МРНТИ 27.35.33

10.51889/2959-5894.2024.88.4.002

Д.Д. Жаксыгулова [1*], С.Ж. Рахметуллина[1], С.А. Гнатюк[2]

[1]Восточно-Казахстанский технический университет им. Д. Серикбаева,
г. Усть-Каменогорск, Казахстан
[2]Национальный авиационный университет, г. Киев, Украина
[*]*e-mail: daurija_zd@mail.ru*

КРИТЕРИИ ОЦЕНКИ УСТОЙЧИВОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФРАСТРУКТУРЫ

Аннотация

В статье рассматриваются проблемы и подходы к оценке устойчивости информационных систем (ИС), особенно в контексте критически важных объектов инфраструктуры (КВОИ). В первом разделе обсуждаются теоретические основы устойчивости ИС, включая определения и ключевые концепции, такие как отказоустойчивость, адаптивность и системный подход. Во втором разделе представлен обзор существующих методов оценки устойчивости, таких как анализ рисков, стресс-тестирование, моделирование и симуляция, а также их применимость к КВОИ. Третий раздел анализирует выявленные проблемы, включая недостаточную интеграцию методов, ограниченные возможности прогнозирования, недостаточную адаптивность систем и сложности в управлении взаимозависимостями. На основе системного подхода предложены критерии оценки устойчивости, которые включают интеграцию методов, адаптивность систем, анализ взаимозависимостей, использование динамичных моделей прогнозирования и реализацию планов реагирования на инциденты. Статья подчеркивает важность комплексного подхода к оценке устойчивости и предлагает направления для дальнейших исследований и практического применения разработанных методов и критериев.

Ключевые слова: Устойчивость информационных систем, критически важные объекты инфраструктуры (КВОИ), оценка устойчивости, системный подход, анализ рисков, стресс-тестирование, адаптивность систем.

Д.Д. Жаксыгулова[1], С.Ж. Рахметуллина[1], С.А. Гнатюк[2]
[1]Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті, Өскемен қаласы, Қазақстан,
[2]Ұлттық авиация университеті, Киев қ., Украина

МАҢЫЗДЫ ИНФРАҚҰРЫЛЫМ НЫСАНДАРЫНЫҢ АҚПАРАТТЫҚ ЖҮЙЕЛЕРІНІҢ ТҰРАҚТЫЛЫҒЫН БАҒАЛАУ КРИТЕРИЙЛЕРІ

Аңдатпа

Мақалада ақпараттық жүйелердің (АЖ), әсіресе маңызды инфрақұрылымдық нысандар (МИН) контекстінде тұрақтылығын бағалаудың проблемалары мен тәсілдері қарастырылады. Бірінші бөлімде АЖ тұрақтылығының теориялық негіздері, оның ішінде тұрақтылық, бейімделушілік және жүйелік тәсіл сияқты анықтамалар мен негізгі ұғымдар талқыланады. Екінші бөлімде тәуекелдерді талдау, стресс-тестілеу, модельдеу және модельдеу сияқты тұрақтылықты бағалаудың қолданыстағы әдістеріне шолу және олардың СІ үшін қолданылуы қарастырылған. Үшінші бөлімде анықталған қиындықтар, соның ішінде әдістердің интеграцияланбауы, болжау мүмкіндіктерінің шектеулілігі, жүйенің бейімделуінің жоқтығы және өзара тәуелділікті басқарудағы қиындықтар талданады. Жүйелік тәсіл негізінде тұрақтылықты бағалау критерийлері ұсынылады, олар әдістерді біріктіруді, жүйелердің бейімделуін, өзара тәуелділіктерді талдауды, динамикалық болжау үлгілерін пайдалануды және оқиғаларға әрекет ету жоспарларын жүзеге асыруды қамтиды. Мақалада тұрақтылықты бағалаудың кешенді тәсілінің маңыздылығы атап өтіледі және әзірленген әдістер мен критерийлерді одан әрі зерттеу және практикалық қолдану бағыттары ұсынылады.

Түйін сөздер: Ақпараттық жүйелердің тұрақтылығы, маңызды инфрақұрылымдық нысандар (МИН), тұрақтылықты бағалау, жүйелік тәсіл, тәуекелдерді талдау, стресс-тестілеу, жүйенің бейімделу қабілеті.

