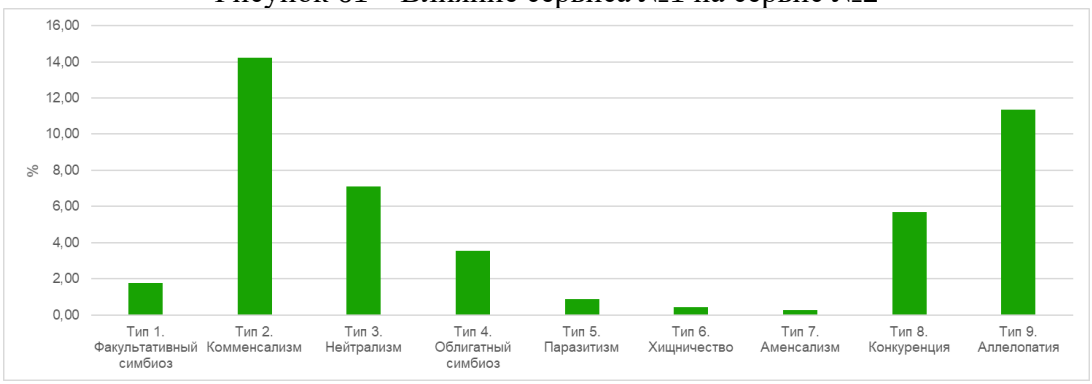

Рисунок 62 – Влияние сервиса №1 на сервис №3

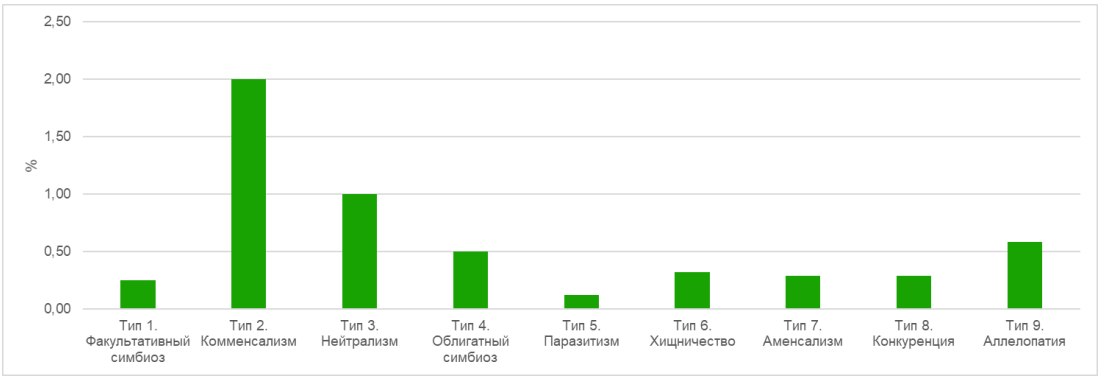

Рисунок 63 – Влияние сервиса №1 на сервис №4

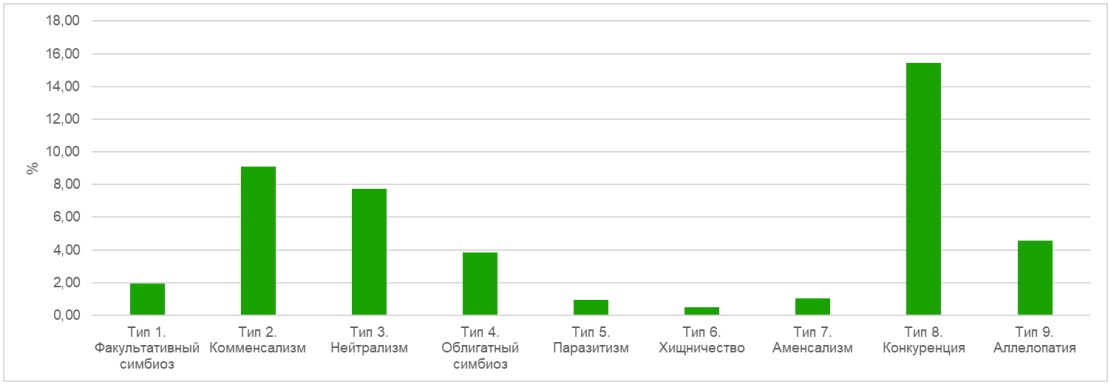

Рисунок 64 – Влияние сервиса №1 на сервис №5

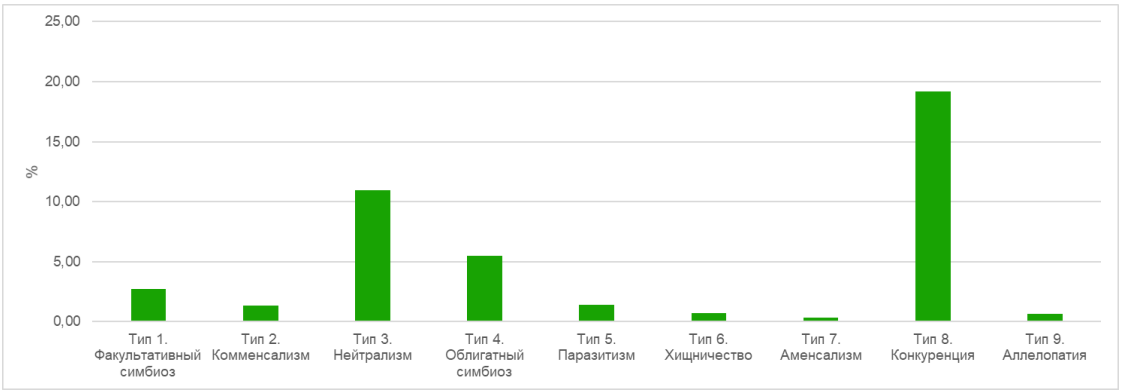

Рисунок 65 – Влияние сервиса №1 на сервис №6

Также можно построить общую диаграмму, содержащую все данные из рисунков 61 – 65, как показано на рисунке 66

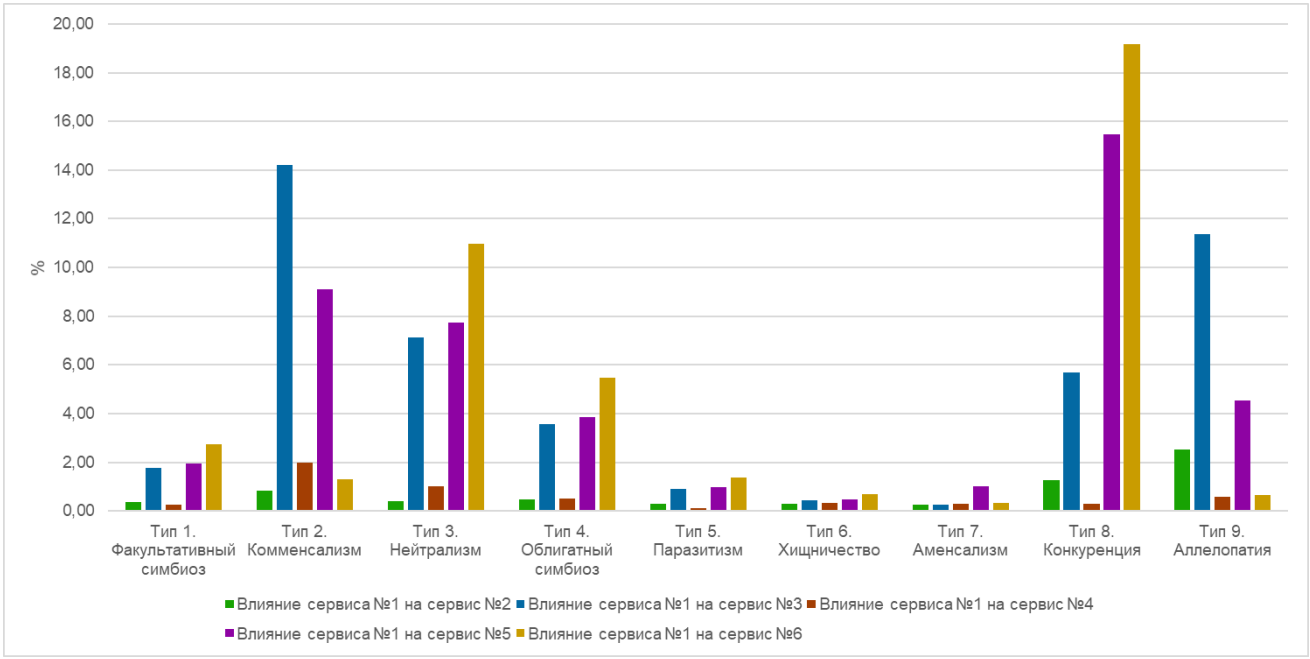

Рисунок 66 – Общее взаимное влияние 6 сервисов за 10 минут 13.08.2021

Таким образом, проанализировав значения взаимодействия процессов, представленных на рисунке 66 можно сделать следующие выводы.

Процесс сервиса №1 оказывает негативное влияние по типу 6 Конкуренция по отношению к процессам сервисов №5 и №6.

Это означает что у сервиса №1 имеются узкие места, связанные с деятельностью сервисов №5 и №6.

Предполагается, что применение механизмов кэширования позволит устранить данную проблему. Также стоит отметить, что процесс сервиса №1 способствует эффективному функционированию сервисов №3 и №5, что свидетельствует об оптимальной архитектуре РИС в данной части.

При анализе межсервисных взаимодействий РИС по антропоморфическим типам особый интерес представляет изучение сценариев воздействия ВПО.

Особо значимой является оценка динамики рисков проявления эффектов ИД. Описание соответствующих случаев представлено в последующих подразделах.

4.6 Исследование эпидемиологической модели распространения вирусов с учетом антропоморфических эффектов взаимодействия вредоносного программного обеспечения

В эпидемиологической SEIR-модели учитывается возможность того, что деструктивное воздействие инфраструктурного генеза может иметь некий "латентный период", во время которого оно не наносит какого-либо вреда РИС [209]. Обычно деструктивное воздействие вредоносного программного обеспечения поражает уязвимую инфраструктуру (S) до входа в свою латентную стадию, в течение латентного периода (Ex, Exposed) элемент инфраструктуры считается заражённым, но не распространяет деструктивные воздействия, через некоторое время он становиться способным к заражению других (I) и далее становиться "вылеченным" (R) [209]. Предложенная модель реализована на основе многоагентной системы моделирования NetLogo [223] и позволяет оценивать динамику рисков ДВ ИГ с учетом

антропоморфической модели взаимодействия вредоносного программного обеспечения [64, 155].

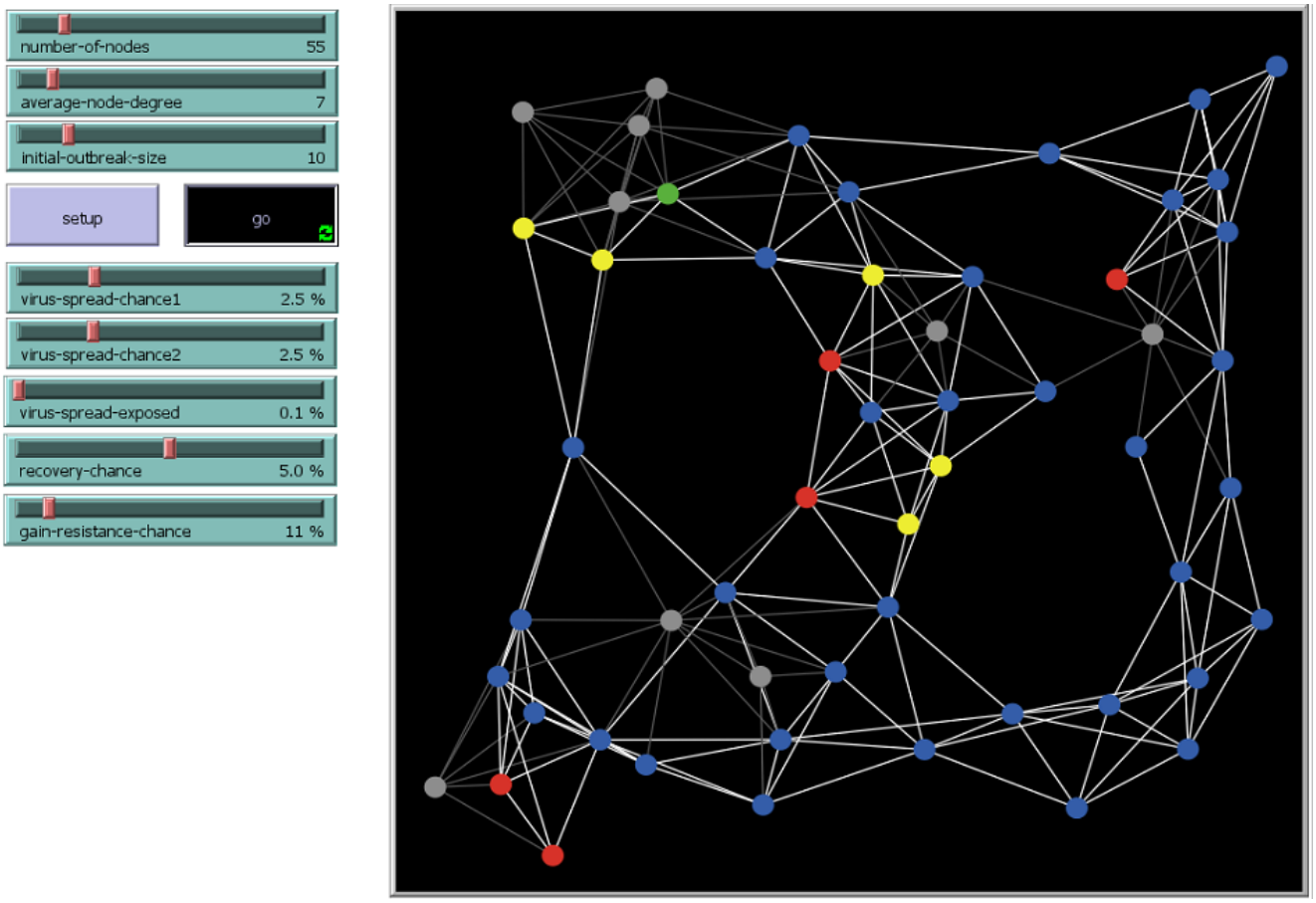

Рисунок 67 – Программное обеспечение для оценки динамики рисков инфраструктурного генеза деструктивных воздействий вредоносного программного обеспечения

Данное программное обеспечение реализовано в [64, 155] и описано в [147]. На рисунке 67 представлено основное окно программного средства динамики рисков инфраструктурного генеза деструктивных воздействий.

Результат работы отображается в белом окне «System Status», как показано на рисунке 68. По оси абсцисс отображается время выполнения модуля, по оси ординат отображается изменение процентного отношения состояний узлов (susceptible, infected1, infected2, resistant, exposed).

Отображены графики состояния ИТ-Инфраструктуры РИС при деструктивных воздействиях вредоносного программного обеспечения. Благодаря данному программному средству стало возможным оценить риски как на этапе проектирования, так и на этапе эксплуатации РИС.

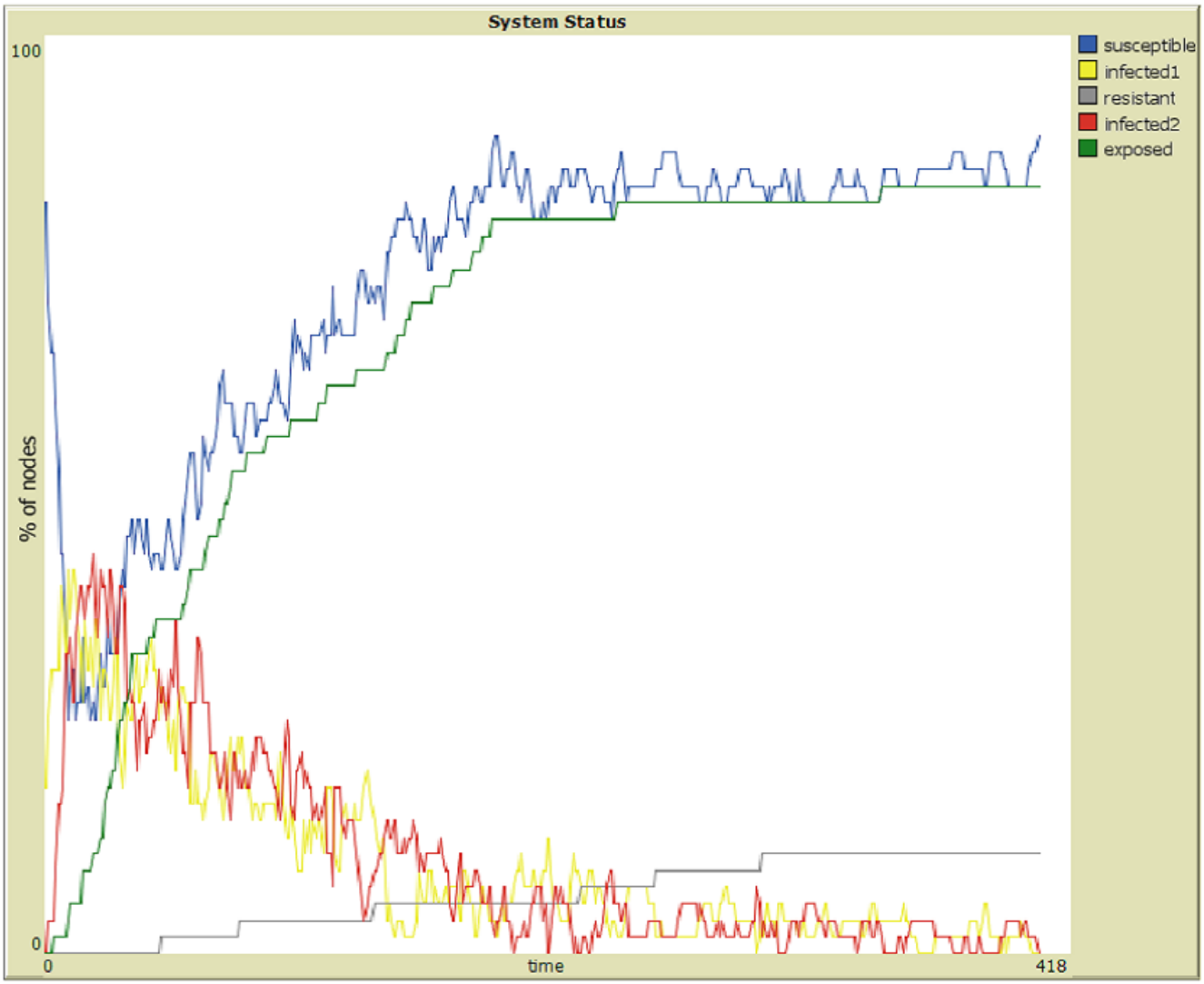

Рисунок 68 – Графики состояния информационной инфраструктуры при деструктивных воздействиях вредоносного программного обеспечения

Алгоритм работы программного обеспечения представлен на рисунке 69. Сначала осуществляется ввод параметров архитектуры сети. Для работы модуля необходимо задать значения параметрам:

1) initial-outbreak-size: начальный размер зараженной части сети;

2) number-of-nodes: общее количество узлов в сети;

3) average-node-degree: среднее количество связей у каждого узла в сети;

4) virus-spread-chance1, virus-spread-chance2, virus-spread-exposed: вероятности распространения вирусов разных типов между узлами;

5) recovery-chance: вероятность выздоровления зараженных узлов;

6) gain-resistance-chance: вероятность развития устойчивости к деструктивному воздействию после выздоровления.

Затем система выполняет действия модуля setup-nodes.

Модуль выполняет функцию инициализации узлов в модели.

Устанавливается форма по умолчанию для всех узлов в модели в виде круга (circle). Это определяет, как будет выглядеть каждый узел;

Создается заданное количество узлов (number-of-nodes). Каждый узел создается в соответствии с блоком кода.

Для каждого создаваемого узла выполняются следующие шаги:

1) задается случайное местоположение каждого узла, при этом координаты выбираются случайным образом в пределах 95% от максимальных координат. Это необходимо для визуальных целей, чтобы узлы не находились слишком близко к краям экрана;

2) устанавливается начальное состояние узла как чувствительного к деструктивному воздействию (синий цвет в данной модели).

Таким образом, в результате выполнения данного модуля создаются узлы с случайными координатами, установленной формой и начальным состоянием, делая их чувствительными к деструктивному воздействию вредоносного программного обеспечения.

Далее вводные данные передаются в модуль setup-spatially-clustered-network.

Данный модуль отвечает за создание связей между узлами сети, чтобы моделировать пространственно-кластерную структуру сети.

Определяется желаемое количество связей (num-links) в сети на основе средней степени узла (average-node-degree) и общего числа узлов в сети (number-of-nodes).

Запускается цикл while, который выполняется, пока количество созданных связей (count links) меньше желаемого количества связей (num-links). Внутри цикла, для каждого прохода, выбирается случайный узел среди всех узлов.

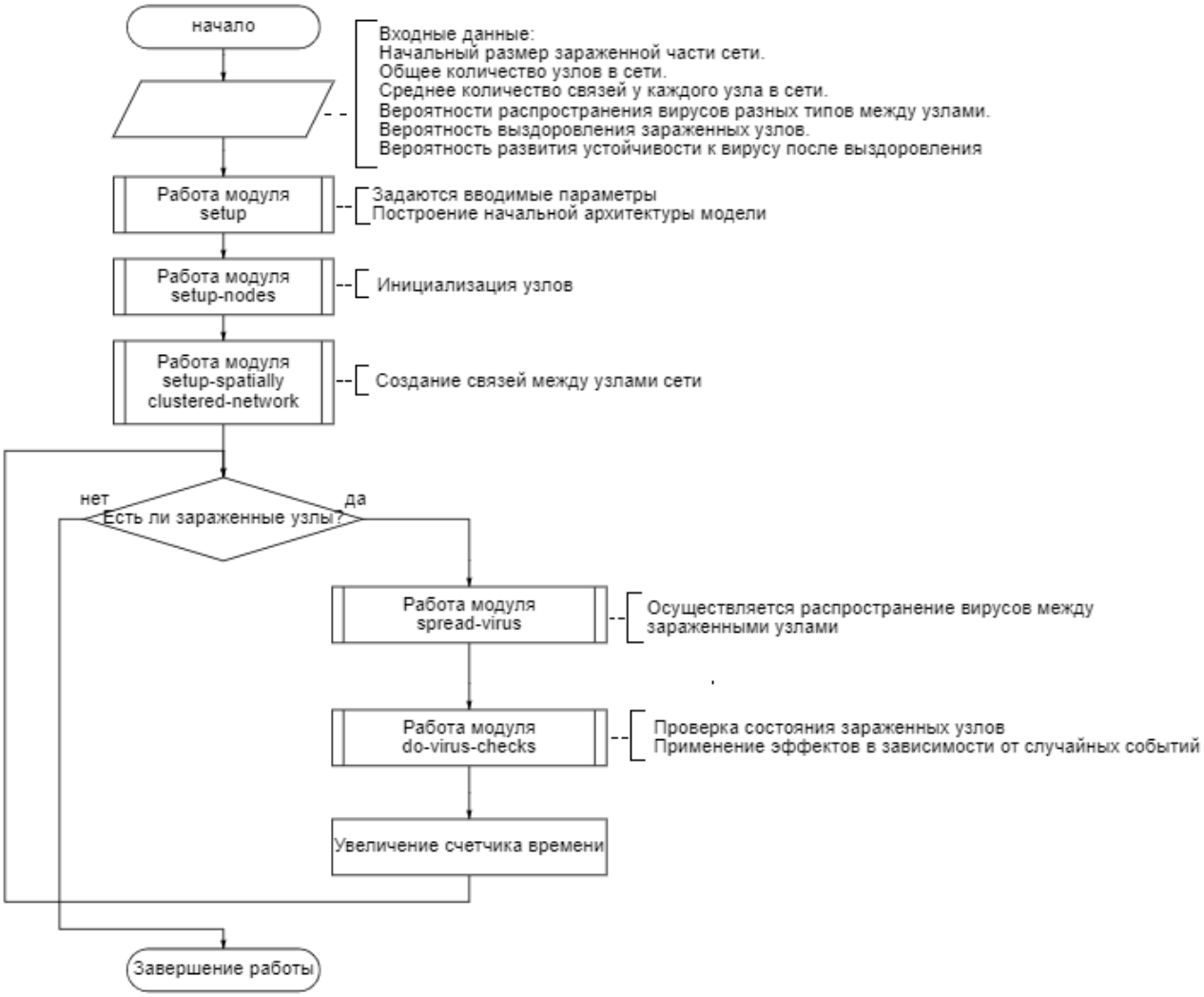

Рисунок 69 – Алгоритм работы программного средства

Для выбранного узла, согласно алгоритму работы программного средства выполняются следующие шаги:

1) выбирается соседний узел, который еще не соединен с текущим узлом. min-one-of используется для выбора ближайшего соседа, a distance myself вычисляет расстояние между текущим узлом и потенциальным соседом;

2) если найден сосед (choice не равен nobody), создается связь между текущим узлом и выбранным соседом с помощью create-link-with;

3) дополнительный код, который выполняет следующее десятикратное действие;

4) используется функция layout-spring, которая придает сети более аккуратный вид. Это осуществляется путем применения алгоритма пружинной раскладки (spring layout), который рассчитывает координаты узлов в сети так, чтобы связи

между узлами подобны пружинам. Этот шаг улучшает визуальное представление структуры сети.

Таким образом, эта процедура создает пространственно-кластерную сеть, соединяя узлы соседними связями и улучшая визуальное представление сети.

После того, как узлы и связи сформированы, программа начинает свою основную часть работы. Запускается цикл, который проверяет на наличие зараженных узлов. Цикл работает до тех пор, пока не останется ни одного зараженного узла. Открывает начало работы цикла модуль spread-virus. Здесь осуществляется распространение вирусов между зараженными (или латентными) узлами и их соседями в сети. Выбираются все узлы, которые являются зараженными первым типом вируса (infected1?), зараженными вторым типом вируса (infected2?) или находятся в латентном состоянии (exposed?). Затем для каждого выбранного узла выполняется следующий блок кода. Он выбирает соседей текущего узла, которые не являются сопротивляемыми деструктивному воздействию (not resistant?) и не находятся в латентном состоянии (not exposed?). Затем по условию выбирается каким вирусом будет заражен узел, либо же узел переходит в латентное состояние. Этот модуль моделирует случайное взаимодействие между зараженными узлами и их соседями, где вероятность заражения зависит от типа вируса и уровня распространения (virus-spread-chance1, virus-spread-chance2, virus-spread-exposed).

