DOI 10.37882/2223-2966.2025.01.36

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ И СХЕМА ОРГАНИЗАЦИИ АРХИТЕКТУРЫ СИСТЕМЫ ПРОГНОЗИРОВАНИЯ ЭФФЕКТОВ ИНФРАСТРУКТУРНОГО ДЕСТРУКТИВИЗМА

CONCEPTUAL MODEL AND ORGANIZATION SCHEME OF THE ARCHITECTURE OF THE SYSTEM FOR FORECASTING THE EFFECTS OF INFRASTRUCTURAL DESTRUCTION

A. Rusakov

Summary. The article considers one of the important issues related to ensuring the security of information infrastructures. Information infrastructure (IT infrastructure) includes a wide range of elements: servers, networks, data storage, cloud services and user devices. Information security in infrastructures is ensured both by infrastructure objects and by the infrastructure itself — connections and inter-object interactions between infrastructure elements. At present, against the background of widespread import substitution, it is especially important to ensure the security of the infrastructure itself as a system of inter-object interactions. The presence of the effects of infrastructure destructiveness, consisting in the self-destruction of infrastructure and the slowdown of its work processes, is ubiquitous and requires the development of new approaches to their forecasting. The article provides the author's conceptual model and organization scheme of the architecture of the system for assessing the effects of infrastructure destructiveness.

Keywords: information infrastructure, IT infrastructure, information security of infrastructure, infrastructure destruction, forecasting of infrastructure destruction.

Русаков Алексей Михайлович
старший преподаватель, МИРЭА Российский технологический университет
rusakov_a@mirea.ru

Аннотация. В статье рассматривается один из важных вопросов связанный с обеспечением безопасности функционирования информационных инфраструктур. Информационная инфраструктура (ИТ-инфраструктура) включает в себя широкий спектр элементов: серверы, сети, хранилища данных, облачные сервисы и пользовательские устройства. Безопасность информации в инфраструктурах обеспечивают как со стороны объектов инфраструктуры, так и со стороны самой инфраструктуры — связей и меж объектными взаимодействиями между элементами инфраструктуры. В настоящий момент на фоне повсеместного импортозамещения особенно важным является обеспечение безопасности самой инфраструктуры как системы меж объектных взаимодействий. Наличие эффектов инфраструктурного деструктивизма, состоящих в саморазрушении инфраструктуры и замедлении процессов её работы, встречается повсеместно и требует развития новых подходов к их прогнозированию. В статье приводится авторская концептуальная модель и схема организации архитектуры системы оценки эффектов инфраструктурного деструктивизма.

Ключевые слова: информационная инфраструктура, ИТ-инфраструктура, информационная безопасность инфраструктуры, инфраструктурный деструктивизм, прогнозирования инфраструктурного деструктивизма.

Введение

Современное общество переживает стремительную цифровую трансформацию, при которой информационные технологии становятся неотъемлемой частью всех сфер деятельности — от бизнеса и здравоохранения до государственного управления и личной жизни. Информационная инфраструктура (ИТ-инфраструктура), представляющая собой совокупность аппаратных, программных и сетевых компонентов, обеспечивает функционирование этих процессов, выступая критически важным звеном в поддержке их надежности и доступности.

Развитие технологий сопровождается ростом угроз информационной безопасности, что делает защиту информационной инфраструктуры одной из приоритетных задач для организаций, независимо от их масштаба и отрасли. Однако параллельно с развитием технологий растет и количество угроз, связанных с безопасностью информационных инфраструктур. Кибератаки, утечка данных, целенаправленные взломы и ошибки конфигурации систем могут привести к серьезным последствиям, включая финансовые убытки, утрату конфиденциальной информации и нарушение общественной безопасности. В условиях глобальной взаимосвязанности, когда компании и государства становятся все более зависимыми от цифровых систем, обеспечение безопасности информационных инфраструктур приобретает первостепенное значение [1–3].

