DOI: https://doi.org/10.36910/6775-2524-0560-2024-57-16
УДК 004.056
Розломій Інна Олександрівна[1], к.т.н., доцент
https://orcid.org/0000-0001-5065-9004
Науменко Сергій Васильович[2], аспірант
https://orcid.org/0000-0002-6337-1605
[1]Черкаський державний технологічний університет, м. Черкаси, Україна
[2]Черкаський національний університет імені Богдана Хмельницького, м. Черкаси, Україна

МОДЕЛЮВАННЯ ВЗАЄМОВПЛИВУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ОБЧИСЛЮВАЛЬНИХ ВИТРАТ У ВБУДОВАНИХ ПРИСТРОЯХ

Розломій І.О., Науменко С.В. Моделювання взаємовпливу інформаційної безпеки та обчислювальних витрат у вбудованих пристроях. У статті запропоновано математичну модель, яка описує взаємовплив інформаційної безпеки та обчислювальних витрат у вбудованих пристроях. Вбудовані системи, такі як IoT-пристрої, медичні прилади та промислові контролери, працюють в умовах обмежених обчислювальних ресурсів, що створює значні виклики для забезпечення належного рівня інформаційної безпеки без перевантаження системи. Запропонована модель враховує ключові параметри, включаючи енергоспоживання, час обробки, обсяг пам'яті та рівень криптографічного захисту, що дозволяє дослідити баланс між безпекою та ресурсоємністю. Проведено аналіз ефективності полегшених – PRESENT, SPECK, SIMON та стандартних криптографічних алгоритмів – Blowfish, AES. Результати симуляцій, виконаних у середовищах MATLAB та Python із використанням бібліотек для тестування криптографії, демонструють, що полегшені алгоритми забезпечують значно нижчі показники енергоспоживання та часу обробки. Це робить їх оптимальним вибором для пристроїв з обмеженими ресурсами. Зокрема, алгоритми SPECK і PRESENT показали найкращі результати щодо енергоспоживання та швидкодії, тоді як AES, хоча і забезпечує високий рівень безпеки, є більш ресурсоємним. Практична значимість розробленої моделі полягає у її застосуванні для вибору оптимальних криптографічних рішень під час проектування енергоефективних вбудованих систем. Модель може бути інтегрована в процеси проектування для оптимізації безпеки та продуктивності пристроїв, що особливо важливо для IoT-архітектур, де критичним є збереження енергії та забезпечення безпеки даних.
Ключові слова: вбудовані пристрої, інформаційна безпека, обчислювальні витрати, енергоспоживання, час обробки, полегшені криптографічні алгоритми, моделювання, ресурсоємність.

Rozlomii I., Naumenko S. Modeling the interplay of information security and computing costs in embedded devices. The article proposes a mathematical model that describes the interplay of information security and computing costs in embedded devices. Embedded systems, such as IoT devices, medical devices, and industrial controllers, operate under limited computing resources, which poses significant challenges to ensuring an adequate level of information security without overloading the system. The proposed model takes into account key parameters, including power consumption, processing time, memory size, and cryptographic protection level, which allows exploring the balance between security and resource consumption. The effectiveness of lightweight – PRESENT, SPECK, SIMON and standard cryptographic algorithms – Blowfish, AES were analyzed. The results of simulations performed in MATLAB and Python environments using libraries for cryptography testing demonstrate that lightweight algorithms provide significantly lower power consumption and processing time. This makes them an optimal choice for devices with limited resources. In particular, the SPECK and PRESENT algorithms showed the best results in terms of power consumption and speed, while AES, although providing a high level of security, is more resource-intensive. The practical significance of the developed model lies in its application for selecting optimal cryptographic solutions when designing energy-efficient embedded systems. The model can be integrated into design processes to optimize the security and performance of devices, which is especially important for IoT architectures, where energy conservation and data security are critical.
Key words: embedded devices, information security, computational costs, power consumption, processing time, lightweight cryptographic algorithms, modeling, resource intensity.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. Сучасні вбудовані пристрої відіграють ключову роль у різних сферах, включаючи промислові системи, медичні прилади, розумні будинки та транспортні засоби. Зростаюча кількість пристроїв, підключених до Інтернету, створює нові можливості, але також посилює загрози безпеці, оскільки вбудовані системи часто мають обмежені ресурси, такі як потужність процесора, обсяг пам'яті та енергоспоживання [1]. В таких умовах забезпечення інформаційної безпеки стає складним завданням, оскільки традиційні криптографічні алгоритми можуть виявитися занадто ресурсоємними для цих пристроїв [2]. Це спонукає до використання полегшених криптографічних методів, однак їх впровадження повинно забезпечити необхідний рівень захисту при мінімальних обчислювальних витратах [3].