Далее выполняется следующий модуль do-virus-checks.

Модуль отвечает за проверку состояния зараженных узлов и применение эффектов в зависимости от случайных событий. Он моделирует возможность выздоровления зараженных узлов с определенной вероятностью и их последующее приобретение или потерю сопротивляемости к деструктивному воздействию.

Затем идет обновление счетчика на 1 тик. Проверяется условие на наличие зараженных узлов. Если таковых не имеется – программа завершает свою работу.

План проведения экспериментального исследования.

В каждом рамках каждого эксперимента (ситуации) задается:

количество узлов = 10, 20, 40, 60, 80, 100, 120, 140.

Выполняется 5 генераций для каждого количества узлов.

Эксперимент 1. N – количество деструктивных воздействий = 1;

Эксперимент 2. N – количество деструктивных воздействий = 2;

Эксперимент 3. N – количество деструктивных воздействий = 3;

Эксперимент 4. N – количество деструктивных воздействий = 4;

Эксперимент 5. N – количество деструктивных воздействий = 5;

Эксперимент 6. N – количество деструктивных воздействий = 10;

Эксперимент 7. N – количество деструктивных воздействий = 20.

Точка бифуркации — критическое состояние системы, при котором система становится неустойчивой относительно флуктуаций и возникает неопределённость: станет ли состояние системы хаотическим или она перейдёт на новый, более дифференцированный и высокий уровень упорядоченности.

В каждой генерации находится точка бифуркации архитектуры, что свидетельствует о том, что архитектура справилась с атаками.

Затем в каждом эксперименте высчитывается среднее значение точки бифуркации при разных количествах узлов. Полученные результаты выводятся в итоговую таблицу.

Результаты экспериментального исследования разработанной методики, получены наихудшие, средние значения, а также то, насколько затраты по плану отличаются в процентах от затрат по оптимальному плану (последний столбец) (см. таблицы 16–22 и рисунок 70).

Таблица 16 – Эксперимент 1. N – количество деструктивных воздействий = 1

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	78,9	78,9	89,5	67,7	66,9	88,6	72,6
Генерация 2	88,6	66,5	90,2	63,2	59,9	68,4	64,7
Генерация 3	50,1	68,4	55,1	97	64	96	93,3
Генерация 4	77,7	53,9	70,7	92,8	78,2	101	80,1
Генерация 5	55,8	67,7	57,1	53,7	72,9	82	83,9

Аналогично примеру, описанному выше ищем, точку бифуркации для остальных экспериментов.

Таблица 17 – Эксперимент 2. N – количество деструктивных воздействий = 2

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	62.8	45.8	47	83.1	67.3	72.9	78
Генерация 2	64.1	57.4	70	72	71	76	75.3
Генерация 3	63.5	71.5	62.6	59.6	58.8	84.1	80.3
Генерация 4	68.5	76.5	61.6	60.4	56	71	72
Генерация 5	43.5	64.7	50.7	65.4	64.8	72.3	70.1

Таблица 18 – Эксперимент 3. N – количество деструктивных воздействий = 3

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	72,2	45,3	53,2	54,4	50,4	50	68,5
Генерация 2	54,3	80,3	73,6	61,8	48	56	59,1
Генерация 3	64,2	57	70,1	60	64,1	79,4	54
Генерация 4	54,8	59,5	74,7	61,1	55	44,8	45,5
Генерация 5	54,9	82,7	54,4	53,6	70	50,4	47,6

Таблица 19 – Эксперимент 4. N – количество деструктивных воздействий = 4

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	48.2	59.4	55.2	43.2	71	56	41.1
Генерация 2	37.3	61.7	46.9	60.7	53.6	54.2	67.3
Генерация 3	35.4	54.3	54	53.2	52.3	47	59.8
Генерация 4	86.9	37.3	48.6	65.3	53	50.7	75
Генерация 5	70	97.3	51.4	43.2	57	68.2	53.2

Таблица 20 – Эксперимент 5. N – количество деструктивных воздействий = 5

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	112.1	44.7	48	59.8	46.7	57.4	63
Генерация 2	52.7	52.2	49	70	44.7	62.6	71
Генерация 3	59.3	60	73	44	60.7	71	50.7
Генерация 4	102	49.9	45.5	62	63.5	63	62.6
Генерация 5	62.8	48.7	63.5	47.6	44.8	56	77

Таблица 21 – Эксперимент 6. N – количество деструктивных воздействий = 10

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	48.7	74.5	36.8	53.6	46.9	35.8	45.8
Генерация 2	49.1	35.8	56	38.7	63.5	48.4	55.1
Генерация 3	65.3	44.2	30.2	51.4	55.1	55.1	49.5
Генерация 4	102.1	104.2	47.2	64.4	49.9	44.7	44.8
Генерация 5	33.2	46.9	49.9	57.9	55.9	51.4	54

Таблица 22 – Эксперимент 7. N – количество деструктивных воздействий = 20

№/Кол-во узлов	20	40	60	80	100	120	140
Генерация 1	31.2	47.7	46.3	36.2	36.4	29.8	44.7
Генерация 2	47.6	54.6	40.2	39.2	33.6	30.8	31.8
Генерация 3	50.1	26.1	35	65.4	39.5	44.8	41.7
Генерация 4	88	49.2	51.4	43.9	29.9	41.1	36.2
Генерация 5	64.7	60	41.1	37.3	46.7	39.2	44.8

Выбор NetLogo обоснован его удобством для многоагентного моделирования. Эпидемиологическая SEIR-модель интегрирована с целью анализа распространения вредоносного программного обеспечения в контексте информационно-технологических инфраструктур. Методика работы с программой обеспечивает адаптивность и итеративное улучшение модели для широкого спектра сценариев.

Исследовав данные закономерности, представленные на рисунке 70. Можно сделать следующий вывод.

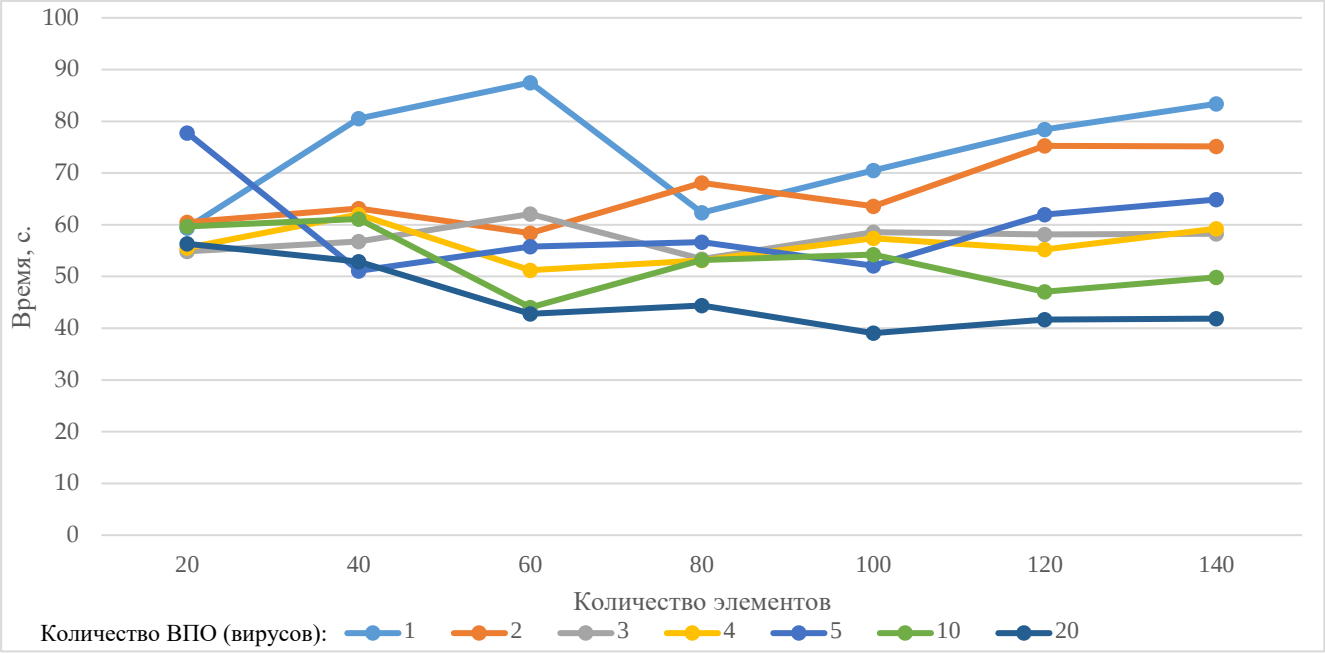

Рисунок 70 – Усреднённые показатели время реакции и восстановления системы на деструктивные воздействия деструктивных воздействий (таблицы 16–22)

При одном деструктивном воздействии на систему точка бифуркации имеет координату 68,38 отсчета.

При появлении 2, 3, 4 и 5 одновременных деструктивных воздействиях форма графика становится иной и на этих показаниях уже есть две явных точки бифуркации первая в районе 60 отчетов и вторая в районе 75 отсчетов.

Далее эти графики начинаю расти вверх. Это означает, что с увеличением количества элементов система становится более устойчивой и менее восприимчивой к деструктивным воздействиям вредоносного программного обеспечения. То есть при данных показаниях в среднем время возникновения точки бифуркации

становится больше, но при этом показания по отдельным экспериментам более вариативны.

При появлении 10 и 20 одновременных деструктивных воздействиях получается, что система уже имеет точку бифуркации гораздо ниже, чем при 2-5 деструктивных воздействиях. То есть получается, что при 10 и более одновременных деструктивных воздействиях система гораздо более защищена от киберугроз вредоносного программного обеспечения и становится более устойчивой поскольку система быстрее восстанавливается.

Таким образом данное программное средство [64, 155], экспериментальным путем показало, что с увеличением числа одновременных деструктивных воздействий заметны эффекты взаимной компенсации деструктивных воздействий. То есть при 10 и более одновременных деструктивных воздействиях система более устойчива за счет эффекта компенсации самих же этих деструктивных воздействий. Однако количество пораженных узлов при этом также возрастает.

Разработанное программное средство показало [64, 155], что при превышении пяти одновременных деструктивных воздействий дальнейшее наращивание производительности средств защиты РИС становится нецелесообразным.

При уровне пяти и более одновременных воздействий наблюдаются эффекты взаимной компенсации деструктивных факторов. Независимо от архитектуры системы она самостоятельно справляется с большим количеством вредоносных воздействий, что позволяет при расчёте систем защиты ограничиваться пятью одновременных атак.

4.7 Прогнозирование угроз инфраструктурного генеза и оценка эффектов инфраструктурного деструктивизма

4.7.1 Исследование распределенной системы распознавания лиц «Персона ID»

В качестве исследуемой системы на предмет наличия эффектов ИД исследуется распределенная интеллектуальная система распознавания лиц «Персона ID»

[135, 158]. Данная система является совместной разработкой двух кафедр КБ-2 «Информационно-аналитические системы кибербезопасности» и КБ-3 «Разработка программных решений и системное программирование» института кибербезопасности и цифровых технологий РТУ МИРЭА. В 2022 году данная система успешно внедрена в качестве системы для регистрации и приветствия участников всероссийской научно-практической конференции с международным участием «Россия в Десятилетии наук об океане».

Система распознавания лиц основывается на библиотеках OpenCV, Dlib, DeepFace, а также на фреймворке MediaPipe. Аналитическим ядром РИС является система видео аналитики, для реализации которой используется язык программирования Python с библиотеками обработки изображений. Задачи, связанные с распознаванием лиц, включают в себя следующее:

1) обнаружение лица — определение местоположения лица на изображении с выделением ключевых точек (глаза, нос, рот и др.), результатом которого служит bounding box;

2) отслеживание лица — анализ динамики перемещения лица в видеопотоке;

3) верификация лица — сравнение двух изображений для установления принадлежности одному человеку;

4) идентификация лица — сопоставление входного изображения с базой данных зарегистрированных лиц.

Программное обеспечение системы «Персона ID» разработано на основе сервисной архитектуры и состоит из следующих сервисов. Полные исходные коды доступные в свободном доступе [62, 63].

Для запуска системы необходимо последовательно запустить каждый из сервисов в следующем порядке: «app.py», «capture_streamer.py», «process.py», «cleanerDB.py», «bot.py». Для увеличения производительности при наличии необходимых аппаратных ресурсов возможен запуск нескольких сервисов «process.py». Описание и функциональное назначение и принцип работы каждого из взаимодействующих сервисов опишем с упором на поведенческую активность в виде таблицы 23.

Таблица 23 – Описание поведенческой активности

Наименование сервиса	Поведенческая активность сервиса
«app.py»	Реализует API интерфейс отображения информации на Интернет-портале.
«bot.py»	Реализует функционал добавления фото пользователей и управления системой.
«capture_streamer.py»	Реализует захват изображений лиц и их обрезку.
«cleanerDB.py»	Реализует функционал проверки ошибок и очистки устаревших изображений.
«playsound.py»	Реализует функционал проигрывания звуковых сопровождений для найденных и распознанных в текущий момент изображений лиц.
«process.py»	Реализует непосредственно процесс распознавания лиц.
«video_enhance.py»	Реализует функционал улучшения изображений по цвета передаче, балансу белого, яркости и контрастности. Реализован механизм приближения к лицу за счет цифрового увеличения изображений.
«zdata.py»	Реализует функционал получения сжатых портретов изображений (эмбедингов) для их загрузки во внутреннюю базу данных системы. Реализован механизм сравнения эмбедингов.

Особенность работы системы распознавания лиц [135] является то, что сервис «process.py» обрабатывает данные с постоянной производительностью, условно до 5 лиц в секунду. Если в кадре присутствуют два или три человека, то такой производительности становится недостаточно. Требуется запускать одновременно несколько сервисов «process.py». Рассмотрим три различных сценария работы системы «Персона ID». Более подробное описание сервисов дано в [135].

Сценарий 1. Обработка данных в системе происходит с помощью одного сервиса «process.py». Недостаточная производительность системы.

Сценарий 2. Обработка данных в системе происходит с помощью трех сервисов «process.py». Производительность обработки данных достаточно. Сервисы «process.py» не мешают друг другу.

Сценарий 3. Обработка данных в системе происходит с помощью семи сервисов «process.py». Производительность обработки данных достаточно. Однако сервисы «process.py» мешают друг другу. В целом система работает не стабильно, что выражается зависанием и долгим откликом без каких-либо видимых для это го причин.

Таким образом для сценария 3 возможно появления эффектов инфраструктурного деструктивизма. Поскольку сервисы «process.py» мешают друг другу работать эффективно. В итоге система работает не стабильно. Этот эффект неоднократно наблюдался автором при испытаниях данной системы. Отметим, что и других системах проявляется данный эффект, связанный с конфликтами обработчиков данных. Поскольку данные не всегда заметен сразу. Поскольку в обработке данных часто бывают пиковые нагрузки из-за непредсказуемых факторов. Например, для системы «Персона ID» это может быть вызвано появлением в кадре более 10 человек. Таким образом обнаружение и прогнозирование эффектов инфраструктурного деструктивизма является необходимой задачей обеспечивающую защиту данной системы от отказов в обслуживании. Данный подход позволяющая защитить имеющиеся системы от угрозы реализации техники T1499 «Точечный отказ в обслуживании» из матрицы MITRE ATT&CK [216].

Для прогнозирования возникновения угрозы ИБ ИГ использовано разработанное программное обеспечение [152, 154, 158]. Для всех трех сценариев работы системы с помощью разработанного ПО построим временные диаграммы процессов для одной и тоже видео записи общей длительностью 120 с., но с разной конфигурацией.

На рисунках 71, 72 и 73 красным цветом на временной диаграмме процессов обозначены временные участки, которые выполнялись дольше по отношению к прогнозируемому значению. Зеленым цветом обозначены соответственно меньше. Таким образом наглядно видно, как изменяется длительность время работы процесса «process.py» в зависимости от конфигурации системы.

Рисунок 71 – График процессов системы распознавания лиц для сценария 1

Рисунок 72 – График процессов системы распознавания лиц для сценария 2

Рисунок 73 – График процессов системы распознавания лиц для сценария 3

Далее с помощью разработанного ПО для каждого сценария и его процессов проведем расчёт взаимодействия процессов по антропоморфическим типам, как показано в разделах 2 и 3. В таблице 24 приведены данные взаимодействия процессов по антропоморфическим типам, где указаны величины в процентах от длительности процесса.

Таблица 24 – Данные взаимодействия процессов системы распознавания лиц по антропоморфическим типам

Наименование сервиса / антропоморфический тип поведения	Тип 1. Факультативный симбиоз	Тип 2. Комменсализм	Тип 3. Нейтрализм	Тип 4. Облигатный симбиоз	Тип 5. Паразитизм	Тип 6. Хищничество	Тип 7. Аменсализм	Тип 8. Конкуренция	Тип 9. Аллелопатия
Сценарий 1									
capture_streamer	3,21	1,28	1,03	0,00	0,05	0,31	0,15	5,13	1,55
Processing 1	8,97	2,40	2,83	0,57	0,76	0,21	0,20	8,97	0,88
Сценарий 2									
capture_streamer	6,73	0,86	0,44	0,29	0,36	0,47	0,12	1,19	0,03
Processing 1	12,82	3,04	0,14	0,58	0,15	0,22	3,07	0,10	0,24
Processing 2	12,82	1,15	1,64	0,12	0,35	0,02	3,68	0,05	0,01
Processing 3	1,60	0,52	0,23	0,06	0,07	0,14	0,00	0,80	0,08
Сценарий 3									
capture_streamer	3,59	1,02	0,09	0,14	0,10	0,23	0,17	2,56	0,79
Processing 1	2,82	0,52	0,93	0,14	0,17	0,14	0,05	13,25	0,62
Processing 2	4,62	1,07	1,73	0,19	0,15	0,28	1,32	13,25	0,00
Processing 3	4,65	1,18	1,20	0,22	0,39	0,18	0,72	4,10	0,17
Processing 4	3,48	0,31	0,72	0,30	0,26	0,16	0,76	15,64	0,04
Processing 5	3,59	1,28	0,32	0,01	0,05	0,33	0,39	4,17	0,04
Processing 6	5,31	0,03	2,11	0,18	0,13	0,39	1,08	15,64	0,70
Processing 7	2,35	0,68	0,23	0,02	0,08	0,09	0,55	1,28	0,60

Визуализируем данные их таблицы 24 в виде столбчатых диаграмм взаимодействия процессов как показано на рисунках 74, 75 и 76.

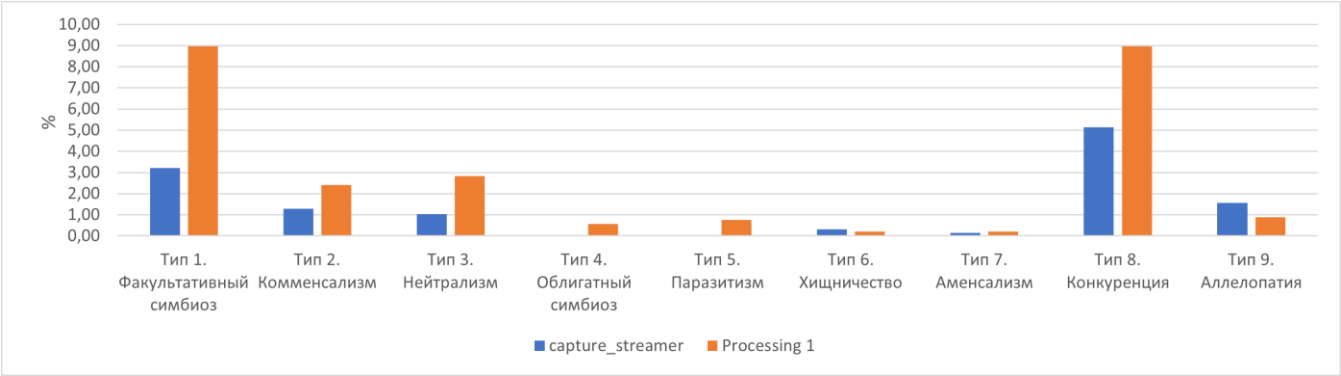

Рисунок 74 – Взаимное влияние сервисов системы распознавания лиц для сценария 1.

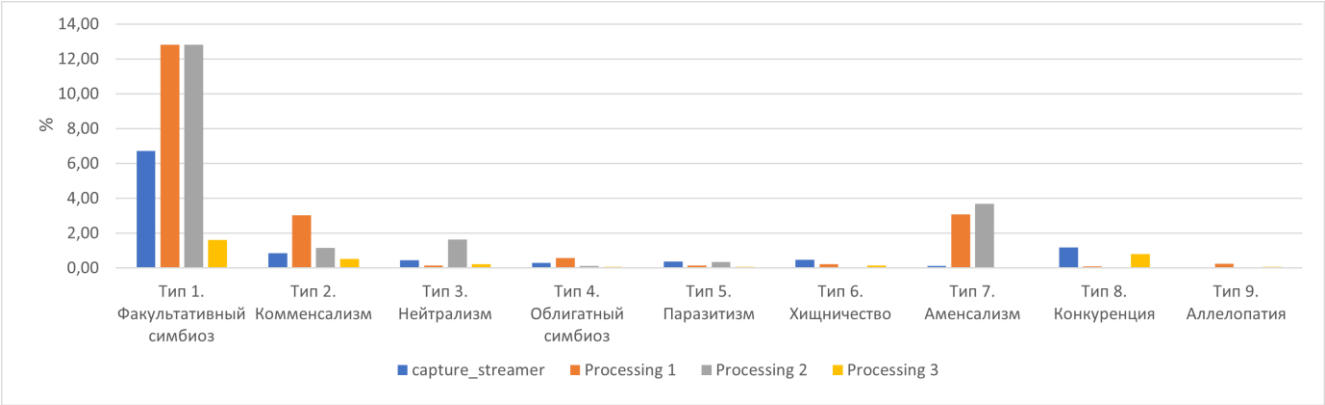

Рисунок 75 – Взаимное влияние сервисов системы распознавания лиц для сценария 2.

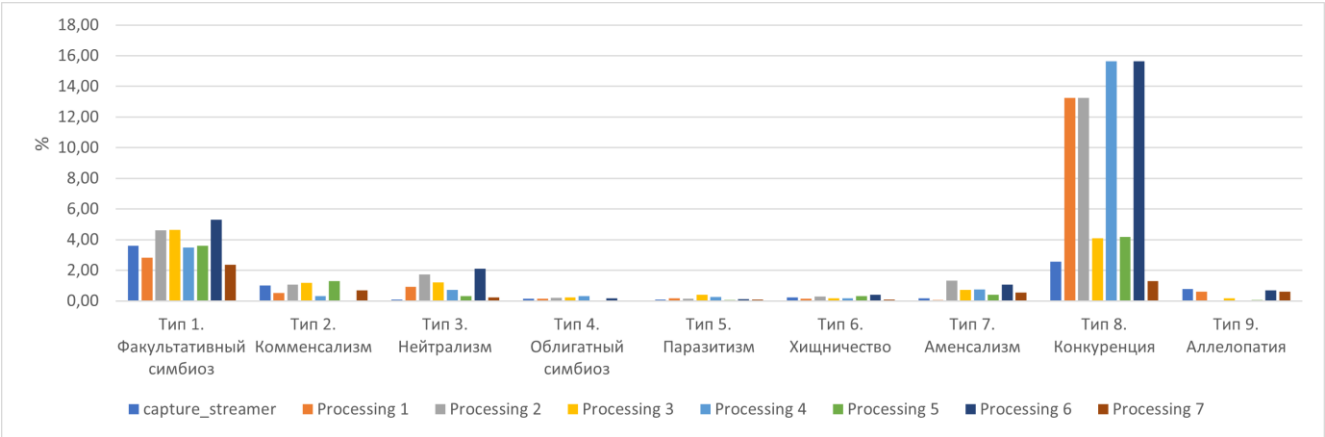

Рисунок 76 – Взаимное влияние сервисов системы распознавания лиц для сценария 2.

Из диаграммы 74 видно, что в системе процессы взаимодействуют, используя в основном тип 1 факультативный симбиоз и тип 8 конкуренция.

Это означает что исследуемые процессы взаимосвязаны, и система работает не на полную.

Это особенно заметно по сравнению со значениями, приведенными на диаграммах 75 и 76, видно, что они отличаются в большую сторону.

На диаграмме 75 показано, что в системе процессы взаимодействуют, используя в основном тип 1 факультативный симбиоз и тип 8 конкуренция также как и на диаграмме 74.

Однако интенсивность взаимодействия больше и более выражен тип 1 факультативный симбиоз, то есть процессу помогают друг другу и системе от этого лучше работать

На диаграмме 76, показана противоположная ситуация с диаграммой 75. Также выражены в основном тип 1 факультативный симбиоз и тип 8 конкуренция.

Однако тип 8 конкуренция гораздо выше, чем на диаграмме 75 и при этом уровень тип 1 факультативный симбиоз в несколько раз ниже.

Таким образом по данной диаграмме можно сделать вывод, что процессов сервиса «process.py» слишком много и они мешают друг другу, что может привести к появлению эффектов инфраструктурного деструктивизма.

Для прогнозирования рисков ИД исследуется динамика возникновения негативных поведенческих процессов.

Для удобства отображения результатов предлагается объединить типы антропоморфического взаимодействия процессов в группы и классифицировать динамику взаимного влияния сервисов:

1) положительный класс: тип 1 «Облигатный симбиоз», тип 2 «Факультативный симбиоз», тип 3 «Комменсализм»;

2) нейтральный класс: тип 4 «Нейтрализм»;

3)отрицательный класс: тип 5 «Паразитизм», тип 6 «Хищничество», тип 7 «Аменсализм», тип 8 «Аллелопатия», тип 9 «Конкуренция».

Таким образом применив данную классификацию, повышается наблюдаемость поведенческой активности процессов ИС распознавания лиц.

