DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-17
УДК 004.056.55:004.738.5:681.518.5:004.94
Авдалов Герман Вікторович[1], аспірант
https://orcid.org/0009-0007-7728-6659
Самарай Валерій Петрович[2], к.т.н., с.н.с., доцент
https://orcid.org/0000-0003-4419-1366
[1]Відкритий Міжнародний Університет Розвитку Людини «Україна», м. Київ, Україна
[2]Центр воєнно-стратегічних досліджень, Національного університету оборони України, м. Київ, Україна

ЗАХИСТ КОМУНІКАЦІЙНОГО ТРАФІКУ В SCADA-СИСТЕМАХ З ВИКОРИСТАННЯМ ГІБРИДНИХ АЛГОРИТМІВ СТІЙКИХ ДО КВАНТОВИХ АТАК

Авдалов Г.В., Самарай В.П. Захист комунікаційного трафіку в SCADA-системах з використанням гібридних алгоритмів стійких до квантових атак. У статті досліджено проблему захисту комунікаційного трафіку в SCADA-системах в умовах підвищених загроз, зумовлених відкритістю інфраструктури та розвитком квантових обчислень. Обґрунтовано доцільність використання гібридного криптографічного підходу, що поєднує симетричне шифрування та постквантовий обмін ключами, з урахуванням обмежених обчислювальних ресурсів пристроїв та особливостей промислових протоколів (Modbus, DNP3, IEC 60870-5-104). Розроблено модель криптомодуля, який інтегрується в комунікаційні вузли SCADA-мережі. Запропоновано математичне формалізоване представлення процедури генерації гібридного ключа з використанням алгоритму CRYSTALS-Kyber, а також реалізовано схему балансування криптографічного навантаження між шлюзами та периферійними пристроями. Проведено порівняльне експериментальне дослідження, яке продемонструвало зменшення затримки передачі, енергоспоживання і використання пам'яті порівняно з TLS 1.2. Запропонована модель показала високу адаптивність до промислових умов, масштабованість, стійкість до атак у квантовій моделі обчислень і сумісність з обмеженими апаратними платформами. Перспективи подальших досліджень включають розробку інтелектуального модуля адаптивного керування параметрами шифрування в реальному часі та впровадження в SCADA-системи критичної інфраструктури.
Ключові слова: SCADA-системи, захист комунікаційного трафіку, гібридна криптографія, постквантова криптографія, промислові протоколи, критична інфраструктура

Avdalov G., Samaraj V. Protection of communication traffic in SCADA systems using hybrid algorithms resistant to quantum attacks. The article explores the challenge of securing communication in SCADA systems within critical infrastructure such as energy, water, transport, and industrial automation. These systems often lack cryptographic protection, making them vulnerable to cyber threats like man-in-the-middle, command spoofing, data interception, and replay attacks, potentially causing severe operational and safety consequences. With quantum computing emerging as a threat to traditional cryptographic schemes like RSA and ECC, there is a pressing need for new approaches. However, SCADA devices are often limited in computational resources, restricting the use of post-quantum algorithms. To overcome this, the article introduces a hybrid cryptographic model that combines efficient symmetric encryption with quantum-resistant key exchange protocols. The hybrid module is designed for the communication layer in SCADA environments, operating between controllers and gateways or within servers. It integrates a post-quantum key exchange mechanism (e.g., CRYSTALS-Kyber, NTRU), a symmetric cipher for data encryption, and a session key manager. A mathematical model of key generation is proposed, with mechanisms for offloading heavy computations to more capable nodes via precomputation, caching, and adaptive segmentation of encrypted traffic. The solution was tested through simulations approximating real SCADA environments. Performance metrics included session setup time, latency, memory load, and energy consumption, compared across configurations: unprotected, TLS 1.2, and the proposed hybrid. Results showed the hybrid scheme provided lower latency and energy consumption than TLS while maintaining robust cryptographic strength. It supports integration with Modbus TCP, DNP3, and IEC 60870-5-104 without altering protocol frames. The model is scalable, compatible with constrained hardware like STM32 and ESP32, and easily integrates into existing SCADA infrastructures. Scientific novelty includes a tailored hybrid cryptographic framework for SCADA, a context-aware key exchange formalization, and optimized post-quantum techniques for embedded applications.
Key words: SCADA systems, communication traffic protection, hybrid cryptography, post-quantum cryptography, industrial protocols, critical infrastructure

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. Сучасні SCADA-системи відіграють ключову роль у керуванні критичною інфраструктурою, зокрема в енергетиці, водопостачанні, транспорті, промисловості та телекомунікаціях [1]. Їх відкритість, підключення до мереж загального користування та зростання складності створюють нові вектори атак, зокрема через комунікаційні канали, що перетворює захист переданих даних на пріоритетне завдання [2]. Вразливість трафіку в таких системах може призвести до серйозних наслідків: порушення технологічних процесів, фінансових втрат, загроз для довкілля та безпеки людей [3].

