СОВРЕМЕННЫЕ МЕТОДЫ ПРОГНОЗИРОВАНИЯ И ОЦЕНКИ НАДЕЖНОСТИ МАШИН НА ЭТАПЕ ПРОЕКТИРОВАНИЯ И ЭКСПЛУАТАЦИИ

И. С. А. Х. Альнакиб[1], М. Ф. С. Х. Аль-Камали[2]

[1]Южно-Уральский государственный университет, г. Челябинск, Российская Федерация

[2]Гомельский государственный технический университет имени П. О. Сухого, Республика Беларусь

Представлен системный обзор современных методов прогнозирования и оценки надежности машин на ключевых этапах их жизненного цикла: проектировании и эксплуатации. Рассмотрены классические вероятностно-статистические подходы и их цифровая эволюция на основе больших данных и машинного обучения. Особое внимание уделено предиктивной аналитике и цифровым двойникам как инструментам перехода от планово-предупредительных ремонтов к обслуживанию по фактическому состоянию. Анализируются синергетические эффекты от интеграции данных проектирования, испытаний и реальной эксплуатации для построения сквозных моделей надежности.

Ключевые слова: надежность машин, прогнозирование отказов, предиктивная аналитика, цифровой двойник, машинное обучение, эксплуатационная диагностика, расчет на долговечность.

MODERN METHODS OF FORECASTING AND ASSESSING THE RELIABILITY OF MACHINES AT THE DESIGN AND OPERATION STAGE

I. S. A. H. Alnakib[1], M. F. S. H. AL-Kamali[2]

[1]South Ural State University, Chelyabinsk, Russian Federation.

[2]Sukhoi State Technical University of Gomel, Gomel, Belarus

This paper presents a systematic review of modern methods for predicting and assessing machine reliability at key stages of their lifecycle: design and operation. Classic probabilistic-statistical approaches and their digital evolution based on big data and machine learning are considered. Attention is paid to predictive analytics and digital twins as tools for transitioning from scheduled preventive maintenance to condition-based maintenance. The synergistic effects of integrating design, testing, and real-world operation data to build end-to-end reliability models are analyzed.

Keywords: machine reliability, failure prediction, predictive analytics, digital twin, machine learning, operational diagnostics, durability calculation.

Надежность как комплексное свойство технической системы сохранять во времени способность выполнять требуемые функции является ключевым фактором конкурентоспособности, безопасности и экономической эффективности. Традиционная парадигма, разделяющая процессы расчета на этапе проектирования и оценки в ходе эксплуатации, уступает место целостному, сквозному подходу. Современные методы направлены на создание единой информационно-аналитической среды, связывающей виртуальные прототипы, данные стендовых испытаний и телеметрию реальной работы. Данная работе ставит целью структурировать и проанализировать современный инструментарий для решения этой задачи [1–3].

Проведенный анализ позволяет утверждать, что современная методология надежности трансформировалась из набора разрозненных инструментов в целостную

сквозную систему. Ключевым результатом является четкое подтверждение, что до 80 % потенциала надежности закладывается на этапе проектирования, где традиционные эмпирические подходы уступают место комплексному компьютерному моделированию. В частности, детерминированное моделирование на основе МКЭ позволяет прогнозировать усталостную долговечность и оптимизировать геометрию, в то время как вероятностный анализ (например, методом Монте-Карло) оценивает не абсолютный запас прочности, а статистическую степень риска с учетом естественного разброса свойств. FMEA-анализ, эволюционировав в цифровые базы знаний, интегрированные с CAD-моделями, обеспечивает структурное управление рисками на протяжении всего жизненного цикла изделия.

В ходе эксплуатации валидация и коррекция этих моделей осуществляется через призму данных. Фундаментальный статистический анализ отказов, автоматизированный через ERP-системы, дополняется передовой предиктивной аналитикой. Алгоритмы машинного обучения, обрабатывающие большие данные телеметрии, выявляют сложные корреляции для прогнозирования остаточного ресурса, что является основой для перехода к обслуживанию по фактическому состоянию (Condition-Based Maintenance). Высшей формой интеграции проектных и эксплуатационных методов выступает технология цифрового двойника, которая выполняет опережающее моделирование, оценивая влияние текущих режимов работы на будущую надежность.

Однако наиболее значимый синергетический эффект достигается при создании единого информационного контура. Данные эксплуатационного мониторинга используются для калибровки расчетных моделей МКЭ, повышая точность прогнозов для будущих модификаций. Обратная связь в виде проанализированной статистики отказов формирует целевую выборку для совершенствования FMEA при проектировании новых поколений техники. Наконец, точные прогнозы ресурса позволяют внедрять прескриптивную аналитику, которая оптимизирует логистику запчастей и планирование ремонтов, минимизируя общую стоимость владения (LCC). Следовательно, современные методы формируют не просто инструментарий оценки, а динамическую систему управления надежностью, основанную на данных и непрерывном обучении.