Выполним анализ рисков возникновения эффектов ИД для этого приведем следующие таблицы и: 25, 26 и 27, используя разработанное ПО в [159].

Таблица 25 – Анализ рисков возникновения эффектов ИД для сценария 1

Период анализа (с.)		Взаимное влияние сервисов		
Начало	Конец	Положительное	Нейтральное	Отрицательное
12	18	0	0	0
18	24	0	1	1
24	30	0	0	0
34	40	0	1	5
38	44	0	0	0
44	50	12	0	0
48	54	0	0	5
54	60	0	0	0
61	67	0	1	1
67	73	0	0	0
72	78	0	0	2
79	85	5	0	0
84	90	0	1	0
91	97	0	0	0
98	104	0	0	5
103	109	0	0	0
109	115	0	1	3
114	120	0	0	0
Сумма		17	5	22
Среднее значение		8,50	1	3,14

Таблица 26 – Анализ рисков возникновения эффектов ИД для сценария 2.

Период анализа (с.)		**Взаимное влияние сервисов**		
Начало	**Конец**	**Положительное**	**Нейтральное**	**Отрицательное**
12	18	6	1	3
18	24	11	0	2
24	30	14	1	4
30	36	11	1	9
36	42	6	1	4
42	48	18	0	6
48	54	1	3	3
54	60	12	2	6
60	66	2	0	3
66	72	0	0	3
72	78	9	0	7
78	84	8	0	3
84	90	8	0	3
90	96	7	2	5
96	102	38	0	7
102	108	3	0	0
108	114	41	1	5
114	120	1	0	3
Сумма		196	12	76
Среднее значение		11,53	1,5	4,47

Таблица 27 – Анализ рисков возникновения эффектов инфраструктурного деструктивизма для сценария 3.

Период анализа (с.)		Взаимное влияние сервисов		
Начало	Конец	Положительное	Нейтральное	Отрицательное
12	18	3	0	7
18	24	7	1	9
24	30	2	0	4
30	36	5	1	9
36	42	6	0	17
42	48	3	1	6
48	54	1	0	8
54	60	7	1	11
60	66	2	0	3
66	72	1	0	9
72	78	7	3	7
78	84	8	0	17
84	90	2	1	9
90	96	7	0	5
96	102	4	1	13
102	108	3	0	17
108	114	2	0	13
114	120	1	1	4
Сумма		71	10	168
Среднее значение		3,94	1,25	9,33

Используя таблицы 25, 26 и 27 построим следующие диаграммы представленные на рисунках 77, 78, 79.

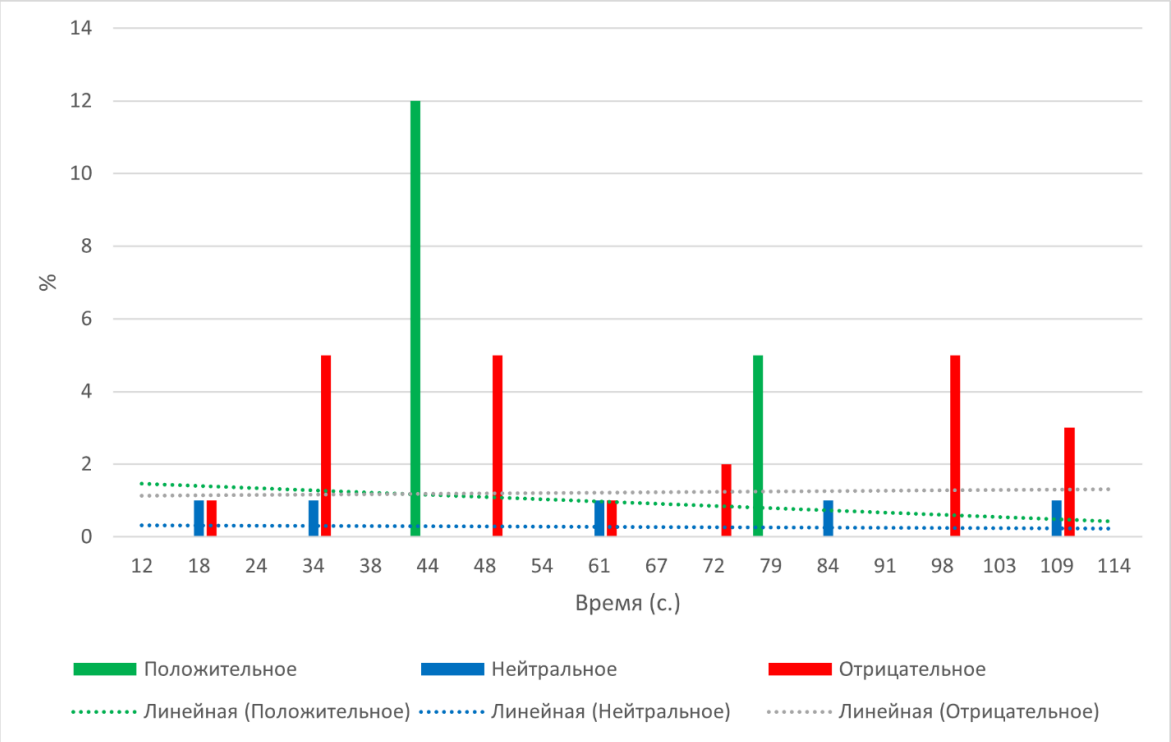

Рисунок 77 – Диаграмма анализа рисков возникновения эффектов инфраструктурного деструктивизма для сценария 1

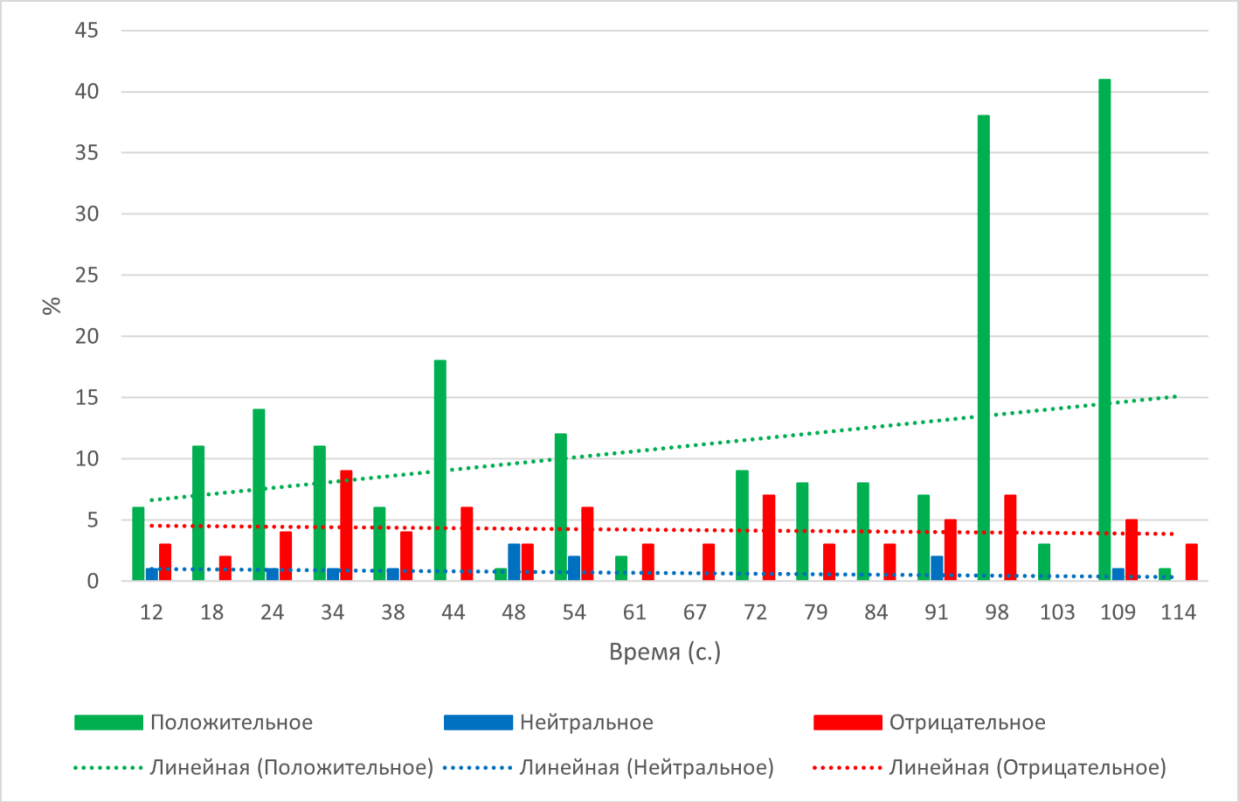

Рисунок 78 – Диаграмма анализа рисков возникновения эффектов инфраструктурного деструктивизма для сценария 2

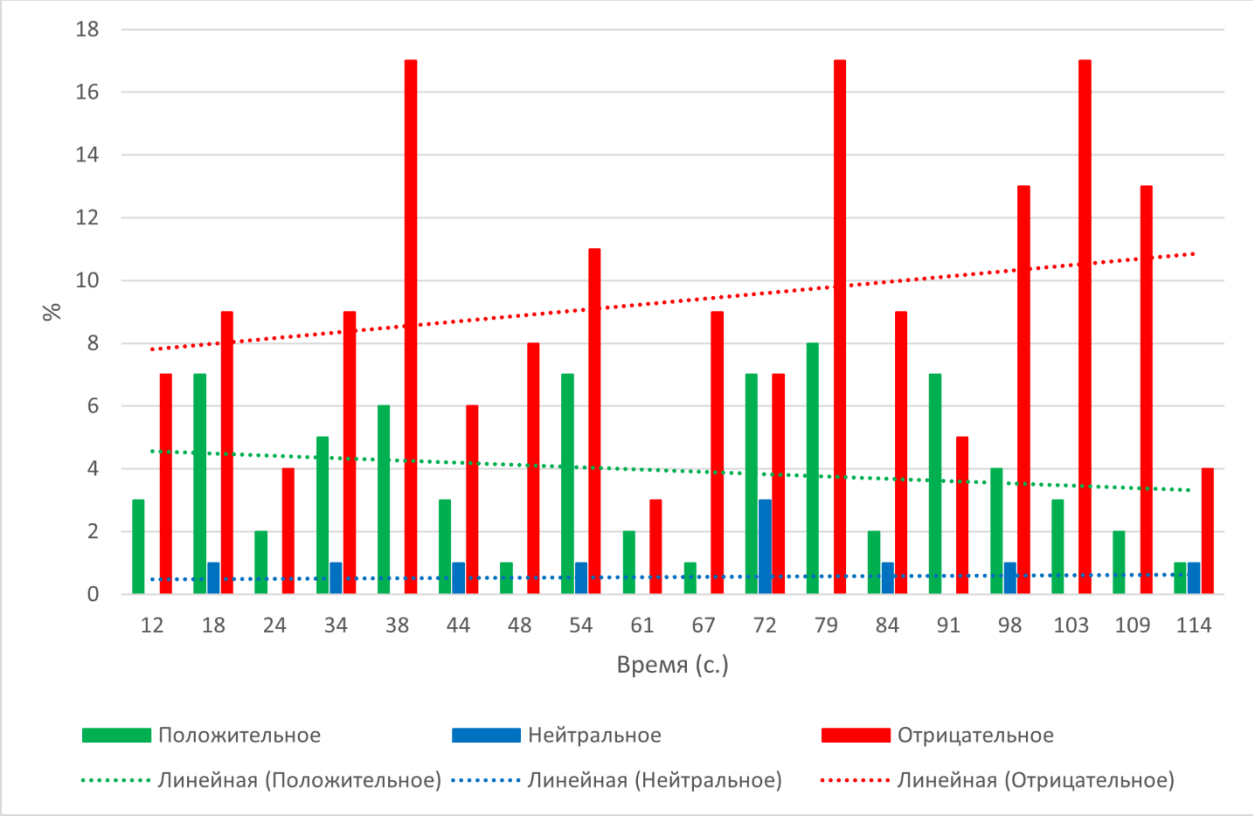

Рисунок 79 – Диаграмма анализа рисков возникновения эффектов инфраструктурного деструктивизма для сценария 3

Проанализировав таблицы 25, 26 и 27 рисунки 77, 78, 79 можно сделать следующие выводы:

1) эффекты ИД возможно прогнозировать, анализируя динамику положительного, нейтрального и отрицательного взаимодействия и строя для них тренды;

2) анализ поведенческой активности на основе антропоморфических типов позволяет по-новому оценивать характеристики ИС;

3) на основе антропоморфических типов возможно находить на ранних негативные взаимодействия сервисов и тем самым защищать ИС от угроз отказа в обслуживании;

4) точка пересечения трендов будет являться точкой, в которой система будет саморазрушаться в необратимом режиме.

Далее рассмотрим взаимное влияние для положительного и отрицательного взаимодействия процессов ИС системы распознавания лиц. Данные расчеты также выполним, используя разработанное ПО в [159]. Результаты приведены в таблицах 28, 29, 30 и 31. Значения взаимного влияния сервисов даны в секундах.

Таблица 28 – Данные положительного и отрицательного взаимодействия процессов системы распознавания лиц для сценария 1

ФФЦНаименование сервиса	Положительное взаимодействие								Отрицательное взаимодействие								Среднее положительное взаимодействие	Среднее отрицательное взаимодействие	Общая длительность
	app	bot	capture_streamer	cleanerDB	playsound	process	video_enhancer	zdata	app	bot	capture_streamer	cleanerDB	playsound	process	video_enhancer	zdata			
app														2,6			2,6		31
bot																			4
capture_streamer							5,1							5,1	1,3		3,2	5,1	112
cleanerDB																			23
process			20,5		1,3		5,1				15,4				2,6		9,0	9,0	11
playsound																			67
video_enhancer			44,9			15,4					24,4			1,3			12,8	30,1	116
zdata			20,5								15,4			5,1			10,3	20,5	7

Таблица 29 – Данные положительного и отрицательного взаимодействия процессов системы распознавания лиц для сценария 2

Наименование сервиса	Положительное взаимодействие										Отрицательное взаимодействие										Среднее положительное взаимодействие	Среднее отрицательное взаимодействие	Общая длительность
	app	bot	capture_streamer	cleanerDB	playsound	process1	process2	process3	video_enhancer	zdata	app	bot	capture_streamer	cleanerDB	playsound	process1	process2	process3	video_enhancer	zdata			
app								2,6								1,3		1,3			1,3	1,0	32
bot																							4
capture_streamer	1,3						1,3	1,3	26,9	1,3						1,3	1,3	1,3	23,1		6,7	1,2	116
cleanerDB																							24
playsound																							12
process1							2,6	2,6					46,2				1,3	1,3	2,6		12,8	0,1	56
process2								2,6					46,2			1,3		1,3	2,6		12,8	0,1	54
process3						1,3	2,6			1,3						1,3	1,3		2,6	1,3	1,6	0,8	69
video_enhancer	1,3		46,2			2,6	2,6	2,6		1,3						1,3	1,3	1,3		1,3	1,3	11,0	116
zdata								2,6								1,3			2,6		1,9	0,7	10

Таблица 30 – Данные положительного взаимодействия процессов системы распознавания лиц для сценария 3

Наименование сервиса	Положительное взаимодействие														Среднее положительное взаимодействие	Длительность
	app	bot	capture_streamer	cleanerDB	playsound	process1	process2	process3	process4	process5	process6	process7	video_enhancer	zdata		
app											1,3					32
bot									1,3		1,3				4,3	4
capture_streamer								1,3	1,3	1,3	1,3		12,8		2,6	117
cleanerDB																24
playsound																13
process1			71,8					1,3	1,3	1,3	1,3		2,6		2,8	54
process2			71,8					1,3	1,3	1,3	1,3		2,6		4,6	60
process3			14,1						1,3	1,3	1,3		2,6		4,6	60
process4			71,8					1,3		1,3	1,3		2,6		3,5	58
process5								1,3	1,3		1,3		12,8		3,6	67
process6			71,8					1,3	1,3	1,3			2,6		5,3	62
process7								1,3	1,3	1,3	1,3				2,4	53
video_enhancer								1,3	1,3	1,3	1,3				13,2	116
zdata								1,3	1,3	1,3					17,4	13

Таблица 31 – Данные отрицательного взаимодействия процессов системы р аспознавания лиц для сценария 1

Наименование сервиса	Отрицательное взаимодействие														Среднее отрицательное взаимодействие	Длительность
	app	bot	capture_streamer	cleanerDB	playsound	process1	process2	process3	process4	process5	process6	process7	video_enhancer	zdata		
app															1,3	32
bot						2,6		1,3			9,0				1,3	4
capture_streamer														2,6	3,6	117
cleanerDB																24
playsound																13
process1							1,3	1,3	2,6	6,4		2,6			13,2	54
process2						2,6		1,3	7,7		9,0	2,6			13,2	60
process3						2,6	2,6		2,6	6,4	2,6	1,3	16,7	2,6	4,1	60
process4						2,6	1,3	1,3		6,4	9,0	1,3		2,6	15,6	58
process5						2,6	2,6	1,3			9,0	2,6			4,2	67
process6						1,3		1,3	7,7	6,4		1,3	16,7	2,6	15,6	62
process7						2,6	1,3	1,3	1,3	6,4	1,3				1,3	53
video_enhancer			71,8				1,3	1,3		1,3		1,3		2,6	1,3	116
zdata			71,8			2,6		1,3			9,0	2,6			1,3	13

Таким образом для сценария 1 как показано в таблице 28 можно отметить, что наиболее мешающим сервисом является сервис «video_enhancer» поскольку оказывает самое продолжительное негативное воздействие. Также видно, что система сконфигурирована не оптимальным образом, так как не один из сервисов не оказывает значимого положительного воздействия.

Сервис «video_enhancer» является одним из возможных источников ИД, так как по данным таблицы 28 более четверти общего времени работы ИС системы данный сервис оказывает негативное на неё влияние.

Для сценария 2 как показано в таблице 29 отметим, что для данной ИС системы это является наиболее оптимальный режим работы поскольку отрицательное воздействие сервисом сведено к минимуму и наличествует положительное взаимодействие сервисов «process1» и «process2». При этом в отличие от сценария 1, сервис «video_enhancer» оказывает соизмеримое негативное влияние с сервисами «process1» и «process2», которые более в чем два оказывают положительное влияние.

Для сценария 3 как показано в таблицах 30 и 31 показано наличие эффектов ИД. В таблице 30 отмечено малое положительное взаимодействие всех сервисов, особенно сервисов «process».

Однако в таблице 31 сервисы с меткой «process» оказывают негативное воздействие в общей сложности более 20% времени работы системы. Таким образом получается, что сервисы «process» мешают друг другу работать, что приводит недостаточной скорости обработки информации. При этом возникает ситуация неправильной работы системы в результате чего ярко выражены эффекты ИД, которые приводят блокировки работы системы в целом, а также реализации техники T1499 «Точечный отказ в обслуживании» [216], за счет не верной настройки. Следует отметить, что данный эффект невозможно объяснить иным способом. Для данной системы распознавания лиц входящей в состав контроля и управления доступа угроза ИГ способна привести к отключению контроля периметра.

Таким образом, для имеющейся ИС распознавания лиц удалось повысить точность оценки эффектов ИД и выполнить прогнозирование угроз ИБ ИГ. Повышена точность определения эффектов ИД. Представленное решение позволяет оперативно в режиме реального времени защитить имеющуюся ИС распознавания лиц от угрозы ИГ.

4.7.2 Исследование облачной платформы «OpenStack»

В качестве данных для анализа облачной платформы OpenStack использованы данные журналов событий системы из открытого набор данных DeepTraLog [203 и 227]. Облачная платформа OpenStack представляет собой комплекс проектов свободного программного обеспечения для создания инфраструктурных облачных сервисов, облачных хранилищ, центров обработки данных, разработки и предоставления приложений. Набор данных включает в себя журналы событий трассировки микросервисной распределенной тестовой системы бронирования билетов на поезд (41 микросервис). Данные «DeepTraLog» использовались для проведения соревнований по обнаружению аномалий в журналах событий для инфраструктур,

построенных на сервисах с использованием облачной платформы OpenStack. Фрагмент журнала событий облачной платформы OpenStack представлен на рисунке 59.

Для исследования взаимодействия сервисов на основе антропоморфических моделей, разработанных во 2 разделе, воспользуемся программным средством разработанным автором в [154 и159]. В отличие от результатов, представленных в пункте 4.5 продолжим исследование и выполним анализ динамики рисков тех же процессов, но с учетом более длительных интервалов анализа с обобщением на «положительное», «нейтральное» и «отрицательное» взаимное влияние процессов также как это сделано в пункте 4.7.1. Результат анализа приведен в таблице 32, значения взаимного влияния сервисов приведено как процентное отношение к общему времени работы сервиса. Интервал анализа выбран 7 дней. Отметим, что на практике для других систем интервал анализа может быть другим. Также возможно ситуация в которой система не имеет эффектов инфраструктурного деструктивизма. Иногда в некоторых открытых источниках данных, приводятся данные, которые явно обрабатывались вручную для обезличивания и также не содержат данных позволяющих определить наличие эффектов ИД.

Таблица 32 – Анализ динамики рисков возникновения ИД

Период анализа (даты)		Взаимное влияние сервисов		
Начало	Конец	Положительное	Нейтральное	Отрицательное
05.08.2021	12.08.2021	11,28	2,8	5,55
13.08.2021	20.08.2021	14,40	2,84	2,99
21.08.2021	28.08.2021	15,57	2,26	1,90
29.08.2021	05.09.2021	16,37	2,43	1,92
06.09.2021	13.09.2021	14,92	2,62	1,96
14.09.2021	21.09.2021	13,98	2,79	2,35
22.09.2021	29.09.2021	14,42	2,67	2,42
30.09.2021	07.10.2021	13,75	3,06	2,80
08.10.2021	15.10.2021	12,95	2,97	3,50
16.10.2021	23.10.2021	13,38	2,33	4,04
24.10.2021	31.10.2021	12,93	2,58	4,21
01.11.2021	08.11.2021	11,98	2,74	3,00
09.11.2021	16.11.2021	12,67	2,77	3,12
17.11.2021	24.11.2021	14,00	3,09	3,56
25.11.2021	02.12.2021	13,46	3,18	3,34
03.12.2021	10.12.2021	11,58	2,72	5,22
11.12.2021	18.12.2021	9,17	3,36	7,24
19.12.2021	26.12.2021	7,60	3,33	9,31
27.12.2021	03.01.2022	6,35	2,98	10,90

Используя данные, представленные в таблице 32 визуализируем их в виде столбчатой диаграммы.

Диаграмма оценки динамики рисков возникновения эффектов ИД представлена на рисунке 80.

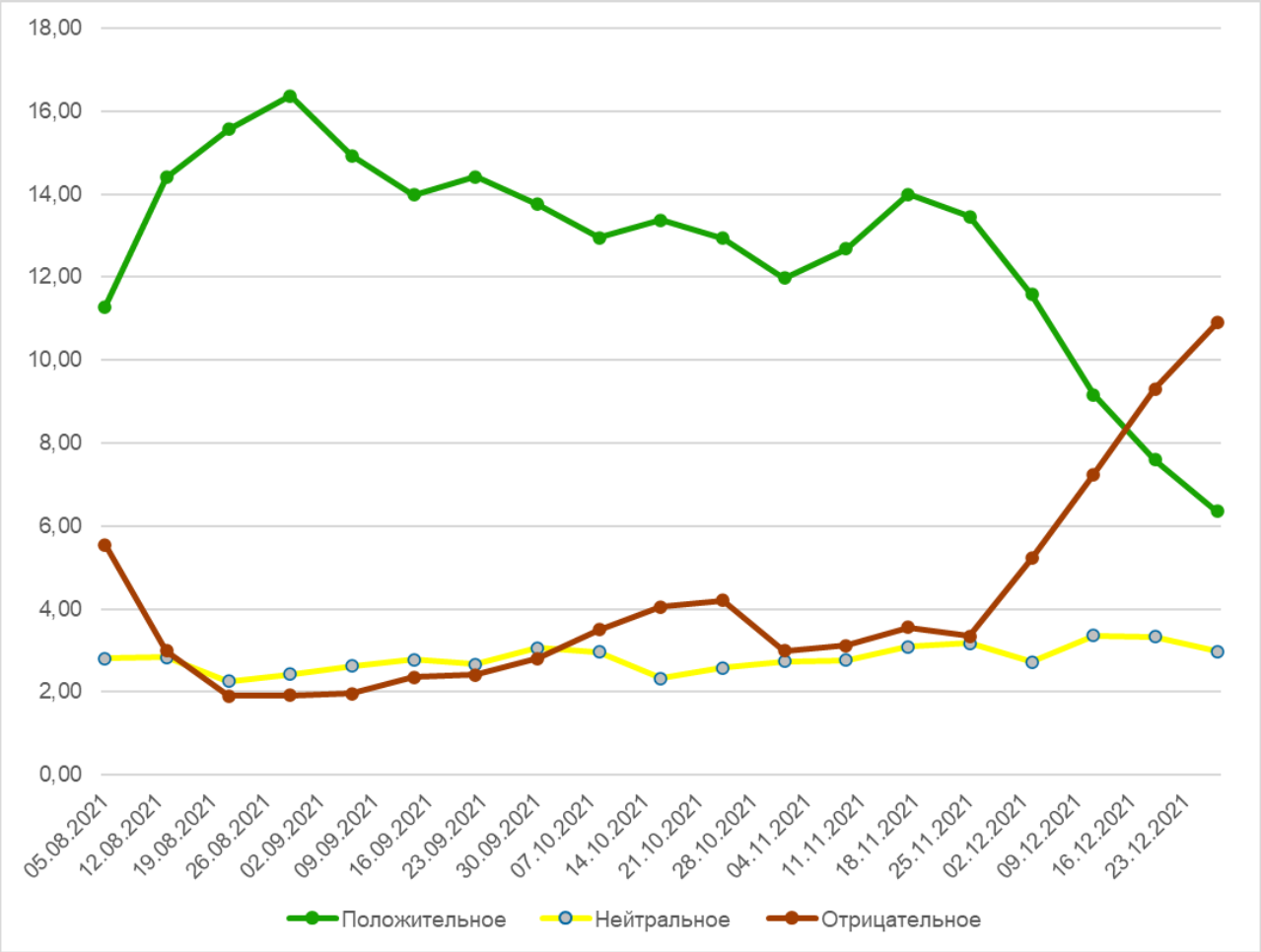

Рисунок 80 – Диаграмма оценки динамики рисков возникновения эффектов ИД

Точка пересечения положительного и отрицательного взаимодействия сервисов для диаграммы на рисунке 80 вероятнее всего является точкой бифуркации. Таким образом можно сделать вывод, что эффекты ИД наиболее вероятны в момент после 10.12.2021. Данный вывод подтверждается практически, так как инфраструктура престала функционировать после 27.12.2021 без видимых на это причин [203 и 227].