Ситуація ускладнюється з огляду на прогнозований розвиток квантових обчислювальних систем, здатних подолати традиційні криптографічні алгоритми. Більшість класичних методів

шифрування, таких як RSA, DSA або ECC, базуються на складності задач факторизації та дискретного логарифмування, що вже мають ефективні алгоритмічні рішення у квантовій моделі (наприклад, алгоритм Шора) [4]. Це створює нагальну потребу у впровадженні криптографічних механізмів, стійких до квантових атак.

Додатковим викликом є обмежені обчислювальні ресурси багатьох SCADA-компонентів, що часто базуються на мікроконтролерах або вбудованих платформах із низькою продуктивністю. У таких умовах класичні постквантові алгоритми можуть бути надто ресурсоємними. Водночас спостерігається підвищення інтересу до гібридних криптографічних схем, які поєднують переваги класичних та постквантових підходів, забезпечуючи баланс між безпекою, сумісністю та ефективністю.

Наукова спільнота наразі зосереджує увагу на розробці адаптивних, ресурсоефективних і масштабованих методів захисту комунікаційного трафіку SCADA-систем з урахуванням загроз майбутніх квантових обчислень [5]. Практичні завдання включають побудову моделей загроз, розробку механізмів автентифікації і шифрування, що забезпечують цілісність і конфіденційність даних у реальному часі, а також забезпечення сумісності із чинними стандартами промислових протоколів.

Метою дослідження є розробка моделі захисту комунікаційного трафіку в SCADA-системах з використанням гібридних криптографічних алгоритмів, стійких до квантових атак, з урахуванням обмежень ресурсів та специфіки промислових мереж.

Аналіз останніх досліджень та публікацій. Захист інформації в SCADA-системах є предметом численних досліджень, що охоплюють різні аспекти безпеки: від виявлення вторгнень до криптографічного захисту трафіку. У наукових роботах підкреслюється, що SCADA-системи, на відміну від традиційних IT-систем, функціонують в умовах жорстких обмежень за часом, ресурсами та доступністю, що ускладнює впровадження класичних механізмів інформаційної безпеки. Дослідники відзначають зростання кількості атак, орієнтованих на порушення цілісності, автентичності та конфіденційності переданих даних, особливо через уразливі промислові протоколи, такі як Modbus, DNP3, IEC 60870-5-104 [6].

Одним із напрямів забезпечення захищеності є впровадження криптографічних засобів, які можна адаптувати до особливостей SCADA-середовища. У цьому контексті дедалі більше уваги приділяється легковаговим криптографічним алгоритмам, що мають низькі вимоги до пам'яті та обчислювальної потужності [7]. Водночас у публікаціях останніх років зазначається, що класичні алгоритми шифрування, такі як RSA або ECC, стають вразливими в умовах розвитку квантових обчислювальних систем. Дослідники зосереджують увагу на постквантових алгоритмах, зокрема на основі решіток (CRYSTALS-Kyber, NTRU), кодів (Classic McEliece), ізогеній еліптичних кривих (SIKE), хешування (SPHINCS+), а також на гібридних схемах, що поєднують кілька підходів для посилення захисту [8, 9].

На тлі загального інтересу до постквантової криптографії з'являються праці, присвячені її адаптації до обмежених середовищ, таких як IoT та SCADA. Зокрема, досліджується впровадження полегшених варіантів криптографічних протоколів у пристрої з низькою енергоспоживчою моделлю. У роботах, що торкаються гібридного підходу, аналізуються схеми, де симетричне шифрування поєднується з асиметричним постквантовим обміном ключами, що дозволяє забезпечити як продуктивність, так і стійкість до майбутніх атак [10].