Таким образом, интеграция цифрового моделирования, анализа больших данных и технологий цифровых двойников формирует новую парадигму сквозного управления надежностью на основе данных. Это обеспечивает стратегический переход от реактивного исправления отказов к проактивному управлению ресурсом и рисками, создавая ключевое конкурентное преимущество за счет снижения стоимости владения и роста операционной эффективности. Однако реализация потенциала требует преодоления системных вызовов: преодоления «цифрового разрыва» (разнородные стандарты данных), масштабного развития цифровых компетенций персонала и обеспечения кибербезопасности распределенных систем. Решение этих задач зависит от скоординированных усилий промышленности, отраслевых ассоциаций и образовательных учреждений. Успешная трансформация откроет путь к созданию новых сервисных моделей и обеспечению технологического лидерства в условиях Четвертой промышленной революции.

Литература

1. AL-Kamali, M. F. S. H. Hiding of heat radiation by means of nanoporous anodic alumina films / M. F. S. H. AL-Kamali, Y. T. A. AL-Ademi, V. Lobunov ; supervisor I. Vrublevsky // Актуальные вопросы физики и техники : материалы V Респ. науч. конф. студентов и аспирантов, Гомель, 21 апр. 2016 г. В 3 ч. Ч. 1 / Гомел. гос. ун-т им. Ф. Скорины. – Гомель : ГГУ им. Ф. Скорины, 2016. – С. 6–7.

2. AL-Aimiri, M. A. M. K. ERPNEXT: revolutionizing manufacturing management in factories / M. A. M. K. AL-Aimiri, M. F. S. H. AL-Kamali / Инновационное станкостроение, технологии и инструмент : материалы I Междунар. науч.-практ. конф., Гомель, 30 нояб. 2023 г. / М-во пром-сти Респ. Беларусь [и др.] ; под общ. ред. М. И. Михайлова. – Гомель : ГГТУ им. П. О. Сухого, 2024. – С. 102–104.
3. AL-Aimiri, M. A. M. K. Streamlining factory operations: designing an effective manufacturing management program / M. A. M. K. AL-Aimiri, M. F. S. H. AL-Kamali // Инновационное станкостроение, технологии и инструмент : материалы I Междунар. науч.-практ. конф., Гомель, 30 нояб. 2023 г. / М-во пром-сти Респ. Беларусь [и др.] ; под общ. ред. М. И. Михайлова. – Гомель : ГГТУ им. П. О. Сухого, 2024. – С. 105–106.

МЕТОДЫ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ОТ КИБЕРАТАК

П. С. Мырадов

Государственный энергетический институт Туркменистана, г. Мары

Проведен анализ особенностей уязвимости АСУ, обусловленных их архитектурой и спецификой взаимодействия человек–машина. Рассмотрены современные методы защиты, основанные на комплексном подходе: технические, криптографические, организационные и нормативные меры. Особое внимание уделено роли стандартов ISO/IEC 27001 и ГОСТ Р 56939-2016, а также влиянию человеческого фактора и системного мониторинга на обеспечение киберустойчивости.

Ключевые слова: кибербезопасность, кибератаки, защита информации, криптография, мониторинг.

METHODS FOR PROTECTING AUTOMATED CONTROL SYSTEMS FROM CYBERATTACKS

P. S. Myradov

The State Energy Institute of Turkmenistan, Mary

This paper analyzes the vulnerabilities of ACS resulting from the convergence of information and operational technologies and examines modern protection methods such as network segmentation, cryptographic tools, intrusion detection systems, and organizational measures. It is demonstrated that effective defense against cyber threats requires a comprehensive approach that combines technical, software, and managerial solutions. Special attention is given to the human factor, the role of international standards, and the need for continuous security monitoring.

Keywords: cybersecurity, cyberattacks, information protection, cryptography, monitoring.

Автоматизированные системы управления (АСУ) являются фундаментом современной технологической инфраструктуры. Они интегрируют в себе программное обеспечение, датчики, контроллеры и коммуникационные протоколы, обеспечивая бесперебойное выполнение производственных процессов. Однако переход таких систем на цифровые и сетевые платформы существенно повысил их уязвимость. Если раньше АСУ функционировали в изолированных сетях, то сегодня они подключены к внешним системам для удаленного управления и анализа данных. Это сделало их объектом интереса злоумышленников, использующих методы кибератак для воздействия не только на информационные, но и на физические процессы. Серьезность угроз подтверждается инцидентом с вирусом Stuxnet, который впервые продемонстрировал, как цифровой код способен разрушить промышленное оборудование [3].

Особенности АСУ определяют специфическую структуру рисков. Их архитек-