Информационная инфраструктура включает в себя широкий спектр элементов: серверы, сети, хранилища данных, облачные сервисы и пользовательские устройства. Уязвимости в этих системах могут привести к серьезным последствиям, включая утрату данных, на-

рушение конфиденциальности, финансовые убытки и подрыв репутации. В последние годы увеличение числа кибератак, использование сложных вредоносных программ и целевых атак подчеркивают необходимость комплексного подхода к обеспечению безопасности [4]. Информационная безопасность в инфраструктурах обеспечивается как со стороны объектов инфраструктуры, так и со стороны самой инфраструктуры — связей и меж объектными взаимодействиями между элементами инфраструктуры. В настоящий момент на фоне повсеместного импортозамещения особенно важным является обеспечение безопасности самой инфраструктуры как системы меж объектных взаимодействий. Наличие эффектов инфраструктурного деструктивизма, состоящих в саморазрушении инфраструктуры и замедлении процессов её работы, встречается повсеместно и требует развития новых подходов к их прогнозированию.

Концептуальная модель системы прогнозирования эффектов инфраструктурного деструктивизма

Введем основные понятия для описания феномена инфраструктурного деструктивизма, а также деструктивных воздействий инфраструктурного генеза.

Определение. Инфраструктурный деструктивизм — не способность информационной инфраструктуры реализовывать свой функционал в полном объеме под воздействием процессов внутри инфраструктуры [5,6].

Определение. Информационная инфраструктура — это единый комплекс программных, технических, коммуникационных, информационных и организационно-технологических средств обеспечения функционирования предприятия, а также средств управления ими [2, 6]. В качестве аналога ИнИ можно также рассматривать инфраструктуру информационных технологий.

Определение. Под деструктивным воздействием инфраструктурного генеза будем понимать воздействие, в результате которого проявляется непредвиденное и(или) нежелательное событие, вызванное совокупностью факторов и условий инфраструктурного генеза, создающих опасность нарушения информационной безопасности информационной инфраструктуры [5,6].

С целью описания основных процессов, влияющих на развитие ИнИ, рассмотрим концептуальную модель предметной области. ИнИ можно представить через систему взаимодействующих объектов. Особый интерес представляет меж объектное взаимодействие в ИнИ, реализуемое через сервисы.

Таким образом на каждом из объектов можно выделить множества ошибок и уязвимостей программного кода, а также множество особенностей меж объектного взаимодействия.

В настоящее время уже рассматриваются проблемы информационной безопасности инфраструктур. В работах [1-4] к ним отнесены проблемы сервисов в контексте:

— координации меж объектного взаимодействия;
— развертывание инфраструктуры;
— сетевое взаимодействие сервисов;
— управление данными;
— отладка и мониторинг процессов;
— безопасность;
— архитектурные особенности.

В качестве источников «конфликтов интересов» в ИнИ обозначены []:

— данные;
— сетевое взаимодействие;
— ресурсы;
— конфигурации.

На практике феномен инфраструктурного деструктивизма может проявляться в виде событий информационной безопасности, приводящих к необратимым последствиям. Например, «совокупность случайных факторов» проявление «непредвиденных событий», «закономерных случайностей» и др. Данные ситуации, возникшие на одном из объектов инфраструктуры в итоге, влияют на её работу в целом.

Данные события, ситуационно, предлагается классифицировать следующим образом.

Ситуация 1. Возникновение инфраструктурного деструктивизма при условии наличия внешних деструктивных воздействий. Это могут быть различные кибератаки, вирусные атака и другие возможные злонамеренные воздействия на объекты инфраструктуры из вне. В данной ситуации генез деструктивных воздействий не конкретизирован.

Ситуация 2. Возникновение инфраструктурного деструктивизма 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 информационной инфраструктуры.

Ситуация 3. Возникновение инфраструктурного деструктивизма при отсутствии влияния внешних факторов и изменений в информационной инфраструктуре. Данная ситуация возникает за счет факторов, не зависящих от инфраструктуры и внешних деструктивных воздействий. 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.