Попри наявність перспективних теоретичних моделей, більшість доступних рішень зосереджена на загальних цифрових мережах і не враховує особливості SCADA-систем. Лише окремі публікації порушують питання адаптації постквантових алгоритмів до специфіки промислових протоколів, високої критичності переданих даних, суворих вимог до часу відповіді та мінімального споживання ресурсів. Наголошується на необхідності зменшення криптографічного навантаження, оптимізації розміру ключів та підвищення швидкодії, особливо у середовищах із обмеженими можливостями мікроконтролерів.

Особливої уваги потребують моделі, що дозволяють динамічно керувати параметрами шифрування залежно від мережевого контексту, типу переданих даних або поточного рівня загрози. Такий підхід дає змогу підвищити гнучкість захисту в SCADA-системах, не перевантажуючи ресурси. Проте широкої апробації ці механізми в контексті SCADA ще не набули, що зумовлює актуальність подальших досліджень у цьому напрямі.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. SCADA-системи складаються з керуючого центру, віддалених терміналів (RTU), програмованих

логічних контролерів (PLC) та каналів зв'язку, які забезпечують обмін технологічними командами та телеметричними даними. У типовій архітектурі комунікаційні канали між центральним сервером та польовими пристроями найчастіше реалізуються через TCP/IP або серійні інтерфейси з використанням промислових протоколів, зокрема Modbus, DNP3, IEC 60870-5-104. Основними вразливими місцями є нешифровані дані в каналі, відсутність автентифікації, передача команд у відкритому вигляді та нестача контролю цілісності повідомлень. Ці вразливості створюють умови для атак типу man-in-the-middle, replay-атак, підміни даних і впровадження шкідливих команд.

Для підвищення рівня захищеності в комунікаційний канал вводиться гібридний криптографічний модуль, що реалізується на прикордонних вузлах мережі – між контролером та мережею, або між шлюзом і віддаленим пристроєм. Такий модуль складається з блоку постквантового асиметричного обміну ключами, симетричного блоку шифрування основного трафіку та керувального блоку генерації і оновлення ключів сесії. Додатково передбачається механізм автентифікації вузлів за допомогою хеш-функцій, стійких до квантових обчислень.

На рисунку 1 представлено структурну схему взаємодії між компонентами SCADA-системи з інтегрованим гібридним криптомодулем.

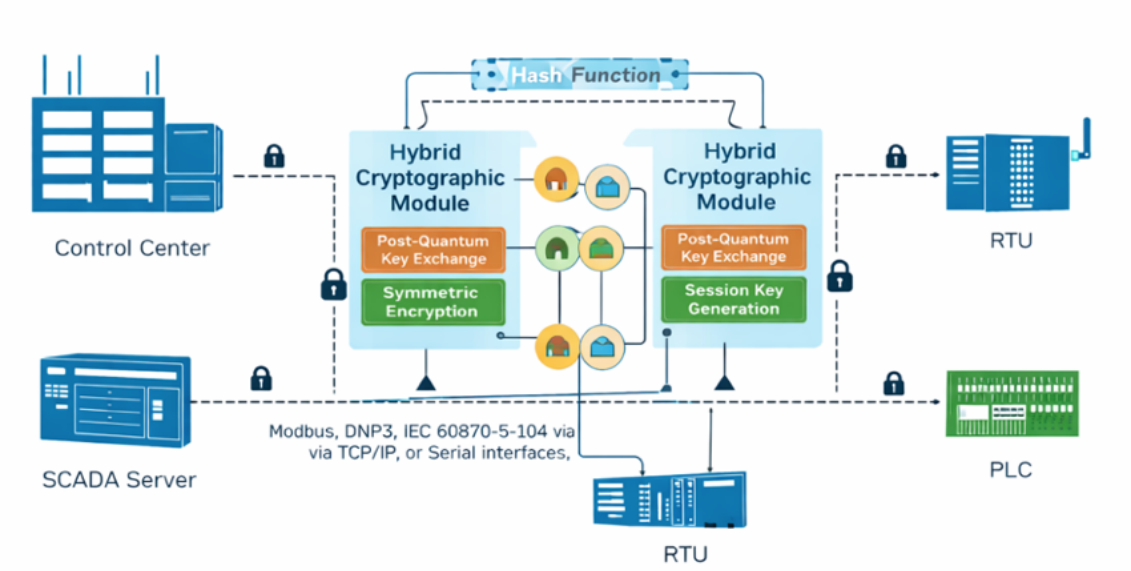

Рис. 1 – Архітектура SCADA-системи з вбудованим гібридним криптомодулем

Сценарії використання передбачають обмін технологічними командами та телеметрією між польовими пристроями й центром управління через захищений канал, що ініціалізується асиметричним ключовим обміном і підтримується симетричним шифруванням з періодичним оновленням параметрів. Захист трафіку включає перевірку цілісності, автентифікацію вузлів, а також синхронізацію ключових значень для збереження узгодженості шифрування.

