https://doi.org/10.31891/2219-9365-2025-81-4
УДК 004.056

РОЗЛОМІЙ Інна
Черкаський державний технологічний університет
https://orcid.org/0000-0001-5065-9004
e-mail: inna-roz@ukr.net
ФАУРЕ Еміль
Черкаський державний технологічний університет
https://orcid.org/0000-0002-2046-481X
e-mail: e.faure@chdtu.edu.ua
НАУМЕНКО Сергій
Черкаський національний університет ім. Б. Хмельницького
https://orcid.org/0000-0002-6337-1605
e-mail: naumenko.serhii1122@vu.cdu.edu.ua

МЕТОДИ АУТЕНТИФІКАЦІЇ У ВБУДОВАНИХ СИСТЕМАХ З ОБМЕЖЕНИМИ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ

У статті розглядаються методи аутентифікації, що застосовуються у вбудованих системах з обмеженими обчислювальними ресурсами. З огляду на зростаючу потребу в безпеці інформаційних технологій, автори аналізують різні підходи до аутентифікації, їх переваги та недоліки. Зокрема, акцентується увага на методах, таких як паролі, одноразові коди, токени та багатофакторна аутентифікація. Досліджуються параметри оцінки ефективності, такі як швидкість, безпека та споживання ресурсів, що є критично важливими для вбудованих систем. Результати тестування демонструють вплив обраних методів на загальну продуктивність системи, що дозволяє зробити обґрунтовані висновки про їх доцільність у конкретних умовах експлуатації.

Ключові слова: аутентифікація, вбудовані системи, обмежені ресурси, безпека даних, паролі, OTP, токени, MFA, полегшені криптоалгоритми.

ROZLOMII INNA, FAURE EMIL
Cherkassy State Technological University
NAUMENKO SERHII
Bohdan Khmelnytsky National University of Cherkasy

AUTHENTICATION METHODS IN EMBEDDED SYSTEMS WITH LIMITED COMPUTING RESOURCES

The article discusses various authentication methods used in embedded systems with limited computing resources. In today's world, the growing need for information technology security necessitates the implementation of effective data protection solutions. Embedded systems, as a rule, have limited capabilities in terms of memory, computing power and power consumption, which makes it difficult to implement complex authentication algorithms.

The article analyzes the main authentication approaches, including passwords, one-time codes (OTPs), tokens, and multi-factor authentication (MFA). Each of these methods has its advantages and disadvantages, which the authors consider in detail. Authentication using passwords, although an easy method to implement, is vulnerable to match-based attacks. This necessitates the implementation of more complex security policies.

At the same time, one-time codes generated for each authentication session provide an additional layer of protection, but their use may require additional resources for generation and verification. Tokens, both hardware and software, provide a higher level of security, but can be less convenient to use. Multi-factor authentication combines several methods, increasing security, but requires more resources and execution time, which can be critical for embedded systems.

The authors of the article conducted comprehensive testing of various authentication methods in order to evaluate their effectiveness according to three main parameters: speed, security and resource consumption. The results of the study show that authentication methods differ significantly in execution speed and energy consumption. For example, authentication with passwords proved to be the fastest but with the lowest level of security, while one-time codes and tokens offered a higher level of protection but required more time to process.

In conclusion, the article emphasizes the importance of choosing appropriate authentication methods that take into account the specifics of embedded systems. Recommendations from testing can be useful for developers and engineers working in the field, helping to balance security, speed, and resource efficiency. The study points to the need for further developments in the field of authentication to meet the needs of modern embedded systems and guarantee their reliability in the context of data security.

Keywords: authentication, embedded systems, limited resources, data security, passwords, OTP, tokens, MFA, lightweight cryptoalgorithms.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Вбудовані системи стали невід'ємною частиною сучасного життя, забезпечуючи широкий спектр функцій у різних сферах, таких як промисловість, охорона здоров'я, автомобільна техніка та побутова

електроніка. Ці системи характеризуються обмеженими ресурсами, такими як процесорна потужність, пам’ять і енергоспоживання, що ускладнює реалізацію складних алгоритмів безпеки та аутентифікації [1]. Незважаючи на свою простоту, вбудовані системи часто містять чутливу інформацію і взаємодіють із зовнішніми мережами, що підвищує ризик атак і зловживань. Для забезпечення надійного захисту та безпечного інформаційного обміну важливо розуміти архітектуру вбудованої системи, оскільки це дозволяє оцінити вразливості, які можуть бути використані зловмисниками. Правильний вибір методів аутентифікації залежить від структури системи, її компонентів та їх взаємозв'язків [2]. Важливо також врахувати, які дані обробляються, як вони передаються та зберігаються, щоб розробити ефективні рішення для захисту.

