НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

$$H = L \cdot log_2(N) \quad (1)$$

де L – довжина пароля,

N – кількість можливих символів у вибраному наборі.

На основі значення H пароль класифікують за рівнями стійкості:

– до 28 біт дуже слабкий;
– 28–36 біт слабкий;
– 36–60 біт середній;
– понад 60 біт сильний.

Результат оцінки відображатиметься користувачеві у графічній формі, наприклад, у вигляді смайлика або кольорового індикатора надійності.

Висновки. У результаті виконання роботи розроблено концепцію та прототип локального застосунку для генерування та оцінки надійності паролів на мобільних пристроях. Система працює автономно, без підключення до інтернету. Застосунок може бути інструментом навчання користувачів та частиною комплексних систем захисту інформації. Подальший розвиток проєкту – інтеграція модулів перевірки паролів за локальними словниками витоків, додавання рекомендацій із кібергігієни та впровадження адаптивних алгоритмів оцінювання на основі штучного інтелекту.

Список використаної літератури:

1. Alsharaya H. Password managers: a critical review of security, usability, and innovative designs. Journal of Computer Sciences Institute,2025, Т.36, №9, с. 28-35.
2. Oesch S., Ruoti S. Evaluating Password Managers Against Real-World Phishing Pages. IJCT Journal, 2025.

Ключові слова: пароль, застосунок, надійність, мобільний пристрій.
Keywords: password, application, reliability, mobile device

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНТЕЛЕКТУАЛЬНИХ ЖИТЛОВИХ СИСТЕМАХ

Неділенко Валерій

аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»

Вступ

Сучасні технології Інтернету речей (IoT) розвиваються з надзвичайною швидкістю, що створює нові виклики у сфері безпеки інформаційних систем. Одним із актуальних напрямів є захист розумних пристроїв та систем IoT, які активно інтегруються у побутові, промислові та енергетичні рішення. Пристрої IoT можуть містити різні бінарні дані, пов’язані з безпекою, для того щоб уможливити використання відповідних протоколів, наприклад, сертифікати

для безпечного зв'язку з віддаленими серверами (mqtt, http тощо). Зловмиснику, який має фізичний доступ до пристрою, дуже легко отримати бінарні образи зі сховища пристрою та шукати такі фрагменти тексту. Можливий витік сертифіката безпеки може призвести до ескалації атак на інші частини інфраструктури, особливо якщо відповідні дозволи є неправильними або досить послабленими.

Огляд літературних джерел

Серед сучасних підходів до забезпечення кібербезпеки IoT виділяють використання сертифікатів, криптографічних протоколів, механізмів автентифікації та постійного моніторингу. Зокрема, OWASP щорічно оновлює перелік найбільш критичних вразливостей для IoT-пристроїв [1]. Дослідники також розглядають постквантові методи шифрування [2], системи легковагової автентифікації для промислових застосувань [3] та технології керування сертифікатами для промислових мереж [4]. Автори [5] відзначають, що стандартні криптографічні методи не забезпечують повного захисту даних під час бездротової передачі в IoT. Перспективним підходом є обфускація сигналів - контрольоване спотворення даних, яке ускладнює їх перехоплення сторонніми особами. Ще одна цікава ідея представлена в роботі [6], де пропонується метод симуляції ідентифікаторів для пристроїв IoT. Завдяки цьому підходу можна визначати, до якої групи належить той чи інший об'єкт, і водночас ідентифікувати кожен пристрій у межах цієї групи.

Отже, хоча окремі методи, такі як криптографія, автентифікація чи обфускація, відіграють важливу роль у захисті конкретних ланок IoT-системи (наприклад, пристроїв, мереж чи даних), їх ефективність обмежена без комплексного підходу. Необхідно впроваджувати інтегровані стратегії, що охоплюють весь життєвий цикл системи - від апаратного рівня до хмарних сервісів, включаючи постійний моніторинг, оновлення вразливостей та комбінацію кількох технологій. Такий всебічний захист мінімізує ризики ланцюгових атак і забезпечує стійкість IoT-екосистеми в цілому, особливо в умовах зростання складності та взаємозв'язків сучасних мереж.

Цілі дослідження

Основною метою дослідження є розробка ефективного та надійного механізму захисту, що забезпечить безпеку зберігання та передачі даних від пристрою до хмарного сервісу AWS IoT Core.

Особлива увага приділена використанню сучасних методів шифрування та захисту від зламу для забезпечення конфіденційності, цілісності та доступності інформації. Щоб уникнути витоків, потрібно шифрувати пам'ять пристрою, щоб жодна конфіденційна інформація з образу мікропрограми або з іншого місця не могла бути прочитаної навіть за наявності фізичного доступу до пристрою.

Дослідження включає в себе не лише розробку апаратно-програмного комплексу, але й вивчення та аналіз відповідних аспектів кібербезпеки, зокрема у сфері захисту IoT-пристроїв від потенційних загроз та атак. Подальше вдосконалення та розширення можливостей захисту та взаємодії з AWS IoT Core є ключовими аспектами цього дослідження.