Гібридна криптографічна модель реалізується як композиція алгоритмів $E_s: M \to C$ та K_p, $K_s \in K$, де E_s – симетрична функція шифрування з ключем K_s, який отримується в результаті постквантового обміну на основі K_p, що належать до простору дозволених ключів K. Початковий обмін відбувається шляхом обчислення гібридного секрету $K_s = f(K_a, K_b)$, де f – функція злиття відкритого ключа абонента K_a та тимчасового епізодичного ключа K_b, згенерованого в рамках постквантового алгоритму.

У випадку використання CRYSTALS-Kyber ключова згортка здійснюється за схемою (1).

$$K_s = SHA3_{512}(Enc(K_a, r)||Dec(C, K_b)) \quad (1)$$

де Enc, Dec – функції шифрування та розшифрування Kyber, r – випадкова матриця, а C – закодоване повідомлення.

На рисунку 2 представлено спрощену схему динамічного ключового обміну із зменшенням обчислювального навантаження на слабкі вузли.

Реалізація передбачає делегування обчислень вузлам з більшою обчислювальною потужністю, попереднє кешування результатів криптографічних операцій і використання змінної довжини ключів відповідно до критичності трафіку. Для мінімізації затримки передбачено розщеплення криптографічного потоку на контрольні та експлуатаційні сегменти з незалежними

ключами. Це дозволяє знизити вплив на час відповіді системи, забезпечуючи при цьому високий рівень захисту від атак із застосуванням квантових обчислень.

Інтеграція гібридного криптографічного модуля в SCADA-середовище потребує урахування особливостей промислових протоколів. У протоколі Modbus TCP/IP дані передаються без шифрування й автентифікації, що робить його одним із найуразливіших для атак на канальному рівні. У випадку DNP3 специфікація передбачає базову підтримку Secure Authentication, однак більшість реалізацій її не використовують. Протокол IEC 60870-5-104 передбачає лише базові механізми цілісності на транспортному рівні й не включає криптографічного захисту. Запропонований гібридний модуль інтегрується на рівні канального або транспортного рівня без порушення структури кадрів даних, що дозволяє уникати конфлікту з регламентованими специфікаціями протоколів.