На рис. 1 представлена схема, що демонструє структуру вбудованої системи, включаючи основні компоненти, такі як мікроконтролер, пам'ять, датчики та мережеві інтерфейси.

Мікроконтролер виступає центральним елементом, відповідальним за виконання обчислень та управління іншими компонентами. Пам’ять забезпечує зберігання програмного забезпечення та даних, необхідних для функціонування системи. Датчики, що інтегровані в систему, збирають інформацію з навколишнього середовища, а мережеві інтерфейси забезпечують зв’язок із зовнішніми системами або інтернетом [3].

Актуальність проблеми аутентифікації в умовах обмежених ресурсів зумовлена необхідністю забезпечення безпеки даних і захисту від несанкціонованого доступу. Традиційні методи аутентифікації, які використовуються в більш потужних системах, не завжди можуть бути ефективно реалізовані у вбудованих системах через їх обмеження. Тому важливо розробити нові або адаптувати існуючі методи, щоб забезпечити достатній рівень захисту при збереженні оптимальних показників ресурсів.

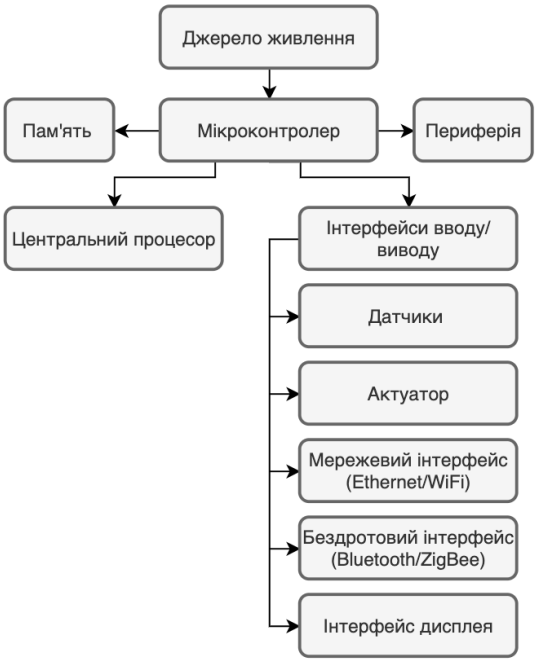


Рис. 1 Схема архітектури вбудованої системи

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета дослідження полягає в аналізі та оцінці різних методів аутентифікації, що можуть бути застосовані у вбудованих системах з обмеженими ресурсами. Завданнями дослідження є вивчення сучасних підходів до аутентифікації, аналіз їх ефективності в умовах обмежених ресурсів, а також розробка рекомендацій щодо впровадження найбільш підходящих методів у практику.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Проблематика забезпечення безпеки цих систем стає дедалі актуальнішою у зв’язку з зростанням використання IoT-пристроїв, які все частіше інтегруються в критично важливі інфраструктури, такі як охорона здоров'я, енергетика та транспорт. Робота [4] акцентує увагу на важливості розробки полегшених криптографічних алгоритмів для вбудованих систем. Автори пропонують новий підхід до аутентифікації на основі симетричних криптографічних методів, що забезпечують високий рівень захисту при обмежених ресурсах. Дослідження показало, що використання адаптивних алгоритмів дозволяє зменшити навантаження на обчислювальні ресурси без шкоди для безпеки.

