УДК 621.311:004.052

КИБЕРУСТОЙЧИВОСТЬ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ

М.Д. Шубин, А.Ю. Русин
Тверской государственный технический университет (г. Тверь)

Аннотация. В статье представлена модель цифрового двойника, предназначенная для критически важных киберинфраструктур. Она сосредоточена на анализе возможных проблем, возникающих при интеграции вычислительных, коммуникационных и физических компонентов данных киберинфраструктур. Особое внимание уделяется электроэнергетическому сектору, поскольку нарушения его устойчивости могут привести к серьезным рискам для страны. Для расширения возможностей взаимодействия с системой, повышения осведомленности о происходящих событиях и улучшения мер реагирования на киберинциденты разработана комплексная модель. Она основана на исследованиях в области информационной безопасности, ситуационной осведомленности и формирования общей оперативной картины. Применение модели способствует сокращению времени реагирования, что позволяет минимизировать ущерб от кибератак для электроэнергетических систем. В заключение обсуждены перспективы применения данного подхода в будущих исследованиях и отмечена его значимость для электроэнергетики.

Ключевые слова: цифровой двойник, устойчивость, реагирование на инциденты, предотвращение инцидентов, ситуационная осведомленность, искусственный интеллект.

DOI: 10.46573/2658-7459-2025-2-74-80

Социальные, экономические и политические системы в значительной мере зависят от критически важных киберинфраструктур (CCI), которые обеспечивают ключевые услуги для их функционирования. За последние двадцать лет эти системы активно интегрируют вычислительные, коммуникационные и киберфизические компоненты. С одной стороны, такая интеграция повышает удобство, эффективность и устойчивость систем. С другой стороны, выход в киберпространство сопровождается новыми рисками. Основная проблема состоит в том, что указанные инфраструктуры становятся уязвимыми к кибератакам, которые направлены как на системы управления, так и на кражу данных [1].

В настоящей статье фокус сделан на энергетическом секторе, особенно на анализе электроэнергетических CCI, таких как операторы электросетей. Уязвимости цифровых систем и длительное воздействие расширенных постоянных угроз (APT) создают серьезные риски и потенциально могут нанести ущерб политическим и экономическим системам, а также поставить под угрозу национальную безопасность [2]. Таким образом, для обеспечения устойчивости CCI необходимо разрабатывать и внедрять эффективные механизмы предотвращения инцидентов и реагирования на них.

В рамках статьи представлена модель киберустойчивости для CCI. Она объединяет профилактику и реагирование на различных уровнях организации, предлагая интегрировать систему цифровых двойников [3, 4]. Цифровые двойники позволяют

создать безопасную тестовую среду для киберфизических систем, повышают ситуационную осведомленность и эффективность операционных сценариев, что улучшает координацию при реагировании на инциденты, киберготовность и управление киберинцидентами.

Предыдущие исследования в области управления информационной безопасностью, акцентированные на инцидентах, составляют основу для метода исследования дизайна действий (ADR) [5]. Эта концептуальная модель включает в себя возможности для обнаружения атак на CCI с помощью детальной аналитики данных и причинного анализа, позволяющего определять источники аномалий, что дает возможность использовать цифрового двойника для тестирования стратегий смягчения последствий, включая превентивные меры и обучение.

В литературе по киберустойчивости выделяют две ключевые парадигмы, применяемые организациями для защиты своих информационных ресурсов: парадигму предотвращения и парадигму реагирования.

Парадигма предотвращения ориентирована на внедрение зрелой системы разведки угроз, адаптированной к нуждам критически важной киберинфраструктуры. Такие превентивные структуры формируются на основе анализа прошлого опыта с целью предсказания будущих угроз.

Парадигма реагирования, напротив, направлена на обеспечение готовности организации к противодействию новым, непредсказуемым угрозам. Данный подход требует быстрых и решительных действий; гибкость в данном случае особенно важна для обеспечения оперативного реагирования [6].