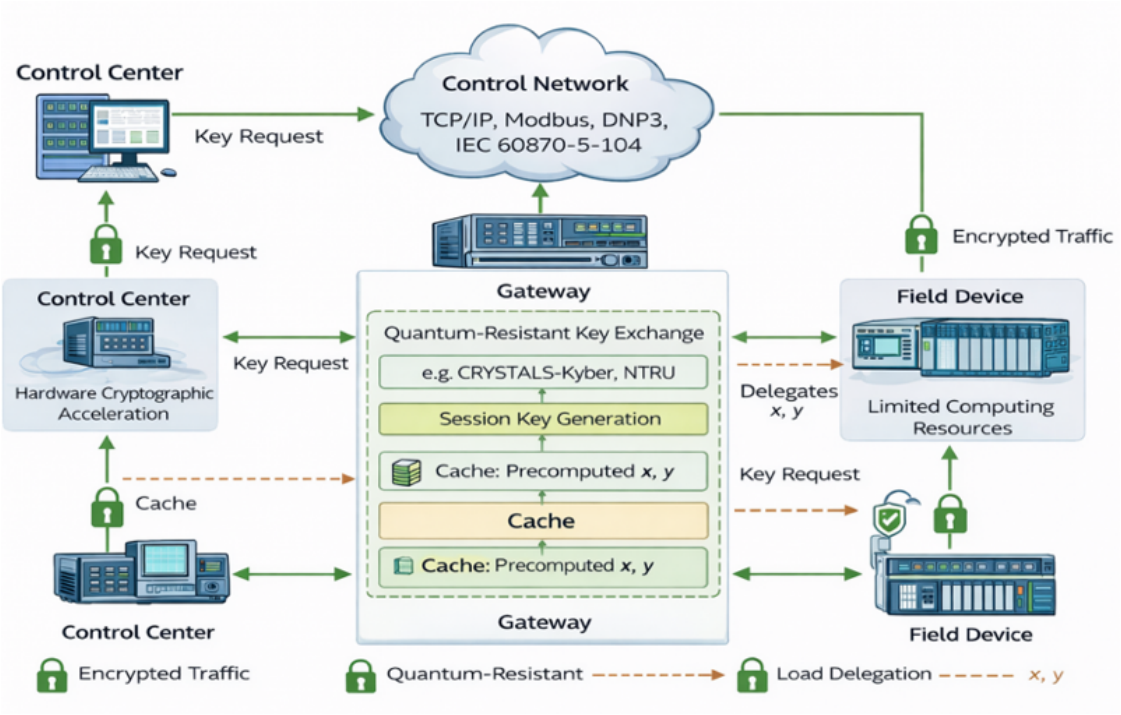

Рис. 2 – Схема гібридного ключового обміну з балансуванням навантаження

Для адаптації до систем із обмеженими обчислювальними ресурсами реалізовано низку оптимізацій. По-перше, відбувається зменшення довжини параметрів ключового обміну при збереженні прийнятного рівня стійкості. По-друге, попередні обчислення симетричних ключів кешуються на шлюзах або контрольних вузлах, а результати передаються польовим пристроям у зашифрованому вигляді. По-третє, у випадку наявності апаратних криптомодулів (наприклад, ARM TrustZone, STM32 CCA), основні обчислення делегуються апаратним засобам із підтримкою алгоритмів AES, SHA-3 та модульної арифметики.

В таблиці 1 показано сумісність запропонованої моделі з типовими промисловими протоколами та мікроконтролерами.

Таблиця 1 – Сумісність гібридного криптомодуля з промисловими реалізаціями

Протокол/ Платформа	**Підтримка шифрування**	**Можливість інтеграції модуля**	**Особливості реалізації**
Modbus TCP/IP	Ні	Так	Потребує шифрування на рівні сокета
DNP3	Частково	Так	Рекомендовано замінити автентифікацію
IEC 60870-5-104	Ні	Так	Шифрування реалізується через проксі-шлюз
STM32F407 (Cortex-M4)	Так (AES, SHA)	Так	Апаратна підтримка криптографічних інструкцій
ESP32-S3	Так (AES, ECC)	Так	Підтримка апаратного прискорення для ECC

Моделювання та експериментальна оцінка виконувались у віртуальному середовищі, наближеному до реального розгортання SCADA. Було змодельовано взаємодію SCADA-сервера, шлюзу та трьох польових пристроїв через TCP/IP-мережу з використанням протоколів Modbus TCP та IEC 104. Трафік формувався на основі реальних шаблонів телеметрії та команд, характерних для об'єктів енергетичної інфраструктури.

Вимірювались такі параметри:

1) середній час встановлення з'єднання;
2) затримка передачі повідомлення;
3) обсяг оперативної пам'яті, необхідної для обчислення ключа;
4) споживання енергії в період ініціалізації з'єднання.

Результати порівнювались для трьох конфігурацій:

1) відкрите з'єднання без захисту;
2) захист із використанням TLS 1.2;
3) захист із гібридною постквантовою схемою.

На рисунку 3 подано графік середньої затримки в залежності від кількості пристроїв у мережі.

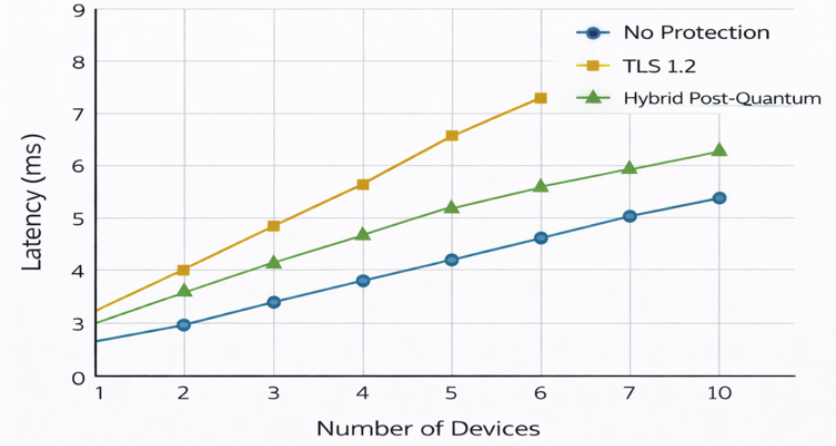

Рис. 3 – Залежність затримки передачі від кількості пристроїв

На рисунку 4 відображено порівняння енергоспоживання в режимі встановлення з'єднання.