Определение@. «Деструктивный мусор» — программный код, внесенный в инфраструктуру после устранения уязвимостей информационной безопасности и ошибок программного кода, реализованный не оптимальным образом.

Накопление «деструктивного мусора» является не контролируемым процессом и приводит к необратимым процессам на объектах инфраструктуры.

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 инфраструктуру 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 эффекта инфраструктурного деструктивизма, во многом зависит от внутренних состояний, внутренних целей и сценариев работы объектов инфраструктуры (рисунок 1).

Обозначенное необходимо рассматривать на уровне сервисов, так как в основе современных инфраструктурах заложены сервисные архитектуры. Одним из приоритетных вопросов является вопрос, связанный с обнаружением эффектов инфраструктурного деструктивизма сервисов, что предлагается решить на основе разных подходов.

Схема организации системы оценки эффектов инфраструктурного деструктивизма

На основе антропоморфических моделей, представленных в [5,7], разработана схема организации архитектуры системы оценки деструктивных возможностей для двух взаимодействующих сервисов инфраструктуры, которая представлена на рисунке 2.

Исходной точкой при организации архитектуры схема организации (рис. 2) 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 инфраструктуры. В том числе здесь реализуется информационно аналитическая система анализа антропомор-

Рис. 1. Структурная схема факторов влияющих на инфраструктурный деструктивизм

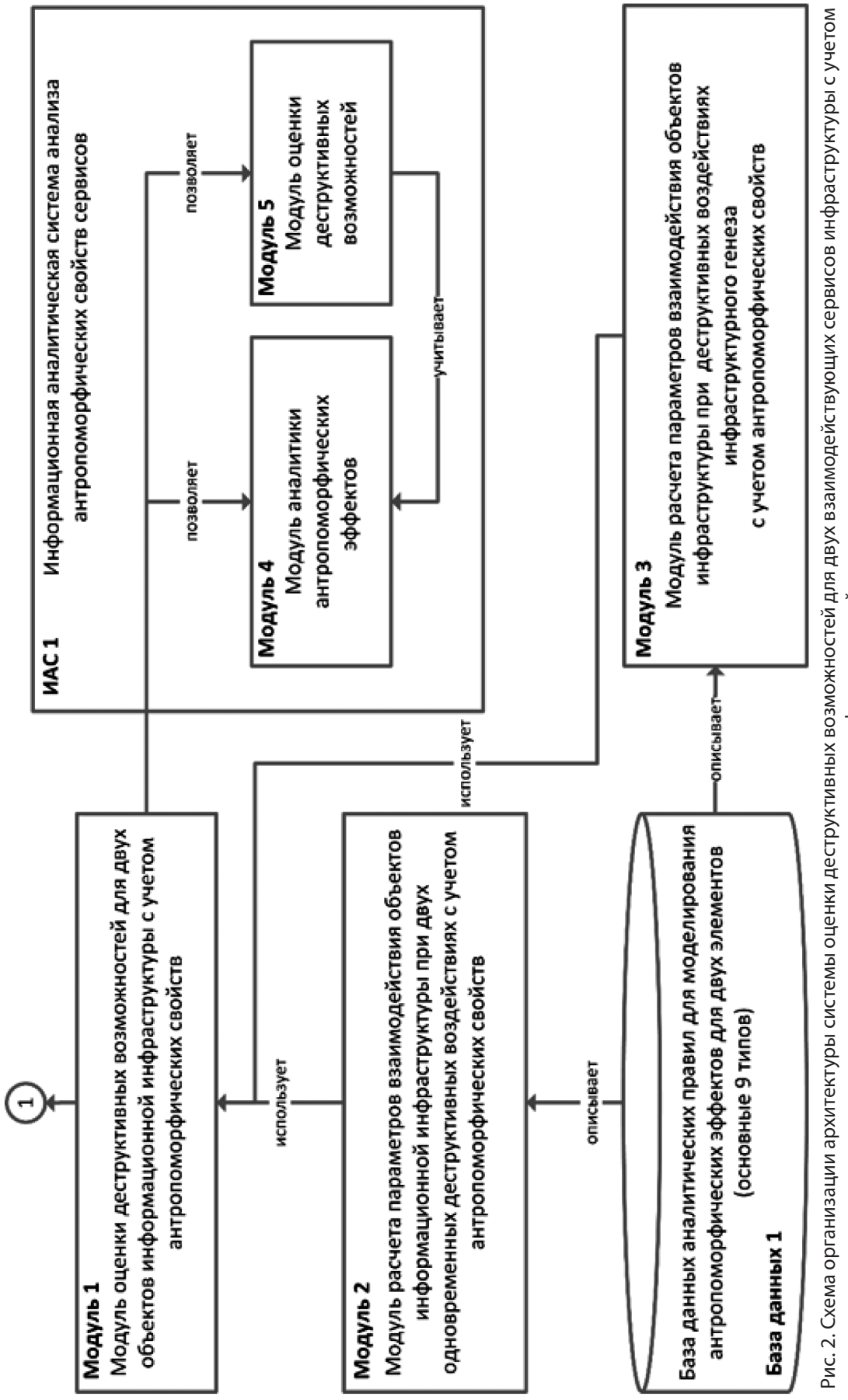