Несмотря на различия, данные подходы не исключают друг друга и могут эффективно объединяться для повышения устойчивости и гибкости организации [7]. Некоторые авторы отмечают, что ситуация реагирования в таком контексте обладает обучающим потенциалом, создавая «формирующую среду», способствующую инновациям и обучению. Хотя основная цель реагирования заключается в обеспечении его непрерывности, успешное решение этой задачи требует четкой, оперативной и скоординированной коммуникации с теми, кто отвечает за превентивные меры [8].

Кроме того, в литературе подчеркивается, что работа в пространстве ситуационной осведомленности (SA) улучшает оценку рисков и управление ими в CCI. Ситуационная осведомленность описывается как метод мониторинга состояния сетевой инфраструктуры организации и оценки влияния текущей сетевой ситуации на критические задачи. Преимущества SA затрагивают обе парадигмы и усиливаются при их совместном использовании, поддерживая организационное обучение.

Исследования также указывают на разрыв между теорией и практикой в межорганизационном управлении кризисами, где ключевым аспектом является обмен информацией [9]. Этот обмен зачастую отсутствует или работает неэффективно из-за внутренних политик, таких как принцип «необходимости знать или не знать», который активируется во время кризисов. Организации также могут воздерживаться от раскрытия информации из-за стратегических или репутационных рисков. В этих условиях общая оперативная картина (COP) может служить посредником, особенно в межорганизационном взаимодействии.

Цифровые двойники играют важную роль в киберустойчивости как технологический артефакт. Цифровой двойник представляет собой виртуальное отражение физической системы, такой как CCI [3, 4]. В отличие от традиционных офлайн-моделей, он

более детально воспроизводит функциональность системы, включая как физические характеристики, так и ИТ-интерфейсы, протоколы, а также высокоуровневую операционную и управляющую логику. Как правило, цифровые двойники работают в реальном времени, параллельно с физической системой. Кроме того, цифровые двойники могут использоваться как платформа для тестирования новых технологий и процедур.

Несмотря на широкое признание цифровых двойников в практике, отсутствует систематическая модель, описывающая их организационное применение. Требуется исследование взаимодействия между участниками CCI и уровнями, на которых оно происходит. В этом контексте цель исследования – разработать и проверить модель киберустойчивости критической киберинфраструктуры с помощью интеграции цифрового двойника.

Литературные данные стали основой для представления результатов проекта, выполненного в рамках подхода ADR, направленного на повышение киберустойчивости критически важной инфраструктуры. ADR является специализированным ответвлением метода научных исследований дизайна (DSR) [5], в границах которого анализируется процесс непрерывной адаптации артефакта к специфике его локального применения. В методологии выделено три исследовательских цикла DSR: строгость, дизайн (или проектирование) и релевантность.

Цикл строгости связывает мероприятия проектирования с существующими знаниями, одновременно интегрируя и расширяя их. Цикл проектирования, являющийся основным из трех циклов DSR, фокусируется на итеративном процессе создания и оценки артефакта. Цикл релевантности увязывает проектные задачи с их практической средой, обеспечивая соответствие дизайна требованиям реальных задач. В качестве теоретической основы исследования были использованы знания об управлении рисками в сложных технологических системах [7].

Первоначально использовались предыдущие исследования в области киберустойчивости для определения главной проблемы проектирования. В частности, для разработки модели, ориентированной на инциденты и объединяющей парадигмы реагирования и предотвращения на основе двухконтурного процесса обучения, был использован подход, базирующийся на концептуальной модели Баскервиля.

Изложенные ранее концепции, касающиеся рисков в высокотехнологичных системах, активно использовались при разработке комплексной модели киберустойчивости критической информационной инфраструктуры. Созданная модель представляет собой теоретически обоснованный артефакт, сочетающий объяснительные аспекты теорий организационного обучения с проектной направленностью цикла действий, цель которого заключается в обеспечении безопасности [5].