Методи та засоби

Для побудови безпечної системи IoT використано мікроконтролер ESP32 з операційною системою реального часу FreeRTOS. Застосовано шифрування енергонезалежної пам'яті (NVS), автентифікацію пристрою через сертифікати X.509 та взаємодію з AWS IoT Core за протоколом MQTT через захищене з'єднання TLS. Для оновлення програмного забезпечення реалізовано механізм OTA (Over-the-Air), що дозволяє дистанційно надсилати оновлення з перевіркою цілісності коду за допомогою цифрового підпису.

Результати дослідження

На рис.1 представлені методи захисту від кібератак, що реалізовані у роботі і які є відповідями на виклики TOP-10 OWASP IoT Vulnerabilities. Розроблена система інтегрується з хмарною платформою AWS IoT Core та забезпечує захищений обмін даними між пристроєм і сервером. Застосування апаратного шифрування пам'яті ESP32 унеможливлює отримання критичних даних навіть при фізичному доступі до пристрою.

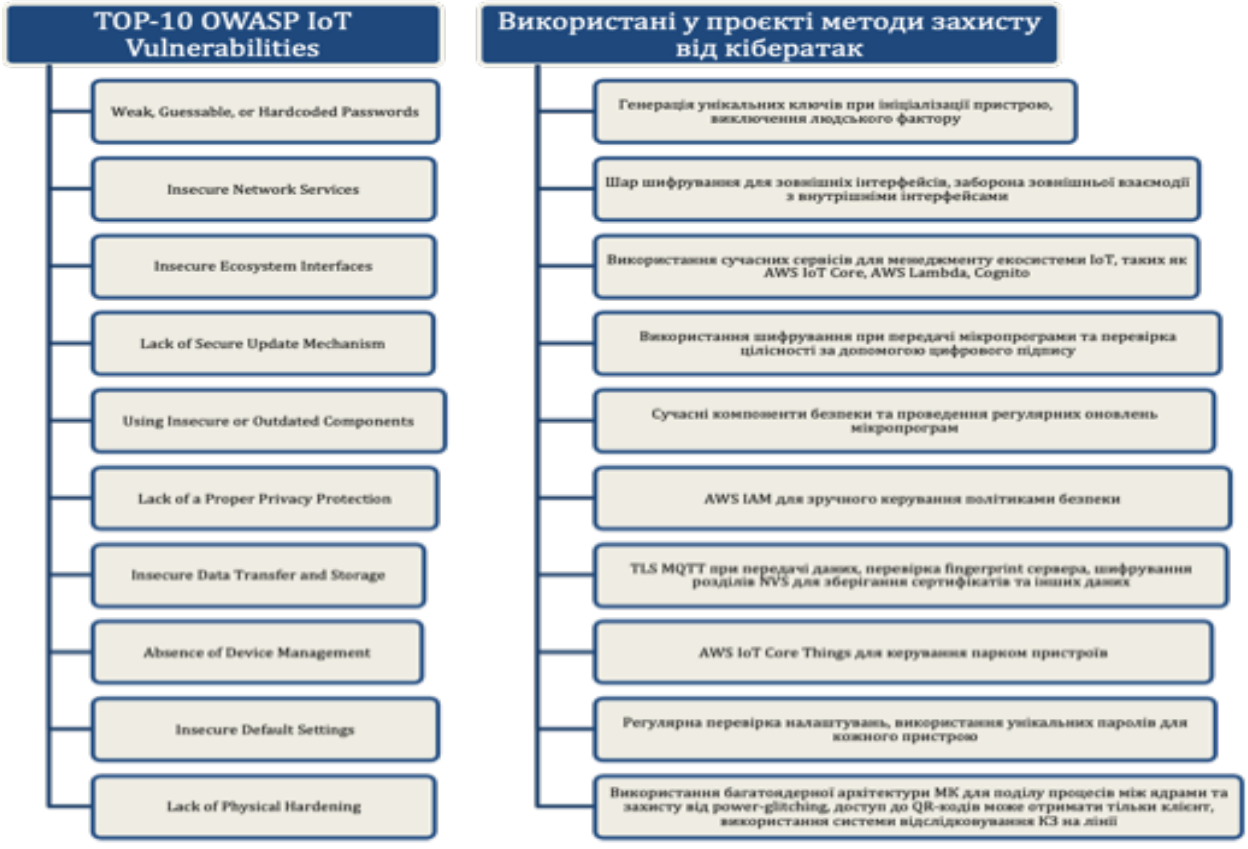

Рис.1. Відповідність між загрозами та реалізованими методами їх усунення

Для забезпечення належного рівня захисту IoT-системи від потенційних загроз було використано наступні ключові сучасні технології:

1. AWS IoT Core (хмарний шлюз для IoT пристроїв).

2. AWS IoT Core Shadow (створення постійної віртуальної версії кожного пристрою).

3. AWS Cognito (реєстрація та аутентифікація користувачів у мобільних та інтернет-додатках).

4. Центр ідентифікації AWS IAM Identity Center (сувора автентифікація на основі стандартів для всіх користувачів).