Рис. 2. Схема организации архитектуры системы оценки деструктивных возможностей для двух взаимодействующих сервисов инфраструктуры с учетом антропоморфических свойств

фических 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 инфраструктуры, которая позволяет учитывать антропоморфические свойства сервисного взаимодействия.

Схема организации системы оценки взаимодействия нескольких сервисов инфраструктуры

Представленный инструментарий выше является ограниченным в связи с количеством рассматриваемых объектов инфраструктуры, а именно рассматривается ситуация, когда количество сервисов равно двум. Для универсализации рассматриваемого решения опишем каким образом будет выполняться оценка взаимодействия нескольких сервисов. На рисунке 3 представлена схема организации архитектуры системы оценки взаимодействия нескольких сервисов инфраструктуры.

Исходной точкой схемы организации (рис. 3) является «Модуль 10», который генерирует сценарии взаимодействия агентов объектов ИнИ 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 меж объектного взаимодействия агентов объектов инфраструктуры. «Модуль 7» и «Модуль 8» обеспечивают моделирование среды и поведения агентов объектов информационной инфраструктуры с помощью «модуля 6», который является инструментарием, описанным в предыдущем пункте. Также для «Модуля 8» возможно использование «Модуля 9», который описывает механизмы взаимодействия агентов на основе эпидемиологических состояний.

Система агент-ориентированного имитационного моделирования меж объектного взаимодействия множества агентов объектов инфраструктуры «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 инфраструктуры с учетом различных сценариев их взаимодействия.