Актуальність теми полягає в необхідності знаходження балансу між безпекою даних та ефективним використанням обмежених обчислювальних ресурсів вбудованих пристроїв. Недостатній рівень безпеки може призвести до порушення конфіденційності, цілісності або

доступності даних, що є критичним для таких сфер, як медицина або транспорт. З іншого боку, надмірне споживання ресурсів знижує продуктивність і автономність пристроїв, що може обмежити їх практичне використання. Таким чином, дослідження взаємодії між інформаційною безпекою та обчислювальними витратами є важливим для розробки ефективних і безпечних рішень для вбудованих систем [4].

Аналіз останніх досліджень та публікацій. Сфера В останні роки тема забезпечення інформаційної безпеки в умовах обмежених обчислювальних ресурсів привернула значну увагу дослідників, що пов'язано з швидким зростанням Інтернету речей (IoT), розумних пристроїв та кіберфізичних систем [5]. В умовах ресурсних обмежень вбудовані пристрої потребують спеціалізованих рішень для захисту даних, що не перевантажують системи та забезпечують достатній рівень безпеки. Однією з ключових проблем є оптимізація криптографічних алгоритмів для зменшення їх ресурсоємності. Більшість сучасних досліджень спрямовані на розробку та вдосконалення полегшених криптографічних алгоритмів, які є адаптованими для використання у вбудованих системах з обмеженими ресурсами. Зокрема, роботи, присвячені алгоритмам SIMON, SPECK, PRESENT і більш сучасним підходам, демонструють ефективність полегшених криптографічних методів. Вони здатні забезпечувати прийнятний рівень безпеки з меншими витратами на енергоспоживання і обчислювальні ресурси. Автори [6] порівняли ефективність кількох полегшених алгоритмів та виявили, що деякі з них значно знижують використання енергії, що є критично важливим для IoT пристроїв з автономним живленням.

Інші дослідження зосереджені на моделях для аналізу взаємодії між обчислювальними витратами та рівнем безпеки. Зокрема, в роботі [7] запропоновано математичні моделі, які дозволяють оцінювати вплив різних рівнів шифрування на продуктивність пристроїв, зокрема на час виконання операцій та споживання енергії. Такі моделі забезпечують можливість прогнозування наслідків використання певних методів захисту, що є важливим для балансування між вимогами до безпеки та наявними ресурсами пристроїв.

Також важливий внесок у дослідження робить аналіз параметрів продуктивності та енергоспоживання. У праці [8] проведено порівняльний аналіз криптографічних алгоритмів на вбудованих платформах з метою оцінки їх ресурсоємності, виявивши, що деякі з них мають значні переваги в енергозбереженні, але водночас можуть поступатися у рівні безпеки, що вимагає ретельного вибору алгоритмів залежно від конкретних потреб системи.

Крім того, велика увага приділяється інтеграції моделей безпеки у вбудовані системи. Робота [9] присвячена розгляду підходів до оптимізації використання полегшених криптографічних алгоритмів шляхом інтеграції захисних механізмів безпосередньо в апаратну частину пристрою, що дозволяє зменшити затрати ресурсів і підвищити загальну ефективність захисту.

Незважаючи на значний прогрес у розробці полегшених криптографічних рішень та моделей для оцінки їх впливу на ресурсоємність, дослідження взаємодії між інформаційною безпекою та обчислювальними витратами залишається актуальним напрямком. Існує потреба у створенні нових моделей, які дозволять більш точно прогнозувати взаємодію цих двох факторів, забезпечуючи оптимальний баланс між безпекою та продуктивністю вбудованих систем.

