Интеллектуальная защита критических информационных инфраструктур: интеграция цифровых двойников и нейросетевых методов обнаружения угроз

Е. С. Митяков[1], А. И. Ладынин[2], А. Г. Шмелева[3]

МИРЭА – Российский технологический университет

[1]iyao@mail.ru, [2]andrey.ladynin@hotmail.com, [2]ann_shmeleva@mail.ru

И. Д. Казакевич

Нижегородский государственный технический университет им. Р.Е. Алексеева; МИРЭА – Российский технологический университет

kazakevich.igor2000@gmail.com

***Аннотация*. В статье рассматривается интеграция цифровых двойников и нейросетевых методов для интеллектуальной защиты критических информационных инфраструктур (КИИ). Предлагается архитектура, в которой цифровые двойники используются для моделирования атак и тестирования защитных механизмов, а нейросетевые алгоритмы (автоэнкодеры, LSTM, CNN) применяются для анализа аномалий, прогнозирования угроз и оптимизации стратегий реагирования. Разработанная модель агент-ориентированного моделирования позволяет эффективно выявлять уязвимости и адаптировать защитные меры в режиме реального времени. Представлены экспериментальные результаты, демонстрирующие эффективность гибридного подхода, сочетающего цифровые двойники и искусственный интеллект.**

Ключевые слова: критическая информационная инфраструктура, цифровые двойники, нейросетевой анализ, обнаружение аномалий, искусственный интеллект, машинное обучение, кибербезопасность, моделирование атак

I. Введение

Современные КИИ сталкиваются с растущими угрозами кибератак, требующими инновационных подходов к обеспечению безопасности [1]. Цифровые двойники (ЦД), изначально разработанные для оптимизации производственных процессов, стали ключевым инструментом моделирования атак и тестирования защитных механизмов. Их способность воспроизводить поведение физических систем в виртуальной среде позволяет анализировать уязвимости без риска для реальных объектов [2].

ЦД являются ключевой технологией Индустрии 4.0, обеспечивающей передовые возможности моделирования для оптимизации и прогнозирования промышленных процессов. Однако их широкое внедрение сопровождается серьезными проблемами безопасности, которые необходимо учитывать для обеспечения надежности и защиты критически важных систем. Цифровые двойники, по определению в работе [3], представляют собой виртуальные копии физических систем, интегрирующие данные в реальном времени. В контексте кибербезопасности они используются для симуляции атак, таких как DDoS или эксплуатация уязвимостей IoT-устройств [4]. Технологии искусственного интеллекта, интегрированные в ЦД, позволяют автоматизировать обнаружение аномалий и реагирование на инциденты [5].

ЦД интегрируют различные технологии, включая киберфизические системы, промышленный Интернет вещей (IIoT) и искусственный интеллект, создавая сложную среду с множеством потенциальных уязвимостей. Эти угрозы обусловлены взаимодействием цифровых и физических компонентов, что пока недостаточно изучено [6]. Дополнительную сложность вносит концепция Интернета цифровых двойников (IoDT), который требует безопасного обмена данными и защищенной коммуникации [7]. Использование цифровых двойников в критической инфраструктуре, например в энергосистемах, может представлять значительные риски.

Высокоточный цифровой двойник может быть использован злоумышленниками для выявления уязвимостей энергосети, что потенциально ведет к целевым атакам и нарушению работы инфраструктуры [8]. Таким образом, ЦД выступают одновременно и инструментом для оценки рисков, и возможной точкой входа для атак. Современные исследования предлагают архитектуры безопасности для цифровых двойников, ориентированные на управление процессами и защиту данных от несанкционированного доступа. Однако безопасность часто не является приоритетом при разработке ЦД, что приводит к их потенциальному неправильному использованию и увеличению уязвимостей [10].

Агент-ориентированные модели, как показано в исследованиях [11] и [12], эффективны для имитации поведения разнородных агентов — от хакеров до систем защиты. Агент-ориентированное моделирование (АОМ), применяемое в промышленном контексте, адаптировано для имитации действий злоумышленников и оценки устойчивости систем. Работа [13], демонстрируют эффективность комбинации АОМ и ЦД для прогнозирования сложных сценариев, включая целенаправленные атаки на цепочки поставок.