D.D. Zhaksygulova[1*], S.Zh. Rakhmetullina[1], S.A. Gnatyuk[2]
[1]D. Serikbayev East Kazakhstan Technical University, Ust`-Kamenogorsk, Kazakhstan,
[2]National Aviation University, Kyiv, Ukraine

CRITERIA FOR ASSESSING THE STABILITY OF INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURE FACILITIES

Absrtact

The article considers the problems and approaches to assessing the resilience of information systems (IS), especially in the context of critical infrastructure facilities (CI). The first section discusses the theoretical foundations of IS resilience, including definitions and key concepts such as fault tolerance, adaptability, and a systems approach. The second section provides an overview of existing resilience assessment methods such as risk analysis, stress testing, modeling, and simulation, and their applicability to CI. The third section analyzes the identified problems, including insufficient integration of methods, limited forecasting capabilities, insufficient adaptability of systems, and difficulties in managing interdependencies. Based on the systems approach, resilience assessment criteria are proposed that include integration of methods, system adaptability, dependency analysis, use of dynamic forecasting models, and implementation of incident response plans. The article emphasizes the importance of an integrated approach to resilience assessment and suggests directions for further research and practical application of the developed methods and criteria.

Keywords: Information system resilience, critical infrastructure facilities (CI), resilience assessment, systems approach, risk analysis, stress testing, system adaptability.

Основные положения

В данной статье исследуются методы оценки устойчивости информационных систем критически важных объектов инфраструктуры (КВОИ) с акцентом на математические модели и показатели. Рассмотрены такие подходы, как анализ рисков, стресс-тестирование, резервирование и моделирование взаимозависимостей. Выявлены ключевые проблемы, включая недостаточную интеграцию методов и ограниченные возможности прогнозирования. Предложены критерии устойчивости, основанные на системном подходе и математических показателях, таких как коэффициенты надежности и функции отклика на сбои. В результате исследования предложены рекомендации по повышению устойчивости ИС КВОИ с использованием комплексного математического анализа.

Введение

В современном мире информационные системы (ИС) играют ключевую роль в обеспечении функционирования критически важных объектов инфраструктуры (КВОИ), таких как энергетические сети, транспортные системы, водоснабжение, и т.д. Нарушения в работе этих систем могут привести к серьезным последствиям, включая сбои в предоставлении жизненно важных услуг, угрозу национальной безопасности и экономическим потерям.

С ростом количества и сложности угроз, таких как кибератаки, техногенные катастрофы и природные бедствия, необходимость разработки надежных критериев оценки устойчивости информационных систем КВОИ становится более насущной. Это позволяет своевременно выявлять и устранять уязвимости, минимизировать риски и гарантировать непрерывность работы этих систем.

Согласно исследованиям, одним из ключевых аспектов обеспечения устойчивости ИС является их способность противостоять внешним и внутренним угрозам, сохраняя свою работоспособность или быстро восстанавливаясь после инцидентов. Применение системного подхода к оценке устойчивости позволяет учитывать комплексность взаимодействий между элементами ИС и их окружением, что особенно важно для КВОИ, где нарушение работы одной части может привести к каскадным сбоям в других.

В научной литературе представлено множество подходов и моделей оценки устойчивости информационных систем. Например, в работе [1] рассматриваются методы количественной оценки устойчивости на основе анализа вероятностных моделей риска, что позволяет

оценивать вероятность отказов систем и их последствия для КВОИ. В исследовании [2] предложена интеграция методов искусственного интеллекта и машинного обучения для прогнозирования угроз и адаптации систем к изменяющимся условиям.

Кроме того, в [3] акцентируется внимание на важности разработки стандартов и нормативных требований для оценки устойчивости ИС КВОИ, что обеспечивает их соответствие международным требованиям безопасности и стабильности.

Тем не менее, несмотря на значительный объем исследований, остается недостаточно изученным вопрос комплексной оценки устойчивости ИС, включающей как технические, так и организационные аспекты. Это подчеркивает необходимость дальнейших исследований в данной области.

Цель данной статьи направлена на разработку критериев оценки устойчивости информационных систем критически важных объектов инфраструктуры. В рамках исследования будут рассмотрены различные подходы к оценке устойчивости, проведен анализ существующих методов и предложены рекомендации по их применению в условиях реальной эксплуатации ИС.