Інше важливе дослідження [5] зосереджене на використанні біометричних методів аутентифікації у вбудованих системах. Автори доводять, що інтеграція біометричних даних може суттєво підвищити рівень безпеки, проте наголошують на необхідності оптимізації алгоритмів для забезпечення швидкості обробки даних. Це особливо важливо для систем, де швидка аутентифікація є критично важливою, наприклад, у медичних пристроях. У дослідженні [6] розглядаються протоколи аутентифікації, що поєднують кілька факторів, включаючи паролі та токени. Автори зазначають, що багатофакторна аутентифікація може суттєво знизити ризик несанкціонованого доступу, проте реалізація таких рішень у вбудованих системах вимагає ретельного підбору методів, які враховують обмежені ресурси.

Окрему увагу також привертають дослідження, які зосереджені на енергозбереженні в процесах аутентифікації. Автори [7] виявили, що використання спеціалізованих протоколів, оптимізованих для зниження енергоспоживання, може покращити тривалість роботи батарей в IoT-пристроях, не жертвуючи при цьому рівнем безпеки.

В праці [8] пропонують застосування методів машинного навчання для оптимізації процесів аутентифікації. Використання штучного інтелекту дозволяє автоматизувати ідентифікацію користувачів, виявляти аномалії в поведінці та адаптувати аутентифікаційні процеси в реальному часі, що може суттєво покращити безпеку вбудованих систем.

Дослідження у сфері аутентифікації для вбудованих систем з обмеженими ресурсами активно розвиваються та пропонують нові підходи і рішення. Водночас існують значні виклики, які потребують подальшого вивчення, включаючи баланс між безпекою, ефективністю та економічною доцільністю. Пошук оптимальних методів аутентифікації в умовах обмежених ресурсів залишається важливим завданням, яке має як наукове, так і практичне значення.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Вбудовані системи з обмеженими ресурсами відіграють ключову роль у сучасних технологіях, забезпечуючи функціонування різноманітних пристроїв, таких як сенсори, медичні імплантати, промислові контролери та IoT-пристрої [9]. Оскільки ці системи часто інтегруються в критично важливі сфери, де безпека та надійність є пріоритетними, необхідно ретельно враховувати їх специфічні характеристики. Вони мають обмежені ресурси, які суттєво впливають на їх можливості виконання складних завдань, зокрема аутентифікації [10]. Важливість цих параметрів полягає не лише в забезпеченні базової функціональності системи, але й у забезпеченні її захищеності від потенційних загроз.

Основними ресурсами, що впливають на їх продуктивність, є:

1. Процесорна потужність. Вбудовані системи зазвичай оснащені простими мікроконтролерами, які мають обмежені тактові частоти (зазвичай від 8 до 32 МГц) і малу кількість ядер. Це обмежує обчислювальні можливості для виконання складних алгоритмів аутентифікації.
2. Пам'ять. Вбудовані системи часто мають обмежений обсяг оперативної пам'яті (від кількох кілобайт до кількох мегабайт) і постійної пам'яті (Flash). Це означає, що вони можуть зберігати лише обмежену кількість даних, що ускладнює використання складних структур даних і великих ключів шифрування.
3. Енергоспоживання. Багато вбудованих систем працюють від батарей або мають обмежене живлення, що вимагає оптимізації алгоритмів аутентифікації для мінімізації споживання енергії. Високе енергоспоживання може суттєво скоротити термін служби пристрою.

Обмежені ресурси вбудованих систем суттєво впливають на вибір методів аутентифікації, оскільки недостатня процесорна потужність, обмежена пам'ять і високі вимоги до енергоспоживання змушують розробників шукати оптимальні рішення [11].

В умовах низької обчислювальної потужності, що характерна для вбудованих систем, прості методи аутентифікації, такі як паролі або PIN-коди, залишаються найбільш поширеними. Ці методи не вимагають значних обчислень та витрат пам'яті, але їх використання підвищує ризик несанкціонованого доступу, адже паролі можуть бути вгадані або викрадені.