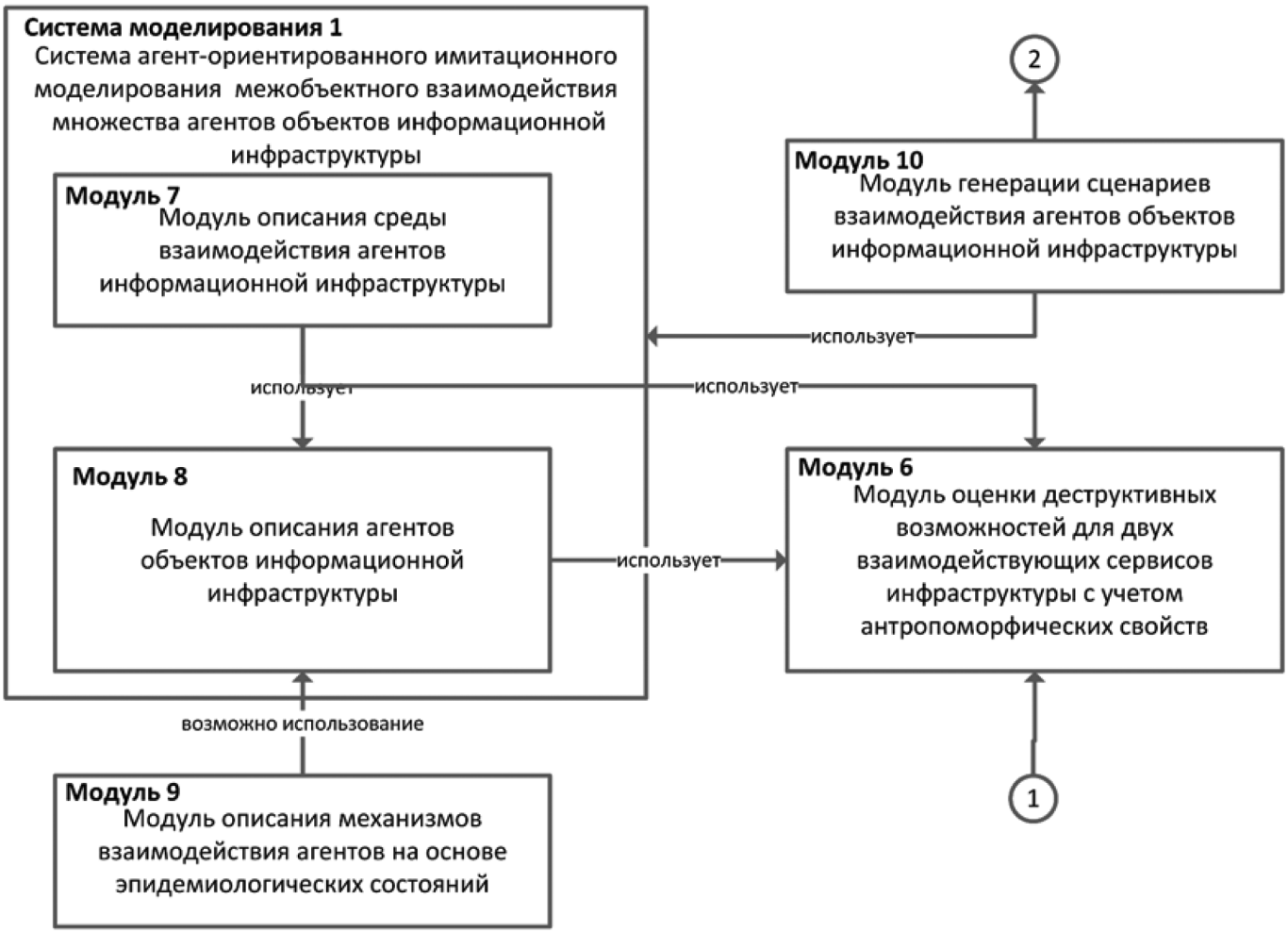

Рис. 3. Схема организации архитектуры системы оценки взаимодействия нескольких сервисов инфраструктуры

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 предыдущем пункте.

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 информационной инфраструктуры.

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 вирус для описания поведенческой активности агентов объектов информационной инфраструктуры.

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 информационной инфраструктуры и определить: худший, нейтральный и наилучший случай.

Приведем описание алгоритма имитационного моделирования взаимодействия множества объектов информационной инфраструктуры на основе онтологии архитектуры системы, представленной на рисунке 4.

Шаг 1. Начало.