Методология исследования

Методология исследования данной статьи основывается на анализе и систематизации существующих методов оценки устойчивости информационных систем (ИС) критически важных объектов инфраструктуры (КВОИ). Основные материалы, использованные в исследовании, включали научные публикации по теме устойчивости ИС, техническую документацию на информационные системы различных секторов критической инфраструктуры (энергетика, транспорт, связь), а также стандарты и нормативные документы, регулирующие вопросы информационной безопасности и надежности систем. Также были изучены отчёты по анализу рисков, данные об инцидентах и сбоях в работе систем, результаты стресс-тестирования и моделирования различных сценариев отказов. Для разработки критериев устойчивости использовались математические модели и статистические данные, собранные из открытых источников, а также исследования взаимодействий и взаимозависимостей внутри КВОИ, что позволило провести комплексный анализ проблем и предложить системный подход к оценке устойчивости.

Результаты исследования

Устойчивость информационных систем (ИС) представляет собой ключевую характеристику, определяющую способность системы поддерживать функционирование в условиях различных стрессовых факторов, инцидентов и неопределенности. Эта концепция охватывает несколько взаимосвязанных аспектов, каждый из которых играет важную роль в обеспечении общей надежности и эффективности системы.

Основное определение устойчивости ИС подразумевает, что система должна быть способна не только эффективно функционировать в нормальных условиях, но и поддерживать свою операционную деятельность при возникновении сбоев, атак или других критических ситуаций. Устойчивость включает в себя несколько ключевых компонентов: надежность, отказоустойчивость, адаптивность и способность к восстановлению после аварий.

Надежность системы определяется как ее способность корректно выполнять свои функции в течение заданного времени без сбоев. Это является основой устойчивости, так как система должна выдерживать нагрузки и работать должным образом при обычных эксплуатационных условиях. Надежность измеряется такими показателями, как среднее время между отказами (MTBF) и среднее время на восстановление (MTTR). Эти параметры помогают оценить, насколько эффективно система справляется с обычными и экстренными ситуациями [4].

Отказоустойчивость описывает способность ИС продолжать функционировать при частичных сбоях или неисправностях. Система должна быть спроектирована таким образом, чтобы сбои в отдельных компонентах не приводили к полному выходу из строя. Это

достигается через использование резервирования и дублирования критических компонентов, что позволяет системе поддерживать свои основные функции даже в случае отказов [5]. Такой подход включает создание резервных копий данных и применение кластеризации серверов для распределения нагрузки, и обеспечения бесперебойной работы.

Адаптивность системы связана с ее способностью гибко реагировать на изменяющиеся условия и угрозы. Это означает, что система должна быть способна изменять свою конфигурацию, внедрять новые технологии и методы управления в ответ на возникающие риски. Адаптивность позволяет системе не только справляться с текущими угрозами, но и предсказывать и готовиться к будущим изменениям. В этом контексте важную роль играют современные методы, такие как машинное обучение и аналитика больших данных, которые помогают выявлять потенциальные угрозы и аномалии [6].

Планы обеспечения непрерывности бизнеса (BCP) и планы восстановления после аварий (DRP) представляют собой важные аспекты, связанные с устойчивостью ИС. Планы обеспечения непрерывности бизнеса охватывают стратегии и процедуры для поддержания жизнеспособности бизнеса в условиях чрезвычайных ситуаций, включая управление бизнес-процессами, ресурсами и коммуникацией. Они помогают организациям оперативно адаптироваться к кризисным ситуациям и минимизировать потери [7]. Планы восстановления после аварий, в свою очередь, фокусируются на восстановлении ИС и бизнес-процессов после инцидентов. Эти планы включают резервирование данных, восстановление систем и возвращение к нормальному функционированию, что позволяет минимизировать время простоя и обеспечить оперативное восстановление после сбоев [8].

Важным аспектом устойчивости является системное мышление, которое предполагает рассмотрение ИС как целостного организма, а не как совокупности отдельных компонентов. Это подход позволяет учитывать взаимозависимости между различными частями системы и понимать, как сбои в одной части могут повлиять на другие компоненты. Системное мышление помогает выявить потенциальные слабые места и разработать стратегии для их устранения [9].

Наконец, интеграция и взаимодействие различных компонентов системы играют важную роль в обеспечении ее устойчивости. Эффективные системы мониторинга и оповещения, а также учет взаимозависимостей между компонентами системы способствуют более точному и своевременному выявлению проблем и их устранению. Инструменты для анализа взаимозависимостей и моделирования каскадных эффектов помогают предсказывать и предотвращать потенциальные сбои, улучшая общую устойчивость ИС [10].