Полегшені криптографічні алгоритми стають важливими для підвищення рівня безпеки вбудованих систем [12]. Ці алгоритми спеціально розроблені для роботи в умовах обмежених ресурсів, що дозволяє забезпечити належний рівень захисту без великих витрат на обчислення та пам'ять. Наприклад, алгоритми на зразок PRESENT або SPECK демонструють високу ефективність у використанні пам'яті та енергоспоживанні, що робить їх оптимальними рішеннями для застосування у вбудованих системах [13]. У табл. 1 наведено порівняння відомих полегшених криптографічних алгоритмів, які використовуються в умовах обмежених ресурсів. Всі представлені шифри є симетричними. SPECK та SIMON забезпечують високий рівень безпеки, тоді як PRESENT, HIGHT і KATAN мають середній рівень безпеки.

Хоча багатофакторна аутентифікація (MFA) здатна забезпечити високий рівень безпеки, її реалізація в умовах обмежених ресурсів є складним завданням. Поєднання кількох методів аутентифікації потребує додаткових ресурсів, що може негативно вплинути на продуктивність системи. Проте адаптація полегшених методів у рамках MFA може допомогти знайти баланс між безпекою та ефективністю [14].

Таблиця 1

Порівняння полегшених шифрів

Алгоритм	Використання пам'яті (КБ)	Швидкість (операцій/с)
PRESENT	8-16	1.0-1.5
SPECK	4-8	1.2-1.8
SIMON	4-16	0.8-1.5
HIGHT	8-16	1.0-2.0
KATAN	4-16	1.0-2.0

Не менш важливим є енергоспоживання. При виборі методів аутентифікації потрібно враховувати, що методи з тривалими обчисленнями можуть призвести до швидкого розряджання батареї. Наприклад, біометрична аутентифікація, хоча і є дуже безпечною, може вимагати значних енергетичних витрат для обробки даних. Тому вибір алгоритмів, оптимізованих для енергозбереження, стає критично важливим для тривалої роботи вбудованих систем.

Оптимізація алгоритмів під специфічні характеристики вбудованих систем також може суттєво підвищити ефективність аутентифікації. Використання команд, специфічних для архітектури системи, або налаштування параметрів алгоритму може зменшити вимоги до ресурсів і поліпшити швидкість виконання.

Вбудовані системи з обмеженими ресурсами використовують різноманітні методи аутентифікації, адаптовані до специфічних умов і вимог. Одним із найпоширеніших підходів є аутентифікація на основі паролів. Хоча цей метод простий у реалізації, він має суттєві недоліки, зокрема вразливість до атак на основі підбору паролів. Для підвищення безпеки часто використовуються кодові запити, які генерують одноразові коди, що додають додатковий рівень захисту, хоча й вимагають більше ресурсів для генерації та перевірки.

Аутентифікація за допомогою токенів, як апаратних, так і програмних, також використовується у вбудованих системах [15]. Апаратні токени можуть генерувати одноразові паролі, що значно підвищує рівень безпеки [16]. Програмні токени, які реалізуються в мобільних додатках або програмному забезпеченні, пропонують зручність використання, проте можуть бути менш безпечними, якщо пристрій зламаний або під загрозою.

MFA стає все більш популярною, поєднуючи кілька методів, таких як паролі, токени та біометричні дані. Хоча MFA забезпечує вищий рівень захисту, її реалізація у вбудованих системах може бути ускладнена через обмежені ресурси, що викликає необхідність у ретельному підборі методів.

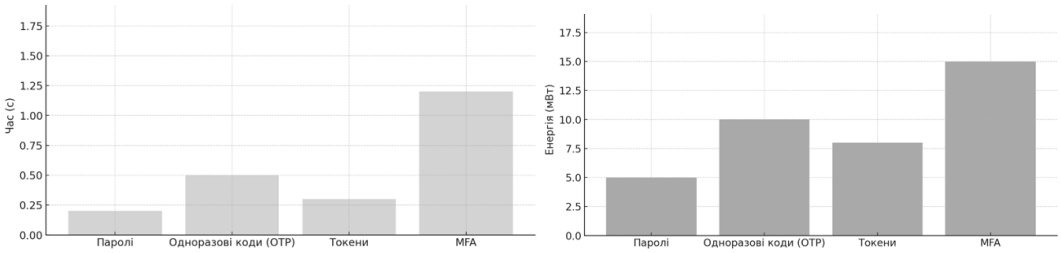
Оцінка ефективності методів аутентифікації є критично важливим етапом у розробці безпечних вбудованих систем. Для цього використовувалися кілька параметрів оцінки, зокрема безпека, швидкість та споживання ресурсів. Безпека визначає здатність методу захищати дані від несанкціонованого доступу і атак. Швидкість відображає, як швидко система може аутентифікувати користувача або пристрій, що є особливо важливим у реальному часі. Споживання ресурсів, зокрема процесорної потужності та енергоспоживання, має вирішальне значення для вбудованих систем, де ресурси часто обмежені.