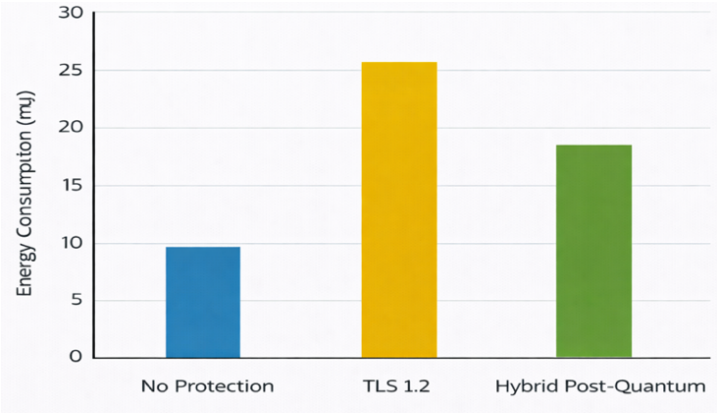

Рис. 4 – Споживання енергії під час криптографічного обміну

В таблиці 2 представлено результати експериментального оцінювання.

Таблиця 2 – Порівняння моделей захисту для SCADA-середовища

Параметр	**Без захисту**	**TLS 1.2**	**Гібридна модель**
Час встановлення з'єднання	4 мс	28 мс	16 мс
Затримка передачі кадру	1.2 мс	4.9 мс	3.1 мс
Використання оперативної пам'яті	-	43 КБ	36 КБ
Споживання енергії	-	9.3 мДж	6.7 мДж

Отримані результати свідчать про здатність гібридної моделі забезпечити прийнятний баланс між продуктивністю та криптографічною стійкістю, що є критично важливим для SCADA-систем з обмеженими ресурсами та вимогами до реального часу.

Ефективність розробленої гібридної моделі оцінюється за трьома ключовими параметрами: продуктивністю, криптографічною стійкістю та масштабованістю. У ході експериментів зафіксовано скорочення затримок при передаванні даних порівняно з TLS 1.2, зокрема в умовах обмежених ресурсів. Це досягається за рахунок делегування важких обчислень на шлюзи, використання кешованих обчислень та зменшення складності сесійної ініціалізації. Гібридна модель зберігає постквантову стійкість, оскільки обмін ключами реалізовано на основі сучасних схем, таких як CRYSTALS-Kyber або NTRU, що пройшли оцінювання в рамках NIST-конкурсу. З погляду масштабованості, модель демонструє стабільну роботу при збільшенні кількості вузлів у мережі, без різкого зростання навантаження на центральний сервер або вузли керування. Використання автономного оновлення сесійних ключів, обмеження частоти ключового обміну та можливість використання попередньо згенерованих параметрів дають змогу ефективно масштабувати захищену архітектуру.

Гібридний підхід виявляється найбільш доцільним саме для SCADA-середовища. Тут класичні TLS-рішення часто є надмірно важкими для вбудованих пристроїв, а традиційні симетричні методи не гарантують захисту в умовах розвитку квантових технологій. Запропонована модель забезпечує необхідний рівень стійкості при обмеженому навантаженні, а також дозволяє впроваджувати захист у вже наявну інфраструктуру без повного її переоснащення.

Модель досягає найкращих результатів у таких умовах: пристрої мають обмежені обчислювальні ресурси та енергобюджет, немає підтримки апаратного прискорення TLS, а мережа побудована на відкритих або застарілих протоколах. Також модель є ефективною у випадках, коли необхідно швидко додавати нові вузли до системи без попереднього обміну ключами або сертифікатами. Практична цінність розробленого підходу полягає в його здатності адаптуватися до обмежень польових пристроїв без зниження рівня безпеки. Модель враховує реалії SCADA-систем: роботу в реальному часі, критичність до затримок, чутливість до навантажень і необхідність сумісності зі стандартними протоколами. Наукова новизна полягає у створенні гібридного криптографічного механізму з контекстно-залежним балансуванням навантаження між вузлами, формалізації обчислювальної схеми ключового обміну для промислових систем, а також в адаптації постквантових алгоритмів до середовищ із жорсткими обмеженнями.