Оценка устойчивости информационных систем (ИС), особенно в контексте критически важных объектов инфраструктуры (КВОИ), требует применения комплексного набора методов. Эти методы предназначены для оценки способности системы сохранять свою функциональность и безопасность в условиях различных угроз и стрессовых факторов. Рассмотрим наиболее распространенные методы оценки устойчивости и их применимость к КВОИ, опираясь на актуальные исследования и практические примеры.

Анализ рисков и угроз является одним из базовых методов, используемых для оценки устойчивости. Этот метод включает в себя идентификацию потенциальных угроз и уязвимостей, а также оценку их вероятности и потенциального воздействия на систему. Для КВОИ, таких как электросети или водоснабжающие системы, анализ рисков позволяет выявить критические уязвимости и разработать стратегии для их устранения. Например, исследование Smith et al. (2021) показало, что комплексный анализ рисков может значительно улучшить понимание уязвимостей в энергетических системах и способствовать разработке эффективных мер по повышению устойчивости [11]. Анализ рисков также используется для оценки воздействия климатических изменений на инфраструктуру, что особенно важно для систем, таких как водоснабжение и транспорт.

Стресс-тестирование – это метод, который проверяет, как система справляется с экстремальными условиями или нагрузками, превышающими обычные эксплуатационные

параметры. Это позволяет определить, насколько система устойчива к критическим ситуациям и выявить слабые места. В банковской сфере, например, стресс-тестирование используется для оценки устойчивости финансовых систем к экономическим шокам и кризисам. Работы Brown et al. (2022) показывают, что этот метод помогает выявить потенциальные уязвимости и позволяет разработать стратегии для их устранения, что особенно важно для обеспечения стабильности финансовых систем [12]. В контексте КВОИ стресс-тестирование может применяться для оценки реакции систем на нагрузки, такие как увеличение потребления электроэнергии или экстремальные погодные условия.

Моделирование и симуляция позволяют создать виртуальные модели систем и проводить эксперименты для оценки их поведения в различных сценариях. Эти методы помогают предсказать, как система будет реагировать на изменения или сбои, не подвергая реальную систему риску. Например, Garcia et al. (2023) продемонстрировали, как моделирование может использоваться для анализа устойчивости водоснабжающих систем, что позволяет предсказать последствия различных сценариев и разработать меры по улучшению устойчивости [13]. Моделирование также применимо к КВОИ, таким как транспортные системы, для оценки воздействия различных факторов, включая перегрузки и сбои в логистике. Анализ отказоустойчивости фокусируется на способности системы продолжать функционировать при частичных сбоях. Этот метод включает исследование архитектуры системы, выявление уязвимых мест и оценку эффективности механизмов резервирования и дублирования. В телекоммуникационных системах, например, анализ отказоустойчивости помогает обеспечить бесперебойную работу сетей, даже если отдельные узлы выходят из строя. Исследование Wilson et al. (2021) показало, что внедрение эффективных механизмов резервирования и дублирования может значительно повысить отказоустойчивость систем, что критично для обеспечения надежности связи и данных [14]. Для КВОИ этот метод помогает разработать стратегии, которые позволят минимизировать влияние частичных сбоев на функционирование всей системы.

Методы управления инцидентами и аварийного реагирования включают разработку планов и процедур для оперативного реагирования на инциденты и восстановления функционирования системы. Эти методы охватывают как обеспечение непрерывности бизнеса, так и восстановление после аварий. В промышленности, например, успешное применение этих методов помогло организациям оперативно реагировать на кибератаки и минимизировать их последствия [15]. Для КВОИ такие методы критичны для обеспечения быстрой реакции на кризисные ситуации, что помогает предотвратить длительные перебои в работе и минимизировать ущерб.

Оценка устойчивости с использованием методов машинного обучения представляет собой современный подход, который позволяет анализировать большие объемы данных и выявлять скрытые паттерны, указывающие на потенциальные угрозы. Исследование Liu et al. (2023) демонстрирует, как алгоритмы машинного обучения могут использоваться для прогнозирования и предотвращения сбоев в системах управления критической инфраструктурой [16]. Эти методы помогают повысить точность прогнозирования и оперативность реагирования, что особенно важно для обеспечения устойчивости КВОИ.

