Этот принцип может проявляться в повседневной жизни, но осознаётся не всегда. Все соглашаются, что в природе много прекрасного, но найти единомышленников в отношении возвышенного сложнее, так как размышление о величии требует не только развитого эстетического восприятия, но и способности к познанию, которая лежит в его основе.

Подводя итоги можно сказать, что склонность сердца к чувству возвышенного требует восприимчивости к идеям. Когда природа противоречит этим идеям, а человек пытается воспринять её как своего рода меру или образец для идей, возникает сильное напряжение воображения, что приводит одновременно к страху и притяжению. Именно в этой несоразмерности проявляется верховенство разума над чувствами.

Список литературы

1. Кант И. Критика способности суждения // Собр. соч. в 8 т. - Т.5.- М., 1994.
2. Критика телеологической способности суждений // Собр. соч. в 6 т. - Т.6.- М., 1966.
3. Саидов А.Х. Иммануил Кантнинг фалсафий-ҳуқуқий мероси ва замонавий юриспруденция. – Ташкент: Niso-Poligraf, 2012.
4. Чижов П.Г. Дух гуманизма в философии И. Канта // Кантовские чтения в КРСУ (22 апреля 2004 г.); Общечеловеческое и национальное в философии: II Международная научно-практическая конференция КРСУ (27-28 мая 2004 г.). Материалы выступлений / Под общ.ред. И.И. Ивановой. - Бишкек, 2004.
5. Immanuel Kant. Kritik der Ulteilskraft. Moskow: Astrel. 2005.
6. Robb D.L. Operation Hollywood: How the Pentagon Shapes and Censors the Movies. N.Y.: Prome- theus Books, 2004. 384 p.
7. Pallacken Abdul Wahid. Memetics of the Computer Universe Based on the Quran // J. Software Engineering & Applications. 2010. #3. P.728–735.
8. Dalacoura K. US democracy promotion in the Arab Middle East since 11 September 2001: A critique // International Affairs. 2005. October. 81/5. The CNN effect: The Myth of News, For- eign Policy and Intervention. L., 2002.

АНАЛИЗ УЯЗВИМОСТЕЙ РАСПРЕДЕЛЕННЫХ СИСТЕМ УПРАВЛЕНИЯ В УСЛОВИЯХ КИБЕРАТАК ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

Васиков А.Р.
магистрант
Бадриев А.И.
доцент, кандидат технических наук Набережночелнинский институт Казанского (Приволжского) федерального университета, г. Набережные Челны, Россия
ainur.vasikov@gmail.com

Аннотация: в статье рассматривается проблема кибербезопасности SCADA-систем распределенных систем управления промышленных предприятий. Предлагается архитектура распределённой системы обеспечения целостности и аутентичности технологических данных на основе технологии блокчейн. Предложен блокчейн-модуль с использованием криптографических алгоритмов и механизма консенсуса. Произведена интеграция с промышленным контроллером через протокол, разработан интерфейс для визуализации цепочки блоков и обнаружения атак. Результаты моделирования подтверждают способность системы гарантировать неизменность данных и выявлять попытки подделки.

Ключевые слова: SCADA-системы, блокчейн, кибербезопасность, OPC UA, целостность данных, цифровая подпись, хеширование SHA-512, Proof-of-Work.

ANALYSIS OF VULNERABILITIES OF DISTRIBUTED CONTROL SYSTEMS UNDER

CYBERATTACKS IN INDUSTRIAL ENTERPRISES

Vasikov A.R.
Master's Student

Badriev A.I.,
Associate Professor, Candidate of Technical Sciences Naberezhnye Chelny Institute (branch) of Kazan (Volga Region) Federal University, Naberezhnye Chelny, Russia
ainur.vasikov@gmail.com

Annotation: The article addresses the cybersecurity problem of SCADA systems within distributed control systems of industrial enterprises. An architecture of a distributed system ensuring the integrity and authenticity of technological data based on blockchain technology is proposed. A blockchain module using cryptographic algorithms and a consensus mechanism is introduced. Integration with an industrial controller via a protocol is performed, and an interface for visualizing the blockchain and detecting attacks is developed. Simulation results confirm the system's ability to guarantee data immutability and detect tampering attempts.

Keywords: SCADA systems, blockchain, cybersecurity, OPC UA, data integrity, digital signature, SHA-512 hashing, Proof-of-Work.

SANOAT KORXONALARIDA KIBERHUJUMLAR SHAROITIDA TAQSIMLANGAN BOSHQARUV TIZIMLARINING ZAIFLIKLARINI TAHLIL QILISH

Vasikov A.R.
Magistrant
Badriev A.I.,
Dotsent, texnika fanlari nomzodi
Qozon (Volga bo'yi) federal universitetining Naberejnye Chelni instituti (filiali),
Naberejnye Chelni, Rossiya
ainur.vasikov@gmail.com

Annotatsiya: Maqolada sanoat korxonalarining taqsimlangan boshqaruv tizimlari tarkibidagi SCADA tizimlarining kiberxavfsizlik muammosi ko'rib chiqiladi. Blokcheyn texnologiyasiga asoslangan texnologik ma'lumotlarning yaxlitligi va haqiqiyligini ta'minlovchi taqsimlangan tizim arxitekturasi taklif etiladi. Kriptografik algoritmlar va konsensus mexanizmidan foydalanadigan blokcheyn moduli taqdim etilgan. Sanoat boshqaruvchisi bilan protokol orqali integratsiya amalga oshirilgan, bloklar zanjirini vizualizatsiya qilish va hujumlarni aniqlash uchun interfeys ishlab chiqilgan. Modellashtirish natijalari tizimning ma'lumotlarning o'zgarmasligini kafolatlash va soxtalashtirish urinishlarini aniqlash qobiliyatini tasdiqlaydi.