Отметим, что данный эффект впервые обнаружен в работах [85,89]. В указанных исследованиях рассмотрены модели взаимодействия объектов КИИ и методы определения момента достижения точки бифуркации. В отличие от существующих

подходов, в настоящей работе предлагается методология оценки динамики рисков возникновения эффектов ИД, основанная исключительно на анализе журналов событий ИТ-инфраструктуры РИС. Поскольку в реальных условиях данных для анализа, может оказаться гораздо меньше чем использовано в данном расчёте, то предлагается построить следующие диаграммы как показано на рисунках 81 и 82.

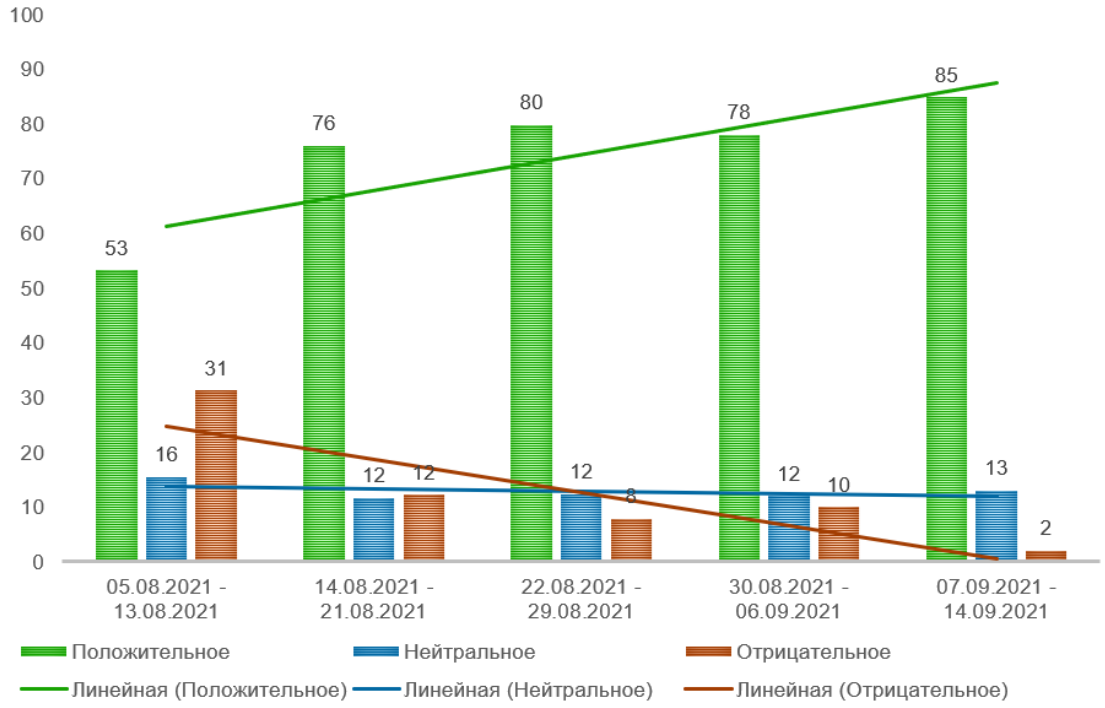

Рисунок 81 – Диаграмма анализа динамики рисков возникновения эффектов ИД за период с 05.08.2021 по 14.09.2021

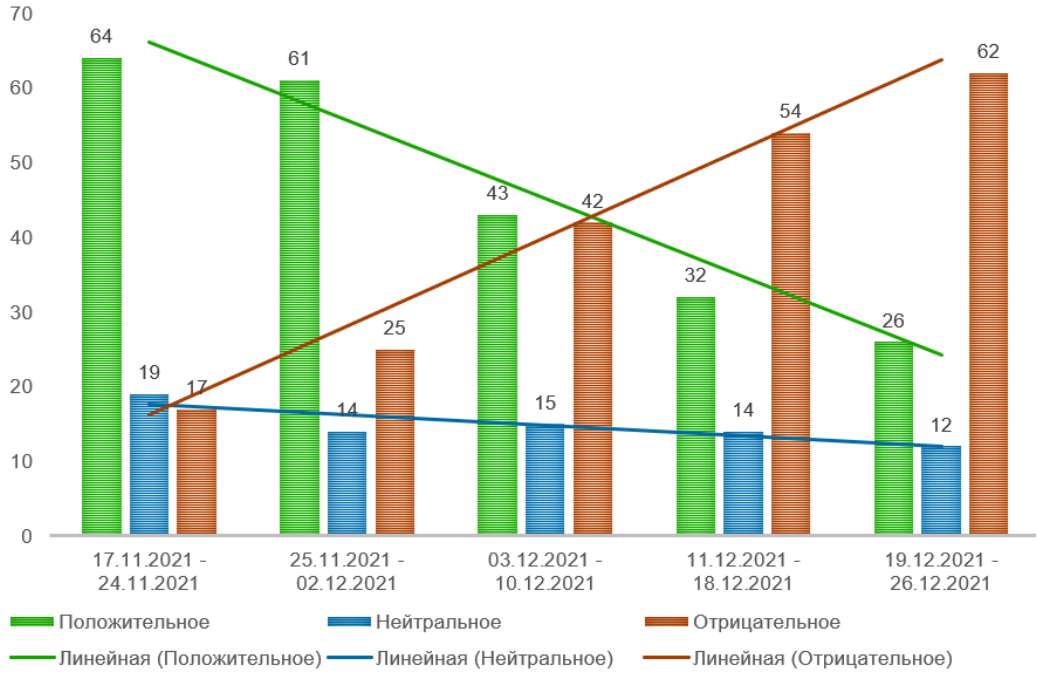

Рисунок 82 – Диаграмма анализа динамики рисков возникновения эффектов ИД за период с 17.11.2021 по 26.12.2021

Проанализировав отображение значений данных для меньшего количество данных из таблицы 32 и построив линейные тренды – красные, синие и зеленые линии на рисунках 81 и 82 также можно определить примерное расположение точки бифуркации.

Таким образом, полученные результаты еще раз подтверждают, что имеется пропорциональная зависимость между «отрицательным» межсервисным взаимодействием и вероятностью появления эффектов инфраструктурного деструктивизма. Вероятнее всего эффект инфраструктурного деструктивизма будет себя проявлять, когда возрастает показатель отрицательного» межсервисного взаимодействия (см. рис. 82). Предложенный подход прогнозирования угрозы ИБ ИГ, возможно также использовать как метрику (показатель) «здоровья» ИТ-инфраструктуры РИС. Используя данную метрику возможно заранее прогнозировать эффекты возникновения инфраструктурного деструктивизма для сервисных архитектур облачных платформ таких, как например платформа OpenStack. Разработанная антропоморфическая модель является одним из перспективных подходов для анализа поведенческой активности сервисов в ИТ-инфраструктуры РИС.

Предложенное решение задачи обнаружения ситуаций, связанных с отказом в обслуживании рассматриваемой РИС позволило более точно найти все факторы – проявления эффектов ИД. По имеющихся размеченным данным [203] было найдено 93 случая возникновения эффектов ИД. По другим данным, представленным в [227] было обнаружено 79 проблемных ситуаций.

Предложенное решение обеспечивает повышение точности выявления эффектов ИД более чем на 10%.

Кроме того, разработанная методика повышает оперативность обнаружения угроз ИБ ИГ, поскольку подход, изложенный в пункте 4.1, позволяет реализовать реагирование на угрозы ИБ в режиме реального времени.

4.7.3 Исследование вычислительного облачного кластера «Alibaba cloud»

В качестве данных для анализа использованы данные трассировки микросервисов одного из кластеров облачной платформы Alibaba cloud.

Для анализа выбран открытый датасет «Cluster-trace-v2022», который включает в себя данные журналов событий примерно 4000 машин за период 8 дней [186, 221].

В отличие от предыдущих открытых датасетов типа «Cluster-trace-v2021», данный набор данных содержит более детализированную трассировку параметров функционирования сервисов, включая информацию о рабочих нагрузках процессов (процессорное время, использование оперативной памяти и другие метрики).

Для прогнозирования угрозы возникновения и оценки динамики рисков инфраструктурного деструктивизма использовано разработанное программное обеспечение [152, 154, 159]. На рисунке 83 представлен «График процессов РИС» для анализируемого датасета. Красным цветом на временной диаграмме выделены участки выполнения процессов, превышающие ожидаемые значения по времени. Зелёным цветом обозначены интервалы с временем выполнения ниже ожидаемого.

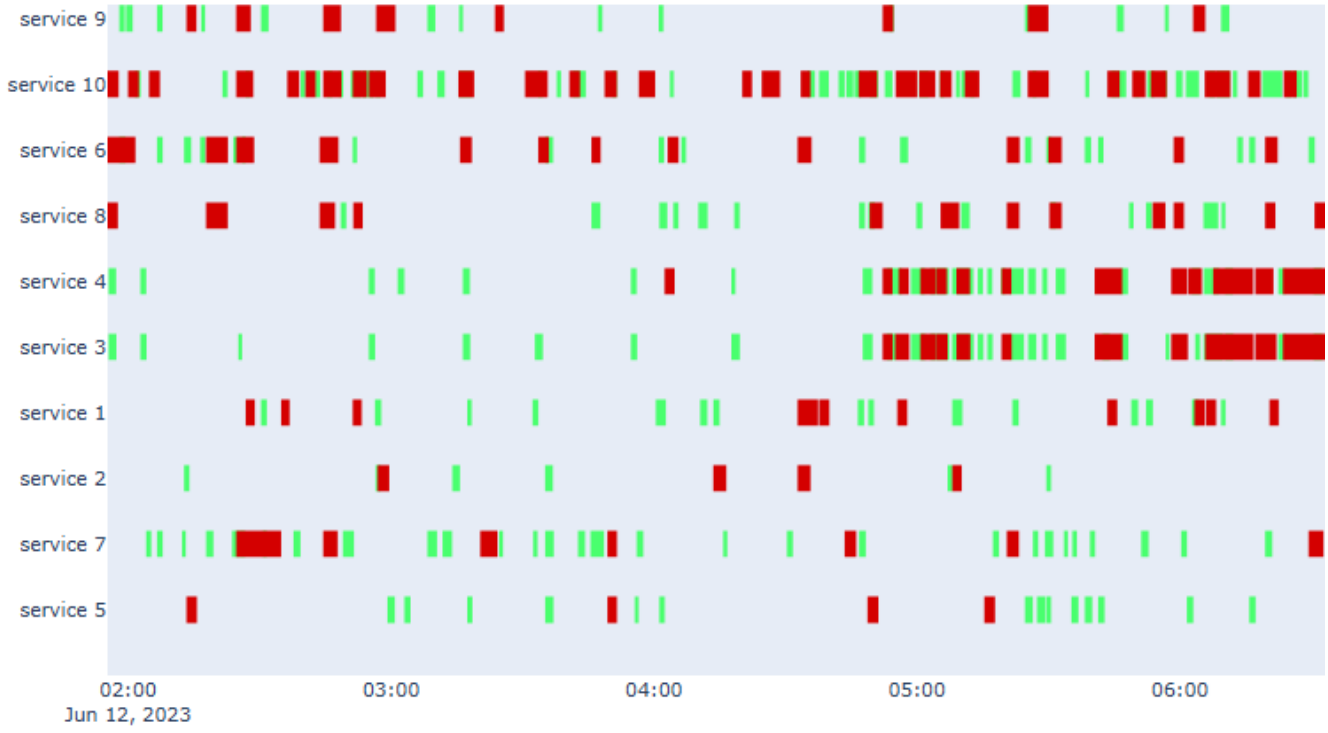

Рисунок 83 – График процессов РИС

Результат анализа приведен в таблице 33, значения взаимного влияния сервисов приведено как процентное отношение к общему времени работы сервиса. Интервал анализа выбран 7 дней.

Таблица 33 – Данные положительного и отрицательного взаимодействия процессов РИС

Наименование сервиса	Тип 1. Факультативный симбиоз	Тип 2. Комменсализм	Тип 3. Нейтрализм	Тип 4. Облигатный симбиоз	Тип 5. Паразитизм	Тип 6. Хищничество	Тип 7. Аменсализм	Тип 8. Конкуренция	Тип 9. Аллелопатия
service 1	11,69	3,36	8,53	0,28	0,06	2,33	2,14	7,92	1,64
service 2	16,20	5,94	5,53	0,98	1,58	1,32	3,52	7,77	0,96
service 3	14,49	4,11	4,50	4,15	0,74	2,98	4,18	7,75	0,72
service 4	20,91	3,73	18,08	2,02	2,29	2,48	6,10	10,96	2,53
service 5	14,88	0,48	3,45	3,94	3,05	0,59	2,86	10,54	0,54
service 6	11,40	2,63	6,29	0,47	1,64	1,70	0,76	7,67	1,13
service 7	21,37	0,67	0,30	0,42	4,28	2,38	4,05	10,20	0,73
service 8	15,05	1,82	2,42	3,71	1,48	0,79	3,79	10,12	0,71
service 9	21,32	0,86	5,64	3,65	3,09	4,43	5,11	9,24	1,26
service 10	11,99	2,23	2,76	2,20	2,90	2,88	1,49	7,99	2,39

Используя данные, представленные в таблице 33 визуализируем их в виде столбчатой диаграммы. Диаграмма анализа динамики рисков возникновения эффектов ИД представлена на рисунке 84.

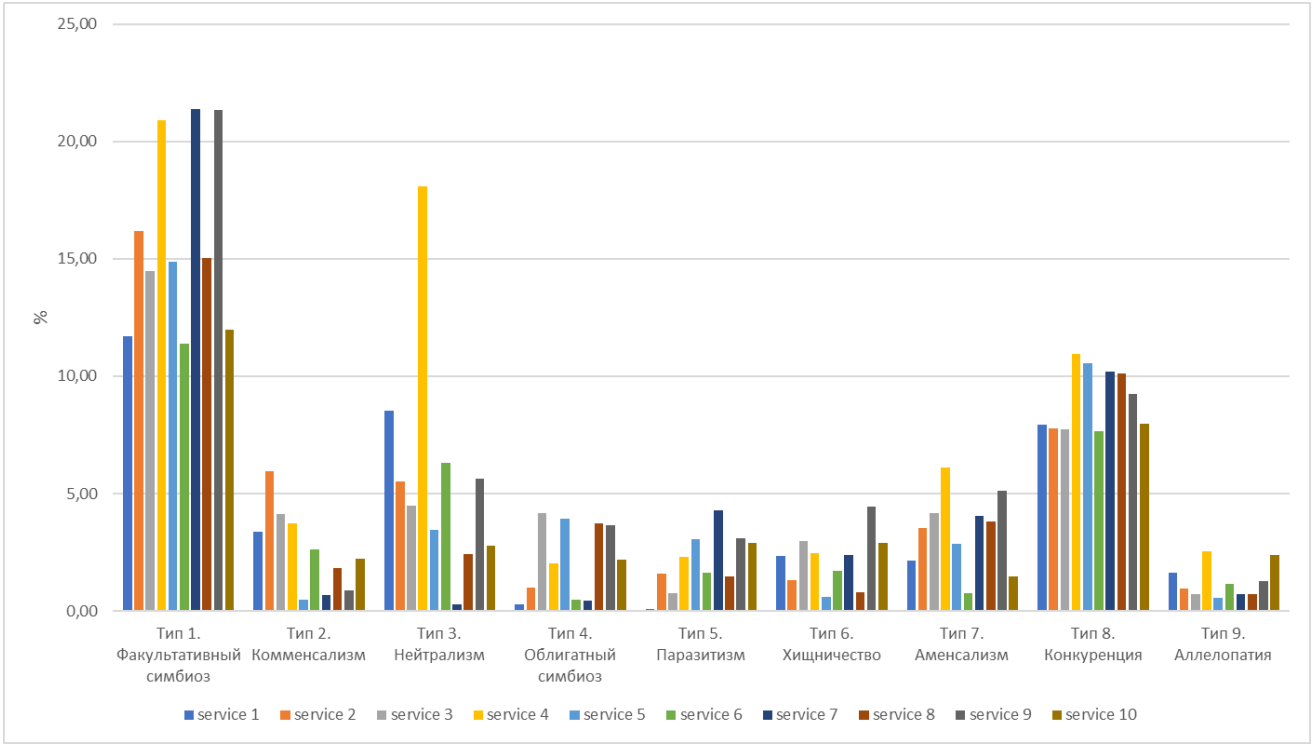

Рисунок 84 – Взаимное влияние сервисов РИС

На рисунке 84 показано, что наибольшая активность сервисов выражена в типе 1 «Факультативный симбиоз», также заметен тип 4 «конкуренция», но он в два раза менее интенсивен, чем тип 1.

Также для сервиса 4 заметно его положительное влияние на все остальные сервисы и особо выражен тип 3 «нейтрализм». Данные показатели являются обобщением общего взаимодействия сервисов.

При этом по таблице 33 и диаграмме на рисунке 84, нельзя определить какой именно сервис мешает работе системе в какой момент и сопоставить обстоятельства.

Для более точного описания взаимодействий сервисов построим таблицу 34, в которой представлен результат оценки положительного и отрицательного взаимодействия сервисов.

Значения взаимного влияния сервисов в таблице 34 приведено как процентное отношение к общему времени работы сервиса. Интервал анализа выбран 7 дней.

Таблица 34 – Данные положительного и отрицательного взаимодействия процессов ИС

Наименование сервиса	Положительное взаимодействие										Отрицательное взаимодействие										Среднее положительное взаимодействие	Среднее отрицательное взаимодействие
	service 1	service 2	service 3	service 4	service 5	service 6	service 7	service 8	service 9	service 10	service 1	service 2	service 3	service 4	service 5	service 6	service 7	service 8	service 9	service 10		
service 1	0,0	13,0	16,8	2,6	2,4	16,1	35,1	8,6	3,3	7,3	0,0	10,1	12,8	1,3	9,5	12,4	1,5	1,8	11,7	10,1	11,69	7,92
service 2	34,0	0,0	17,9	13,7	35,5	16,8	1,3	8,6	7,3	10,8	4,6	0,0	6,0	0,2	1,5	7,1	12,8	11,9	12,8	13,0	16,20	7,77
service 3	33,1	15,0	0,0	18,3	2,4	16,8	3,5	8,6	12,4	20,3	1,8	11,3	0,0	12,8	9,0	2,0	12,8	11,9	7,3	0,9	14,49	7,75
service 4	34,0	15,0	7,7	0,0	35,5	16,8	1,3	36,6	21,2	20,1	12,8	13,5	12,8	0,0	5,1	12,4	12,8	11,9	7,3	10,1	20,91	10,96
service 5	33,1	31,5	17,9	2,6	0,0	16,8	3,5	13,5	12,4	2,6	8,6	10,1	5,1	15,2	0,0	6,2	13,5	11,9	11,7	12,6	14,88	10,54
service 6	33,1	15,0	7,7	13,7	2,4	0,0	3,5	8,6	12,4	6,2	1,8	11,3	1,3	12,8	9,0	0,0	12,8	11,9	7,3	0,9	11,40	7,67
service 7	33,1	33,8	17,9	32,4	16,3	25,1	0,0	8,6	12,4	12,8	13,5	9,0	3,3	15,2	9,0	15,4	0,0	1,8	11,5	13,0	21,37	10,20
service 8	33,1	6,6	17,9	4,6	16,3	9,7	1,3	0,0	31,5	14,3	13,5	11,3	1,1	15,2	9,5	2,4	12,8	0,0	12,4	13,0	15,05	10,12
service 9	34,0	31,5	7,7	11,9	35,5	16,8	3,5	36,6	0,0	14,3	8,6	13,5	1,1	15,2	9,0	12,4	10,6	11,9	0,0	0,9	21,32	9,24

Проанализировав таблицу 34 можно сделать вывод о том, что наибольшее положительное воздействие (столбец «среднее положительное взаимодействие») оказывают сервисы 4, 7 и 9.

Наибольшее отрицательное воздействие (столбец «среднее отрицательное взаимодействие») оказывают сервисы 4, 5 и 7, 8.

Данная система и сбалансирована и нет особых перекосов не положительном не в отрицательном взаимодействии.

Обычно при проявлении эффектов ИД, должны присутствовать перекосы в сторону отрицательных взаимодействий. Для исследуемой системы нет предпосылок возникновения эффектов ИД.

Далее выполним анализ динамики рисков возникновения ИД, для этого используем интервал анализа 17 минут. Фрагмент результатов анализа представлен в таблице 35.

Таблица 35 –Анализ динамики рисков возникновения ИД

Период анализа	**Взаимное влияние сервисов**		
	Положительное	**Нейтральное**	**Отрицательное**
12.02.2023 11:00	0,49	0,94	0,21
12.02.2023 11:17	8,37	3,25	3,64
12.02.2023 11:34	0,88	0,89	2,58
12.02.2023 11:51	1,50	0,88	0,57
12.02.2023 12:08	4,42	1,89	1,77
12.02.2023 12:25	1,84	1,68	1,28
12.02.2023 12:42	2,84	1,31	2,21
12.02.2023 12:59	5,39	2,20	3,15
12.02.2023 13:16	6,20	2,70	3,57
12.02.2023 13:33	2,70	2,09	3,48
12.02.2023 13:50	4,81	1,85	1,62
12.02.2023 14:07	4,39	2,68	4,15
12.02.2023 14:24	7,46	3,96	5,43
12.02.2023 14:41	2,63	1,85	1,62
12.02.2023 14:58	3,06	2,06	1,36

Полный анализ представлен на диаграмме на рисунке 85.

На диаграмме, представленной на рисунке 85 показана оценка динамики рисков возникновения эффектов ИД, из которой видно, что система устойчива и возникновение эффектов ИД маловероятно.

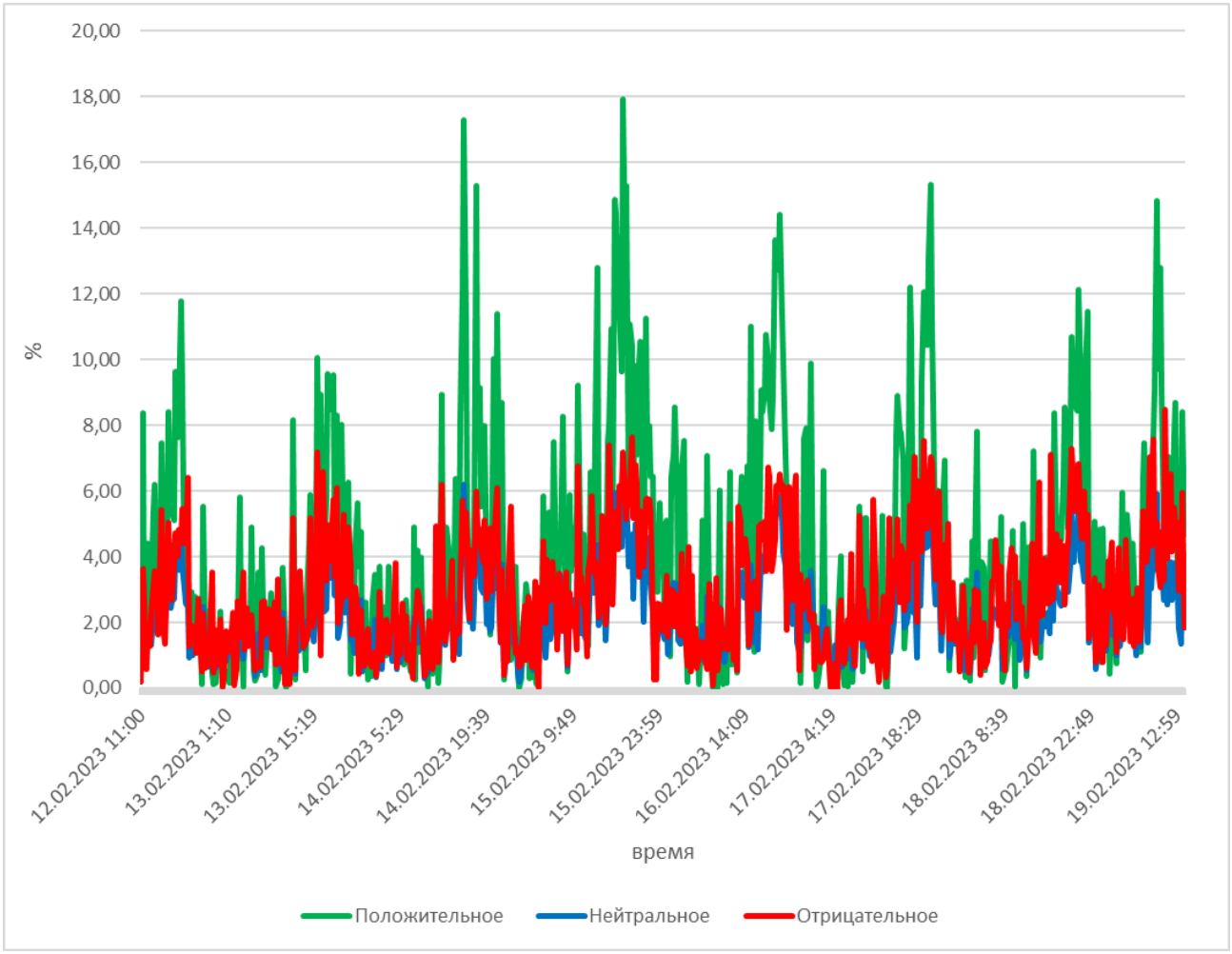

Рисунок 85 – Анализ динамики рисков возникновения эффектов ИД

Однако предполагается, что данные подверглись специальной обработке с целью сокрытия системных сбоев, приводящих к проявлению эффектов инфраструктурного деструктивизма. Данный факт становится очевидным при детальном анализе журналов событий. Некоторые временные интервалы, особенно в периоды пиковых нагрузок, лишены информации о функционировании системы.