Мета. Мета дослідження полягає в розробці математичних моделей, які дозволяють оцінювати і прогнозувати взаємодію між інформаційною безпекою та обчислювальними витратами у вбудованих пристроях, з метою забезпечення оптимального балансу між безпекою даних і ресурсоємністю системи.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Вбудовані пристрої, такі як IoT-системи, медичні прилади та промислові контролери, функціонують в умовах обмежених обчислювальних ресурсів, що робить ресурсоємність центральним питанням їхнього проектування [10]. Ресурсоємність охоплює такі ключові аспекти, як обчислювальні потужності, енергоспоживання та обсяг пам'яті. Обчислювальні потужності вбудованих пристроїв обмежені через необхідність забезпечення автономної роботи та зниження енергоспоживання, що може негативно вплинути на можливості використання традиційних криптографічних алгоритмів [11]. Енергоспоживання є критично важливим, оскільки більшість пристроїв працюють від батарей або мають інші обмежені джерела живлення. Це вимагає мінімізації енергетичних витрат, особливо в контексті безпекових операцій [12]. Оперативна пам'ять та постійна пам'ять також обмежені, що накладає додаткові обмеження на зберігання криптографічних ключів або виконання складних алгоритмів шифрування.

Загрози інформаційній безпеці вбудованих систем включають фізичні атаки, які є особливо небезпечними, оскільки вбудовані пристрої часто доступні зловмисникам фізично. Це може дозволити здійснити атаки, спрямовані на зчитування пам'яті або аналіз енергоспоживання під час виконання криптографічних операцій [13]. Такі атаки дозволяють отримати доступ до шифрованих даних або криптографічних ключів, ставлячи під загрозу цілісність і конфіденційність інформації. У відповідь на ці загрози використовуються полегшені криптографічні алгоритми, які були розроблені для роботи в умовах обмежених ресурсів. Однак ці алгоритми можуть мати менший рівень захисту порівняно з традиційними алгоритмами, що може підвищувати ризики, пов'язані з безпекою [14].

Взаємодія між безпекою і обчислювальними витратами є складною проблемою, оскільки підвищення рівня безпеки часто вимагає значних обчислювальних ресурсів, що може негативно вплинути на продуктивність пристрою. Використання складних криптографічних алгоритмів підвищує обчислювальні витрати, що знижує загальну ефективність пристроїв. З іншого боку, спрощення алгоритмів для зниження обчислювальних витрат може зменшити рівень безпеки і зробити систему більш вразливою до атак. Тому пошук оптимального балансу між забезпеченням належного рівня безпеки та мінімізацією обчислювальних витрат є актуальним завданням для дослідників і розробників вбудованих систем.

В рамках дослідження взаємодії між інформаційною безпекою та обчислювальними витратами у вбудованих пристроях важливим етапом є побудова математичної моделі, яка дозволяє оцінити ефективність захисних заходів при мінімальних витратах ресурсів. Така модель повинна враховувати як обмеженість ресурсів (процесорна потужність, пам'ять, енергоспоживання), так і рівень криптографічного захисту, який вимагається для підтримання необхідного рівня безпеки даних.

Модель базується на основних змінних і параметрах, що впливають на обчислювальні витрати та безпеку вбудованих систем. Основними змінними моделі є параметри, що визначають ресурсоємність пристрою та рівень захисту інформації. До таких параметрів відносяться:

1) кільність пам'яті (M), необхідна для зберігання криптографічних ключів, шифрованих даних та інших параметрів безпеки. вимірюється в кілобайтах або мегабайтах;
2) потужність процесора (P), виражена у кількості обчислювальних операцій за одиницю часу (MIPS);
3) енергоспоживання пристрою (E), яке вимірюється в ватах або джоулях на операцію;
4) рівень криптографічного захисту (S), який можна визначати через кількість біт шифру або інші метрики стійкості до атак;
5) час виконання криптографічної операції (T), вимірюваний у секундах.

Модель, що описує взаємодію між обчислювальними витратами та рівнем безпеки, може виражається через співвідношення між обчислювальними параметрами та параметрами безпеки. Залежність часу виконання операції від рівня захисту і ресурсів, доступних пристрою представлена рівністю (1).

$$T = (S \cdot M)/P \quad (1)$$

Рівність (1) показує, що збільшення рівня захисту або обсягу використаної пам'яті призводить до збільшення часу обробки даних, що вказує на підвищення обчислювальних витрат.

Енергоспоживання також відіграє важливу роль у взаємодії між безпекою і продуктивністю. Залежність енергоспоживання від рівня безпеки та потужності процесора виражена моделлю (2).

$$E = f(S, P) = \alpha \cdot S + \beta \cdot P \quad (2)$$

де α і β – це коефіцієнти, що залежать від конкретної архітектури пристрою. Зокрема, ці коефіцієнти можуть відображати вплив рівня криптографічного захисту та потужності процесора на загальне енергоспоживання пристрою. Модель демонструє, що підвищення рівня захисту збільшує енергоспоживання пристрою, але його також можна знизити шляхом використання процесорів з нижчою потужністю.