В то же время взаимодействие с практиками выявило, что базовая модель недостаточно учитывает высокую степень автоматизации современных CCI и их взаимосвязь с внешними субъектами. На этапе разработки, реализации и оценки проекта ADR участники выделили цифровой двойник и компьютерное моделирование как ключевые элементы для создания киберустойчивой структуры CCI. Эта структура включает три основных уровня, соответствующих вертикальной иерархии большинства организаций, связанных с CCI. Технический уровень охватывает непосредственно саму CCI, и при возникновении инцидента процесс реагирования организации инициирует обнаружение угрозы и реагирование на нее, за которыми следует подтверждение инцидента, а также фазы восстановления и укрепления системы. По мере продвижения

мероприятий подключается операционный уровень, охватывающий координацию, коммуникацию, контроль и разведку.

Функционирует CCI и в более широкой экосистеме, где на этапе обнаружения на техническом уровне запускается процесс обмена информацией с внешними субъектами. Этот обмен направлен на формирование межсекторального стратегического взаимодействия в отношении инцидента, охватывающего не только другие организации, но и институциональных участников, таких как государственные и правоохранительные органы. На организационном и экосистемном уровнях выполняются три ключевые функции – информирование, сдерживание и установление стандартов, – которые обеспечивают обратную связь для профилактических мер. На операционном уровне они переводятся в организационные требования, а на уровне экосистемы – в политические стандарты. Оба набора требований воплощаются в виде превентивных технических решений, таких как индикаторы и системы раннего оповещения [3, 4].

С использованием интегрированного цифрового двойника, имитирующего исходную CCI, эти элементы могут быть направлены на реализацию превентивных мер. Такой подход имеет ряд преимуществ. Во-первых, цифровой двойник представляет собой ценность для технического уровня, предлагая CCI-платформу в виде «песочницы» для киберфизических систем и возможности киберполигона. Таким образом, цифровые двойники могут частично разгрузить реальную CCI. Кроме того, на операционном уровне они позволяют интегрировать обучение, ориентированное на ситуационную осведомленность, во все функции организации. Тот же подход применим и на межведомственном уровне экосистемы, где цифровой двойник помогает принимать решения, фокусируясь на COP. Основное преимущество этой модели заключается в том, что интегрированный цифровой двойник предоставляет тестовую среду и механизмы для проверки набора превентивных мер, включая контрольные индикаторы и раннее предупреждение. Таким образом, он эффективно соединяет парадигмы предотвращения и реагирования благодаря централизации инцидента в процессе обучения. Еще одним преимуществом является экосистемная природа такой интеграции [8].

Энергетическая инфраструктура – это одна из наиболее критически важных систем, поддерживающих функционирование многих других отраслей. Однако уникальные особенности культур и процедур каждой организации затрудняют координацию при киберинцидентах, так как взаимодействие между участниками усложняется конфликтами и отсутствием единого механизма обмена данными. Информация о киберугрозах часто распространяется через неформальные, доверительные сети, что снижает осведомленность об уязвимостях.

Для повышения киберустойчивости в критически важных инфраструктурах проводились значительные исследования, включая разработку процессов и стандартов для разных отраслей. Операторам электросетей важно своевременно выявлять угрозы и быстро передавать информацию как внутри отрасли, так и регулирующим органам. Международное сотрудничество и согласованные приоритеты в реагировании на инциденты помогут быстрее выявлять угрозы и ликвидировать их, что позволит защитить CCI в энергетическом секторе.

В то же время цифровизация CCI, несмотря на свои преимущества, увеличивает сложность системы и повышает риски кибератак. Уязвимости присутствуют на всех уровнях: от генерации до распределения и рыночных услуг, что требует постоянного обновления решений по защите. Кроме атак, усилившаяся взаимосвязанность

инфраструктуры также создает риск непреднамеренных инцидентов, таких как ошибки персонала или технические сбои [10].

Внедрение цифрового двойника в критически важные инфраструктуры способствует повышению их киберустойчивости, объединяя функции профилактики и реагирования и поддерживая как внутриорганизационное, так и межорганизационное обучение. Значима роль SA и COP, которые способствуют согласованности действий и, как следствие, эффективной защите CCI в рамках действующих правовых норм.