4.8 Выводы по разделу 4

В качестве объекта исследовалась методика и реализация программно-аналитического комплекса оценки угроз информационной безопасности инфраструктурного генеза в распределенных информационных системах на предмет решения прикладных задач оценки влияния эффектов деструктивного воздействия инфраструктурного генеза.

В ходе исследования:

1) Разработана методика оценки угроз информационной безопасности, обусловленных инфраструктурным генезисом, в сервис-ориентированных информационных системах. Проведённое экспериментальное исследование показало эффективность её применения для проактивного прогнозирования рисков информационной безопасности и позволило разработать организационную схему использования методики при прогнозировании угроз инфраструктурного генеза в распределённых информационных системах.

2) Проведено экспериментальное исследование программного интерфейса сервисов информационной системы на предмет проявления эффекта инфраструктурного деструктивизма. В качестве примера использован датасет «DVD RENTAL». Определён параметр инфраструктурного деструктивизма программного интерфейса сервисов информационной системы для различных версий инфраструктуры СУБД PostgreSQL. Экспериментальные результаты показали, что данный параметр зависит исключительно от версии программного обеспечения инфраструктуры и не коррелирует с содержимыми данными. Во всех экспериментах использовался один и тот же датасет при изменении только версии программного обеспечения.

3) Обоснован результат интеллектуального анализа функционирования хранилища данных GreenPlum с точки зрения оценки угроз информационной безопасности инфраструктурного генеза и прогнозирования эффектов инфраструктурного деструктивизма на основе обработки журналов событий хранилища. Представленные результаты были продемонстрированы в рамках открытого соревнования «онлайн-хакатон SkolkovoHack 2022», проходившего с 23 по 25 сентября 2022 года, организованного ПАО «Ростелеком» (проект занял первое призовое место).

4) Проведена оценка взаимодействия сервисов с использованием антропоморфических поведенческих моделей. Выполнен анализ журналов событий облачной платформы OpenStack. В исследовании использован датасет «DeepTraLog», предоставленный лабораторией разработки программного обеспечения Фуданьского университета (Шанхай, Китай). [154]. В результате проведённого

исследования определена структура взаимодействия сервисов. Выделены и обоснованы негативные факторы, служащие индикаторами проявления эффектов инфраструктурного деструктивизма. Проанализирована возможность интерпретации взаимного влияния сервисов и представлен подход к оценке воздействия негативных эффектов инфраструктурного деструктивизма на отказоустойчивость информационной системы.

5) Проведено экспериментальное исследование активности вредоносного программного обеспечения с применением эпидемиологической модели SEIR, адаптированной с учётом антропоморфических состояний. Установлено, что при наличии эффектов взаимного взаимодействия между вредоносными программами наблюдается компенсационный эффект. Экспериментально обосновано, что в системах, где одновременно функционирует девять и более вредоносных программных средств, совокупный вредоносный эффект нивелируется. Обнаруженный компенсационный эффект может рассматриваться как потенциальный механизм защиты, направленный на нейтрализацию угрозы реализации техники T1499 «Точечный отказ в обслуживании» из матрицы MITRE ATT&CK. [216].

6) Выполнено прогнозирование угроз и оценка эффектов инфраструктурного деструктивизма на основе анализа журналов событий облачных систем трёх различных архитектур. Проведён анализ журналов работы интеллектуальной распределённой системы распознавания лиц «Персона ID» в различных тестовых режимах, журналов событий облачной платформы гипервизора OpenStack, а также вычислительных кластеров системы «Alibaba Cloud». В результате установлена зависимость параметра отрицательного межсервисного взаимодействия от вероятностей проявления эффектов инфраструктурного деструктивизма. Обоснована применимость метрики «здоровье» ИТ-инфраструктуры информационной системы для прогнозирования и оценки угроз инфраструктурного генеза. Применение данной метрики позволяет осуществлять прогнозирование эффектов инфраструктурного деструктивизма для сервисно-ориентированных архитектур, вычислительных кластеров и облачных платформ. Апробация предложенной системы, выполненная

для оптимизации кластера РТУ МИРЭА, подтвердила практическую востребованность и эффективность разработанной методики.

7) Разработана шкала преобразования качественных показателей в количественные значения при оценке поведенческой активности сервисов на основе комплекса антропоморфических моделей. Предложен метод расчёта метрик, предназначенных для оценки показателя «здоровье» ИТ-инфраструктуры информационной системы и определения возможных сценариев её развития, включая вероятности возникновения эффектов инфраструктурного деструктивизма.

Основным научным результатом, изложенным в четвертом разделе, является разработка методики выявления угроз информационной безопасности инфраструктурного генеза в сервис-ориентированных информационных системах.

Частными научными результатами, изложенными в четвертом разделе, являются:

1) факторы развития ИД;

2) критерии оценки эффективности работы сервиса ИС с позиции ИД;

3) программно-аналитический комплекс для оценки и прогнозирования эффектов ДВ ИГ.

Основное содержание раздела и изложенных в нем научных результатов опубликовано в работах автора [91, 60, 127, 211, 151, 152, 144, 137, 133].

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 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 СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

API – application programming interface (интерфейс программирования приложения, тоже что и программный интерфейс информационной системы).

ESB – enterprise service bus (сервисная шина предприятия).

SOA – service-oriented architecture (сервис-ориентированная архитектура).

ВПО – вредоносное программного обеспечение.

ДВ – деструктивное воздействие.

ИБ – информационная безопасность.

ИД – инфраструктурный деструктивизм.

ИГ – инфраструктурный генез.

ИИ – искусственный интеллект.

ИС – информационная система.

ИТ-инфраструктура – информационно-технологическая инфраструктура.

ОС – операционная система.

ПИ – программный интерфейс.

ПО – программное обеспечение.

РИС – распределенная информационная система.

СПИСОК ТЕРМИНОВ

балансировщик нагрузки (Load balancer): компонент в РИС, который распределяет входящие клиентские запросы между группой серверов, в каждом случае возвращая ответ от выбранного сервера соответствующему клиенту.

брокер сообщений: компонент в РИС, который выступает посредником в коммуникации между различными частями системы. Обозначенные выше элементы сервис-ориентированных ИС являются возможными источниками возникновения эффектов ИД.

взаимная блокировка (*deadlock*): в контексте ИБ это состояние, при котором два или более процесса или компонента системы блокируют доступ друг другу к необходимым ресурсам, в результате чего ни один из них не может продолжить выполнение.

гонка ресурсов (race condition): в РИС состояние, при котором два или более процесса или потока одновременно пытаются получить доступ к общим ресурсам (например, файлам, переменным, базам данных), и результат их взаимодействия зависит от порядка выполнения.

горизонтальное масштабирование: это подход к обеспечению эффективного роста программных приложений, особенно в контексте сценариев высокой нагрузки и корпоративных сценариев.

деструктивные воздействия (ДВ) инфраструктурного генеза (ИГ): воздействия, в результате которых проявляется непредвиденное и (или) нежелательное событие, вызванное совокупностью факторов и условий инфраструктурного генеза (ИГ), создающих опасность нарушения ИБ РИС.

деструктивный мусор: программный код, внесенный в РИС после устранения уязвимостей ИБ и ошибок программного кода, реализованный не оптимальным образом.

достоверность последовательности запросов (confidence): последовательности запросов риводящая к возникновению эффектов инфраструктурного

деструктивизма – показатель того, как часто последовательности запросов встречаются вместе $conf\,(Q_1^{item} \cup Q_2^{item}) = \mathrm{supp}(Q_1^{item} \cup Q_2^{item}) / \mathrm{supp}(Q_1^{item}) \cdot \mathrm{supp}(Q_2^{item})$.

идемпотентность: свойство операции, при котором повторное выполнение этой операции с одинаковыми входными данными не изменяет результат.

информационно-технологическая инфраструктура (ИТ-инфраструктура): совокупность всех аппаратных, программных, сетевых, коммуникационных и сервисных компонентов (объектов), которые обеспечивают функционирование и поддержку информационных технологий в организации, предприятии, государственной структуре, промышленном производстве, и других областях.

информационная инфраструктура: совокупность систем, сетей и сервисов, которые поддерживают сбор, обработку, хранение, передачу и доступ к информации

инфраструктура: комплекс взаимосвязанных обслуживающих структур или объектов, составляющих и обеспечивающих основу функционирования системы.

инфраструктурный деструктивизм (ИД): это феномен, возникающий в ИС, когда в результате деструктивных воздействий (ДВ) инфраструктурного генеза (ИГ) происходят системные изменения, ведущие к нарушению устойчивости, целостности, доступности, функциональности и управляемости информационной системы (ИС).

Примечание

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

киберустойчивость РИС: способность организаций и их информационных ресурсов сохранять функциональность, противостоять кибератакам и сбоям, а также быстро восстанавливаться после инцидентов, обеспечивая непрерывность операций и защиту данных.

конечные точка входа программного интерфейса: точка входа в программную часть сервиса, через которую осуществляется взаимодействие.

критическая информационная инфраструктура (КИИ): совокупность ИС и/или телекоммуникационных сетей, критически важных для работы ключевых сфер жизнедеятельности государства и общества: здравоохранения, промышленности, связи, транспорта, энергетики, финансового сектора и городского хозяйства.

кэширующий сервис: компонент в РИС, не является авторитативным ни для одной зоны сервером, но используется для исполнения запросов. Он обслуживает запросы и опрашивает другие сервера, отвечающие за необходимую информацию.

метрика: количественный или качественный показатель работы подсистем и систем РИС.

набор последовательности запросов (itemset): последовательность наборов цепочек запросов $Q^{item} = \{q_a, q_b, ...q_c\}$, которая часто встречается в журналах событий вместе и приводит возникновению эффектов ИД.

обратный прокси-сервер (Reverse Proxy): компонент в РИС, который принимает запрос от клиента, пересылает его на сервер, который может его выполнить, и возвращает ответ сервера клиенту. Другими словами, обратные прокси-серверы действуют как таковые для HTTP-трафика и интерфейсов прикладного программирования.

отношение поддержки последовательности запросов (lift): отношение зависимости набора Q_1^{item} к другому набору Q_2^{item}, которое показывает, насколько наборы зависят друг от друга $lift(Q_1^{item} \cup Q_2^{item}) = \text{supp}(Q_1^{item} \cup Q_2^{item}) / \text{supp}(Q_1^{item}) \cdot \text{supp}(Q_1^{item})$.

оптимизатор запросов: компонент в РИС, который отвечает за создание плана запроса. Он оценивает несколько альтернативных подходов к решению запроса к базе данных и выбирает наиболее оптимальный план с учётом различных

факторов, таких как доступные аппаратные ресурсы, схема базы данных, распределение данных и статистика, сложность запроса и системные настройки.

параметры запроса: параметры, передаваемые запросу (опции), которые можно передать вместе с конечной точкой, чтобы повлиять на ответ.

планировщик запросов: компонент сервисных архитектур ИС, который формирует упорядоченный набор шагов, используемых для доступа к данным.

платежная инфраструктура: совокупность организаций и процессов, обеспечивающих обработку и передачу платёжной информации от плательщика к получателю денег.

поведенческий интеллект: применение методов машинного обучения и искусственного интеллекта для анализа поведения пользователей, систем и сетей с целью обнаружения аномалий и угроз в режиме реального времени.

поддержка последовательности запросов (support): последовательности запросов приводящая к возникновению эффектов ИД – это отношение количества последовательностей запросов с к общему числу запросов: $\mathrm{supp}(Q^{item}) = \left|Q^{item}\right| / \left|Q\right|$.

программный интерфейс (ПИ): программный интерфейс, с помощью которого приложения, веб-сервисы и программы обмениваются информацией.

процесс управления компьютерными инцидентами: система взаимосвязанных этапов, направленных на быстрое и эффективное реагирование на сбои, атаки и иные нештатные ситуации в информационных системах организации. Цель — минимизировать ущерб, восстановить нормальную работу и не допустить повторения инцидентов в будущем

проявления эффектов инфраструктурного деструктивизма: информация, оставленная действиями пользователей, систем или злоумышленников в ИС, приводящей к ИД. Например: журналы событий; сетевые потоки; изменения конфигураций; аномалии в данных или процессах.

распределённая информационная система (РИС): информационная система, объекты данных и/или процессы которой физически распределены на две или более компьютерные системы и функционируют в составе единой ИТ-инфраструктуры, включающей программно-аппаратные ресурсы, коммуникационные

средства и организационные компоненты, обеспечивающие взаимодействие, хранение, обработку и передачу информации для удовлетворения информационных потребностей пользователей и поддержки деятельности организации.

сервис: компонент приложения в сервисной архитектуре, который можно разрабатывать, развёртывать, эксплуатировать, изменять и развёртывать повторно, не нарушая работу других сервисов и целостность приложения.

сетевая инфраструктура: совокупность аппаратных, программных и коммуникационных компонентов, которые обеспечивают передачу данных, связь и взаимодействие между устройствами и системами в пределах одной или нескольких сетей.

система расширенного обнаружения и реагирования (XDR, Extended Detection and Response): технология, которая объединяет различные методы обнаружения и реагирования на угрозы безопасности. Она позволяет организациям получать более полную картину угроз и принимать более обоснованные решения о реагировании

система управляемого обнаружения и реагирования (MDR, Managed Detection and Response): служба кибербезопасности, которая помогает активно защищать организации от киберугроз с помощью расширенных возможностей обнаружения и быстрого реагирования на инциденты.

система EDR (Endpoint Detection and Response): технология, предназначенная для обнаружения и реагирования на инциденты безопасности на конечных точках сети. EDR-системы собирают данные с конечных точек и анализируют их на предмет подозрительной активности.

система SIEM (Security Information and Event Management): система, которая собирает, анализирует и коррелирует события безопасности из различных источников. SIEM-системы помогают организациям выявлять аномалии и потенциальные угрозы, а также отслеживать активность пользователей.

система SOAR (Security Orchestration, Automation and Response): платформа, которая автоматизирует процессы обеспечения безопасности, такие как обнаружение угроз, реагирование на инциденты и управление уязвимостями. SOAR-

платформы позволяют организациям быстрее реагировать на угрозы и снижать нагрузку на специалистов по безопасности

точность (accuracy): отсутствие ошибок, искажений или неточностей, позволяющее использовать информацию для принятия решений без дополнительных проверок или коррекции.

убедительность последовательности запросов (Conviction): частота появления набора Q_1^{item} без набора Q_2^{item} : $conv(Q_1^{item} \cup Q_2^{item}) = 1 - \text{supp}(Q_1^{item})/1 - conf(Q_1^{item} \cup Q_2^{item})$.

угроза инфраструктурного генеза (происхождения) : угроза, возникающая не из-за злонамеренных действий человека, а из самой природы и ИТ-инфраструктуры РИС. Источником угрозы является не нарушитель, а структурные особенности, взаимодействия и зависимости между компонентами ИС.

управление журналами событий (log management): процесс сбора, хранения и анализа данных, которые отслеживают каждое действие или событие в программном обеспечении, приложениях и информационной инфраструктуре.

центр обеспечения безопасности (SOC, Security Operations Center): центр, который занимается мониторингом и анализом событий информационной безопасности в организации.

шаблон последовательности запросов: последовательность наборов, которая часто встречается в журналах событий и содержит параметры обработки запросов *Q*.

шлюз программных интерфейсов (API Gateway): серверный прокси, который предоставляет интерфейс для клиентов (приложений, устройств, пользователей) для доступа к сервисам инфраструктуры.

СПИСОК ЛИТЕРАТУРЫ

1. Азбука киберустойчивости. Бизнес в стадии принятия: как подготовиться к тому, что вас все же взломают. – Режим доступа: https://www.kaspersky.ru /blog/cyber-resilience-101/39564/ (дата обращения: 29.05.2025).

2. Айдынов, З. П. Основы прогнозирования временных рядов на основе метода ARIMA / З. П. Айдынов, Н. С. Нуркашева, Р. А. Қарабасов // Статистика, учет и аудит. – 2019. – № 4(75). – С. 184-191.

3. Акимова, Г. П. Моделирование надежности распределённых информационных систем / Г. П. Акимова, А. В. Соловьев, И. А. Тарханов // Информационные технологии и вычислительные системы. – 2019. – № 3. – С. 79-86.

4. Анализ рисков информационной безопасности экономических информационных систем / М. А. Лапина, А. С. Медведева, В. Г. Лапин [и др.] // Auditorium. – 2024. – № 2(42). – С. 79-85.

5. Архитектурные уязвимости моделей телекоммуникационных сетей / М. В. Буйневич, О. В. Щербаков, А. Г. Владыко, К. Е. Израилов // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2015. – № 4. – С. 86-93.

6. Аткина, В. С. Разработка метода, алгоритмов и программы для анализа катастрофоустойчивости информационных систем : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : диссертация на соискание ученой степени кандидата технических наук / Аткина Владлена Сергеевна. – Волгоград, 2013. – 186 с.

7. Ауад, М. Модель распределения ресурсов в сетевых информационных структурах / М. Ауад, Ю. В. Минин, Ю. Ю. Громов // Вестник Воронежского института МВД России. – 2013. – № 4. – С. 215-220.

8. Банк данных угроз безопасности информации: ФСТЭК. [Электронный ресурс]. – Режим доступа: https://bdu.fstec.ru (дата обращения: 29.03.2025).

9. Балябин, А. А. Методика контроля и восстановления целостности вычислительных процессов в информационных системах на основе приобретаемого кибериммунитета / А. А. Балябин // I-methods. – 2022. – Т. 14, № 2.

10. Баранов, В. В. Методика и алгоритмы оценки деструктивного воздействия нарушителей на элементы распределенных информационных систем / В. В. Баранов, А. А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2024. – Т. 27, № 4. – С. 49-60.

11. Баранова, Е. К. Методики анализа и оценки рисков информационной безопасности / Е. К. Баранова // Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73-79.

12. Баранова, Е. К. Сравнительный анализ программного обеспечения для анализа рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-10 / Е. К. Баранова, А. А. Мурзакова, Е. А. Мурзакова // Информационные технологии и вычислительные системы. – 2019. – № 2. – С. 75-83.

13. Барсегян А. А., Куприянов М. С., Степаненко В. В., Холод И. И. Технологии анализа данных: Data Mining, Visual Mining, Text Mining, OLAP: учеб. пособие. 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2007. — 384 с.: ил.

14. Басыня, Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия / Е. А. Басыня // Безопасность информационных технологий. – 2018. – Т. 25. – № 4. – С. 42-51.

15. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. М.: Горячая линия – Телеком, 2006. 544 с.

16. Билятдинов, К. З. Процессы обеспечения устойчивого функционирования информационных систем / К. З. Билятдинов, А. З. Арсеньева // Век качества. – 2023. – № 3. – С. 245-259.

17. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 1. Типы взаимодействий // Защита информации. Инсайд. 2019. № 5 (89). – С. 78-85.

18. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Часть 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 6 (90). – С. 61-65.

19. Булдакова, Т. И. Обеспечение согласованности и адекватности оценки факторов риска информационной безопасности / Т. И. Булдакова, Д. А. Миков // Вопросы кибербезопасности. – 2017. – № 3(21). – С. 8-15.

20. Виноградова, Е. П. Метрики качества алгоритмов машинного обучения в задачах классификации / Е. П. Виноградова, Е. Н. Головин // Научная сессия ГУАП : сборник докладов: в 3 частях, Санкт-Петербург, 10–14 апреля 2017 года. Том Часть II. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2017. – С. 202-206.

21. Витенбург, Е. А. Архитектура программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информационной системы предприятия / Е. А. Витенбург // Вестник кибернетики. – 2019. – № 4(36). – С. 46-51.

22. Вовик, А. Г. О возможности численных метрик в управлении информационной безопасностью / А. Г. Вовик, А. И. Ларин // Наукоемкие технологии в космических исследованиях Земли. – 2022. – Т. 14, № 6. – С. 12-19.

23. Врагов, С. А. Парадигмы программирования в условиях развития языков программирования и компьютерной техники / С. А. Врагов, В. С. Врагов, А. А. Огурцов // Моделирование информационных систем : Материалы Международной научно-практической конференции, Воронеж, 19–20 мая 2021 года. – Воронеж: ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова», 2021. – С. 42-47.

24. Вульфин, А. М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных / А. М. Вульфин // Системная инженерия и информационные технологии. – 2023. – Т. 5, № 4(13). – С. 50-76.

25. Гайфулина, Д. А. Анализ моделей глубокого обучения для задач обнаружения сетевых аномалий интернета вещей / Д. А. Гайфулина, И. В. Котенко // Информационно-управляющие системы. – 2021. – № 1(110). – С. 28-37.

26. Городецкий, В. И. Архитектура базовых агентов многоагентной системы защиты информации в компьютерных сетях / В. И. Городецкий, И. В. Котенко // Известия ТРТУ. – 2000. – № 2(16). – С. 38-51.

27. ГОСТ 34.321-96 Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными. — М.: ИПК Издательство стандартов, 2001. – 118 с.

28. ГОСТ Р 27.102-2021 Надежность в технике. Надежность объекта. Термины и определения. — М.: ИПК Издательство стандартов, 2021. – 43 с.

29. ГОСТ Р 53131-2008 Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. — М.: ИПК Издательство стандартов, 2009. – 113 с.

30. ГОСТ Р 56875-2016 Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорий. — М.: ИПК Издательство стандартов, 2021. – 73 с.

31. ГОСТ Р 56939-2024 Защита информации. Разработка безопасного программного обеспечения. Общие требования. — М.: Российский институт стандартизации, 2024. — 36 с.

32. ГОСТ Р 57700.37-2021 Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения. — М.: ИПК Издательство стандартов, 2021. – 87 с.

33. ГОСТ Р 58771-2019 Менеджмент риска. Технологии оценки риска. — М.: ИПК Издательство стандартов, 2019. – 64 с.

34. ГОСТ Р 58811-2020 Центры обработки данных. Инженерная инфраструктура. — М.: ИПК Издательство стандартов, 2020. – 78 с.

35. ГОСТ Р 57580.1-2017 от 01.01.2018 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. — М.: ИПК Издат-во стандартов, 2017. – 76 с.

36. ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. — М.: ИПК Издательство стандартов, 2022. – 67 с.

37. ГОСТ Р 59547-2021. Государственный стандарт Российской Федерации: «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами». — М.: ИПК Издательство стандартов, 2022. — М.: ИПК Издательство стандартов, 2022. – 45 с.

38. ГОСТ Р 59711-2022. Государственный стандарт Российской Федерации: «Защита информации. Мониторинг информационной безопасности. Общие положения». — М.: ИПК Издательство стандартов, 2021. – 49 с.

39. ГОСТ Р 59712-2022. Государственный стандарт Российской Федерации: «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты». — М.: ИПК Издательство стандартов, 2022. – 54 с.

40. ГОСТ Р 59795-2021 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов. — М.: ИПК Издательство стандартов, 2021. – 92 с.

41. ГОСТ Р 70860-2023 Информационные технологии. Облачные вычисления. Общие технологии и методы. — М.: ИПК Издательство стандартов, 2023. – 87 с.

42. ГОСТ Р ИСО МЭК 18384-1-2017 Информационные технологии. Эталонная архитектура для сервис-ориентированной архитектуры (SOA RA). Часть 1. Терминология и концепции SOA. — М.: ИПК Издательство стандартов, 2017. – 35 с.

43. ГОСТ Р ИСО МЭК 20000-1-2021 Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов. — М.: ИПК Издательство стандартов, 2021. – 44 с.

44. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. — М.: ИПК Издательство стандартов, 2010. – 78 с.

45. Грызунов, В. В. Адаптивное управление доступностью ресурсов геоинформационной системы критического применения в условиях деструктивных воздействий : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : диссертация на соискание ученой степени доктора технических наук / Грызунов Виталий Владимирович. – Санкт-Петербург, 2022. – 395 с.

46. Демидов, Р.А. Унифицированная модель многоуровневых угроз нарушения информационной безопасности в сетях с динамической топологией / Р.А. Демидов, П.Д. Зегжда // Intellect Technologies on Transport. – 2019. – № 2. – С. 10–14.

47. Демидов, А. В. Анализ уязвимостей и разработка требований к безопасности в современной IT-инфраструктуре / А. В. Демидов, А. А. Емельянов // Цифровые опасности информационного общества: Сборник статей / Под редакцией И.Л. Коршунова. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2023. – С. 42-48.

48. Джалолов, А. Ш. Повышение адекватности экспертных оценок при принятии управленческих решений / А. Ш. Джалолов // Теоретические и прикладные аспекты современной науки. – 2014. – № 2-1. – С. 44-47.

49. Дородников, Н. А. Разработка вероятностной поведенческой модели для защиты вычислительной сети с использованием деревьев атак / Н. А. Дородников, С. А. Арустамов // Научно-технический вестник информационных технологий, механики и оптики. – 2016. – Т. 16, № 5. – С. 960-962.

50. Ерастов, В. О. Исследование проблем аудита информационной безопасности географически распределенных устройств Интернета вещей / В. О. Ерастов, Е. А. Зубков, Д. П. Зегжда // Проблемы информационной безопасности. Компьютерные системы. – 2024. – № 4(62). – С. 42-52.

51. Ерофеев А. А. Теория автоматического управления: Учебник для вузов. – 3-е изд., стереотип. СПб.: Политехника, 2015. – 302 с.

52. Есиков, Д. О. Оценка эффективности методов решения задач обеспечения устойчивости функционирования распределенных информационных систем / Д. О. Есиков // Программные продукты и системы. – 2017. – № 2. – С. 241-256.

53. Жернова, В. М. Катастрофоустойчивость информационных систем / В. М. Жернова, Н. В. Плотникова; Министерство науки и высшего образования Российской Федерации, Южно-Уральский государственный университет, Кафедра «Защита информации». – Челябинск: Издательский центр ЮУрГУ, 2020. – 90 с.

54. Зефиров, С.Л. Способы оценки информационной безопасности организации / С.Л. Зефиров, В.М. Алексеев // Труды Международного симпозиума «Надежность и качество»: в 2-х томах. – Пенза: Федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный университет», 2011. – 2 т. – 692 с.