Найближчими напрямками впровадження можуть стати енергетичні об'єкти, системи диспетчерського керування міською інфраструктурою, автоматизовані водоочисні та транспортні станції, а також об'єкти критичної інфраструктури, які експлуатують SCADA-системи з незахищеними або слабко захищеними протоколами. У майбутньому модель може стати основою для розробки нових галузевих стандартів з кіберзахисту у промисловому секторі.

Висновки та перспективи подальшого дослідження. Проведене дослідження підтверджує доцільність впровадження гібридних криптографічних алгоритмів стійких до квантових атак у SCADA-системи для захисту комунікаційного трафіку. Запропонована модель забезпечує високий рівень захищеності переданих даних за рахунок поєднання переваг симетричного шифрування та постквантового асиметричного обміну ключами. Під час експериментальної оцінки модель показала кращий баланс між продуктивністю, криптографічною стійкістю та ресурсозбереженням порівняно з традиційними рішеннями, такими як TLS 1.2.

Архітектурне рішення дозволяє адаптувати механізм захисту до обмежених можливостей польових пристроїв SCADA-систем без втручання в логіку технологічного процесу. Це створює передумови для поступового впровадження моделі у промислових об'єктах із мінімальними змінами в наявній інфраструктурі. Визначено сценарії, за яких модель є найбільш ефективною, зокрема у системах з низьким енергобюджетом, обмеженим обсягом пам'яті та відкритими каналами зв'язку.

У подальших дослідженнях планується розширити математичну модель криптографічного навантаження з урахуванням типу пристрою, типу трафіку та частоти оновлення ключів. Перспективним напрямом є розробка інтелектуального модуля адаптивного керування криптографічними параметрами в режимі реального часу залежно від контексту передачі даних і рівня загроз. Також доцільним є тестування моделі в умовах мультисегментованих мереж SCADA та її інтеграція з механізмами виявлення аномалій для побудови комплексної системи кіберзахисту.

Список бібліографічного опису

1. Nuruzzaman, M., Rana, S. IoT-enabled condition monitoring in power distribution systems: A review of SCADA-based automation, real-time data analytics, and cyber-physical security challenges. Journal of Sustainable Development and Policy. 2025. Vol. 1. No. 01. P. 25–43. https://doi.org/10.63125/pyd1x841
2. Karthikeyan, K., Sanjeevikumar, P., Thomas, S. K., Babu, A. Critical review of SCADA and PLC in smart buildings and energy sector. Energy Reports. 2024. Vol. 12. P. 1518–1530. https://doi.org/10.1016/j.egyr.2024.07.041
3. Urooj, B., Ullah, U., Shah, M. A., Sikandar, H. S., Stanikzai, A. Q. Risk assessment of SCADA cyber attack methods: A technical review on securing automated real-time SCADA systems. Proceedings of the 27th International Conference on Automation and Computing (ICAC). 2022. P. 1–6. IEEE. 10.1109/ICAC55051.2022.9911122
4. Tidrea, A., Korodi, A., Silea, I. Elliptic curve cryptography considerations for securing automation and SCADA systems. Sensors. 2023. Vol. 23. No. 5. 2686. https://doi.org/10.3390/s23052686
5. Naz, M. T., Elmedany, W., Ali, M. Securing SCADA systems in smart grids with IoT integration: A self-defensive post-quantum blockchain architecture. Internet of Things. 2024. Vol. 28. 101381. http://dx.doi.org/10.2139/ssrn.4733522
6. Narayanan, M., Hafeez, M. A., Munir, A. Encryption for industrial control systems: A survey of application-level and network-level approaches in smart grids. Journal of Cybersecurity and Privacy. 2026. Vol. 6. No. 1. 11. https://doi.org/10.3390/jcp6010011
7. Rozlomii, I., Naumenko, S., Myhailovskyi, P., Lishchuk, R. Methodology for selecting the protection strategy in IoT environments based on the device resource profile. Proceedings of the IEEE 6th KhPI Week on Advanced Technology (KhPIWeek). 2025. P. 1–5. IEEE. DOI: 10.1109/KhPIWeek61436.2025.11288556
8. Yan, H., Wu, L., Sun, Q., He, P. Lattice-based cryptographic accelerators for the post-quantum era: Architectures, optimizations, and implementation challenges. Electronics. 2026. Vol. 15. No. 2. 475. https://doi.org/10.3390/electronics15020475
9. Sane, P., Patel, S. P. Post-quantum cryptography: A review of algorithms, challenges, and future research directions. Proceedings of the 8th International Conference on Signal Processing and Information Security (ICSPIS). 2025. P. 1–6. IEEE. DOI: 10.1109/ICSPIS67605.2025.11318393
10. Шкітов, А., Авдалов, Г. Оцінювання продуктивності гібридних криптографічних схем при впровадженні у системи з обмеженими ресурсами в умовах квантової загрози. Measuring and Computing Devices in Technological Processes. 2025. No. 4. P. 316–322. https://doi.org/10.31891/2219-9365-2025-84-36

