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 архитектура основана на устаревших промышленных протоколах (Modbus, DNP3, Profibus), изначально не рассчитанных на аутентификацию и шифрование. Это означает, что перехват или подмена команд управления может произойти без значительных технических усилий. Более того, многие промышленные контроллеры (PLC, RTU, SCADA) не обновляются из-за опасений вызвать сбой технологического процесса.

Современные кибератаки на АСУ отличаются целенаправленным характером: злоумышленники стремятся не просто нарушить работу системы, а получить контроль над технологическим процессом или вывести оборудование из строя. В результате последствия таких атак выходят за рамки информационной безопасности – они затрагивают безопасность людей, окружающую среду и экономическую стабильность государства.

Защита АСУ не может быть ограничена установкой антивирусов или файрволов. Речь идет о многоуровневой стратегии, объединяющей технические, криптографические и организационные методы.

Основой эффективной защиты является сетевое разделение. Производственная сеть должна быть физически или логически изолирована от корпоративной и от Интернета. Такое разделение минимизирует риск распространения вредоносного кода между сегментами. Согласно ГОСТ Р 56939-2016 [1], обеспечение сегментации является обязательным требованием при проектировании защищенных промышленных систем.

Криптографическая защита данных становится ключевым элементом при передаче управляющих сигналов между контроллерами и серверами. Использование алгоритмов симметричного и асимметричного шифрования, а также электронных подписей, обеспечивает конфиденциальность и аутентичность команд.

Мониторинг и анализ поведения сети позволяют выявлять аномальные события и попытки вторжений на ранней стадии. Системы обнаружения и предотвращения атак (IDS/IPS) анализируют сетевые потоки и реагируют на подозрительные изменения параметров. Однако, как отмечают специалисты [2], эффективность таких систем во многом зависит от регулярного обновления сигнатур и корректной настройки политик безопасности.

Важную роль играет человеческий фактор. Большинство инцидентов в АСУ происходит из-за ошибок персонала: слабых паролей, невнимательности при настройке оборудования или отсутствия понимания угроз. Поэтому обучение операторов и внедрение корпоративной культуры безопасности являются обязательным элементом стратегии киберзащиты.

Современные кибератаки на автоматизированные системы управления демонстрируют возрастающую сложность и разрушительную силу. Защита таких систем требует постоянного совершенствования технологий, нормативных подходов и профессиональных компетенций специалистов.

Ключевым направлением развития является интеграция технологий искусственного интеллекта для анализа инцидентов, развитие концепции «киберустойчивого проектирования» и повышение уровня автоматизации мониторинга. Только соче-

тание технических, организационных и человеческих факторов способно обеспечить реальную устойчивость промышленных систем к киберугрозам.

Литература

1. ГОСТ Р 56939-2016. Защита информации. Обеспечение безопасности промышленных систем управления.
2. ISO/IEC 27001:2022. Information Security Management Systems – Requirements.
3. Грачев, П. А. Кибербезопасность промышленных систем. – СПб. : Питер, 2020.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРИКЛАДНЫХ ПРИЛОЖЕНИЯХ

П. С. Мырадов

Государственный энергетический институт Туркменистана, г. Мары

Современные технологии искусственного интеллекта (ИИ) активно интегрируются в различные сферы человеческой деятельности, такие как медицина, финансы и образование. Машинное обучение и обработка естественного языка становятся основой прикладных решений, способных анализировать большие объемы данных, прогнозировать события и автоматизировать сложные процессы. В медицине ИИ помогает в диагностике заболеваний и персонализированном лечении, в финансовой сфере – в управлении рисками и выявлении мошенничества, а в образовании – в создании адаптивных систем обучения. Использование ИИ способствует повышению эффективности, точности и доступности услуг. Однако его внедрение требует соблюдения этических принципов и защиты персональных данных.

Ключевые слова: искусственный интеллект, машинное обучение, обработка естественного языка, автоматизация.

USING ARTIFICIAL INTELLIGENCE IN APPLICATIONS

P. S. Myradov

The State Energy Institute of Turkmenistan, Mary, Turkmenistan

Modern artificial intelligence (AI) technologies are increasingly integrated into various areas of human activity such as medicine, finance, and education. Machine learning and natural language processing form the basis of applied solutions capable of analyzing large data sets, predicting outcomes, and automating complex processes. In medicine, AI aids in disease diagnosis and personalized treatment; in finance – in risk management and fraud detection; in education – in creating adaptive learning systems. The use of AI improves efficiency, accuracy, and accessibility of services. However, its implementation requires adherence to ethical principles and data protection.

Keywords: artificial intelligence, machine learning, natural language processing, automation.

Развитие искусственного интеллекта (ИИ) стало одним из ключевых направлений цифровой трансформации общества. Сегодня ИИ перестал быть абстрактным понятием из научной фантастики и превратился в мощный инструмент, внедряемый в практические решения, направленные на повышение эффективности и точности в разных сферах деятельности человека. В основе большинства прикладных приложений лежат алгоритмы машинного обучения и методы обработки естественного языка, которые позволяют системам не просто выполнять запрограммированные действия, но и обучаться на данных, выявлять закономерности и принимать решения [1, с. 25].

В медицинской практике искусственный интеллект используется для анализа изображений, прогнозирования заболеваний и выбора оптимальных схем лечения.