55. Иброхимова, Н. П. Современные методы и средства обеспечения информационной безопасности / Н. П. Иброхимова // Экономика и социум. – 2024. – № 8(123). – С. 266-270.

56. Иваненко, В. Г. Оценка рисков информационной безопасности автоматизированных систем управления технологическим процессом / В. Г. Иваненко, Н. Д. Иванова // Вопросы кибербезопасности. – 2024. – № 1(59). – С. 116-123.

57. Иванов, А. В. Информационная безопасность в технологиях виртуализации / А. В. Иванов, С. А. Меркурьев, Л. О. Чернышев // Информационные ресурсы и системы в экономике, науке и образовании : Сборник статей VIII Международной научно-практической конференции, Пенза, 26–27 апреля 2018 года. – Пенза: Автономная некоммерческая научно-образовательная организация «Приволжский Дом знаний», 2018. – С. 29-32.

58. Израилов, К. Е. Метод обнаружения атак различного генеза на сложные объекты на основе информации состояния. Часть 2. Алгоритм, модель и эксперимент / К. Е. Израилов, М. В. Буйневич // Вопросы кибербезопасности. – 2023. – № 4(56). – С. 80-93.

59. Имитационное моделирование эпидемий компьютерных вирусов / В. А. Минаев, М. П. Сычев, Е. В. Вайц, А. Э. Киракосян // Вестник Российского нового

университета. Серия: Сложные системы: модели, анализ и управление. – 2019. – № 3. – С. 3-12.

60. 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.

61. ИТ-архитектура от А до Я: Теоретические основы // Системный администратор. – 2020. – № 6(211). – С. 30-40.

62. Исходный код интеллектуальной самообучающейся системы распознавания лиц «Персона ID». [Электронный ресурс]. – Режим доступа: https://github.com/RusAl84/PersonaID/ (дата обращения: 7.02.2025).

63. Исходный код интеллектуальной самообучающейся системы распознавания лиц «Персона ID». [Электронный ресурс]. – Режим доступа: https://gitverse.ru/RusAl84/PersonaID/ (дата обращения: 7.02.2025).

64. Исходный код системы моделирования вирусной активности на основе эпидемиологической SEIR модели с учетом антропоморфических состояний. URL: https://github.com/RusAl84/Destr_SIER (дата обращения: 3.10.2024).

65. Как можно и нужно пользоваться метриками информационной безопасности – Режим доступа: https://habr.com/ru/articles/827178/ (дата обращения: 17.09.2024).

66. Как UEBA помогает повышать уровень кибербезопасности – Режим доступа: https://habr.com/ru/companies/roi4cio/articles/436082/ (дата обращения: 7.10.2024).

67. Касс, А. К. «Архитектура предприятия», «информационная структура», «информационная инфраструктура»: уточнение терминологии / А. К. Касс // Неделя науки СПбПУ : материалы научной конференции с международным участием, Санкт-Петербург, 13–19 ноября 2017 года. Том Часть 2. – Санкт-Петербург: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого», 2017. – С. 44-46.

68. Клеппман М. Высоконагруженные приложения. Программирование, масштабирование, поддержка. – СПб.: Питер, 2018. – 640 с.

69. Клочкова, А. М. Возможности использования защищенной, киберимунной операционной системы Kaspersky OS для дистанционного управления мобильным роботом / А. М. Клочкова, Н. А. Максимов // Информационные технологии в деятельности органов внутренних дел: Сборник научных статей Всероссийской научно-практической конференции, Москва, 20 апреля 2023 года. – Москва: Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя, 2023. – С. 205-208.

70. Кокурин, Д.И. Формирование и реализация инфраструктурного потенциала экономики России / Д.И. Кокурин, К.Н. Назин. – М.: Транслит, 2011. – С. 58–336 с.

71. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ / пер. с англ. — 3-е изд. — М.: Вильямс, 2013. — 1328 с.

72. Корпоративная ИТ-инфраструктура 2.0 на ПАК Скала^р: суверенный ИТ-ландшафт в сжатые сроки взамен лавины проектов. – Режим доступа: https://www.tadviser.ru/index.php/ Статья: Корпоративная_ИТ-инфраструктура_2.0 (дата обращения: 17.09.2024).

73. Корпоративная ИТ-инфраструктура 2.0 (TAdviser.ru) – Режим доступа: https://infra.tadviser.ru/ (дата обращения: 17.09.2024).

74. Котенко, И.В. Анализ моделей и методик, используемых для атрибуции нарушителей кибербезопасности при реализации целевых атак / И. Котенко, С. С. Хмыров // Вопросы кибербезопасности. – 2022. – № 4(50). – С. 52-79.

75. Котенко, И. В. Имитационное моделирование механизмов защиты компьютерных сетей от инфраструктурных атак на основе подхода «нервная система сети»/ И. В. Котенко, А. В. Шоров // Труды СПИИРАН. – 2012. – № 3(22). – С. 45-70.

76. Костенко, А. Т. Особенности тестирования современных архитектур: микросервисы / А. Т. Костенко, А. З. Ядута // Современные методы и инновации в науке : Сборник статей XL международной научной конференции, Санкт-

Петербург, 09 декабря 2024 года. – Санкт-Петербург: Гуманитарный национальный исследовательский институт НАЦРАЗВИТИЕ, 2024. – С. 37-39.

77. Котенко, И. В. Оценка рисков в компьютерных сетях критических инфраструктур / И. В. Котенко, И. Б. Саенко, Е. В. Дойникова // Инновации в науке. – 2013. – № 16-1. – С. 84-88.

78. Лапсарь, А. П. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам / А. П. Лапсарь, С. А. Назарян, А. И. Владимирова // Вопросы кибербезопасности. – 2022. – № 2(48). – С. 39-51.

79. Лось, В. П. Методы интеллектуального анализа данных, применяемые в задаче обнаружения вторжений / В. П. Лось, Д. Д. Маланьин // Информация и безопасность. – 2022. – Т. 25, № 4. – С. 599-608.

80. Ланцов, А. Е. Инфраструктура: понятие, виды и значение / А. Е. Ланцов // Экономика, статистика и информатика. Вестник УМО. – 2013. – № 3. – С. 49-54.

81. Левшун, Д. А. Обнаружение и объяснение аномалий в индустриальных системах Интернета вещей на основе автокодировщика / Д. А. Левшун, Д. С. Левшун, И. В. Котенко // Онтология проектирования. –2025. –Т.15, № 1(55). –С.96-113.

82. Любухин, А. С. Методы анализа рисков информационной безопасности: нечеткая логика / А. С. Любухин // International Journal of Open Information Technologies. – 2023. – Т. 11, № 2. – С. 66-71.

83. Макаренко, С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса / С. И. Макаренко // Системы управления, связи и безопасности. – 2017. – № 1. – С. 60-97.

84. Макаренко, С. И. Защита компьютерных сетей и телекоммуникаций: Учебное пособие / С. И. Макаренко. – Санкт-Петербург: ООО «Корпорация «Интел Групп», 2024. – 311 с.

85. Максимова, Е. А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры / Е. А. Максимова // Информатизация и связь. – 2022. – № 1. – С. 68-74.

86. Максимова, Е.А. Инфраструктурный деструктивизм субъектов критической информационной инфраструктуры: монография / Е.А. Максимова. – М., Волгоград: Волгоградский государственный университет, 2021. – 181 с.

87. Максимова, Е. А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры / Е. А. Максимова // Труды учебных заведений связи. – 2020. – Т. 6, № 4. – С. 91-103.

88. Максимова, Е.А. Оценка информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях: монография / Е.А. Максимова. – Волгоград: Изд-во ВолГУ. – 2020. – 95 с.

89. Максимова, Е. А. Метод оценки инфраструктурной устойчивости субъектов критической информационной инфраструктуры / Е. А. Максимова, М. В. Буйневич // Вестник УрФО. Безопасность в информационной сфере. – 2022. – №1(43). – С. 50-63.

90. Максимова Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза: диссертация на соискание ученой степени доктора технических наук / Е.А. Максимова, 2022. – 456 с.

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

92. Максимова, Е.А. Современные технологии и информационные войны / Е.А. Максимова, В.В. Баранов, Г.Н. Чурилин // Состояние и перспективы развития современной науки по направлению «Информационная безопасность»: Сборник статей II Всероссийской научно-технической конференции (Анапа, 19–20 марта 2020 г.). – Анапа: ФГАУ «Военный инновационный технополис «ЭРА», 2020. – С. 137–147.

93. Маклафлин, Л. Управляемые услуги, сервисы хостинга и облачные сервисы: в чем разница? / Л. Маклафлин // БИТ. Бизнес & Информационные технологии. – 2022. – № 4(117). – С. 39-41.

94. Малюк А.А, Горбатов В.С., Королев В.И., Фомичев В.И., Дураковский А.П., Кондратьева Т.А. Ведение в информационную безопасность. М.: Горячая линия – Телеком, 2014. – 288 с.

95. Мамойленко, С. Н. Алгоритмы планирования решения масштабируемых задач на распределённых вычислительных системах / С. Н. Мамойленко, А. В. Ефимов // Вестник СибГУТИ. – 2010. – № 2(10). – С. 66-79.

96. Марков, А. С. Техническая защита информации. Курс лекций: Учебное пособие для слушателей, обучающихся по курсу «002. Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа» / А. С. Марков. – Москва: АИСНТ, 2020. – 234 с.

97. Мартин Р. Чистая архитектура. Искусство разработки программного обеспечения. – Питер, 2022. – 362 с.

98. Менщиков, А. Киберустойчивость систем искусственного интеллекта: учебно-методическое пособие / А. Менщиков, Н. Кармановский. – Санкт-Петербург: ИТМО, 2024. – 52 с.

99. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения / И. В. Котенко, И. Б. Саенко, О. С. Лаута, А. М. Крибель // Информатика и автоматизация. – 2022. – Т. 21, № 6. – С. 1328-1358.

100. Методики оценки рисков для информационных систем. [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/practice/methods/risk-assessment-methods-for-information-systems (дата обращения: 24 марта 2024 года).

101. Методический документ. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05 февраля 2021 г.). ФСТЭК. [Электронный ресурс]. – Режим доступа: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 29.05.2025).

102. Метрики здоровья ИТ-инфраструктуры, пороговые значения и пользователи ИТ-сервисов [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/prolan/articles/182504/ (дата обращения: 11.09.2024).

103. Милославская, Н. Г. Управление информационной безопасностью: Конспект лекций / Н. Г. Милославская, А. И. Толстой; Международный научно-методический центр. – М.: Национальный исследовательский ядерный университет «МИФИ», 2020. – 536 с.

104. Михельсон, О. Ю. Инфраструктура как код: обзор и применение / О. Ю. Михельсон // Актуальные исследования. – 2023. – № 20-1(150). – С. 57-59.

105. Мухаметшин, В. Н. Сервис-ориентированная архитектура и BPM / В. Н. Мухаметшин // Инновационные, информационные и коммуникационные технологии. – 2018. – № 1. – С. 331-334.

106. Наумова, К. С. Безопасность виртуальной контейнеризации в ИТ-технологиях / К. С. Наумова, А. В. Переспелов // Информационные технологии и системы: управление, экономика, транспорт, право. – 2020. – № 4(40). – С. 22-25.

107. Национальный проект «Экономика данных и цифровая трансформация государства», Период реализации нацпроекта — с 2025 по 2030 годы. [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/target/naczionalnyj-proekt-ekonomika-dannyh-i-czifrovaya-transformacziya-gosudarstva (дата обращения: 01.06.2024).

108. Никитин, И. В. Сравнение подходов монолитной архитектуры и микросервисной архитектуры при реализации серверной части веб-приложения / И. В. Никитин, Т. Ю. Гриценко // Дневник науки. – 2020. – № 3(39). – С. 22.

109. Нуриев, М. Р. Кибериммунный подход к защите промышленного IoT / М. Р. Нуриев // Автоматизация в промышленности. – 2021. – № 7. – С. 12-15.

110. Одоевский, С. М. Метод повышения устойчивости функционирования системы управления инфокоммуникационной сетью специального назначения в условиях воздействия дестабилизирующих факторов / С. М. Одоевский, П. В. Лебедев // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2022. – № 9-10(171-172). – С. 88-95.

111. Организационно-техническое обеспечение устойчивости функционирования и безопасности сетей связи общего пользования / М. В. Буйневич, А. Г. Владыко, С. М. Доценко, О. А. Симонина. – Санкт-Петербург : Санкт-Петербургский

государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2013. – 144 с.

112. Остапенко, Г. А. Предупреждение и минимизация последствий компьютерных атак на элементы критической информационной инфраструктуры и автоматизированные информационные системы критически важных объектов: риск-анализ и оценка эффективности защиты / А. Г. Остапенко, Е. В. Ермилов, А. Н. Шершень [и др.] // Информация и безопасность. – 2013. – Т. 16. – № 2. – С. 167-178.

113. Оценка и анализ рисков: процесс и методы. [Электронный ресурс]. – Режим доступа: https://visuresolutions.com/ru/alm-guide/risk-assesment-and-analysis/ (дата обращения: 3.03.2024).

114. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей / И. В. Котенко, И. Б. Саенко, М. А. Коцыняк, О. С. Лаута // Труды СПИИРАН. – 2017. – № 6(55). – С. 160-184.

115. Павлович, Н. В. Оптимизация запросов в Greenplum / Н. В. Павлович // Электронные системы и технологии: Сборник материалов 58-й научной конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18–22 апреля 2022 года. – Минск: Белорусский государственный университет информатики и радиоэлектроники, 2022. – С. 53-56.

116. Пищугина, Е. М. Возможности применения API технологий в разработке web-сайтов / Е. М. Пищугина, М. Ю. Пивненко, Р. С. Панов // Инновационное развитие техники и технологий в промышленности : Сборник материалов Всероссийской научной конференции молодых исследователей с международным участием, Москва, 16 апреля 2024 года. – Москва: Российский государственный университет имени А.Н. Косыгина (Технологии. Дизайн. Искусство), 2024. – С. 155-157.

117. Поиск последовательных шаблонов. Часть 2. Алгоритм AprioriAll. [Электронный ресурс]. – Режим доступа: https://loginom.ru/blog/sequential-patterns-2#алгоритм-aprioriall (дата обращения: 14.09.2024).

118. Положение Банка России № 719-П от 04.06.2020. О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и

о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств. [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/74609682/ (дата обращения: 14.02.2024).

119. Положение Банка России № 821-П от 17.08.2023 О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств. [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/408082189/ (дата обращения: 16.02.2024).

120. Полтавцева, М. А. Многоуровневая концепция безопасности систем управления большими данными / М. А. Полтавцева, Д. П. Зегжда, М. О. Калинин // Вопросы кибербезопасности. – 2023. – № 5(57). – С. 25-36.

121. Постановление Правительства РФ от 28.11.2011 N 977 «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (с изменениями и дополнениями). [Электронный ресурс]. – Режим доступа: https://base.garant.ru/12192469/ (дата обращения: 16.01.2024).

122. Постановление Правительства РФ № 258 от 01.03.2024 «Об утверждении требований к антитеррористической защищенности объектов (территорий) промышленности, находящихся в ведении или относящихся к сфере деятельности Министерства промышленности и торговли РФ, и формы паспорта безопасности этих объектов». [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/408551807/ (дата обращения: 26.01.2024).

123. Приказ Минздрава № 911н от 24.12.2018 Требования к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и

информационным системам. [Электронный ресурс]. – Режим доступа: https://www.garant.ru/ products/ipo/prime/doc/72117630/ (дата обращения: 29.01.2024).

124. Приказ Минцифры России от 12.05.2023 N 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц» (Зарегистрировано в Минюсте РФ 30.05.2023 n 73620). [Электронный ресурс]. – Режим доступа: http://publication.pravo.gov.ru/document/0001202305310045 (дата обращения: 17.01.2024).

125. Приказ Федеральной службы безопасности России № 282 от 19.06.2019 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/72198410/ (дата обращения: 23.01.2024).

126. Применение методов машинного обучения к задачам обнаружения вредоносного программного обеспечения / И. В. Абашева, М. А. Еремеев, А. А. Криулин [и др.] // Труды Военно-космической академии имени А.Ф.Можайского. – 2020. – № 675. – С. 164-171.

127. 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.

128. Распоряжение Правительства Российской Федерации от 28 июля 2017 года № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации». [Электронный ресурс]. – Режим доступа: http://government.ru/docs/28653/ (дата обращения: 24 марта 2024 года).

129. Рассветалова, А. Д. Методы поведенческого анализа атак на искусственный интеллект и машинное обучение / А. Д. Рассветалова, М. А. Полтавцева // Неделя науки ИКНК: Материалы докладов научно-практической конференции, Санкт-Петербург, 15–17 апреля 2024 года. – Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого, 2024. – С. 91-94.

130. Рекомендации по созданию инфраструктуры доверия системы цифрового рубля / Д. А. Мельников, Д. А. Будников, И. Г. Коннова, А. В. Кубаев // Безопасность информационных технологий. – 2024. – Т. 31, № 3. – С. 43-63.

131. Риски информационной безопасности. [Электронный ресурс]. – Режим доступа: https://rt-solar.ru/products/solar_dozor/blog/3320/ (дата обращения: 28.03.2024).

132. 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.

133. 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.

134. 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.

135. Русаков А. М. Интеллектуальная самообучающаяся система распознавания лиц // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. – 2025. – №3. – С. 97-107.

136. 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. – № 6/2. – С. 180-186.

137. 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. – EDN CFSKVG.

138. 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.

139. 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.

140. 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.

141. Русаков А.М. Мессенджер с возможностью интеллектуального анализа текста (онлайн обучающий курс на платформе Stepik) [Электронный ресурс]. – Режим доступа: https://stepik.org/course/182501/promo (дата обращения: 7.05.2025)

142. 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.

143. 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.

144. 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.

145. Русаков А.М. Разработка модели динамики рисков деструктивного воздействия инфраструктурного генеза // 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.

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

147. Русаков, А. М. Эпидемиологическая модель оценки динамики рисков информационной безопасности инфраструктурного генеза / А. М. Русаков // Студенческая наука для развития информационного общества: Материалы XУ Всероссийской научно-технической конференции с приглашением зарубежных ученых, Ставрополь, 28 ноября 2023 года. – Ставрополь: Северо-Кавказский федеральный университет, 2024. – С. 257-269.

148. Селезнев, С. П. Архитектура промышленных приложений IoT и протоколы AMQP, MQTT, JMS, REST, XMPP, DDS / С. П. Селезнев, В. В. Яковлев // International Journal of Open Information Technologies. – 2019. – Т. 7, № 5. – С. 17-28.

149. Свидетельство о государственной регистрации программы для ЭВМ № 2024660851 Российская Федерация. «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.].

150. Свидетельство о государственной регистрации программы для ЭВМ № 2023665252 Российская Федерация. 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.].

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

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

153. Свидетельство о государственной регистрации программы для ЭВМ № 2022660792 Российская Федерация. Программное обеспечение для имитационного моделирования противоборства групп агентов, управляемых роевым интеллектом: № 2022660018: заявл. 27.05.2022: опубл. 09.06.2022 / А. М. Русаков, В. В. Филатов, О. И. Ешкина [и др.].

154. Свидетельство о государственной регистрации программы для ЭВМ № 2023683118 Российская Федерация. Антропоморфическая система моделирования деструктивных воздействий инфраструктурного генеза на объектах критической информационной инфраструктуры: № 2023682500: заявл. 24.10.2023: опубл. 03.11.2023 / А. М. Русаков.

155. Свидетельство о государственной регистрации программы для ЭВМ № 2023683475 Российская Федерация. «Эпидемиологическая система моделирования оценки рисков динамики межобъектного влияния в условиях инфраструктурного

деструктивизма»: № 2023682859: заявл. 24.10.2023: опубл. 038.11.2023 / А. М. Русаков.

156. Свидетельство о государственной регистрации программы для ЭВМ № 2023683299 Российская Федерация. 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.

157. Свидетельство о государственной регистрации программы для ЭВМ № 2022683265 Российская Федерация. 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.].

158. Свидетельство о государственной регистрации программы для ЭВМ № 2025615420 Российская Федерация. Интеллектуальная самообучающаяся система распознавания лиц «Персона ID»: №2025612866: заявл. 12.02.2025: опубл. 04.03.2025 / А. М. Русаков.

159. Свидетельство о государственной регистрации программы для ЭВМ № 2025614582 Российская Федерация. 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.

160. Системно-динамическое моделирование распространения компьютерных вирусов / В. А. Минаев, Е. В. Вайц, А. В. Корячко, А. Э. Киракосян // Технологии техносферной безопасности. – 2017. – № 3(73). – С. 220-229.

161. Системный аналитик. Краткий гайд по профессии. Часть 1. Основы взаимодействия систем. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/841646/ (дата обращения: 1.10.2024).

162. Солянов, Д. А. Стратегии повышения уровня киберустойчивости в корпоративной инфраструктуре / Д. А. Солянов, Д. Р. Тимирянова // Международный студенческий научный вестник. – 2025. – № 1. – С. 11.

163. Современное программирование: материалы III Международной научно-практической конференции, Нижневартовск, 27–29 ноября 2020 года. – Нижневартовск: Нижневартовский государственный университет, 2021. – 314 с.

164. Созонтов, А. В. Распределенные информационные системы: особенности применения и построения / А. В. Созонтов // Актуальные исследования. – 2023. – № 37-1(167). – С. 69-74.

165. Сотавов, А. К. Современные объектно-ориентированные языки программирования / А. К. Сотавов. – Санкт-Петербург: Санкт-Петербургский государственный экономический университет, 2020. – 90 с.

166. Сухова, А. Р. Метрики информационной безопасности / А. Р. Сухова, Т. Р. Гатиятуллин // Символ науки: международный научный журнал. – 2015. – № 12-1. – С. 83-84.

167. Таненбаум Э., Бос Х. Современные операционные системы. – Питер, 2024. – 1120 с.

168. Татаринов, В. В. Глоссарий терминов, применяемых в управлении риском проектов : учебное пособие / В. В. Татаринов. – М.: Постер-М, 2025. – 112с.

169. Тестовый набор базы данных «DVD RENTAL» для системы управления базами данных PostgreSQL [Электронный ресурс]. – Режим доступа: https://github.com/gordonkwokkwok/DVD-Rental-PostgreSQL-Project (дата обращения: 1.09.2024)

170. Технологии MDR, SOC, EDR, XDR, SOAR и SIEM, что это все означает? [Электронный ресурс]. – Режим доступа: https://www.protect.airbus.com/blog/ cyber security-jargon-busting-mdr-soc-edr-xdr-soar-and-siem/ (дата обращения: 1.08.2024)

171. Тимошенков, С. П. Основы теории надежности: учебник и практикум для вузов / С. П. Тимошенков, Б. М. Симонов, В. Н. Горошко. — Москва: Издательство Юрайт, 2023. — 445 с. — (Высшее образование). — ISBN 978-5-9916-8193-3. [Электронный ресурс]. – Режим доступа: https://urait.ru/bcode/511353 (дата обращения: 17.08.2024).

172. Тарасенко, О. А. Понятие и классификация банковской инфраструктуры / О. А. Тарасенко // Право и экономика. – 2014. – № 5(314). – С. 73-79.

173. Травкина, Е. А. Анализ и защита от APT-атак в корпоративных сетях / Е. А. Травкина, Э. В. Бирих // Научный аспект. – 2024. – Т. 49, № 4. – С. 6522-6529.

174. Трофимов, В. В. Алгоритмизация и программирование : Учебник / В. В. Трофимов, Т. А. Павловская. – 1-е изд.. – М.: Издательство Юрайт, 2019. – 137 с.

175. Указ Президента РФ от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года». [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/50542 (дата обращения: 3.07.2024).

176. Управление инцидентами. [Электронный ресурс]. – Режим доступа: https://infosecportal.ru/stati/upravlenie-inczidentami/ (дата обращения: 28.07.2024)

177. Факур М., Груздев А.В. Причинно-следственный анализ для смелых и честных: учебное пособие / М. Факур, А.В. Груздев. – М.: ДМК Пресс, 2025. – 594с.

178. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ. [Электронный ресурс]. – Режим доступа: https://base.garant.ru/71730198/ (дата обращения: 23.03.2024)

179. Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ. [Электронный ресурс]. – Режим доступа: https://base.garant.ru/406051675/ (дата обращения: 30.07.2024)

180. Филимонов, А. А. Микросервисная архитектура в основе создания динамической ИТ инфраструктуры предприятия / А. А. Филимонов // Инжиниринг предприятий и управление знаниями (ИП&УЗ-2024) : сборник научных трудов XXVII Российской научной конференции : в 2 т., Москва, 28–29 ноября 2024 года. – Москва: Российский экономический университет имени Г.В. Плеханова, 2024. – С. 344-351.

181. Фримен Эрик, Робсон Элизабет, Сьерра Кэти, Бейтс Берт Х Head First. Паттерны проектирования. 2-е изд. СПб.: Питер, – 2022. – 640 с.

182. Ченцов, С. В. Обеспечение устойчивости информационных систем с учётом человеческого фактора / С. В. Ченцов, И. З. Краснов, А. А. Сидарас // Фундаментальные исследования. – 2017. – № 11-1. – С. 140-144.

183. Черемисина, М. И. Обзор сетевых проблем / М. И. Черемисина // Проблемы и перспективы внедрения инновационных телекоммуникационных технологий: Сборник материалов VIII Международной научно-практической очно-заочной конференции, Оренбург, 25 марта 2022 года. – Оренбург: Оренбургский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики», 2022. – С. 197-203.

184. Царегородцев, А. В. Современные вызовы системе подготовки кадров в области информационной безопасности / А. В. Царегородцев, А. А. Малюк, С. Д. Волков // Информационное общество. – 2025. – № 2. – С. 119-130.

185. Центральный банк Российской Федерации: Цифровой рубль [Электронный ресурс]. – Режим доступа: https://cbr.ru/fintech/dr/ (дата обращения: 11.09.2024)

186. Цифровые платформы. Методологии. Применение в бизнесе: Коллективная монография / М. Л. Аншина, Е. П. Зараменских, Н. С. Казанцев [и др.]; Под общ. ред. Славина Б.Б., Зараменских Е.П., Механджиева Н.. – Москва: Общество с ограниченной ответственностью «Издательство Прометей», 2019. – 228 с.