Исследование выполнено при финансовой поддержке Российского научного фонда (проект № 23-78-10009).

Область исследования безопасности цифровых двойников продолжает развиваться. Будущие работы должны быть направлены на создание стандартных архитектур защиты и повышение устойчивости ЦД к известным и новым угрозам. С учетом их растущей популярности, особенно в производственном и энергетическом секторах, решение этих вопросов критично для безопасного внедрения технологии. Таким образом, перенос процессов информационной безопасности в цифровую среду и их моделирование с учетом участия различных агентов, несущих различные риски, может стать полезным для КИИ. Цифровой двойник и агенто-ориентированное моделирование могут совместно использоваться для более глубокого понимания и управления сложными системами, обеспечивая более точное и детализированное моделирование взаимодействия между агентами и объектами в цифровой среде.

II. Постановка задачи

Представим авторское видение концептуальной схема агент-ориентированного моделирования КИИ. На рис. 1 представлена концептуальная схема агент-ориентированного моделирования многоуровневых критически важных информационных инфраструктур (КИИ). Данная схема иллюстрирует иерархическую организацию системы управления КИИ с учетом интеграции цифровых двойников для моделирования атак и защиты. В модели выделяются объекты и субъекты управления, каждый из которых представлен агентами, взаимодействующими на различных уровнях иерархии.

Модель управления КИИ представлена в четырехуровневой структуре, где каждый уровень отвечает за решение специфических задач, мониторинг угроз и применение защитных механизмов. Цифровой двойник в данной системе играет ключевую роль, обеспечивая сбор данных, анализ сценариев атак и прогнозирование возможных последствий угроз. Он также используется для оценки эффективности применяемых мер защиты и адаптации стратегии противодействия кибератакам.

Рис. 1. Концептуальная схема агент-ориентированного моделирования КИИ

В рамках данной модели нижний уровень отвечает за мониторинг поведения пользователей и функционирование отдельных узлов инфраструктуры, тогда как верхние уровни обеспечивают стратегическое управление безопасностью на уровне предприятий, отраслей и государства. Взаимосвязь между уровнями представлена потоками управления и данными о выявленных угрозах и атаках.

На рис. 2 представлена схема поддержки принятия решений на основе технологий агент-ориентированного моделирования, интегрированных с цифровыми двойниками.

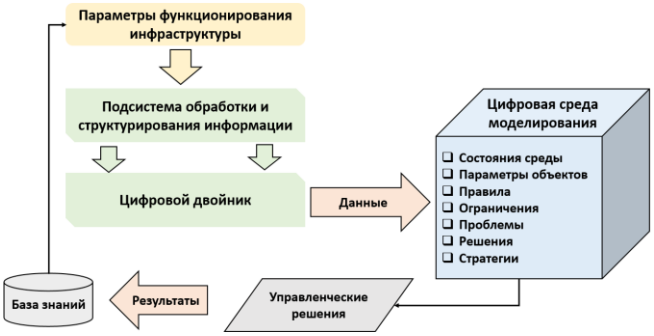

Рис. 2. Система поддержки принятия решений на основе цифровых двойников в КИИ

В систему поддержки принятия решений интегрирован нейросетевой модуль для анализа аномалий. Глубокие нейронные сети (DNN) и автоэнкодеры используются для обработки данных цифрового двойника в реальном времени, выявления отклонений от нормы и классификации потенциальных угроз. На основе предсказаний нейросети система предлагает оптимальные меры реагирования, что повышает скорость и точность принятия решений в условиях кибератак.

Предлагаемая структура удовлетворяет принципам системного анализа, обеспечивая декомпозицию проблемы защиты КИИ, анализ внутренних и внешних угроз, а также оценку влияния атак на различные компоненты инфраструктуры. Основу модели составляет экономико-математическое и компьютерное моделирование, позволяющее анализировать кибератаки, предсказывать их развитие и вырабатывать оптимальные стратегии защиты.