Полегшені криптографічні алгоритми, такі як PRESENT, SIMON та SPECK, розроблені для забезпечення інформаційної безпеки у пристроях з обмеженими ресурсами, таких як вбудовані системи та IoT-пристрої. Ці алгоритми оптимізовані для мінімізації обчислювальних витрат, зокрема для зменшення використання пам'яті, потужності процесора та енергоспоживання, що дозволяє їх застосовувати у пристроях з обмеженою обчислювальною потужністю та автономним живленням.

Для перевірки ефективності запропонованої моделі взаємовпливу інформаційної безпеки та обчислювальних витрат у вбудованих пристроях розроблено метод оцінки, який враховує ключові метрики та дозволяє порівнювати модель із реальними умовами експлуатації. Основна мета методу – забезпечити обґрунтовану оцінку, яка дасть змогу підтвердити адекватність моделі та оптимізувати взаємодію між рівнем безпеки та витратами обчислювальних ресурсів.

На рис. 1 зображено структурну схему алгоритму оцінки ефективності моделі, яка відображає основні етапи процесу аналізу. Схема демонструє послідовність дій, починаючи з підготовки вхідних даних і проведення експериментів до аналізу результатів та формулювання рекомендацій. Такий підхід дозволяє структуровано організувати процес оцінки, забезпечуючи можливість інтегрування різних метрик та сценаріїв для перевірки моделі.

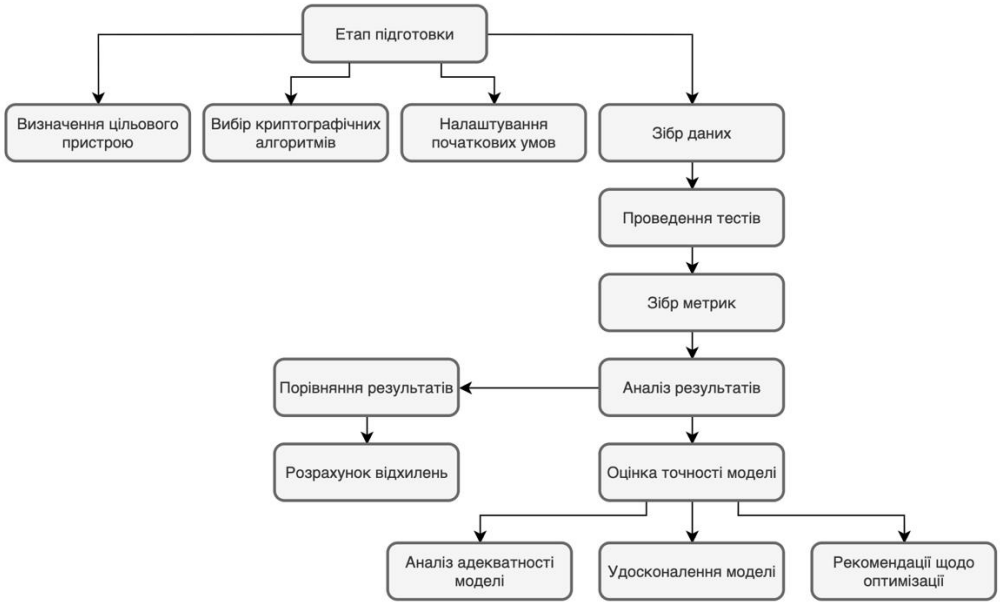

Рис. 1. Структурна схема алгоритму оцінки ефективності моделі

Алгоритм оцінки ефективності моделі включає кілька послідовних етапів. Спочатку визначається цільовий вбудований пристрій, на якому буде проводитися тестування моделі. Для цього обираються криптографічні алгоритми з різними рівнями безпеки, зокрема полегшені та стандартні методи. Встановлюються початкові умови експерименту, такі як тип процесора, обсяг пам'яті та джерело живлення.

На наступному етапі проводиться збір експериментальних даних. Для цього виконуються серії тестів із криптографічними операціями, які моделюють реальні сценарії використання пристрою. Під час тестів фіксуються дані про час виконання операцій, енергоспоживання, обсяг використаної пам'яті та рівень забезпеченої безпеки.

Зібрані результати аналізуються шляхом порівняння експериментальних показників із прогнозованими значеннями, розрахованими за допомогою моделі. Розраховуються відхилення між фактичними та модельними значеннями для кожного із параметрів, що дозволяє оцінити точність моделі.