У тестуванні оцінки ефективності методів аутентифікації проводилися експерименти, які допомагали виявити сильні та слабкі сторони різних підходів. Для цього використовувалися симульовані вбудовані системи в середовищі MATLAB/Simulink. Модель вбудованої системи була створена у Simulink, де були реалізовані різні методи аутентифікації, такі як паролі, одноразові коди, токени та багатофакторна аутентифікація. Це дозволяло імітувати різні сценарії доступу до системи та перевірку аутентифікації в контрольованих умовах.

Для збору даних про час виконання аутентифікації та споживання ресурсів використовувався блок Data Acquisition (DAQ), який забезпечував отримання вимірювань у режимі реального часу. Це допомагало відстежувати, скільки часу займає кожен метод аутентифікації, а також обчислювати енергоспоживання. Швидкість аутентифікації вимірювалася за допомогою функцій tic і toc, що дозволило отримати точний час виконання для кожного методу.

Споживання енергії розраховувалося шляхом моніторингу енергоспоживання мікроконтролера під час виконання кожного методу. Віртуальні блоки моделювали різні сценарії навантаження, що дало змогу визначити, як кожен метод впливає на загальне споживання енергії. Для тестування використовувалися кілька сценаріїв, зокрема перевірка на успішну аутентифікацію з правильними даними, на неуспішну аутентифікацію з неправильними даними, а також тестування з високим навантаженням, щоб оцінити, як методи справляються з одночасними запитами.

Після завершення тестування дані про час виконання та споживання ресурсів оброблялися за допомогою функцій MATLAB, що дозволило побудувати графіки та порівняння різних методів аутентифікації за основними параметрами, рис. 2 – 4.



а) **б)**

Рис. 2. Порівняння методів аутентифікації
а) – час виконання аутентифікації; б) – споживання енергії

З графіка на рис. 2 (а) видно, що різні методи аутентифікації виконуються за різний час. Паролі демонструють найшвидший час виконання, тоді як багатофакторна аутентифікація (MFA) потребує найбільше часу. На рис. 2 (б) представлено споживання енергії різними методами аутентифікації в мВт. Це дозволяє оцінити їх ефективність у вбудованих системах.

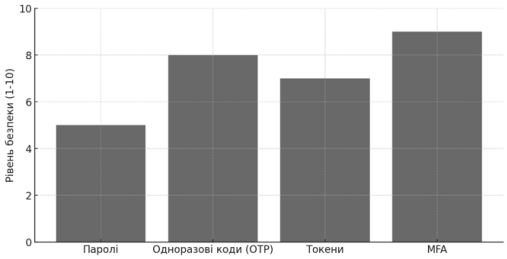


Рис. 3. Порівняння методів аутентифікації за рівенем безпеки

На рис. 3 представлено рівень безпеки (в шкалі від 1 до 10) для кожного методу аутентифікації, що відображає їх вразливість до несанкціонованого доступу.

Результати тестування показали, що метод аутентифікації з паролями мав найшвидший час виконання, в середньому близько 0,2 секунди. Однак рівень безпеки цього методу був нижчим, оскільки паролі можуть бути вразливими до атак на основі підбору.

Одноразові коди забезпечували вищий рівень захисту, але їх реалізація вимагала більшого часу на генерацію та перевірку – в середньому 0,5 секунди. Аутентифікація на основі токенів показала помірну швидкість з середнім часом виконання 0,3 секунди, пропонуючи високий рівень безпеки завдяки використанню фізичного носія. Багатофакторна аутентифікація, яка об'єднує кілька методів, забезпечила найвищий рівень безпеки, але показала найгірші результати в термінах швидкості з середнім часом виконання 1,2 секунди.