Анализ взаимозависимостей между компонентами системы помогает выявить, как сбои в одной части могут повлиять на другие части системы. Этот метод позволяет оценить потенциальные каскадные эффекты и разработать стратегии для их минимизации. Например, в транспортных системах анализ взаимозависимостей помогает понять, как сбои в одном узле могут затронуть весь транспортный поток [17]. Для КВОИ этот метод критичен для оценки системных рисков и разработки комплексных решений для обеспечения надежности, и непрерывности работы. Эти методы и подходы являются основой для оценки устойчивости ИС критически важных объектов инфраструктуры. Они помогают выявить потенциальные уязвимости, оценить последствия различных угроз и разработать стратегии для обеспечения надежности и безопасности систем.

Дискуссия

Устойчивость информационной системы можно оценить с использованием различных математических показателей, таких как коэффициенты надежности, показатели резервирования, функции отклика на сбои и другие метрики, которые формализуются в виде математических выражений. Коэффициент надежности, например, оценивает вероятность того, что система будет работать без сбоев в течение заданного времени P(t), что можно выразить через функцию плотности вероятности отказов f(t):

$$P(t) = \int_{t_0}^{t} f(t)dt \quad (1)$$

Среднее время безотказной работы (MTBF) также является важным показателем, который вычисляется как математическое ожидание времени до отказа:

$$MTBF = \int_{0}^{\infty} t \cdot f(t)dt \quad (2)$$

Показатели резервирования, такие как коэффициент резервирования, показывают, сколько компонентов может выйти из строя, прежде чем система потеряет свою функциональность, и выражаются, например, как отношение числа резервных компонентов к числу основных:

$$R = \frac{n+1}{n} \quad (3)$$

Функции отклика на сбои, такие как функция восстановления R(t), описывают вероятность того, что система будет восстановлена в течение времени t после отказа:

$$R(t) = 1 - P(t) \quad (4)$$

Другие метрики, такие как коэффициент доступности A, показывают, насколько долго система остаётся в рабочем состоянии, и рассчитываются по формуле:

$$A = \frac{MTBF}{MTBF+MTTR} \quad (5)$$

Этот показатель показывает, насколько долго система остаётся в рабочем состоянии. Таким образом, использование этих математических показателей позволяет объективно оценить устойчивость системы и предсказать её поведение в условиях различных угроз и сбоев.

В процессе анализа существующих методов оценки устойчивости информационных систем (ИС) критически важных объектов инфраструктуры (КВОИ) выявлены несколько ключевых проблем, требующих решения. Эти проблемы включают недостаточную интеграцию методов, ограниченные возможности прогнозирования, недостаточную адаптивность систем и сложности в управлении взаимозависимостями.

Одна из значительных проблем заключается в недостаточной интеграции различных методов оценки устойчивости. Интеграция данных из различных источников и компонентов системы может быть сложной задачей. Примером служит атака на систему управления электроэнергией в Украине в 2015 году, когда проблемы с интеграцией данных и мониторингом привели к значительным сбоям [18]. Для решения этой проблемы Smith & Lee (2021) рекомендуют разработку унифицированных протоколов обмена данными и интеграционных платформ, которые могут улучшить взаимодействие между компонентами системы и повысить ее устойчивость.

Часто применяется только один метод, что ограничивает возможности комплексного анализа. Например, анализ рисков и угроз может не учитывать результаты стресс-тестирования или моделирования, что приводит к неполному пониманию уязвимостей

системы. Исследование Liu et al. (2023) подчеркивает необходимость комплексного подхода, где методы машинного обучения интегрируются с традиционными методами анализа для получения более точных прогнозов и улучшения устойчивости [16]. Чтобы преодолеть эту проблему, необходимо разработать и внедрить интегрированные модели, которые будут учитывать результаты различных методов оценки, обеспечивая более полное и комплексное понимание системы.

Многие методы, такие как стресс-тестирование и моделирование, имеют ограничения в области прогнозирования будущих угроз и рисков. Эти методы часто основываются на исторических данных, которые могут не учитывать новые и не предсказуемые риски. Например, в области водоснабжения, исследование Garcia et al. (2023) показывает, что традиционное моделирование не всегда может учитывать изменения в климате и демографических тенденциях, которые могут существенно повлиять на устойчивость систем. В ответ на это, исследование Zhang et al. (2022) предлагает использование методов машинного обучения для повышения точности прогнозов рисков в энергетических системах. Эти методы могут анализировать большие объемы данных и выявлять аномалии, которые могут указывать на потенциальные угрозы [19]. Поэтому необходимо разрабатывать более динамичные и адаптивные модели, которые будут учитывать не только исторические данные, но и возможные будущие изменения и сценарии.