187. Швырев, Б. А. Выявление уязвимостей информационной безопасности в IT-инфраструктуре / Б. А. Швырев, А. С. Макарян. – Москва: Федеральное казенное учреждение Научно-исследовательский институт Федеральной службы исполнения наказаний Российской Федерации, 2018. – 174 с.

188. Швырев, Б. А. Эффективная защита информационной безопасности в IT-инфраструктуре / Б. А. Швырев, А. С. Макарян. – Москва: Федеральное казенное учреждение Научно-исследовательский институт Федеральной службы исполнения наказаний Российской Федерации, 2018. – 172 с.

189. Шелухин, О. И. Диагностика «здоровья» компьютерной сети на основе секвенциального анализа последовательностных паттернов / О. И. Шелухин, А. В.

Осин, Д. В. Костин // T-Comm: Телекоммуникации и транспорт. – 2020. – Т. 14, №2. – С. 9-16.

190. Шелухин, О. И. Мониторинг аномальных состояний компьютерных систем средствами интеллектуального анализа данных системных журналов / О. И. Шелухин, Д. В. Костин // Нейрокомпьютеры: разработка, применение. – 2020. – Т. 22, № 2. – С. 53-65.

191. Шелухин, О. И. Мониторинг и структура аномальных паттернров системных журналов компьютерных систем / О. И. Шелухин, Д. В. Костин, И. Ю. Резник // REDS: Телекоммуникационные устройства и системы. – 2020. – Т. 10, №2. – С. 3-8.

192. Шитиков, В. К. Классификация, регрессия и другие алгоритмы Data Mining с использованием R / В. К. Шитиков, С. Э. Мастицкий. – Тольятти: Creative Commons, 2017. – 351 с.

193. Хардиков, М. В. Гонка данных и условия соревнования: что это и как с этим бороться / М. В. Хардиков, Д. Е. Эминджонов // Научный Лидер. – 2025. – № 6(207). – С. 40-42.

194. Хасанова, А. М. Интеллектуальный анализ процессов по данным журналов событий информационных систем / А. М. Хасанова // International Journal of Open Information Technologies. – 2022. – Т. 10, № 10. – С. 70-77.

195. Хорев А.А. Проблемные вопросы подготовки специалистов по технической защите информации //Защита информации. Инсайд, 2016, №1(67). – С.24-32.

196. Этапы APT-атак. База знаний Positive Technologies. [Электронный ресурс]. – Режим доступа: https://cbr.ru/fintech/dr/ (дата обращения: 18.09.2023).

197. Язов Ю.К., Соловьев С.В. Защита информации в информационных системах от несанкционированного доступа. Воронеж: Кварта, 2015. 440 с.

198. Alibaba Cluster Trace Program. [Электронный ресурс]. – Режим доступа: https://github.com/alibaba/clusterdata/ (дата обращения: 26.10.2024).

199. Best Practices for API Security in 2024 [Электронный ресурс]. – Режим доступа: https://www.geeksforgeeks.org/api-security-best-practices/ (дата обращения: 21.11.2024).

200. Brewer, E. A. A Certain Freedom: Thoughts on the CAP Theorem / E. A. Brewer // Proceeding of the XXIX ACM SIGACT-SIGOPS symposium on Principles of distributed computing. – N. Y. : ACM, 2010. – Vol. 29, № 1. – P. 335-336.

201. Brzychczy, E. Data analytic approaches for mining process improvement-machinery utilization use case / E. Brzychczy, P. Gackowiec, M. Liebetrau // Resources. – 2020. – Vol. 9, No. 2. – P. 17. – DOI 10.3390/resources9020017.

202. C-View – Зонтичная Full-stack платформа мониторинга. [Электронный ресурс]. – Режим доступа: https://www.secure-ly.com (дата обращения: 15.10.2024)

203. DeepTraLog: Trace-Log Combined Microservice Anomaly Detection through Graph-based Deep Learning: [Электронный ресурс]. – Режим доступа: https://github.com/FudanSELab/DeepTraLog (дата обращения: 26.10.2024).

204. Enberg A. Machine Learning Based Detection of Anomalous User Behavior / A. Enberg // Theseus Journal. – 2023. – 45 p.

205. Google cluster workload traces [Электронный ресурс]. – Режим доступа: https://github.com/google/cluster-data (дата обращения: 26.10.2024).

206. Haroon M. et al. A proactive approach to fault tolerance using predictive machine learning models in distributed systems //Int. J. Exp. Res. Rev. – 2024. – T. 44. – P. 208-220.

207. Holt J. A model-based methodology to support systems security design and assessment / J. Holt // Journal of Systems Architecture. – 2023. – P. 211-227.

208. IBM: What is IT infrastructure? [Электронный ресурс]. – Режим доступа: https://www.ibm.com/topics/infrastructure (дата обращения: 17.03.2024)

209. Keeling M. J., Eames K. T. D. Networks and epidemic models //Journal of the royal society interface. – 2005. – T. 2. – №. 4. – С. 295-307.

210. 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.

211. 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.

212. Margański, P. REST and GraphQL comparative analysis / P. Margański, B. Pańczyk // Journal of Computer Sciences Institute. – 2021. – Vol. 19. – P. 89-94.

213. Mariani L. et al. Predicting failures in multi-tier distributed systems //Journal of Systems and Software. – 2020. – Т. 161. – С. 450-464.

214. Max Patrol SIEM. Обзор системы управления событиями информационной безопасности [Электронный ресурс]. – Режим доступа: https://habr.com /ru/companies/tssolution/articles/495280/ (дата обращения: 13.10.2024).

215. Microsoft Azure trace data [Электронный ресурс]. – Режим доступа: https://github.com/Azure/AzurePublicDataset (дата обращения: 23.10.2024).

216. MITRE Matrix ATT&CK. [Электронный ресурс]. – Режим доступа: https://attack.mitre.org/ (дата обращения: 15.12.2023).

217. Monq – Корпоративный ИТ-мониторинг нового поколения. [Электронный ресурс]. – Режим доступа: https://monq.ru/ (дата обращения: 23.10.2024).

218. Monitoring by Service Operation Status (NOC). [Электронный ресурс]. – Режим доступа https://www.inoc.com/network-operations-center (дата обращения: 24.10.2024).

219. Performance and Latency Efficiency Evaluation of Kubernetes Container Network Interfaces for Built-In and Custom Tuned Profiles / V. Dakić, Ja. Redžepagić, M. Bašić, L. Žgrablić // Electronics. – 2024. – Vol. 13, No. 19. – P. 3972-3986.

220. Shostack A. Threat Modeling: Designing for Security / A. Shostack. – Indianapolis: Wiley, 2014. – 624 p.

221. Shutian Luo, Huanle Xu, Chengzhi Lu, Kejiang Ye, Guoyao Xu, Liping Zhang, Yu Ding, Jian He, and Chengzhong Xu. 2022. Characterizing Microservice Dependency and Performance: Alibaba Trace Analysis. In SoCC ’21: ACM Symposium on Cloud Computing, Seattle, WA, USA, November 1 - 4, – 2022, Carlo Curino, Georgia Koutrika, and Ravi Netravali (Eds.). – P. ACM, 412–426.

222. Singer P. W. Cybersecurity and Cyberwar: What Everyone Needs to Know / P. W. Singer, A. Friedman. – Oxford: Oxford University Press, 2014. – 320 p.

223. Wilensky, U. (1999). NetLogo. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL. [Электронный ресурс]. – Режим доступа: http://ccl.northwestern.edu/netlogo/ (дата обращения: 09.10.2024)..

224. Security Operation Center (SOC) на пальцах: из чего состоит и кому нужен. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/770564 (дата обращения: 13.10.2024).

225. System Design 101. [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/775844 (дата обращения: 11.10.2024).

226. Wang Y. et al. Time-Series Learning for Proactive Fault Prediction in Distributed Systems with Deep Neural Structures. [Электронный ресурс]. – Режим доступа: https://arxiv.org/pdf/2505.20705 (дата обращения: 08.07.2025).

227. Whitman M. Principles of Information Security / M. Whitman, H. Mattord. – 7th ed. – Boston: Cengage Learning, 2021. – 672 p.

228. Zhang C. et al. Deeptralog: Trace-log combined microservice anomaly detection through graph-based deep learning //Proceedings of the 44th international conference on software engineering. – 2022. – P. 623-634.

ПРИЛОЖЕНИЕ А. Акты внедрения результатов диссертационной работы

Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМИ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н. ЗИНИЧЕВА» (СПб УГПС МЧС РОССИИ)

УТВЕРЖДАЮ

Заместитель начальника
Санкт-Петербургского университета
ГПС МЧС России
доктор технических наук

А.В. Шестаков

«__» _____ 2025 г.

АКТ

о внедрении научных результатов диссертационной работы
Русакова Алексея Михайловича

Комиссия из числа профессорско-преподавательского состава кафедры прикладной математики и безопасности информационных технологий под председательством заведующего кафедрой кандидата технических наук, доцента Матвеева А.В., и членов комиссии – профессора кафедры доктора технических наук, профессора Буйневича М.В., профессора кафедры доктора технических наук, доцента Грызунова В.В., профессора кафедры кандидата технических наук, доцента Израилова К.Е., доцента кафедры кандидата юридических наук, доцента Метелькова А.Н., составила настоящий акт в том, что научные статьи «Проактивная оценка динамики рисков инфраструктурного деструктивизма для распределенной системы распознавания лиц», «Комплекс антропоморфических моделей поведенческого анализа процессов для обнаружения эффектов инфраструктурного деструктивизма», «Алгоритмическая реализация модели оценки эффектов инфраструктурного деструктивизма информационно-технологической инфраструктуры», «Прогнозирование рисков инфраструктурного деструктивизма с помощью антропоморфического подхода для сервисной архитектуры», опубликованные Русаковым А.М. в рецензируемых изданиях «Защита информации. Инсайд» (2025, № 2, № 4), «Инженерный вестник Дона» (2024, № 11), «Современная наука: актуальные проблемы теории и практики» (2025, № 1), а также предоставленные им результаты инструментальной оценки, полученные на основе реализации авторской методики проверки (апробации) распределенной системы ситуационного мониторинга, были использованы в научно-исследовательской работе «Исследование способов мониторинга и реагирования на возможные инциденты информационной безопасности в цифровой информационной инфраструктуре МЧС России и разработка организационно-технических предложений по их реализации» (шифр «Кибермониторинг», рег. № НИОКТР 125031703734-4) при научном обосновании и доказательстве применимости антропоморфического подхода к выявлению эффектов инфраструктурного деструктивизма в сервис-ориентированных информационных системах, что расширило направленность проблематики исследований, и которые ранее в подобных исследованиях традиционно относились к ограничениям и допущениям, снижая достоверность общих результатов.

Председатель комиссии:	к.т.н., доцент	А.В. Матвеев
Члены комиссии:	д.т.н., профессор	М.В. Буйневич
	д.т.н., доцент	В.В. Грызунов
	к.т.н., доцент	К.Е. Израилов
	к.ю.н., доцент	А.Н. Метельков

АКТ

о внедрении диссертационного исследования на соискание ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»
на тему: «Оценка влияния эффектов деструктивного воздействия инфраструктурного генеза на информационную безопасность распределенных информационных систем»

Комиссия в составе:

- председатель комиссии – Труфанов В.Н., заместитель директора ФГАНУ ЦИТиС;
- член комиссии – Пиун П.В., заместитель начальника отдела Центра безопасности информации ФГАНУ ЦИТиС;
- член комиссии – Смольянников И.В., главный специалист – научный сотрудник Центра безопасности информации ФГАНУ ЦИТиС;
- член комиссии – Нестеров С.Г., главный специалист Центра безопасности информации ФГАНУ ЦИТиС

составила настоящий акт о том, что результаты диссертационного исследования Русакова А.М. в части касающейся метода оценки эффектов деструктивного воздействия инфраструктурного генеза внедрен в информационно-коммуникационную инфраструктуру электронной информационно-образовательной среды научного учреждения ФГАНУ ЦИТиС, осуществляющую подготовку слушателей дополнительного профессионального образования и аспирантов.

Внедрение результатов диссертационного исследования позволило повысить точность обнаружения скрытых синергетических эффектов инфраструктурного деструктивизма в распределенных информационных системах в среднем на 10-15%. Таким образом это позволило улучшить мониторинг и прогнозирование рисков информационной безопасности, связанных с отказоустойчивостью в информационных системах, а также оптимизировать управление инфраструктурными процессами в условиях деструктивных воздействий инфраструктурного генеза.

Подписи членов комиссии:

председатель Комиссии: В.Н. Труфанов
члены Комиссии: П.В. Пиун
И.В. Смольянников
С.Г. Нестеров

Ук.N=14/427/1

НАЦИОНАЛЬНЫЙ ИННОВАЦИОННЫЙ ЦЕНТР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

117246, г. Москва, Научный проезд, д.6, АО «НИЦ»
ИНН 7704599880, КПП 772801001
ОГРН 1067746619380
Тел.: +7 (495) 204-20-86
info@centin.ru, www.centin.ru

АКТ

о внедрении диссертационного исследования на соискание ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность»

на тему: «Оценка влияния эффектов деструктивного воздействия инфраструктурного генеза на информационную безопасность распределенных информационных систем»

Комиссия в составе:

председатель комиссии – Соболев Дмитрий Владимирович, генеральный директор АО «НИЦ»

член комиссии – Анфиногенов А.Ю.

член комиссии – Иванова Е. В.

член комиссии – Сягаев Б. В.

составила настоящий акт о том, что результаты диссертационного исследования Русакова А.М. в части касающейся:

комплекса антропоморфических моделей взаимодействия сервисов информационных систем;

методики оценки угроз инфраструктурного деструктивизма для распределённых информационных систем;

внедрены в службу технической поддержки и информационной безопасности АО «НИЦ» и использовались при сопровождении распределённых информационных систем.

Внедрение результатов диссертационного исследования позволило выявлять угрозы информационной безопасности инфраструктурного генеза, приводящие к отказу в обслуживании и формировать стратегии их предотвращения на основе анализа поведенческих особенностей сервисов и их взаимодействий в имеющихся информационных системах организации.

Подписи членов комиссии:

Соболев Д. В., генеральный директор АО «НИЦ»

Анфиногенов А. Ю.

Иванова Е. В.

Сягаев Б. В.

МИНОБРНАУКИ РОССИИ
Федеральное государственное
бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА
просп. Вернадского, д. 78, Москва, 119454
тел.: (499) 215 65 65 доб. 1140, факс: (495) 434 92 87

УТВЕРЖДАЮ
Заместитель первого проректора
_____ Ю.А. Ефимова
«____» октября 2024 г.

АКТ
о внедрении (использовании) результатов диссертационной работы Русакова Алексея Михайловича на тему «Модели и алгоритмы оценки динамики рисков инфраструктурного деструктивизма»

Материалы диссертационной работы Русакова Алексея Михайловича на тему «Модели и алгоритмы оценки динамики рисков инфраструктурного деструктивизма», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность, используются в учебном процессе Института кибербезопасности и цифровых технологий на кафедре «Информационно-аналитические системы кибербезопасности» РТУ МИРЭА для подготовки специалистов по специальности 10.05.04 «Информационно-аналитические системы безопасности».

Председатель комиссии:
Директор
Института кибербезопасности и
цифровых технологий А.А. Бакаев

Члены комиссии:
Заместитель директора
Института кибербезопасности и
цифровых технологий О.А. Глобенко

Заведующий кафедрой
«Информационно-аналитические системы кибербезопасности» О.В. Трубиенко

Рисунок 86 – Грамота за призовое место автора хакатона SKOLKOVO HACK за 2022 год (результаты позволившие занять призовое место по своей сути показывали способ оценки эффектов инфраструктурного деструктивизма для GreenPlum)

ПРИЛОЖЕНИЕ Б. Полученные свидетельства об интеллектуальной собственности

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2025614582

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2025614582
Дата регистрации: **24.02.2025**
Номер и дата поступления заявки:
2025612939 12.02.2025
Дата публикации и номер бюллетеня:
24.02.2025 Бюл. № 3
Контактные реквизиты:
Нет

Автор(ы):
Русаков Алексей Михайлович (RU)
Правообладатель(и):
Русаков Алексей Михайлович (RU)

Название программы для ЭВМ:
Интеллектуальная система поведенческого анализа процессов в информационно-технологической инфраструктуре на основе антропоморфических типов взаимодействия

Реферат:
Программа представлена в виде законченного программного решения для поведенческого анализа процессов в информационно-технологической инфраструктуре на основе антропоморфических типов взаимодействия. Программа реализована на языке программирования Python и имеет веб-интерфейс на языке программирования JavaScript. Программа реализована на основе сервисной архитектуры с серверной и с клиентской частью. Клиентская часть позволяет визуализировать данные поведенческой активности процессов по антропоморфическим типам поведения. Реализованы 9 моделей антропоморфических типов поведения процессов: Факультативный симбиоз; Комменсализм; Нейтрализм; Облигатный симбиоз; Паразитизм; Хищничество; Аменсализм; Конкуренция; Аллелопатия. Реализована возможность визуализации динамики рисков эффектов инфраструктурного деструктивизма. Серверная часть программы позволяет загружать данные журналов событий практических любых информационно-технологических инфраструктур в формате CSV. При этом для каждого формата журнала событий разработанных архитектур возможна адаптация для работы с разработанным программным обеспечением. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows; Linux; macOS.

Язык программирования: Python, JavaScript

Объем программы для ЭВМ: 8,721 МБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2024660851

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2024660851
Дата регистрации: **14.05.2024**
Номер и дата поступления заявки:
2024618977 18.04.2024
Дата публикации и номер бюллетеня:
14.05.2024 Бюл. № 5
Контактные реквизиты:
нет

Автор(ы):
Русаков Алексей Михайлович (RU),
Филатов Вячеслав Валерьевич (RU),
Коробкова Анастасия Максимовна (RU),
Карташов Игорь Максимович (RU),
Гавриленко Ксения Юрьевна (RU),
Алин Данила Александрович (RU),
Захаров Игорь Артемович (RU),
Емельянова Дарья Алексеевна (RU),
Блинов Владимир Владимирович (RU),
Горбунов Алексей Александрович (RU)
Правообладатель(и):
Русаков Алексей Михайлович (RU),
Филатов Вячеслав Валерьевич (RU),
Коробкова Анастасия Максимовна (RU),
Карташов Игорь Максимович (RU),
Гавриленко Ксения Юрьевна (RU),
Алин Данила Александрович (RU),
Захаров Игорь Артемович (RU),
Емельянова Дарья Алексеевна (RU),
Блинов Владимир Владимирович (RU),
Горбунов Алексей Александрович (RU)

Название программы для ЭВМ:
«Программное обеспечение для оценки рисков информационной безопасности на основе интеллектуального анализа данных репозитория исходного кода»

Реферат:
Программное обеспечение представлено в виде законченного программного решения для оценки рисков информационной безопасности на основе интеллектуального анализа данных репозитория исходного кода. Программное обеспечение разработано на основе языка программирования Python с использованием современных библиотек scipy, numpy, matplotlib. Программное обеспечение реализует алгоритмы анализа данных на основе теории вероятностей и математической статистики для расчёта рисков информационной безопасности. Основным функционалом программного обеспечения является определение основных вероятностей возникновения рисков информационной безопасности. В качестве исходных данных, получаемых из репозитория исходного кода, используются различные метрики: частота коммитов, наличие фрагментов сигнатур вредоносного кода, а также статистические метрики по расчёту основных показателей сложности исходного кода. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows, Linux, MacOS.

Язык программирования: Python

Объем программы для ЭВМ: 749 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023683184

«Антропоморфическая система моделирования деструктивных воздействий инфраструктурного генеза на объектах критической информационной инфраструктуры»

Правообладатель: ***Русаков Алексей Михайлович (RU)***

Автор(ы): ***Русаков Алексей Михайлович (RU)***

Заявка № **2023682500**
Дата поступления **24 октября 2023 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***03 ноября 2023 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2023665252

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2023665252
Дата регистрации: **13.07.2023**
Номер и дата поступления заявки:
2023664031 30.06.2023
Дата публикации и номер бюллетеня:
13.07.2023 Бюл. № 7
Контактные реквизиты:
нет

Автор(ы):
Русаков Алексей Михайлович (RU),
Голубев Данил Дмитриевич (RU),
Сараев Даниил Андреевич (RU),
Шагиджанян Андре Альбертович (RU),
Филатов Вячеслав Валерьевич (RU),
Ягирский Артем Александрович (RU)

Правообладатель(и):
Русаков Алексей Михайлович (RU),
Голубев Данил Дмитриевич (RU),
Сараев Даниил Андреевич (RU),
Шагиджанян Андре Альбертович (RU),
Филатов Вячеслав Валерьевич (RU),
Ягирский Артем Александрович (RU)

Название программы для ЭВМ:
«Программа для анализа веб-приложения на уязвимости на основе интеллектуального моделирования сетевых атак»

Реферат:
Программа для ЭВМ предназначена для анализа веб-приложений на уязвимости с помощью моделирования различных сетевых атак. Программа для ЭВМ выполнена в виде распределенного клиент-серверного приложения. Программа для ЭВМ последовательно анализирует веб-приложения на уязвимости, среди которых проверяются следующие основные типы уязвимостей: SQL-инъекция, межсайтовый скриптинг, подмена запросов на стороне сервера. Тестирование программы для ЭВМ показало возможность эффективного сбора данных об уязвимостях веб-приложений. Тип ЭВМ: IBM PC-совмест. ПК, мобильное устройство. ОС: Windows, Android, Linux, MacOs.

Язык программирования: Клиентская часть написана на языке программирования JavaScript на основе фреймворка React с интеграцией библиотеки компонентов ChakraUI. Серверная часть написана на языке программирования Python с использованием фреймворка FastAPI для связи с клиентами и основных сопутствующих библиотек: BeautifulSoup4, xss, ssrf, beanie, motor, contextlib.

Объем программы для ЭВМ: 46,27 МБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2023684208

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2023684208
Дата регистрации: **14.11.2023**
Номер и дата поступления заявки:
2023682379 24.10.2023
Дата публикации и номер бюллетеня:
14.11.2023 Бюл. № 11

Автор(ы):
Русаков Алексей Михайлович (RU)
Правообладатель(и):
Русаков Алексей Михайлович (RU)

Название программы для ЭВМ:
«Система оценки рисков деструктивного воздействия инфраструктурного генеза на субъекте критической информационной инфраструктуры»

Реферат:
Программа представлена в виде законченного программного решения для оценки рисков деструктивного воздействия инфраструктурного генеза на субъекте критической информационной инфраструктуры. Программа разработана с использованием современных библиотек обработки информации и машинного обучения. Программа реализует функционал оценки рисков ИБ субъектов критических информационных инфраструктур с учетом деструктивного воздействия инфраструктурного генеза. Принцип работы программы построен на использовании технологии цифровых двойников. Для каждой исследуемой инфраструктуры строится модель описывающая процессы деструктивного воздействия на основе имеющихся поведенческих факторов. С помощью имитационного моделирования с использованием методов классификации методов машинного обучения. Отличительной особенностью разработанной системы оценки рисков информационной безопасности на субъекте критической информационной инфраструктуры является возможность оценки рисков деструктивных воздействий субъектов критической информационной инфраструктуры на основе антропоморфического подхода. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows, Linux, macOS.

Язык программирования: Python

Объем программы для ЭВМ: 4,39 МБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023683299

«Средство реализации рекомендательной системы для профилактики и предотвращения инфраструктурного деструктивизма на субъекте критической информационной инфраструктуры»

Правообладатель: ***Русаков Алексей Михайлович (RU)***

Автор(ы): ***Русаков Алексей Михайлович (RU)***

Заявка № **2023682485**
Дата поступления **24 октября 2023 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***07 ноября 2023 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022683265

«Программное обеспечение для гарантированного качества обслуживания в программно-конфигурируемых распределенных информационных системах»

Правообладатели: ***Русаков Алексей Михайлович (RU), Карпусь Павел Сергеевич (RU), Голуб Эдуард Эдуардович (RU), Раманцев Роман Анатольевич (RU), Джлавян Екатерина Кареновна (RU), Янин Андрей Вадимович (RU), Евстигнеев Глеб Денисович (RU), Новокшонов Игорь Дмитриевич (RU), Лаврушин Вадим Максимович (RU)***

Авторы: ***Русаков Алексей Михайлович (RU), Раманцев Роман Анатольевич (RU), Джлавян Екатерина Кареновна (RU), Янин Андрей Вадимович (RU), Евстигнеев Глеб Денисович (RU), Новокшонов Игорь Дмитриевич (RU), Лаврушин Вадим Максимович (RU), Карпусь Павел Сергеевич (RU), Голуб Эдуард Эдуардович (RU)***

Заявка № **2022682346**

Дата поступления **14 ноября 2022 г.**

Дата государственной регистрации в Реестре программ для ЭВМ ***02 декабря 2022 г.***

Руководитель Федеральной службы по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2022685869

«Программное обеспечение системы моделирования межобъектных системных связей инфраструктурного характера в информационных системах»

Правообладатель: ***Русаков Алексей Михайлович (RU)***

Автор(ы): ***Русаков Алексей Михайлович (RU)***

Заявка № **2022685248**
Дата поступления **15 декабря 2022 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***28 декабря 2022 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2023683475

«Эпидемиологическая система моделирования оценки рисков динамики межобъектного влияния в условиях инфраструктурного деструктивизма»

Правообладатель: ***Русаков Алексей Михайлович (RU)***

Автор(ы): ***Русаков Алексей Михайлович (RU)***

Заявка № **2023682859**
Дата поступления **24 октября 2023 г.**
Дата государственной регистрации
в Реестре программ для ЭВМ ***08 ноября 2023 г.***

Руководитель Федеральной службы
по интеллектуальной собственности

Ю.С. Зубов

ПРИЛОЖЕНИЕ В. Результаты сравнительного анализа методик повышения уровня информационной безопасности в распределенных информационных системах

Таблица 36 – Проблемы безопасности РИС

Категория проблемы	Описание	Примеры
Угрозы и атаки	Вредоносные действия, направленные на нарушение работы систем или компрометацию данных.	Malware, Ransomware, DDoS, фишинговые атаки, zero-day уязвимости.
Уязвимости	Технические недостатки или ошибки, позволяющие атакам быть успешными.	Незащищённые сети, устаревшее ПО, ошибки конфигурации, уязвимости в API.
Человеческий фактор	Ошибки или действия сотрудников, приводящие к утечке данных или компрометации систем.	Слабые пароли, инсайдерские угрозы, низкий уровень осведомлённости, случайные ошибки.
Проблемы управления	Недостатки в организации мониторинга и контроля за ИТ-инфраструктурой.	Отсутствие мониторинга, некачественное управление привилегиями, слабая интеграция систем.
Облачная инфраструктура	Особенности безопасности при использовании облачных технологий.	Проблемы мультиаренды, ошибки конфигурации, недостаточная прозрачность со стороны провайдера.
Интернет вещей (IoT)	Слабая защита IoT-устройств и их роль в расширении атакующих векторов.	Устройства с предустановленными паролями, отсутствие обновлений, незащищённые протоколы.
Новые технологии	Угрозы, связанные с использованием современных решений.	Уязвимости AI/ML, эксплуатация 5G, недостаточная защита блокчейн-систем.
Соответствие нормативам	Риски, связанные с невыполнением требований законов и стандартов.	Несоответствие ФСТЭК, ФСБ, Банка России, штрафы за утечки данных.