5. Amazon S3 Bucket (сервіс сховища).

6. Сервіс AWS Lambda (інструмент для керування кінцевими точками).

7. Сервіс AWS IoT Remote Jobs (завдання для набору пристроїв - завантаження та встановлення програм, запуск оновлень мікропрограм, зміна сертифікатів, операції дистанційного усунення несправностей).

8. AWS Signer (можливість підписання коду).

9. Операційна система реального часу FreeRTOS з відкритим кодом для мікроконтролерів.

10. Over-the-Air (оновлення мікропрограм).

Система дозволяє виконувати оновлення прошивки та керування пристроєм через мобільний додаток з обов'язковою автентифікацією користувача. Проведене тестування підтвердило стабільну роботу системи в умовах промислової експлуатації.

Висновки

У результаті виконання проєкту вдалося досягти важливих результатів у сфері захисту IoT-пристроїв. Розроблена система забезпечує високий рівень безпеки в зберіганні та передачі даних. Описана архітектура системи, взаємодія між AWS та ESP-IDF, а також методи шифрування та захисту від зламу для забезпечення безпеки зберігання та передачі даних. Детально проаналізовані технічні аспекти проектування, його інноваційні характеристики та взаємовідносини з вибраними технологічними рішеннями AWS та ESP-IDF. Перспективами подальших досліджень є розширення системи на інші галузі, зокрема медичну та критичну інфраструктуру.

Список використаних джерел:

[1] OWASP IoT Top 10 Vulnerabilities (2024 Updated). URL: https://www.wattle-corp.com/owasp-iot-top-10/.

[2] Zhang Y., Duan P., Li C., Ahmad H. Preserving Privacy of Internet of Things Network with Certificateless Ring Signature Sensors. Sensors (2025). doi:10.3390/s25051321.

[3] Al Ghazo A., Abu Mallouh M., Alajlouni S., Almalkawi I. Securing Cyber Physical Systems: Lightweight Industrial Internet of Things Authentication (LI2A). Appl. Syst. Innov. (2025). doi:10.3390/asi8010011.

[4] Göppert J., Walz A., Sikora A. A Survey on Life-Cycle-Oriented Certificate Management in Industrial Networking Environments. J. Sens. Actuator Netw. (2024). doi:10.3390/jsan13020026.
[5] Renato Lo Cigno, Francesco Gringoli, Stefania Bartoletti, Marco Cominelli, Lorenzo Ghiro, and Samuele Zanini. Communication and Sensing: Wireless PHY-Layer Threats to Security and Privacy for IoT Systems and Possible Countermeasures. Information 2025, 16(1), 31; https://doi.org/10.3390/info16010031.
[6] Volodymyr Maksymovych, Elena Nyemkova, Connie Justice, Mariia Shabatura, Oleh Harasymchuk, Yuriy Lakh and Morika Rusynko. Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators. Electronics 2022, 11(13), 2039; https://doi.org/10.3390/electronics11132039.

Ключові слова: безпека даних; AWS IoT Core; методи шифрування; кіберзахист IoT-пристроїв; апаратно-програмні рішення; ESP32; FreeRTOS.
Keywords: data security; AWS IoT Core; encryption methods; cybersecurity of IoT devices; hardware and software solutions; ESP32; FreeRTOS.

МЕТОД ФАКТОРИЗАЦІЇ ВЕЛИКИХ ЧИСЕЛ

Тимошенко Лідія
кандидат економічних наук, доцент кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»
Алєксєєва Софія
магістрант кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Забезпечення інформаційної безпеки є одним із ключових напрямів сучасної кібербезпеки. Особливе місце посідають асиметричні криптографічні системи, як RSA, надійність яких ґрунтується на складності задачі факторизації великих чисел. Проте з розвитком обчислювальної техніки та появою квантових технологій необхідне вдосконалення існуючих методів. Одним із перспективних підходів є модифікація методу Ферма, який є ефективним для близьких за значенням множників[1]. Його удосконалення може забезпечити підвищення ефективності криптоаналізу сучасних систем шифрування.

Метою дослідження є зменшення обчислювальної складності алгоритму факторизації великих чисел шляхом удосконалення класичного методу Ферма для оцінки криптостійкості RSA-подібних систем.

Факторизація великих чисел є однією з основних математичних задач, що забезпечує безпеку криптографічних систем з відкритим ключем [2]. Метод Ферма базується на представленні непарного числа як різниці двох квадратів $N = x^2 - y^2 = (x - y)(x + y)$. Складність даного методу

ЗМІСТ