Шаг 2. Ввод параметров для агентов объектов информационной инфраструктуры: наборы параметров агентов объектов информационной инфраструктуры

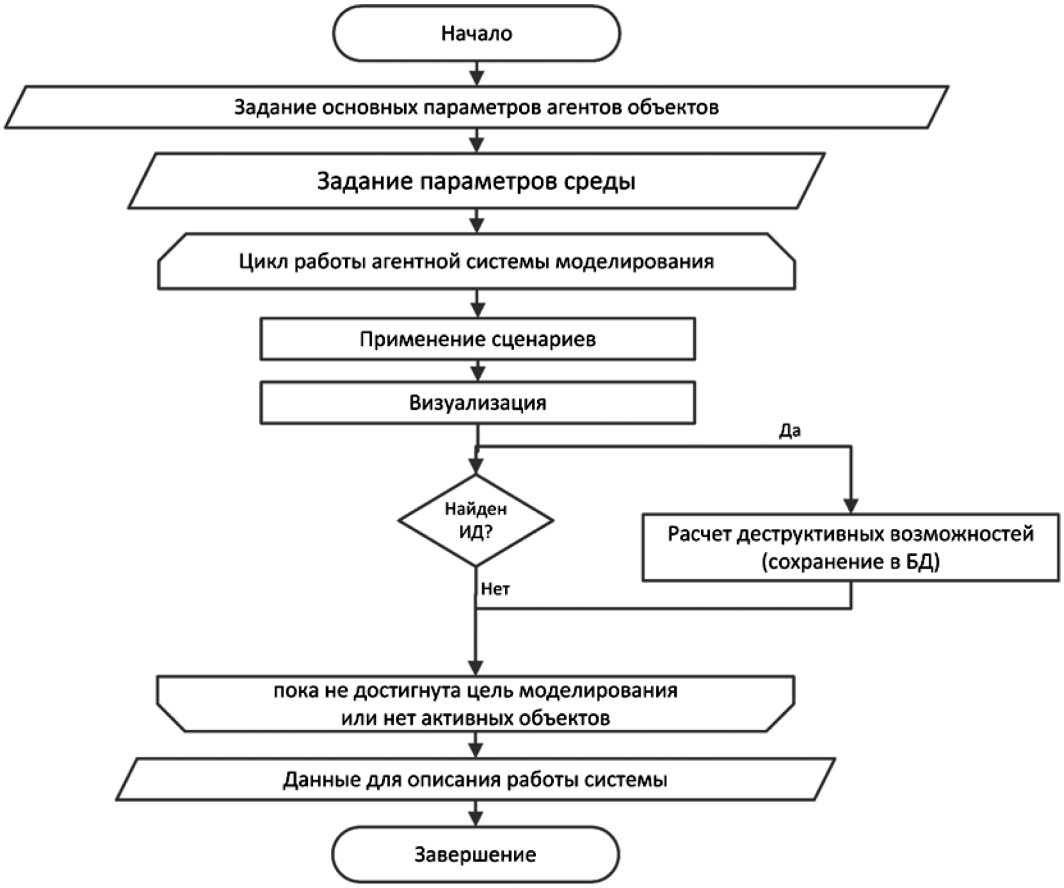

Рис. 4. Обобщенная блок-схема системы имитационного моделирования деструктивных возможностей информационной инфраструктуры

Шаг 3. Генерация сценариев взаимодействия агентов объектов инфраструктуры.

Шаг 4. Имитационное моделирование сценариев взаимодействия агентов объектов информационной инфраструктуры.

Шаг 5. Оценка антропоморфических типов взаимодействия сервисов инфраструктуры

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

Предложенные выше схемы организации и алгоритм объедим в систему имитационной системы информационной инфраструктуры сервисов для прогнозирования эффектов инфраструктурного деструктивизма.

Схема организации имитационной системы информационной инфраструктуры сервисов как средство прогнозирования эффектов инфраструктурного деструктивизма

На рисунке 5 представлена Онтология архитектуры системы оценки меж объектного взаимодействия множества объектов информационной инфраструктуры.

Данную онтологию (Рисунок 5) возможно реализовать, используя технологию цифровых двойников, что позволит на основе анализа журналов событий создать комплекс программных средств для прогнозирования эффектов инфраструктурного деструктивизма для существующих систем, как это сделано в [8].