III. Моделирование аномалий в КИИ

В систему поддержки принятия решений интегрирован нейросетевой модуль для анализа аномалий. Глубокие нейронные сети (DNN) и автоэнкодеры используются для обработки данных цифрового двойника в реальном времени, выявления отклонений от нормы и классификации потенциальных угроз. На основе предсказаний нейросети система предлагает оптимальные меры реагирования, что повышает скорость и точность принятия решений в условиях кибератак.

Предлагаемая структура удовлетворяет принципам системного анализа, обеспечивая декомпозицию проблемы защиты КИИ, анализ внутренних и внешних угроз, а также оценку влияния атак на различные компоненты инфраструктуры. Основу модели составляет экономико-математическое и компьютерное моделирование, позволяющее анализировать кибератаки, предсказывать их развитие и вырабатывать оптимальные стратегии защиты.

Применение агент-ориентированного моделирования для анализа КИИ предполагает классификацию агентов по типу, параметрам, состояниям и стратегиям защиты. Важнейшими параметрами являются уровень угроз, степень цифровизации, зависимости от импортных технологий и уязвимости инфраструктуры. Это представлено на рис. 3.

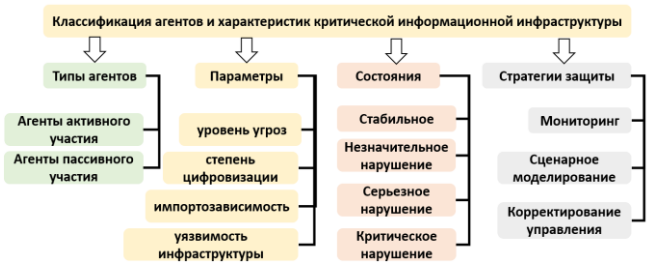

Рис. 3. Классификация агентов и характеристик КИИ

На основе данной классификации выделяются состояния функционирования КИИ, отражающие ее текущий уровень безопасности. Разрабатываются механизмы мониторинга угроз, анализируются сценарии атак и корректируются стратегии защиты в соответствии с выявленными рисками. В результате формируются эффективные управленческие решения, включающие реактивный, проактивный и комбинированный подходы к обеспечению безопасности. В предложенной модели ключевым элементом является многослойная структура цифровых двойников, обеспечивающая комплексный анализ угроз и защитных мер. Каждый уровень модели включает цифровые двойники, разрабатываемые для более детального анализа предыдущего уровня (рис. 4).

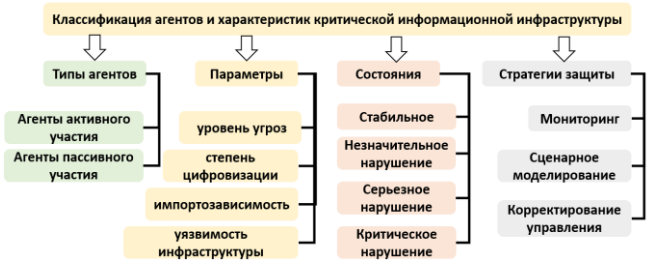

Рис. 4. Взаимосвязь цифровых двойников разного уровня в КИИ

Для реализации данной структуры используются специализированные программные решения, позволяющие интегрировать цифровые двойники в систему управления КИИ. Современные платформы, такие как Mavim и Ortelius DTO, предоставляют инструменты для моделирования атак и разработки мер защиты в режиме реального времени.

На каждом уровне цифрового двойника применяются нейросетевые алгоритмы для анализа угроз. Конволюционные нейронные сети (CNN) обрабатывают визуальные данные и сигналы с датчиков, а рекуррентные сети (LSTM, GRU) анализируют временные ряды параметров системы. Интеграция нейросетей позволяет не только фиксировать атаки, но и прогнозировать их развитие, обеспечивая проактивную защиту КИИ.

Таким образом, цифровой двойник критически важной информационной инфраструктуры представляет собой объект цифровизации, описывающий реальные угрозы и сценарии их реализации, а также позволяющий формировать эффективные стратегии защиты. Он охватывает взаимодействие различных уровней управления КИИ, обеспечивая адаптивное реагирование на угрозы и моделирование последствий атак.

Модель цифровой архитектуры защиты КИИ представлена в трех измерениях (рис. 5):

1. слои управления безопасностью, включающие уровни мониторинга, анализа угроз и принятия решений;
2. этапы жизненного цикла угроз, описывающие их выявление, классификацию, анализ последствий и разработку мер реагирования;
3. используемые ресурсы, включающие технологии защиты, системы мониторинга и базы данных угроз.