References

1. Nuruzzaman, M., Rana, S. IoT-enabled condition monitoring in power distribution systems: A review of SCADA-based automation, real-time data analytics, and cyber-physical security challenges. Journal of Sustainable Development and Policy. 2025. Vol. 1. No. 01. P. 25–43. https://doi.org/10.63125/pyd1x841
2. Karthikeyan, K., Sanjeevikumar, P., Thomas, S. K., Babu, A. Critical review of SCADA and PLC in smart buildings and energy sector. Energy Reports. 2024. Vol. 12. P. 1518–1530. https://doi.org/10.1016/j.egyr.2024.07.041
3. Urooj, B., Ullah, U., Shah, M. A., Sikandar, H. S., Stanikzai, A. Q. Risk assessment of SCADA cyber attack methods: A technical review on securing automated real-time SCADA systems. Proceedings of the 27th International Conference on Automation and Computing (ICAC). 2022. P. 1–6. IEEE. 10.1109/ICAC55051.2022.9911122
4. Tidrea, A., Korodi, A., Silea, I. Elliptic curve cryptography considerations for securing automation and SCADA systems. Sensors. 2023. Vol. 23. No. 5. 2686. https://doi.org/10.3390/s23052686
5. Naz, M. T., Elmedany, W., Ali, M. Securing SCADA systems in smart grids with IoT integration: A self-defensive post-quantum blockchain architecture. Internet of Things. 2024. Vol. 28. 101381. http://dx.doi.org/10.2139/ssrn.4733522
6. Narayanan, M., Hafeez, M. A., Munir, A. Encryption for industrial control systems: A survey of application-level and network-level approaches in smart grids. Journal of Cybersecurity and Privacy. 2026. Vol. 6. No. 1. 11. https://doi.org/10.3390/jcp6010011
7. Rozlomii, I., Naumenko, S., Myhailovskyi, P., Lishchuk, R. Methodology for selecting the protection strategy in IoT environments based on the device resource profile. Proceedings of the IEEE 6th KhPI Week on Advanced Technology (KhPIWeek). 2025. P. 1–5. IEEE. DOI: 10.1109/KhPIWeek61436.2025.11288556
8. Yan, H., Wu, L., Sun, Q., He, P. Lattice-based cryptographic accelerators for the post-quantum era: Architectures, optimizations, and implementation challenges. Electronics. 2026. Vol. 15. No. 2. 475. https://doi.org/10.3390/electronics15020475
9. Sane, P., Patel, S. P. Post-quantum cryptography: A review of algorithms, challenges, and future research directions. Proceedings of the 8th International Conference on Signal Processing and Information Security (ICSPIS). 2025. P. 1–6. IEEE. DOI: 10.1109/ICSPIS67605.2025.11318393
10. Shkitov, A., Avdalov, G. Performance evaluation of hybrid cryptographic schemes when implemented in systems with limited resources under quantum threat conditions. Measuring and Computing Devices in Technological Processes. 2025. No. 4. P. 316–322. https://doi.org/10.31891/2219-9365-2025-84-36

Історія статті:
Отримано: 04.02.2026 Доопрацьовано: 18.02.2026 Прийнято до друку: 23.03.2026 Опубліковано: 29.03.2026