Kalit so'zlar: SCADA tizimlari, blokcheyn, kiberxavfsizlik, OPC UA, ma'lumotlar yaxlitligi, raqamli imzo, SHA-512 xeshlash, Proof-of-Work.

Введение. На опасных производственных объектах промышленных предприятий, одним из решений по обеспечению надежности функционирования технологических процессов является применение программно-аппаратных комплексов распределенных систем управления (РСУ). Однако рост числа кибератак, таких как подмена телеметрических данных, атаки «человек посередине», промышленный шпионаж, указывает на недостаточность традиционных методов

защиты: межсетевых экранов, антивирусного ПО и физической изоляции [1, 2]. В том числе, централизованные системы контроля не гарантируют неизменность истории данных и прозрачность аудита. В данной работе проводится степень уязвимости SCADA-систем РСУ, предложен метод на основе технологии блокчейн, обеспечивающей целостность, аутентичность и отслеживаемость передаваемой информации.

Архитектура системы защиты. Концептуальная модель и схема предлагаемой системы состоит из следующих компонентов (рисунок 1), (рисунок 2):

1. Промышленный контроллер (эмуляция Siemens S7-1500 в TIA Portal), генерирующий данные температуры.
2. OPC UA сервер (S7-PLCSIM Advanced) для стандартизированной передачи данных.
3. Блокчейн-ядро на языке C#, реализующее формирование блоков, криптографическую защиту и валидацию.
4. Графический интерфейс (Windows Forms) для визуализации цепочки, мониторинга статуса и имитации атак.

Рисунок 1 — Концептуальная модель системы

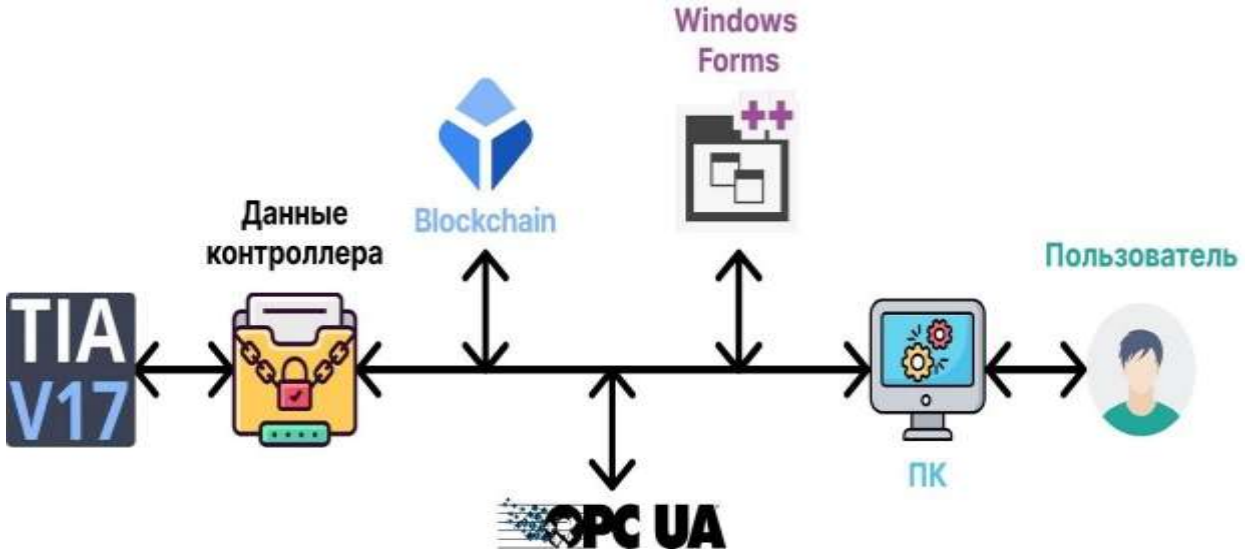

Рисунок 2 — Схема взаимодействия компонентов

Реализация блокчейн-модуля

Каждый блок содержит данные сенсора (идентификатор, значение, временную метку), хеш текущего блока (SHA-512), хеш предыдущего блока, nonce, цифровую подпись (RSA-2048) и открытый ключ отправителя [3]. Механизм консенсуса — Proof-of-Work: требуется подобрать nonce такой, чтобы хеш блока начинался с заданного количества нулевых байт (сложность 0x00, 0x00). Ролевая модель (RBAC): предопределены роли Admin (создание генезис-блока) и Sensor1, Sensor2 (добавление блоков). Каждая роль имеет собственную пару RSA-ключей. При добавлении блока система проверяет соответствие подписи и разрешённой роли. Валидация цепочки осуществляется

методами isValid() (проверка хеша), isPrevBlock() (связь с предыдущим блоком) и IsSignatureValid() (верификация подписи). Полная проверка всех блоков выполняется методом IsValid().