Споживання ресурсів також варіювалося в залежності від методу. Аутентифікація за допомогою паролів вимагала найменшого енергоспоживання, близько 5 мВт, тоді як методи, що включали біометричні дані та багатофакторну аутентифікацію, мали вищі показники споживання енергії через складні алгоритми обробки.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Вибір методу аутентифікації повинен бути обґрунтованим, виходячи з конкретних вимог системи. Оптимальним рішенням для вбудованих систем з обмеженими ресурсами може бути комбінація легковагих методів, таких як паролі та одноразові коди, що забезпечить достатній рівень безпеки при мінімальних витратах на швидкість і ресурси. Це підкреслює важливість оцінки ефективності аутентифікаційних методів у контексті реальних застосувань вбудованих систем.

Подальші напрямки дослідження в цій сфері можуть включати розвиток методів аутентифікації на основі блокчейну. Використання технології блокчейн для аутентифікації забезпечує високий рівень безпеки завдяки децентралізованій природі даних і незмінності записів. Цей підхід може значно знизити ризик несанкціонованого доступу, оскільки зловмиснику буде важче підробити або змінити аутентифікаційні дані. Дослідження можуть зосередитися на інтеграції блокчейн-технологій з існуючими методами аутентифікації, аналізуючи їхню ефективність та споживання ресурсів у вбудованих системах. Крім того, варто звернути увагу на адаптивні методи аутентифікації, які змінюють свою структуру в залежності від контексту та рівня загрози. Це може включати динамічний вибір методів аутентифікації на основі виявлених ризиків, що дозволить ще більше підвищити безпеку. У зв'язку з цим, проведення подальших досліджень у цій галузі може відкрити нові можливості для розвитку безпечних і ефективних вбудованих систем у майбутньому.

Література

1. Розломій І.О., Симонюк В.П., Науменко С.В., Михайловський П.В. Адаптивна криптографія для енергоефективного захисту пристроїв IoT (2024) «Проблеми моделювання та автоматизації проектування», №1(19), 2024, С. 77-83. DOI: 10.31474/2074-7888-2024-1-19-77-83.
2. Melki, R., Noura, H. N., & Chehab, A. (2020). Lightweight multi-factor mutual authentication protocol for IoT devices. International Journal of Information Security, 19(6), 679-694.
3. Rozlomii I.O., Kosenyuk G.V., Naumenko S.V., Mykhaylovskyi P.V. (2023) Modeling a Microcontroller-Based Sensor System in a Smart Home Game Simulation Using Encryption. Computer-Integrated technologies: education, science, production. (53), 292-299. https://doi.org/10.36910/6775-2524-0560-2023-53-43
4. Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. Future generation computer systems, 91, 244-251.
5. Ebrahimi, S., & Bayat-Sarmadi, S. (2021). Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT. IEEE Internet of Things Journal, 8(13), 10706-10713.
6. Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K. & Khan, N. A. (2022). Lightweight multifactor authentication scheme for nextgen cellular networks. IEEE access, 10, 31273-31288.
7. Lara, E., Aguilar, L., Sanchez, M. A., & García, J. A. (2020). Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. Sensors, 20(2), 501.
8. Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. Future Internet, 14(12), 363.
9. Marwedel, P. (2021). Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things (p. 433). Springer Nature.
10. Pereira, F., Correia, R., Pinho, P., Lopes, S. I., & Carvalho, N. B. (2020). Challenges in resource-constrained IoT devices: Energy and communication as critical success factors for future IoT deployment. Sensors, 20(22), 6420.
11. Розломій І.О., Симонюк В.П., Науменко С.В., Михайловський П.В. (2024). Модель безпеки взаємопов'язаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT. Комп'ютерно-інтегровані технології: освіта, наука, виробництво, (55), 191-198.
12. Naumenko, S., Rozlomii, I., & Yarmilko, A. (2024, September). The Built on Feistel Network Architecture Block Ciphers Modification. In 2024 14th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 560-564). IEEE. 10.1109/ACIT62333.2024.10712597
13. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2024, May). The Role of Encryption in Information Protection for Cloud Computing. In 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST) (pp. 70-75). IEEE.
14. Singh, Y., & Singh, A. (2022, October). Lightweight cryptography approach for multifactor authentication in internet of things. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon) (pp. 1-7). IEEE.
15. Michailidis, E. T., & Vouyioukas, D. (2022). A review on software-based and hardware-based authentication mechanisms for the internet of drones. Drones, 6(2), 41.
16. Li, S., Xu, C., Zhang, Y., & Zhou, J. (2022). A secure two-factor authentication scheme from password-protected hardware tokens. IEEE Transactions on Information Forensics and Security, 17, 3525-3538.