Таблица 37 – Угрозы безопасности данных РИС

Проблема	Описание	Последствия
Утечка данных	Неправомерный доступ или передача конфиденциальной информации.	Потеря репутации, финансовые штрафы, юридические последствия, утрата доверия клиентов.
Несанкционированный доступ	Доступ к данным или системам без разрешения.	Повреждение данных, потеря контроля над системами, внедрение вредоносного ПО.
Недостаточное шифрование	Применение слабых или отсутствующих механизмов шифрования для данных в транзите или хранении.	Угроза перехвата данных, утечка личной и финансовой информации, потеря конфиденциальности.

Таблица 38 – Уязвимости ИТ-инфраструктуры РИС

Проблема	Описание	Последствия
Ошибки конфигурации	Некорректная настройка серверов, сетевых устройств, приложений и систем безопасности.	Уязвимости, через которые могут проникать злоумышленники, возможность атаки через открытые порты.
Устаревшее ПО и оборудование	Использование старых версий программного обеспечения или устаревших устройств, которые не поддерживаются.	Повышенная вероятность эксплуатации известных уязвимостей, снижение производительности.
Недостаток обновлений	Необновленные системы, приложения или устройства, оставленные без исправлений для устранения уязвимостей.	Уязвимости становятся доступными для эксплуатации, атаки становятся более эффективными.

Таблица 39 – Атаки на ИТ-инфраструктуры РИС

Проблема	Описание	Последствия
DDoS-атаки	Атаки распределенного отказа в обслуживании, направленные на перегрузку системы или сети.	Потеря доступа к сервисам и системам, нарушение работы бизнеса, финансовые потери.
Вредоносные программы (Malware)	Программы, предназначенные для повреждения, уничтожения или кражи данных, например, вирусы или трояны.	Потеря данных, кража конфиденциальной информации, нарушение работы систем.
Фишинг и социальная инженерия	Манипуляции с целью получения личных данных (логины, пароли, финансовые данные) через обман.	Кража учетных данных, доступ к конфиденциальной информации, финансовые потери.

Таблица 40 – Проблемы управления безопасностью РИС

Проблема	Описание	Последствия
Недостаток мониторинга и аудита	Отсутствие систем мониторинга и аудита действий в сети и приложениях.	Сложности в выявлении инцидентов безопасности, замедленное реагирование на угрозы.
Неадекватная реакция на инциденты	Отсутствие или недостаточная разработанность планов реагирования на инциденты безопасности.	Задержки в обнаружении и ликвидации атак, увеличение ущерба от инцидента.
Нехватка квалифицированных специалистов	Недостаток специалистов по ИТ-безопасности для мониторинга, тестирования и предотвращения угроз.	Риски неправильной конфигурации, упущенные угрозы, недостаток знаний о новых видах атак.

Таблица 41 – Проблемы с управлением доступом РИС

Проблема	Описание	Последствия
Слабые пароли и аутентификация	Использование простых или одинаковых паролей, отсутствие многофакторной аутентификации.	Уязвимость к взлому учетных записей, возможность несанкционированного доступа.
Отсутствие разделения прав доступа	Недостаточное ограничение прав доступа пользователей в зависимости от их роли.	Чрезмерный доступ к конфиденциальной информации, возможность злоупотребления полномочиями.
Управление привилегиями	Неэффективное управление правами привилегированных пользователей (например, администраторов).	Утечка данных, несанкционированные изменения в системе, доступ к критическим данным.

Таблица 42 – Проблемы с облачной и гибридной инфраструктурой РИС

Проблема	Описание	Последствия
Безопасность облачных данных	Риски, связанные с хранением данных в облаке, включая утечку данных, взлом учетных записей.	Потеря контроля над данными, риск их кражи или уничтожения.
Неправильная настройка облачных сервисов	Ошибки в конфигурации облачных сервисов, таких как доступ к данным или конфиденциальной информации.	Утечка данных, уязвимости, возможные штрафы и юридические последствия.
Перехват данных при передаче	Уязвимости при передаче данных в облачные сервисы или между различными инфраструктурами.	Потеря данных, угроза перехвата информации во время передачи, возможные утечки конфиденциальной информации.

Таблица 57 – Основные методы обеспечения ИБ РИС

Метод обеспечения информационной безопасности	Описание	Примеры технологий и инструментов
Защита API	Обеспечение безопасности интерфейсов для предотвращения несанкционированного доступа.	API Gateway (Kong, Apigee), OpenAPI Security.
Контейнерная безопасность	Защита контейнеризированных приложений и инфраструктуры.	Docker Security, Kubernetes Security, runtime-сканеры (Aqua, Twistlock).
Обучение пользователей	Повышение осведомлённости сотрудников о рисках и угрозах.	Курсы по кибербезопасности, регулярные фишинг-тесты.
Аутентификация и MFA	Многофакторная аутентификация для повышения защиты учётных записей.	Google Authenticator, YubiKey, биометрия (сканеры отпечатков, распознавание лица).
Блокчейн для безопасности	Использование распределённых реестров для проверки данных и транзакций.	Защита данных IoT, распределённая идентификация (Decentralized Identity).
Искусственный интеллект и машинное обучение	Автоматическое обнаружение угроз и управление инцидентами.	Darktrace, CrowdStrike, Microsoft Sentinel.

Анализ журналов событий в целях информационной безопасности включает в себя несколько важных этапов, представленных в таблице 43.

Таблица 43 – Основные аспекты анализа ИБ РИС

Категория	Описание
Сбор данных	Логи собираются из серверов, сетевого оборудования, приложений, облачных сервисов, баз данных.
Централизация	Все данные агрегируются в централизованной системе, такой как SIEM, для удобства обработки.
Анализ и корреляция	Используются алгоритмы для выявления взаимосвязей между событиями, которые могли бы ускользнуть от ручного анализа.
Обнаружение аномалий	На основе базового поведения системы выявляются отклонения, которые могут указывать на угрозы.
Визуализация	Визуализация результатов анализа позволяет лучше понять временные паттерны и сделать выводы из данных. Графики, диаграммы и тепловые карты помогают наглядно представить временные зависимости и изменения
Реагирование	Автоматизация действий при обнаружении подозрительных событий, таких как изоляция устройства или блокировка аккаунта.

Таблица 44 – Методы интеллектуального анализа журналов событий РИС

Метод	Описание	Примеры инструментов
Правила и сигнатуры	Сравнение событий с заранее заданными правилами или известными сигнатурами атак.	PT MaxPatrol
Анализ поведения (UEBA)	Выявление аномалий в поведении пользователей или систем.	PT MaxPatrol
Машинное обучение (ML)	Автоматическое обучение на основе данных логов для выявления паттернов и аномалий.	Darktrace, Elastic Stack (с ML модулями).
Обогащение данных	Добавление контекстной информации из внешних источников (например, баз угроз).	Threat Intelligence платформы (MISP, Recorded Future).
Корреляция событий	Связывание разных событий для создания полной картины инцидента.	SIEM-системы PT MaxPatrol
Прогнозирование инцидентов	Применение моделей для предсказания потенциальных угроз на основе исторических данных.	Microsoft Sentinel, AWS GuardDuty.
Анализ в реальном времени	Быстрая обработка и анализ логов с минимальной задержкой.	Graylog, Fluentd.

Временные паттерны обозначают зависимости данных относительно времени. Они играют важную роль в анализе распределенных систем, так как позволяют уловить тренды, циклы и аномалии, происходящие во времени. Анализ временных паттернов может применяться к примеру в этих областях

Таблица 45 – Временные паттерны и зависимости данных событий РИС

Категория	Описание
Тренды	Временные паттерны позволяют выявлять долгосрочные тенденции и изменения данных со временем. Это важно для прогнозирования и планирования в различных отраслях экономики и общественной жизни.
Цикличность	Анализ временных циклов может помочь выявить повторяющиеся события и паттерны, которые могут быть связаны с сезонными изменениями, поведением потребителей или другими периодическими явлениями.
Аномалии	Идентификация временных аномалий в данных может помочь выявить необычные события, которые могут быть связаны с авариями, атаками в кибербезопасности или другими важными событиями, требующими немедленных мер.
Временные корреляции	Анализ временных паттернов позволяет определить связи и зависимости между различными переменными, которые изменяются с течением времени. Это особенно важно в научных исследованиях и прогнозировании будущих событий.

Таблица 46 – Механизм возникновения состояния гонки ресурсов в РИС

Фактор	Описание	Пример
Одновременный доступ	Несколько процессов или потоков обращаются к одному ресурсу без синхронизации.	Одновременная запись в общий файл.
Нарушение порядка выполнения	Порядок операций нарушается, приводя к некорректному состоянию ресурса.	Чтение данных до их полной записи в базу данных.
Недостаточная синхронизация	Отсутствие блокировок или других механизмов управления доступом.	Изменение конфигурационного файла несколькими пользователями одновременно.

Таблица 47 – Примеры гонки ресурсов в ИТ-инфраструктуре РИС

Область	Описание	Пример
Файловые системы	Несинхронизированный доступ к файлам.	Одновременная запись логов разными процессами.
Сетевые приложения	Конкуренция при обработке запросов.	Несогласованная обработка параллельных транзакций.
Системы безопасности	Уязвимости, связанные с состоянием гонки.	Атака TOCTOU, манипуляции между проверкой доступа и использованием ресурса.
Виртуализация и контейнеризация	Конкуренция за аппаратные ресурсы или хранилища.	Несинхронизированный доступ контейнеров к общим дискам.

Таблица 48 – Последствия состояния гонки ресурсов в РИС

Последствие	Описание	Пример
Потеря данных	Некорректная работа с ресурсами может привести к их повреждению или удалению.	Повреждение файлов базы данных при одновременной записи.
Нестабильность системы	Системные сбои или непредсказуемое поведение приложений.	Перезапуск серверов из-за конфликта потоков.
Уязвимости безопасности	Возможность использования состояний гонки для атак.	Эксплуатация состояния гонки для повышения привилегий.
Снижение производительности	Задержки и конфликты при доступе к ресурсам.	Замедление работы базы данных из-за гонки запросов.

Таблица 49 – Методы предотвращения состояния гонки ресурсов в РИС

Метод	Описание	Пример
Синхронизация процессов	Управление доступом с помощью блокировок, мьютексов, семафоров.	Использование «pthread_mutex_lock» для потоков POSIX.
Атомарные операции	Выполнение операций без прерывания другими потоками.	Атомарный инкремент счётчика с использованием процессорных инструкций.
Очереди и пул ресурсов	Упорядочивание доступа к ресурсам через очереди задач.	Использование очередей сообщений (например, RabbitMQ).
Тестирование и мониторинг	Анализ кода и поведенческое тестирование для выявления гонок.	Использование инструментов Valgrind или ThreadSanitizer.
Разделение ресурсов	Изоляция ресурсов для предотвращения конкуренции.	Применение namespaces в контейнерах Docker.

Таблица 50 – Механизм возникновения нарушения идемпотентности в РИС

Фактор	Описание	Пример
Отсутствие контроля состояния	Операции выполняются без учета текущего состояния системы, что приводит к дублированию или изменению данных.	Повторный запрос на создание ресурса без проверки, существует ли уже такой ресурс, приводит к ошибке.
Невозможность отката	Отсутствие механизма для отмены изменений при повторном выполнении операций.	Выполнение финансовой транзакции дважды, когда система не поддерживает отмену или возврат средств.
Несоответствие бизнес-логике	Логика обработки данных не учитывает возможность повторения запроса с одинаковыми параметрами.	Внесение изменений в конфигурацию системы без проверки на идентичность текущего состояния.
Проблемы с синхронизацией	Несоответствие данных или операций из-за параллельных изменений в разных частях системы.	Изменение статуса заказа в электронной торговле без блокировки, что приводит к одновременному изменению статуса.

Таблица 51 – Примеры нарушений идемпотентности в ИТ-инфраструктуре РИС

Область	Описание	Пример
Программные интерфейсы	Нарушение идемпотентности при повторных запросах к API.	Запрос на создание записи в базе данных приводит к созданию дублирующихся записей при многократных вызовах с одинаковыми данными.
Базы данных	Повторное выполнение SQL-запроса без учёта состояния данных может изменить их.	Многократное выполнение SQL-запроса на обновление или удаление данных без проверки их состояния.
Облачные вычисления	При автоматизации работы с облачными сервисами отсутствие идемпотентности может привести к ошибкам в масштабировании.	Автоматическое добавление серверов в кластер без проверки их существования в инфраструктуре.
Системы управления конфигурацией	Несоответствие состояния конфигурации из-за повторного применения одинаковых изменений.	Применение изменения конфигурации, например, с помощью Ansible или Terraform, без учета текущего состояния.

Таблица 52 – Последствия нарушения идемпотентности в РИС

Последствие	Описание	Пример
Дублирование данных	Повторное выполнение операции может привести к созданию дублирующихся или лишних записей.	Создание нескольких одинаковых записей в базе данных или дублирование заказов в электронной торговле.
Нарушение консистентности	Система может стать неконсистентной, когда изменения данных не могут быть корректно отменены.	Несоответствие статуса заказа в разных частях системы из-за повторных запросов.
Неожиданные ошибки	Отсутствие проверки на повторные операции может привести к ошибкам выполнения и сбоям.	Ошибка из-за попытки повторного создания ресурса, который уже существует.
Проблемы с производительностью	Многократное выполнение одной и той же операции может снизить производительность системы.	Снижение скорости работы системы из-за избыточных операций в базе данных или приложении.
Потери финансов	При ошибках в транзакциях может возникнуть риск потери финансовых средств.	Дважды списанные деньги за одну и ту же операцию из-за отсутствия проверки идемпотентности.

Таблица 53 – Причины взаимной блокировки в РИС

Категория	Описание	Примеры	Методы предотвращения
Неправильное управление доступом	Процессы блокируют ресурсы без своевременного их освобождения.	Блокировка файлов, конкуренция за криптографические ключи.	Установка таймаутов для использования ресурсов.
Конкуренция за ресурсы	Несколько процессов одновременно запрашивают доступ к одному и тому же ресурсу.	Одновременный доступ к зашифрованным данным, очереди на доступ к серверу.	Использование алгоритмов управления ресурсами (FIFO, приоритизация).
Ошибки конфигурации и проектирования	Неверное использование механизмов синхронизации или циклические зависимости в процессах.	Блокировка баз данных при одновременных транзакциях, проблемы в работе семафоров.	Анализ циклов зависимостей, корректное использование мьютексов.
Политики безопасности	Жесткие правила доступа вызывают взаимные ожидания процессов.	Системы аутентификации, где несколько процессов ждут верификации друг от друга.	Переработка политик, внедрение правил последовательного доступа.

Таблица 54 – Последствия блокировки в РИС

Категория	Описание	Примеры	Методы предотвращения
Нарушение доступности	Ресурсы становятся недоступными для пользователей и систем.	Блокировка серверов баз данных, отказ веб-приложений.	Реализация систем мониторинга и автоматического снятия блокировок.
Угроза целостности данных	Прерывание операций записи или изменения данных.	Повреждение файлов или баз данных при сбоях транзакций.	Внедрение механизмов отката и журналирования транзакций.
Подверженность атакам	Злоумышленники используют блокировку для атак (например, DoS).	Умышленная перегрузка серверов аутентификации.	Ограничение количества параллельных запросов, защита от перегрузки.
Эскалация привилегий	Процессы получают права доступа выше разрешенных для снятия блокировки.	Запрос высоких прав для освобождения ресурсов.	Применение принципа минимальных привилегий.

Таблица 55 – Методы предотвращения угроз ИБ в РИС

Категория	Описание	Примеры	Методы предотвращения
Избежание циклов ожидания	Исключение ситуации, когда процессы блокируют друг друга из-за циклических зависимостей.	Банковский алгоритм распределения ресурсов.	Упорядочивание доступа к ресурсам.
Таймауты на использование ресурсов	Автоматическое снятие блокировки при долгом ожидании.	Ограничение времени выполнения транзакции в базе данных.	Установка таймеров для операций.
Deadlock-free алгоритмы	Алгоритмы, исключающие возможность взаимной блокировки.	Использование FIFO-очередей для обработки запросов.	Внедрение проверенных алгоритмов управления ресурсами.
Мониторинг и устранение	Постоянный контроль состояния системы с возможностью идентификации блокировок.	Инструменты мониторинга транзакций в реальном времени.	Программное обеспечение для автоматической диагностики (например, AIOps).
Приоритизация процессов	Установка приоритетов для процессов, чтобы критические операции не зависели от менее важных.	Приоритет на выполнение операций в системах безопасности.	Назначение критическим процессам высокого приоритета доступа.

Таблица 56 – Проблемы ИБ на уровне конечных устройств РИС

Проблема	Описание	Последствия
Устройства без защиты	Использование незащищенных мобильных и рабочих устройств для работы с корпоративными данными.	Утечка данных, вредоносные программы, потеря конфиденциальной информации.
Потеря или кража устройства	Устройства, содержащие корпоративную информацию, теряются или становятся объектами кражи.	Потеря контроля над данными, возможность их использования третьими лицами.

Таблица 57 – Расширенные методы обеспечения ИБ РИС

Метод обеспечения информационной безопасности	Описание	Примеры технологий и инструментов
Многоуровневая защита	Использование нескольких слоёв защиты для минимизации рисков.	Антивирусы, брандмауэры, системы предотвращения вторжений (IDS/IPS).
Zero Trust (Нулевая доверенность)	Отказ от доверия к любой сети или пользователю, верификация на всех этапах.	Контроль доступа, микросегментация, MFA (многофакторная аутентификация).
Шифрование данных	Защита данных при хранении и передаче с использованием криптографических методов.	TLS/SSL, шифрование на уровне файлов (AES), VPN.
Управление привилегиями (PAM)	Ограничение прав доступа для предотвращения злоупотреблений.	RBAC (роль-ориентированный доступ), IAM (управление идентификацией).
Мониторинг и реагирование	Постоянный анализ событий и активности для обнаружения угроз.	SIEM-системы (Splunk, QRadar), системы SOAR для автоматизированного реагирования.
Облачная безопасность	Методы и инструменты для защиты облачной инфраструктуры.	CSPM (Cloud Security Posture Management), шифрование данных в облаке.
Технология DevSecOps	Интеграция безопасности на всех этапах жизненного цикла разработки ПО.	Автоматические сканеры кода (Snyk, SonarQube), CI/CD с тестами на уязвимости.
Микросегментация	Разделение сети на изолированные сегменты для снижения риска распространения атак.	VMware NSX, Cisco ACI.
Анализ поведения (UEBA)	Выявление аномалий в поведении пользователей и систем.	Exabeam, User Behavior Analytics.

ПРИЛОЖЕНИЕ Г. Результаты сравнительного анализа методик оценки рисков информационной безопасности в распределенных информационных системах

Таблица 58 – Методы оценки рисков ИБ РИС

Метод	Описание	Процесс	Преимущества	Недостатки
Качественная оценка рисков	Использует субъективную оценку для классификации рисков по вероятности и воздействию.	Идентификация угроз, оценка вероятности и воздействия, классификация рисков (низкий, средний, высокий).	Простота, быстрая оценка, хороша для начальной оценки.	Субъективность, неточность при сложных рисках.
Количественная оценка рисков	Оценка рисков с использованием числовых значений для вероятности и воздействия.	Оценка вероятности и воздействия на основе статистики, расчет общего риска (Риск = Вероятность × Воздействие).	Точная и объективная оценка, расчет стоимости рисков.	Требует большого объема данных, сложность реализации.
Моделирование угроз	Анализ системы для выявления возможных угроз и уязвимостей, которые могут быть использованы для атак.	Определение активов, угроз и уязвимостей, оценка рисков и создание мер защиты.	Ориентирован на реальные угрозы и уязвимости, позволяет сосредоточиться на критических аспектах.	Требует глубокого понимания системы и угроз.
Анализ воздействия	Оценка воздействия рисков на организацию, включая финансовые и репутационные последствия.	Идентификация инцидентов, оценка воздействия на бизнес-процессы, приоритизация активов и систем.	Понимание последствий для бизнеса, приоритеты защиты.	Не оценивает вероятность угроз, фокус на последствиях, а не на вероятности.
Анализ уязвимостей	Фокусируется на выявлении уязвимостей в системе, которые могут быть использованы для атак.	Сканирование и оценка уязвимостей с использованием инструментов, анализ критичности уязвимостей.	Быстрое обнаружение уязвимостей, повышение безопасности.	Может быть трудоемким, не всегда выявляет полное воздействие уязвимостей.
Сценарный анализ	Использование гипотетических сценариев для оценки возможных угроз и их воздействия.	Разработка сценариев атак, оценка их вероятности и воздействия, разработка мер защиты.	Позволяет моделировать различные риски и их последствия, полезен для планирования действий в кризисных ситуациях.	Требует значительных ресурсов для разработки, субъективность в оценке угроз.
Метод критического пути (CPM)	Используется для выявления ключевых рисков и уязвимых точек в процессе или системе, анализируя зависимости.	Оценка зависимостей между элементами системы, выявление критических этапов и узких мест.	Помогает выявить критичные элементы и уязвимости в системе, полезен для управления проектами.	Не всегда применим в условиях неопределенности, требует детальной проработки процессов.

Эта таблица представляет основные методы оценки рисков в информационной безопасности РИС, с указанием их особенностей, преимуществ и недостатков.

Таблица 59 – Основные этапы оценки рисков ИБ НИС

Этап	Описание
Идентификация активов	Определение критически важных ресурсов инфраструктуры (серверы, сети, приложения).
Определение угроз	Выявление потенциальных угроз, которые могут воздействовать на активы (вирусы, хакеры).
Анализ уязвимостей	Оценка слабых мест инфраструктуры, которые могут быть использованы для атаки.
Оценка последствий	Анализ возможного ущерба при успешной реализации угроз (финансовый, репутационный, операционный).
Вероятностный анализ	Оценка вероятности реализации каждой угрозы.
Приоритизация рисков	Классификация рисков по степени их влияния и вероятности, формирование списка приор.
Формирование мер защиты	Разработка и внедрение мер для минимизации риска

Таблица 60 – Методы оценки рисков ИБ РИС

Тип метода	Метод	Описание	Преимущества	Недостатки
Качественные	Анкетирование и интервьюирование	Сбор мнений экспертов и сотрудников для выявления угроз.	Простота, не требует точных данных.	Субъективность результатов.
	Матрица рисков	Оценка вероятности событий и их воздействия в виде матрицы.	Удобная визуализация.	Ограниченная точность.
	SWIFT	Мозговой штурм для анализа возможных сценариев («что будет, если…»).	Идентификация нестандартных угроз.	Требует участия опытных специалистов.
Количественные	ALE (Ожидаемая стоимость потерь)	Рассчитывает годовые потери на основе вероятности и ущерба от одного инцидента.	Простота расчетов, ясность.	Не учитывает сложные взаимосвязи рисков.
	Моделирование Монте-Карло	Статистическое моделирование вероятностей рисков.	Высокая точность для сложных систем.	Требует много данных и вычислительных ресурсов.
	Bayesian Networks	Анализ причинно-следственных связей между событиями.	Учет изменений в реальном времени.	Сложность построения моделей.
	Анализ затрат и выгод (CBA)	Сравнивает затраты на меры безопасности с предотвращенными убытками.	Подходит для принятия решений.	Усложняется при оценке нематериальных активов.
Комбинированные	OCTAVE	Идентификация активов, угроз и уязвимостей с качественным и количественным анализом.	Интегрированный подход.	Требует времени и экспертных знаний.
	FAIR	Разложение рисков на факторы (угрозы, уязвимости, потери) с комбинированным подходом.	Подходит для сложных систем.	Требует значительных усилий для внедрения.
	ISO/IEC 27005	Международный стандарт для систематической оценки и управления рисками.	Подходит для регуляторных требований.	Ограничивается рамками стандарта.

Таблица 61 – Основные предполагаемые угрозы ИБ ДВ ИГ

Тип угрозы	Описание
Технические	Отказ оборудования, ошибки конфигурации, устаревшее ПО.
Человеческий фактор	Ошибки пользователей, инсайдерские угрозы, низкая осведомлённость.
Киберугрозы	Атаки злоумышленников, вирусы, DDoS, фишинг.
Природные	Стихийные бедствия, которые могут повредить физическую инфраструктуру (например, серверные центры).
Организационные	Нарушения процессов управления ИТ-инфраструктурой или политик безопасности.

Таблица 62 – Основные типы методов оценки рисков ИБ РИС

Метод	Описание	Пример применения
Качественная оценка	Оценка на основе экспертного мнения без точных количественных данных.	Используется в начальной стадии анализа.
Количественная оценка	Применение математических моделей для вычисления вероятностей и ущерба.	Использование формул, таких как ALE (Annual Loss Expectancy).
Комбинированный подход	Сочетание качественных и количественных методов.	Применяется для сбалансированного подхода.
Анализ на основе сценариев	Разработка возможных сценариев реализации угроз и их анализ.	Моделирование атак с помощью инструментов Red Team.
Метод матрицы рисков	Визуализация рисков в виде матрицы на основе вероятности и влияния.	Создание таблицы для ранжирования рисков.