Після цього проводиться оцінка адекватності моделі для різних сценаріїв роботи пристрою. У разі значних відхилень між експериментальними та модельними значеннями модель коригується. На фінальному етапі формулюються рекомендації щодо оптимального рівня криптографічного захисту, який дозволяє зберігати необхідний рівень безпеки при мінімальних витратах ресурсів.

Для підтвердження ефективності моделі було визначено набір ключових метрик, які дозволяють оцінити взаємовплив інформаційної безпеки та обчислювальних витрат. До основних метрик належать енергоспоживання, час обробки, рівень криптографічного захисту, обсяг використаної пам'яті та відхилення між прогнозованими і фактичними значеннями.

Енергоспоживання є критично важливою метрикою, оскільки для вбудованих пристроїв із обмеженим живленням необхідно забезпечити максимально тривалий час автономної роботи. На рис. 2 зображена діаграма, яка порівнює енергоспоживання для криптографічних алгоритмів PRESENT, SIMON, SPECK, Blowfish і AES.

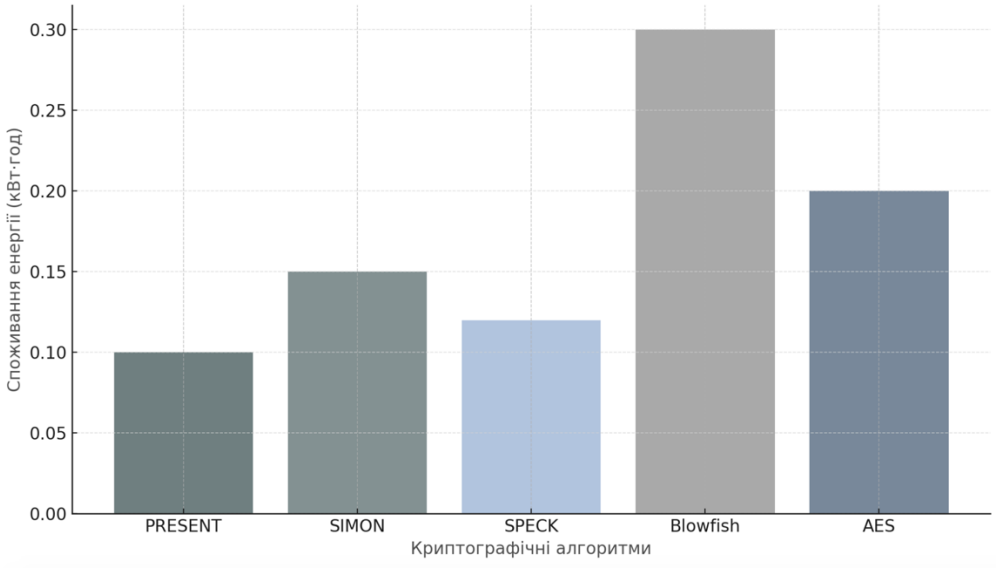

Рис. 2. Діаграма порівняння енергоспоживання

З діаграми видно, як різні алгоритми впливають на обсяги споживаної енергії. Згідно з отриманими результатами, алгоритми PRESENT, SPECK і SIMON демонструють найменші показники енергоспоживання, що робить їх найбільш придатними для енергоефективних вбудованих систем. Дані для побудови діаграми отримані шляхом симуляцій із використанням програмного забезпечення MATLAB, що забезпечує точний розрахунок енергоспоживання залежно від апаратної архітектури та параметрів виконання операцій.

Час обробки дозволяє оцінити швидкодію алгоритмів, особливо в реальних умовах використання, де затримки можуть бути недопустимими. На рис. 3 наведено графік, який демонструє залежність часу обробки від рівня криптографічного захисту для тих самих алгоритмів.