Обобщив онтологию, представленную на рисунке 5, получим онтологию архитектуры системы оценки инфраструктурного деструктивизма сервисной информационной инфраструктуры представленную на рисунке 6.

Онтология, представленная на рисунке 6 некоторые компоненты, данной онтологии уже реализованы в работах автора [9–11]. Реализация представленной онтологии позволит специалистам информационной безопасности прогнозировать и оценивать динамику рисков от эффектов инфраструктурного деструктивизма.

Заключение

Представленные в данной работе подходы и решения позволяют реализовать информационно аналитическую систему для прогнозирования и оценки динамики рисков от эффектов инфраструктурного деструктивизма сервисных архитектур.

Предложенная концептуальная модель оценки эффектов инфраструктурного деструктивизма является авторской разработкой и в отличие от уже имеющихся позволяет оценивать поведенческие особенности процессов, которые выполняются на базе сервисной архитектуры инфраструктуры. Следует отметить, что на данный момент предложенное решение является одним из возможных вариантов по оценке эффектов инфраструктурного деструктивизма и требуется дополнительные исследования в данном направлении.

Рис. 5. Онтология архитектуры системы оценки меж объектного взаимодействия множества объектов информационной инфраструктуры

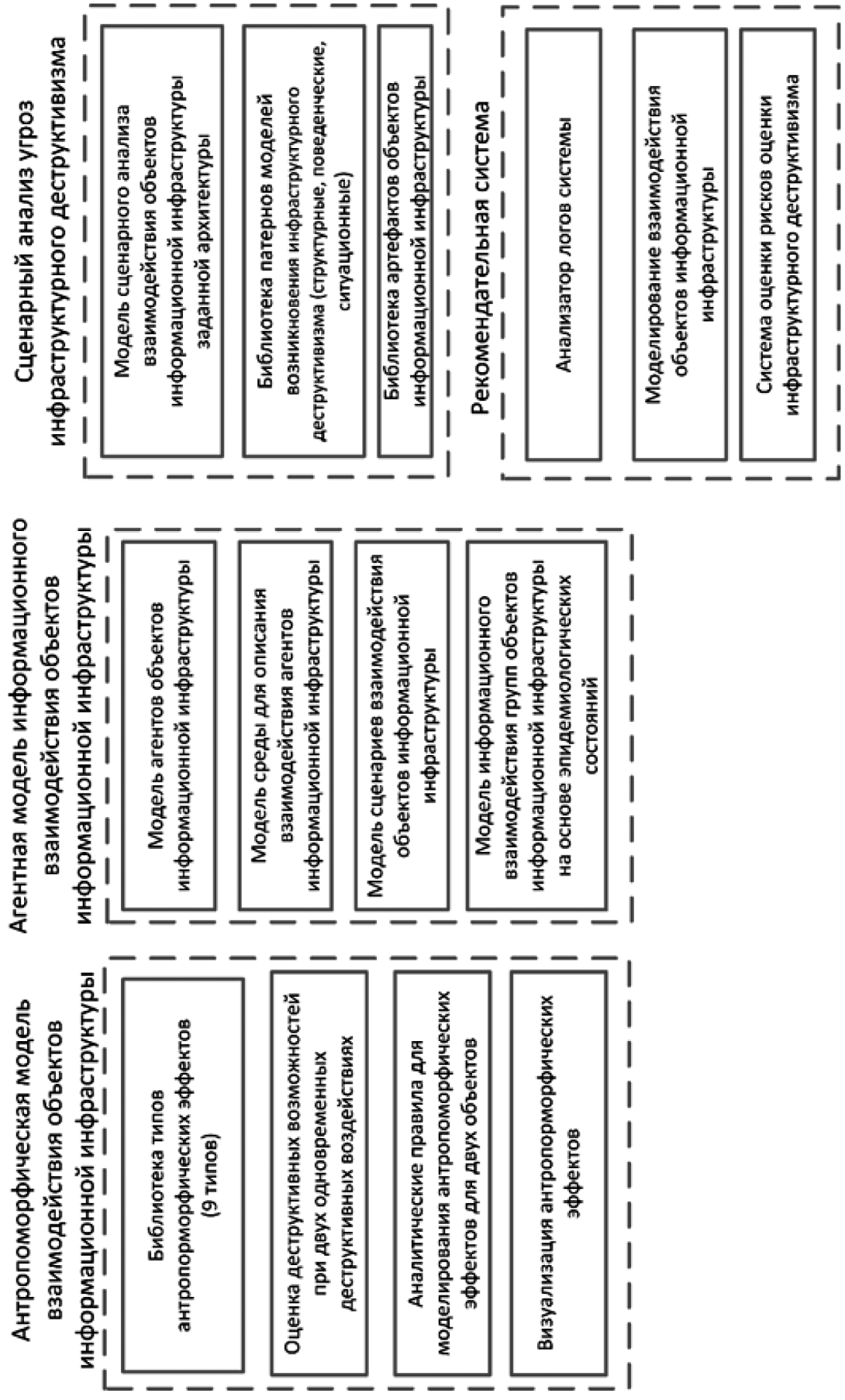

Рис. 6. Онтология архитектуры системы оценки инфраструктурного деструктивизма сервисной информационной инфраструктуры

ЛИТЕРАТУРА

1. Борисовская О.В. Управление рисками безопасности сетевой инфраструктуры при имитационном моделировании бизнес-процессов финансово-кредитных организаций / О.В. Борисовская, А.А. Борисовская // Информационные технологии и математические методы в экономике и управлении (ИТиММ-2023): Сборник статей XII Международной научно-практической конференции имени А.И. Китова. В 2-х книгах, Москва, 23–24 марта 2023 года. — Москва: Российский экономический университет им. Г.В. Плеханова, 2023. — С. 256–264. — EDN FNMNII.