Вклад настоящего исследования в обеспечение устойчивости критических киберинфраструктур состоит в следующем. Во-первых, адаптирована и операционализирована модель Баскервиля, которая теперь учитывает развитие технологий и возможностей мониторинга киберугроз, объединяя инструменты профилактики и реагирования. Во-вторых, добавлен межорганизационный компонент к инцидент-ориентированному подходу, что позволяет учитывать взаимозависимости киберинцидентов на трех уровнях: операционном, внутриорганизационном и экосистемном. В-третьих, рассмотрено новое понимание нормативных рамок, которые становятся более стандартизирующими и превентивными, задавая технологические и организационные требования [7].

Практическое значение модели заключается в интеграции передовых подходов к управлению киберинцидентами и кибербезопасностью [4, 11, 12], что позволяет сократить время реагирования и уменьшить последствия атак на CCI. Эта модель служит обучающей средой для операторов, помогая повышать готовность, SA и формируя COP с другими участниками экосистемы. При этом важной задачей остается укрепление межорганизационного доверия для повышения обмена информацией, что требует надежной защиты данных и соблюдения конфиденциальности.

Таким образом, были представлены результаты проекта ADR, нацеленного на повышение киберустойчивости критически важных инфраструктур. После проведения анализа актуальной литературы в данной области была разработана концептуальная модель, основанная на применении интегрированного цифрового двойника в многоуровневом процессе организационного обучения, сосредоточенном на управлении отказами CCI. Оценка модели проводилась в контексте экосистемы электроэнергетики ЕС, и она включала различные фазы процесса, а также используемые артефакты и вовлеченные субъекты.

Перспективные исследования киберустойчивости децентрализованных инфраструктур могут выявить техносоциальные аспекты использования цифровых двойников, в том числе их влияние на преобразование институциональной логики в вычислительные и алгоритмические структуры. Создание комплексной теории проектирования киберустойчивости в CCI требует прохождения всех этапов процесса ADR, который предполагает рефлексию и обучение после разработки и оценки артефакта в организационной среде.

Кроме того, предложенные принципы проектирования требуют дальнейшей проверки с помощью реализации концептуальных прототипов в различных контекстах CCI. Однако для полноценной оценки предложенной модели нужны длительные исследования, которые должны выполняться междисциплинарными командами, включающими специалистов в области инженерии, управления информацией, науки о данных, информационной безопасности, а также симуляции и обучения для управления рисками стихийных бедствий.

СПИСОК ЛИТЕРАТУРЫ

1. IEC Technology Report. Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment. 2019. URL: https://www.iec.ch/basecamp/cyber-security-and-resilience-guidelines-smart-energy-operational-environment (дата обращения: 25.05.2025).
2. Lemay A., Calvet J., Menet F., Fernandez J.M. Survey of Publicly Available Reports on Advanced Persistent Threat Actors // *Computers & Security*. 2019. Vol. 72. P. 26–59.
3. Dietz M., Pernul G. Digital Twin: Empowering Enterprises Towards a System-of-Systems Approach // *Business & Information Systems Engineering*. 2020. Vol. 62. No. 2. P. 179–184.
4. Meske C., Osmundsen K.S., Junglas I.A. Designing and Implementing Digital Twins in the Energy Grid Sector // *MIS Quarterly Executive*. 2021. Vol. 20. No. 3. P. 45–54.
5. Baskerville R., Baiyere A., Gregor S., Hevner A., Rossi M. Design Science Research Contributions: Finding a Balance between Artifact and Theory // *Journal of the Association for Information Systems.* 2019. Vol. 19. No. 5. P. 358–376.
6. Spagnoletti P., Kazemargi N., Prencipe A. Agile Practices and Organizational Agility in Software Ecosystems // *IEEE Transactions on Engineering Management.* 2021. Vol. 69. No. 6. P. 3604–3617.
7. Spagnoletti P., Za S. Digital Resilience to Normal Accidents in High-Reliability Organizations // *Engineering the Transformation of the Enterprise: A Design Science Research Perspective* / Eds. Aier S., Rohner P., Schelp J. Cham: Springer, 2021. 353 p.
8. Ahmad A., Desouza K.C., Maynard S.B., Naseer H., Baskerville R.L. How Integration of Cyber Security Management and Incident Response Enables Organizational Learning // *Journal of the Association for Information Science and Technology*. 2020. Vol. 71. No. 8. P. 939–953.
9. Steen-Tveit K. Identifying Information Requirements for Improving the Common Operational Picture in Multi-Agency Operations // *Proceedings of the 17th ISCRAM Conference*. 2020. URL: https://idl.iscram.org/files/kristinesteen-tveit/2020/2226_KristineSteen-Tveit2020.pdf (дата обращения: 25.05.2025).
10. Chaudhary T., Jordan J., Salomone M., Baxter P. Patchwork of Confusion: The Cybersecurity Coordination Problem // *Journal of Cybersecurity*. 2019. Vol. 4. No. 1. P. 56–64.
11. Horita F., Baptista J., Albuquerque J.P. Exploring the Use of IoT Data for Heightened Situational Awareness in Centralised Monitoring Control Rooms // *Information Systems Frontiers.* 2020. Vol. 25. No. 1. P. 275–290.
12. Naseer A., Naseer H., Ahmad A., Maynard S.B., Siddiqui A.M. Real-time Analytics, Incident Response Process Agility and Enterprise Cybersecurity Performance: A Contingent Resource-based Analysis // *International Journal of Information*. 2021. Vol 59. No. 8. P. 102–334.