References

1. Rozlomii I.O., Simonyuk V.P., Naumenko S.V., Mykhaylovskyi P.V. Adaptive Cryptography for Energy-Efficient Security of IoT Devices (2024) "Issues in Modeling and Design Automation", №1(19), 2024, С. 77-83. DOI: 10.31474/2074-7888-2024-1-19-77-83.
2. Melki, R., Noura, H. N., & Chehab, A. (2020). Lightweight multi-factor mutual authentication protocol for IoT devices. International Journal of Information Security, 19(6), 679-694.
3. Rozlomii I.O., Kosenyuk G.V., Naumenko S.V., Mykhaylovskyi P.V. (2023) Modeling a Microcontroller-Based Sensor System in a Smart Home Game Simulation Using Encryption. Computer-Integrated technologies: education, science, production. (53), 292-299. https://doi.org/10.36910/6775-2524-0560-2023-53-43
4. Zhou, L., Li, X., Yeh, K. H., Su, C., & Chiu, W. (2019). Lightweight IoT-based authentication scheme in cloud computing circumstance. Future generation computer systems, 91, 244-251.
5. Ebrahimi, S., & Bayat-Sarmadi, S. (2021). Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT. IEEE Internet of Things Journal, 8(13), 10706-10713.
6. Khan, A. S., Javed, Y., Saqib, R. M., Ahmad, Z., Abdullah, J., Zen, K. & Khan, N. A. (2022). Lightweight multifactor authentication scheme for nextgen cellular networks. IEEE access, 10, 31273-31288.
7. Lara, E., Aguilar, L., Sanchez, M. A., & García, J. A. (2020). Lightweight authentication protocol for M2M communications of resource-constrained devices in industrial Internet of Things. Sensors, 20(2), 501.
8. Schizas, N., Karras, A., Karras, C., & Sioutas, S. (2022). TinyML for ultra-low power AI and large scale IoT deployments: A systematic review. Future Internet, 14(12), 363.
9. Marwedel, P. (2021). Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things (p. 433). Springer Nature.
10. Pereira, F., Correia, R., Pinho, P., Lopes, S. I., & Carvalho, N. B. (2020). Challenges in resource-constrained IoT devices: Energy and communication as critical success factors for future IoT deployment. Sensors, 20(22), 6420.

ISSN 2219-9365

11. Rozlomii, I., Symonyuk, V., Naumenko, S., & Mykhailovskyi, P. (2024). A security model of interconnected computing devices based on a lightweight encryption scheme for IoT. Computer-Integrated technologies: education, science, production, (55), 191-198.
12. Naumenko, S., Rozlomii, I., & Yarmilko, A. (2024, September). The Built on Feistel Network Architecture Block Ciphers Modification. In 2024 14th International Conference on Advanced Computer Information Technologies (ACIT) (pp. 560-564). IEEE. 10.1109/ACIT62333.2024.10712597
13. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2024, May). The Role of Encryption in Information Protection for Cloud Computing. In 2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST) (pp. 70-75). IEEE.
14. Singh, Y., & Singh, A. (2022, October). Lightweight cryptography approach for multifactor authentication in internet of things. In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon) (pp. 1-7). IEEE.
15. Michailidis, E. T., & Vouyioukas, D. (2022). A review on software-based and hardware-based authentication mechanisms for the internet of drones. Drones, 6(2), 41.
16. Li, S., Xu, C., Zhang, Y., & Zhou, J. (2022). A secure two-factor authentication scheme from password-protected hardware tokens. IEEE Transactions on Information Forensics and Security, 17, 3525-3538.