Интеграция с SCADA и тестирование

Подключение к контроллеру выполнено через библиотеку OPCFoundation.NetStandard.Opc.Ua. Программа на C# считывает значение температуры из OPC UA-сервера, упаковывает его в блок, выполняет майнинг и добавляет блок в цепочку. Для проверки устойчивости реализован модуль имитации атак:

1. Подделка данных — изменение значений в блоке приводит к нарушению хеша и связи, что немедленно обнаруживается.
2. Подделка подписи — замена подписи на невалидную выявляется при верификации.
3. MITM-атака — внедрение поддельного блока с легитимной подписью (украденными ключами) обнаруживается системой, если реализована проверка источника данных (в прототипе такая проверка включена).
4. Неавторизованная роль — блок с ролью Hacker отклоняется на этапе добавления.

Все события фиксируются в журнале, а невалидные блоки подсвечиваются в интерфейсе (рисунок 3).

Рисунок 3 — Пользовательский интерфейс с отображением цепочки блоков и лога событий (приводится в оригинале статьи).

Заключение

Разработанная система обеспечивает:

1. неизменность данных за счёт связывания блоков через крипто-хеши;
2. аутентичность источника благодаря цифровым подписям и ролевой модели;
3. прозрачность аудита — любой участник может проверить целостность цепочки;
4. защиту от основных видов атак, характерных для SCADA-сред.

Тестирование на эмуляторе контроллера подтвердило, что система гарантирует целостность данных и автоматически сигнализирует о попытках подделки. Предложенное решение может быть интегрировано в существующие SCADA-системы без замены оборудования, что снижает стоимость внедрения. Дальнейшие направления развития — поддержка распределённого хранения блокчейна и интеграция с реальными промышленными объектами.

Список литературы

1. Дрешер Д. Основы блокчейна: вводный курс для начинающих. — М.: ДМК Пресс, 2018. — 312 с.
2. Интегрированные системы проектирования и управления. SCADA: учебное пособие / Х.Н. Музипов и др. — СПб.: Лань, 2022. — 408 с.
3. Тюкачев Н.А., Хлебостроев В.Г. C#. Основы программирования — СПб.: Лань, 2021. — 272 с.

ТРАНСФОРМАЦИЯ ГРАЖДАНСКОЙ ИДЕНТИЧНОСТИ МОЛОДЕЖИ В УСЛОВИЯХ СОВРЕМЕННЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ

Кавылова А. Р.
Старший преподаватель кафедры общественных наук
Филиала КФУ в городе Джизак
adalat.kavylova1958@gmail.com

Аннотация: В данной статье исследуется динамика трансформации гражданской идентичности современной молодежи под воздействием современных интеллектуальных систем (алгоритмов искусственного интеллекта, рекомендательных сетей и систем предиктивной аналитики). Актуальность работы обусловлена переходом процесса социализации молодежи в алгоритмизированную цифровую среду, где традиционные институты гражданского воспитания сталкиваются с технологическими механизмами фильтрации контента. Автор анализирует специфические феномены, такие как «алгоритмические эхо-камеры» и «цифровые пузыри фильтров», которые фрагментируют общественное сознание и создают условия для когнитивных манипуляций. В работе подчеркивается амбивалентный характер влияния интеллектуальных систем: от расширения возможностей глобального гражданского участия до рисков размывания национальной идентичности.

Ключевые слова: гражданская идентичность, молодежь, интеллектуальные системы, искусственный интеллект, цифровая социализация, алгоритмические эхо-камеры, цифровая грамотность, когнитивные манипуляции, цифровое гражданство, информационное пространство, ценностные ориентации, виртуальная среда.

TRANSFORMATION OF CIVIL IDENTITY OF YOUTH IN THE CONTEXT OF MODERN INTELLECTUAL SYSTEMS

A. R. Kavilova
Senior Lecturer, Department of Social Sciences
KFU Branch in Jizzakh
adalat.kavylova1958@gmail.com

Abstract: This article explores the dynamics of the transformation of youth civic identity under the influence of modern intelligent systems (artificial intelligence algorithms, recommendation networks, and predictive analytics systems). The relevance of the study is driven by the shift in the socialization process of young people into an algorithmized digital environment, where traditional institutions of civic education encounter technological mechanisms of content filtering. The author analyzes specific phenomena such as "algorithmic echo chambers" and "digital filter bubbles," which fragment public consciousness and create conditions for cognitive manipulation. The paper emphasizes the ambivalent nature of the influence of intelligent systems: from expanding opportunities for global civic engagement to the risks of eroding national identity.

Keywords: civic identity, youth, intelligent systems, artificial intelligence, digital socialization, algorithmic echo chambers, digital literacy, cognitive manipulation, digital citizenship, information space, value orientations, virtual environment.