2. Кошелев А.С. Защита от кибератак или обеспечение безопасности инфраструктуры информационных ресурсов / А. С. Кошелев // Управление информационными ресурсами: Материалы XX Международной научно-практической конференции, Минск, 29 марта 2024 года. — Минск: Академия управления при Президенте Республики Беларусь, 2024. — С. 281–282. — EDN NZWOET.
3. Шапенская А.М. Безопасность критической информационной инфраструктуры как приоритетное направление деятельности современного информационного общества / А.М. Шапенская, О.М. Голембиовская, А.С. Трошин // Новые горизонты: Сборник материалов и докладов XI научно-практической конференции с международным участием, Брянск, 15 апреля 2024 года. — Брянск: Брянский государственный технический университет, 2024. — С. 525–529. — EDN PZGXKQ.
4. Вершинин А.Н. Цифровая трансформация информационной безопасности критической информационной инфраструктуры в условиях импортозамещения / А.Н. Вершинин // Научный аспект. — 2023. — Т. 2, № 5. — С. 209–217. — EDN GFFAME.
5. 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. — DOI 10.1007/978-3-030-97020-8_51. — EDN GGKXDH.
6. 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. — EDN FWCTSV.
7. Rusakov A., Maksimova E. (2024). 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.
8. ИТ-инфраструктура для построения интеллектуальных систем управления развитием и функционированием систем энергетики на основе цифровых двойников и цифровых образов / Н.И. Воропай, Л.В. Массель, И.Н. Колосок, А.Г. Массель // Известия Российской академии наук. Энергетика. — 2021. — № 1. — С. 3–13.
9. Свидетельство о государственной регистрации программы для ЭВМ № 2022685869 Российская Федерация. Программное обеспечение системы моделирования меж объектных системных связей инфраструктурного характера в информационных системах: № 2022685248: заявл. 15.12.2022: опубл. 28.12.2022 / А.М. Русаков.
10. 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.
11. 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.

Журнал «Современная наука: актуальные проблемы теории и практики»