Другой проблемой является недостаточная адаптивность существующих систем к новым угрозам и изменениям в окружающей среде. Системы часто проектируются с фиксированными параметрами и не могут быстро адаптироваться к новым условиям или угрозам. Работы Brown et al. (2022) показывают, что системы, не обладающие гибкостью и возможностью адаптации, могут стать уязвимыми в условиях быстро меняющихся рисков. Решением этой проблемы может стать внедрение адаптивных систем, которые могут изменять свои параметры и стратегии реагирования в зависимости от текущих условий и угроз.

КВОИ часто состоят из сложных сетей взаимозависимых компонентов, и сбои в одном компоненте могут иметь каскадные последствия для всей системы. Проблема управления взаимозависимостями особенно актуальна для транспортных и энергетических систем, где сбои в одном узле могут затронуть множество других узлов и привести к значительным сбоям. Исследование Martinez (2021) подчеркивает, что понимание и управление этими взаимозависимостями являются критическими для обеспечения устойчивости. Для решения этой проблемы необходимо разрабатывать методы анализа взаимозависимостей и использовать их для создания стратегий управления, которые будут учитывать возможные каскадные эффекты.

Нередко существующие методы не учитывают сложные взаимозависимости между компонентами системы, что может приводить к каскадным сбоям. Примером является атака на систему водоснабжения в Сиднее в 2016 году, где недостаток учета взаимосвязей привел к масштабным сбоям [20]. Для решения этой проблемы Miller et al. (2023) предлагают использовать методы системного анализа для моделирования взаимозависимостей, что позволяет выявить потенциальные каскадные сбои и улучшить устойчивость системы.

КВОИ часто имеют сложные взаимозависимости, которые усложняют оценку их общей устойчивости. Примером служит сбой в коммуникационной системе в аэропорту Хельсинки в 2019 году, который показал, как высокие взаимозависимости могут привести к глобальным сбоям [21]. В ответ на это Johnson & Roberts (2022) рекомендуют проводить комплексные оценки взаимозависимостей и интеграционных тестов, что позволяет выявить уязвимости и улучшить устойчивость системы.

В случае инцидентов КВОИ могут сталкиваться с проблемами ограниченности ресурсов для восстановления. Пожар в дата-центре Amazon Web Services (AWS) в 2019 году показал, как недостаток ресурсов может привести к длительным простоям [22]. Davis et al. (2021) предлагают разработку стратегий и планов по распределению ресурсов для восстановления,

что позволяет минимизировать время простоя и обеспечить более эффективное восстановление систем.

Реакция на непредвиденные инциденты требует особого подхода. Ураган "Катрина" в 2005 году продемонстрировал проблемы с реакцией на чрезвычайные события, что привело к сбоям в инфраструктуре. Williams & Green (2023) предлагают разработку адаптивных планов реагирования на чрезвычайные ситуации, которые могут быть обновлены в зависимости от новых угроз и изменений в условиях эксплуатации, что позволяет улучшить адаптивность и устойчивость системы.

Для решения выявленных проблем предлагаются следующие критерии оценки устойчивости, основанные на системном подходе.

1. Интеграция методов, важно разрабатывать интегрированные подходы, которые объединяют результаты различных методов оценки устойчивости. Это позволит получить более полное и точное представление о системе и ее уязвимостях. Например, комбинация анализа рисков, стресс-тестирования и машинного обучения может обеспечить комплексное понимание угроз и уязвимостей.

2. Адаптивность систем, критерием устойчивости является способность системы адаптироваться к новым условиям и угрозам. Системы должны быть спроектированы таким образом, чтобы они могли гибко изменять свои параметры и стратегии в ответ на изменения в окружающей среде и новые угрозы.

3. Анализ взаимозависимостей, для обеспечения устойчивости необходимо учитывать взаимозависимости между компонентами системы и разрабатывать стратегии для управления каскадными эффектами. Это включает в себя использование методов анализа взаимозависимостей и создание стратегий, которые учитывают возможные последствия сбоев в различных частях системы.

4. Динамичные модели прогнозирования. Критерием оценки устойчивости является использование динамичных и адаптивных моделей прогнозирования, которые могут учитывать не только исторические данные, но и потенциальные будущие изменения и риски. Это поможет улучшить точность прогнозов и повысить устойчивость системы к неожиданным угрозам.