СВЕДЕНИЯ ОБ АВТОРАХ

ШУБИН Михаил Дмитриевич – магистрант, ФГБОУ ВО «Тверской государственный технический университет», 170026, Россия, г. Тверь, наб. А. Никитина, д. 22. E-mail: mikhail-shubin@bk.ru
РУСИН Александр Юрьевич – кандидат технических наук, доцент кафедры электроснабжения и электротехники, ФГБОУ ВО «Тверской государственный технический университет», 170026, Россия, г. Тверь, наб. А. Никитина, д. 22. E-mail: alexrusin@inbox.ru

БИБЛИОГРАФИЧЕСКАЯ ССЫЛКА

Шубин М.Д., Русин А.Ю. Киберустойчивость электроэнергетических систем // Вестник Тверского государственного технического университета. Серия «Строительство. Электротехника и химические технологии». 2025. № 2 (26). С. 74–80.

CYBER-RESILIENCE OF ELECTRIC POWER SYSTEMS

M.D. Shubin, A.Yu. Rusin
Tver State Technical University (Tver)

Abstract. The article presents a digital twin model designed for mission-critical cyberinfrastructures. It focuses on analyzing possible problems that arise when integrating computing, communication, and physical components of these cyberinfrastructures. Particular attention is being paid to the electricity sector, as disruptions to its sustainability can lead to serious risks for the country. A comprehensive model has been developed to expand the possibilities of interacting with the system, increase awareness of ongoing events and improve responses to cyber incidents. It is based on research in the field of information security, situational awareness and the formation of an overall operational picture. The use of the model helps to reduce the response time, which minimizes the damage from cyber attacks to electric power systems. In conclusion, the prospects of applying this approach in future research are discussed and its importance for the electric power industry is noted.

Keywords: digital twin, resilience, incident response, incident prevention, situational awareness, artificial intelligence.

INFORMATION ABOUT THE AUTHORS

SHUBIN Mikhail Dmitrievich – Master's Degree Student, Tver State Technical University, 22, embankment of A. Nikitin, Tver, 170026, Russia. E-mail: mikhail-shubin@bk.ru
RUSIN Aleksandr Yur'evich – Candidate of Engineering Sciences, Associate Professor of the Department of Power Supply and Electrical Engineering, Tver State Technical University, 22, embankment of A. Nikitin, Tver, 170026, Russia. E-mail: alexrusin@inbox.ru

CITATION FOR AN ARTICLE

Shubin M.D., Rusin A.Yu. Cyber-resilience of electric power systems // Vestnik of Tver State Technical University. Series «Building. Electrical engineering and chemical technology». 2025. No. 2 (26), pp. 74–80.