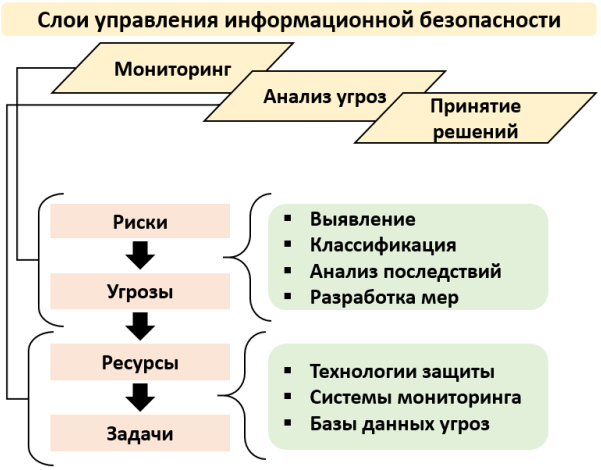

Рис. 5. Модель цифровой архитектуры защиты КИИ

В рамках данного исследования использованы несколько алгоритмов машинного обучения для анализа синтетических данных, моделирующих поведение электрической сети в усло

Первый параметр включает уровни защиты, начиная от операционной деятельности до стратегического управления рисками. Второй параметр отражает жизненный цикл угроз: от их возникновения до реализации мер противодействия. Третий параметр охватывает материальные и нематериальные ресурсы, включая аналитические инструменты, системы обнаружения атак и механизмы реагирования.

Таким образом, цифровой двойник КИИ представляет собой интеграцию различных моделей, включая цифровые двойники узлов инфраструктуры, процессов мониторинга и стратегического управления безопасностью. Его применение позволяет прогнозировать кибератаки, разрабатывать стратегии защиты, повышать устойчивость инфраструктуры к угрозам и обеспечивать эффективное управление безопасностью в условиях динамично изменяющейся внешней среды.

Эксперименты и сценарный анализ наряду с необходимостью учета неопределенности и рисков подталкивают к использованию цифровых двойников для моделирования атак и защиты КИИ, а поддержка стратегического планирования требует цифровых инструментов имитационного моделирования критически важных систем (рис. 6).

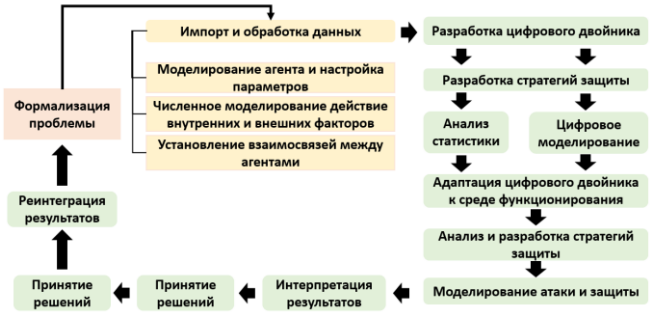

Рис. 6. Механизм работы агент-ориентированной модели

Алгоритм моделирования агент-ориентированной модели можно представить в виде трех этапов:

1. Начальная настройка: создание агентов, определение их параметров, установка окружения и моделирование возможных атак.
2. Симуляция: моделирование сценариев атак, обмен данными между агентами, выбор стратегий защиты и сбор статистики.
3. Получение результатов: анализ данных, оценка эффективности защитных мер, прогнозирование дальнейших угроз и визуализация результатов.

Отметим, что нейросетевые алгоритмы интегрированы в процесс моделирования атак и защиты КИИ. В блоке "Симуляция" используется LSTM для прогнозирования атак на основе исторических данных. В блоке "Получение результатов" нейросети обучаются на синтетических данных, генерируемых цифровыми двойниками, и помогают вырабатывать оптимальные стратегии защиты. Гибридный подход, сочетающий агент-ориентированное моделирование и нейросетевые методы, позволяет достоверно оценивать риски и разрабатывать эффективные контрмеры.