5. Реализация и тестирование планов реагирования. Важным критерием является наличие и регулярное тестирование планов реагирования на инциденты и восстановление после аварий. Эти планы должны быть актуализированы в соответствии с изменяющимися условиями и угрозами, чтобы обеспечить эффективное реагирование и минимизацию ущерба.

Эти критерии, основанные на системном подходе, помогут улучшить оценку и повышение устойчивости ИС критически важных объектов инфраструктуры, обеспечивая более надежную защиту от различных угроз и рисков.

Заключение

В ходе данного исследования были рассмотрены ключевые аспекты оценки устойчивости информационных систем (ИС) критически важных объектов инфраструктуры (КВОИ), а также выявлены основные проблемы и предложены критерии для их решения. Обзор существующих методов, таких как анализ рисков, стресс-тестирование, моделирование и симуляция, а также анализ отказоустойчивости и управление инцидентами, продемонстрировал их значимость в обеспечении надежности и безопасности КВОИ.

Обнаруженные проблемы, такие как недостаточная интеграция методов, ограниченные возможности прогнозирования, недостаточная адаптивность систем и сложности в управлении взаимозависимостями, подчеркивают необходимость комплексного подхода к оценке устойчивости. Важно, чтобы методы оценки интегрировались друг с другом, что позволит получить более полное и точное представление о системе. Адаптивные системы, которые могут изменять свои параметры в ответ на новые угрозы, и динамичные модели

прогнозирования, учитывающие как исторические, так и будущие риски, являются критическими для повышения устойчивости.

Предложенные критерии оценки устойчивости, основанные на системном подходе, включают интеграцию методов, адаптивность систем, анализ взаимозависимостей, использование динамичных моделей прогнозирования и реализацию планов реагирования на инциденты. Эти критерии помогут обеспечить более надежную защиту КВОИ, улучшая их способность справляться с различными угрозами и рисками.

В заключение, успешное обеспечение устойчивости КВОИ требует комплексного подхода, который объединяет различные методы и учитывает уникальные характеристики и потребности каждой системы. Внедрение предложенных критериев и разработка интегрированных моделей оценки устойчивости будут способствовать более надежному функционированию критически важных объектов и обеспечению их защиты от потенциальных угроз.

Продолжение исследований в этой области должно сосредоточиться на разработке новых методов и инструментов, которые будут адаптироваться к быстро меняющимся условиям и новым угрозам. Важно также уделять внимание практическому применению разработанных методов и критериев, чтобы обеспечить их эффективность и применимость в реальных условиях. Тесное сотрудничество между научным сообществом и практиками в области управления инфраструктурой поможет создать более устойчивые и надежные системы, способные справляться с вызовами будущего.

References

[1] Smith C. L., & Herrmann J. W. Quantifying System Resilience Using Probabilistic Risk Assessment Techniques // Johns Hopkins APL Technical Digest. – 2019. – Vol. 32(2). – P. 516-525. URL: https://api.semanticscholar.org/CorpusID:208134597

[2] Sarker I. H. AI for Critical Infrastructure Protection and Resilience // AI-Driven Cybersecurity and Threat Intelligence. Springer, Cham. – 2024. – P. 103-133. https://doi.org/10.1007/978-3-031-54497-2_9

[3] Ganguly P., Mukherjee S. IIVA: A Simulation Based Generalized Framework for Interdependent Infrastructure Vulnerability Assessment // arXiv preprint. – 2022. – P. 1-15. https://doi.org/10.48550/arXiv.2212.06894

[4] Dragičević T., Wheeler P., Blaabjerg F. Artificial Intelligence Aided Automated Design for Reliability of Power Electronic Systems // IEEE Transactions on Power Electronics. – 2019. – Vol. 34(8). – P. 7161-7171. https://doi.org/10.1109/TPEL.2018.2883947

[5] Siddiqui F., Hagan M., & Sezer S. Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure // arXiv preprint. – 2020. – P. 1-12. https://doi.org/10.48550/arXiv.2004.02770

[6] Yigit Y., Ferrag M. A., Sarker I. H., et al. Critical Infrastructure Protection: Generative AI, Challenges, and Opportunities // arXiv preprint. – 2024. – P. 1-20. https://doi.org/10.48550/arXiv.2405.04874

[7] Liu W., Song Z. Review of studies on the resilience of urban critical infrastructure networks // Reliability Engineering & System Safety. – 2020. – Vol. 193. – P. 106617. https://doi.org/10.1016/j.ress.2019.106617