Формализация правил поведения агентов является ключевым аспектом модели. Каждое предприятие выбирает стратегии защиты, исходя из внутренних условий, угроз окружающей среды и стратегий других агентов. Выбор подходов к кибербезопасности также зависит от управленческих решений и готовности к внедрению цифровых технологий.

IV. Выводы

Развитием данной модели является разработка стратегий защиты на основе комплексного анализа, включая экономико-математическое моделирование, сценарно-прогностический анализ и численное моделирование с использованием цифровых двойников. Интеграция современных аналитических инструментов в систему управления КИИ способствует эффективному решению задач кибербезопасности и устойчивости инфраструктуры в условиях цифровизации экономики.

Список литературы

[1] Юдин А., Митяков Е., Грошева П., Ладынин А., Мякишев Ю. Моделирование многоуровневых промышленных экосистем на основе агентно-ориентированного подхода // *Relacoes Internacionais no Mundo Atual*. 2023. Т. 4, № 42. С. 703.

[2] Jiang Y., Yin S., Li K., Luo H., Kaynak O. Industrial applications of digital twins // *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*. 2021. Vol. 379. P. 20200360. DOI: 10.1098/rsta.2020.0360.

[3] Макаров В.Л., Бахтизин А.Р., Бекларян Г.Л. Разработка цифровых двойников для производственных предприятий // *Бизнес-информатика*. 2019. Т. 13, № 4. С. 7–16. DOI: 10.17323/1998-0663.2019.4.7.16.

[4] Lu Y., Liu C., Kevin I., Huang H., Xu X. Digital Twin-driven smart manufacturing: connotation, reference model, applications and research issues // *Robotics and Computer-Integrated Manufacturing*. 2020. Vol. 61. Article ID 101837.

[5] Dirnfeld R., De Donato L., Flammini F., Samanazari M., Vittorini V. Railway Digital Twins and Artificial Intelligence: Challenges and Design Guidelines // *Proceedings of the International Conference on Computer Safety, Reliability, and Security*. 2022. P. 8. DOI: 10.1007/978-3-031-16245-9_8.

[6] Alcaraz C., López J. Digital Twin: A Comprehensive Survey of Security Threats // *IEEE Communications Surveys & Tutorials*. – 2022. Vol. 24. P. 1475–1503. DOI: 10.1109/COMST.2022.3171465.

[7] Wang Y., Su Z., Guo S., Dai M., Luan T., Liu Y. A Survey on Digital Twins: Architecture, Enabling Technologies, Security and Privacy, and Future Prospects // *IEEE Internet of Things Journal*. – 2023. – Vol. 10. P. 14965–14987. DOI: 10.1109/JIOT.2023.3263909.

[8] Guikema S., Flage R. Digital twins as a security risk? // *Risk analysis : an official publication of the Society for Risk Analysis*. 2024. DOI: 10.1111/risa.15749.

[9] Gehrmann C., Gunnarsson M. A Digital Twin Based Industrial Automation and Control System Security Architecture // *IEEE Transactions on Industrial Informatics*. 2020. Vol. 16. P. 669–680. DOI: 10.1109/TII.2019.2938885.

[10] Heluany J., Gkioulos V. Survey on Digital Twins: from concepts to applications // *Proceedings of the 18th International Conference on Availability, Reliability and Security*. 2023. DOI: 10.1145/3600160.3605070.

[11] Коровин Г.Б. Архитектура агентно-ориентированной модели цифровой трансформации промышленного комплекса региона // *Журнал новой экономики*. 2020. Т. 21, № 3. С. 158–174. DOI: 10.29141/2658-5081-2020-21-3.

[12] Huckert J., Sidorenko A., Wagner A. Analysis and Assessment of Multi-Agent Systems for Production Planning and Control // *Proceedings of the International Conference on Industrial Engineering and Operations Management*. 2023. P. 77. DOI: 10.1007/978-3-031-38241-3_77.

[13] Orozco-Romero A., Arias Portela C., Marmolejo J. The Use of Agent-Based Models Boosted by Digital Twins in the Supply Chain: A Literature Review // *Proceedings of the International Conference on Industrial Engineering and Operations Management*. 2020. P. 62. DOI: 10.1007/978-3-030-33585-4_62.