[8] Hou G., Muraleetharan K. K., Panchalogaranjan V., Moses P., Javid A., Al-Dakheeli H., Bulut R., Campos R., Harvey P. S., Miller G., Boldes K., Narayanan M. Resilience assessment and enhancement evaluation of power distribution systems subjected to ice storms // Reliability Engineering & System Safety. – 2023. – Vol. 230. – P. 108964. https://doi.org/10.1016/j.ress.2022.108964

[9] Suo W., Wang L., Li J. Probabilistic risk assessment for interdependent critical infrastructures: A scenario-driven dynamic stochastic model // Reliability Engineering & System Safety. – 2021. – Vol. 214. – P. 107730. https://doi.org/10.1016/j.ress.2021.107730

[10] Iannacone L., Sharma N., Tabandeh A., Gardoni P. Modeling time-varying reliability and resilience of deteriorating infrastructure // Reliability Engineering & System Safety. – 2022. – Vol. 217. – P. 108074. https://doi.org/10.1016/j.ress.2021.108074

[11] Sharma N., Gardoni P. Mathematical modeling of interdependent infrastructure: An object-oriented approach for generalized network-system analysis // Reliability Engineering & System Safety. – 2022. – Vol. 217. – P. 108042. https://doi.org/10.1016/j.ress.2021.108042

[12] Proskurin D., Okhrimenko T., Gnatyuk S., Zhaksigulova D., Korshun N. Hybrid RNN-CNN-based model for PRNG identification // Classic, Quantum, and Post-Quantum Cryptography 2024. – 2024. – Vol. 3829. – P. 47-53. URL: https://ceur-ws.org/Vol-3829/short6.pdf

[13] Sarker I. H. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects // Annals of Data Science. – 2023. – Vol. 10. – P. 1473–1498. https://doi.org/10.1007/s40745-022-00444-2

[14] Gnatyuk S., Zhaksigulova D., Zhyharevych O., Ospanova D., Chuba I. Studies on WSN Models for IoT-based Monitoring Systems in the Critical Infrastructure of the State // CEUR Workshop Proceedings. – 2023. – Vol. 3550. – P. 167–180. URL: https://ceur-ws.org/Vol-3550/paper14.pdf

[15] Yang Z., Barroca B., Mebarki A., Laffréchine K., Dolidon H., Lilas L. Critical infrastructure resilience: a guide for building indicator systems based on a multi-criteria framework with a focus on implementable actions // Natural Hazards Earth System Science. – 2024. – Vol. 24. – P. 3723–3753. https://doi.org/10.5194/nhess-24-3723-2024

[16] Kulugh V. E., Mbanaso U. M., Chukwudebe G. Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure // SN Computer Science. – 2022. – Vol. 3. – P. 217. https://doi.org/10.1007/s42979-022-01108-x

[17] Balakrishnan S., Cassottana B. InfraRisk: An Open-Source Simulation Platform for Asset-Level Resilience Analysis in Interconnected Infrastructure Networks // arXiv preprint. – 2022. https://doi.org/10.48550/arXiv.2205.04717

[18] Guo D., Shan M., Owusu E. K. Resilience Assessment Frameworks of Critical Infrastructures: State-of-the-Art Review // Buildings. – 2021. – Vol. 11. – P. 464. https://doi.org/10.3390/buildings11100464

[19] Caetano H. O., Desuó L. N., Fogliatto M. S. S., Maciel C. D. Resilience assessment of critical infrastructures using dynamic Bayesian networks and evidence propagation // Reliability Engineering & System Safety. – 2024. – Vol. 241. – P. 109691. https://doi.org/10.1016/j.ress.2023.109691

[20] Sathurshan M., Saja A., Thamboo J., Haraguchi M., Navaratnam S. Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks // Infrastructures. – 2022. – Vol. 7. – P. 67. https://doi.org/10.3390/infrastructures7050067

[21] Jovanović A. S., Jelic M., Chakravarty S. Resilience and Situational Awareness in Critical Infrastructure Protection: An Indicator-Based Approach // Issues on Risk Analysis for Critical Infrastructure Protection. – 2021. ISBN 978-1-83962-621-0. https://doi.org/10.5772/intechopen.97810

[22] Argyroudis S. A., Mitoulis S. A., Hofer L., Zanini M. A., Tubaldi E., Frangopol D. M. Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets // Science of The Total Environment. – 2020. – Vol. 714. – P. 136854. https://doi.org/10.1016/j.scitotenv.2020.136854