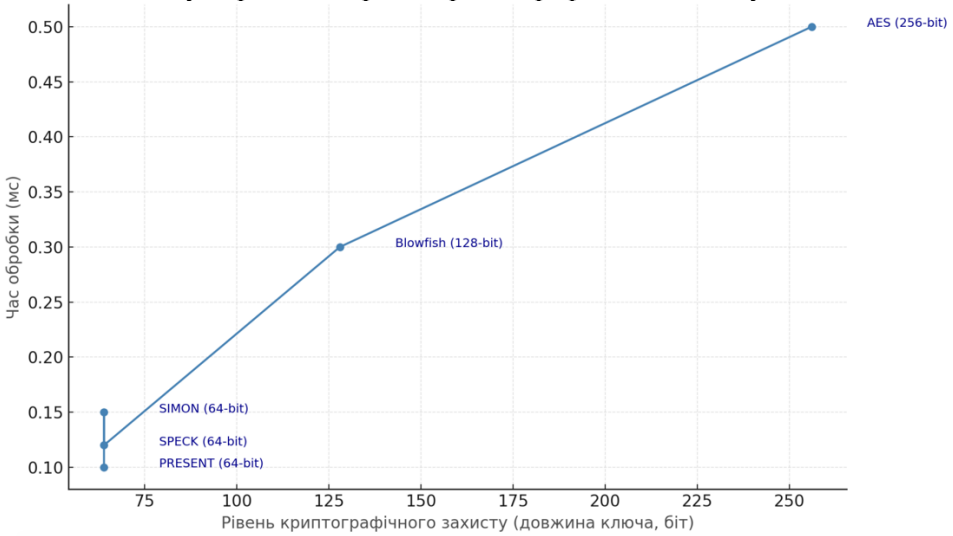

Рис. 3. Графік залежності часу обробки від рівня криптографічного захисту

Графік показує, що алгоритми PRESENT і SPECK мають найменший час обробки, тоді як AES потребує значно більше часу для виконання шифрувальних операцій. Результати симуляції отримані за допомогою інструментів для тестування продуктивності криптографічних алгоритмів у середовищі Python із використанням бібліотек CryptoBench та PyCrypto. Бібліотека CryptoBench була обрана завдяки її можливостям для порівняння продуктивності криптографічних алгоритмів, включаючи оцінку часу виконання, енергоспоживання та використання пам'яті. Вона надає інструменти для детального аналізу ефективності алгоритмів у різних умовах [15]. PyCrypto також є популярною бібліотекою для криптографічних операцій у Python, що забезпечує підтримку широкого спектра алгоритмів і дозволяє легко інтегрувати їх у симуляції. Її перевагою є доступність реалізацій як традиційних, так і полегшених криптографічних алгоритмів, що дає змогу виконувати точні вимірювання їхньої продуктивності

Рівень криптографічного захисту характеризує здатність алгоритму протистояти атакам, що є ключовим фактором для збереження конфіденційності та цілісності даних. Ця метрика дозволяє обирати алгоритми, які забезпечують належний рівень безпеки без перевищення доступних ресурсів системи. Обсяг пам'яті визначає, наскільки економно алгоритм використовує апаратні ресурси, що є критично важливим для систем із малим обсягом оперативної та постійної пам'яті.

Важливою складовою оцінки є порівняння прогнозованих значень з фактичними даними, отриманими під час тестування. Відхилення між ними дозволяють визначити точність моделі та її відповідність реальним умовам експлуатації. Низьке відхилення свідчить про адекватність моделі, тоді як значні розбіжності можуть вимагати її доопрацювання.

Використання цих метрик забезпечує комплексний підхід до аналізу ефективності моделі, дозволяючи отримати збалансоване рішення між рівнем безпеки та витратами обчислювальних ресурсів.

Висновки та перспективи подальшого дослідження. У ході дослідження було розроблено математичну модель, яка дозволяє оцінити взаємозв'язок між рівнем інформаційної безпеки та обчислювальними витратами у вбудованих пристроях. Основними результатами дослідження є формалізація залежності між ключовими параметрами, такими як енергоспоживання, час обробки, обсяг пам'яті та рівень криптографічного захисту. Проведені симуляції підтвердили, що використання полегшених алгоритмів, таких як SPECK і PRESENT, дозволяє досягти оптимального балансу між енергоефективністю та швидкодією без значного компромісу щодо рівня захисту. Модель також показала високу точність у прогнозуванні обчислювальних витрат і рівня безпеки при різних сценаріях використання.

Практична значимість розробленої моделі полягає у її здатності допомогти розробникам систем приймати обґрунтовані рішення щодо вибору криптографічних алгоритмів для конкретних пристроїв із врахуванням їх ресурсних обмежень. Вона може бути інтегрована в процеси проектування вбудованих систем, зокрема для IoT-пристроїв, медичних апаратів та інших критичних додатків, де енергоефективність і безпека є ключовими вимогами. Модель може слугувати основою для розробки автоматизованих інструментів оцінки криптографічних рішень під час проектування.

Напрями для подальших досліджень передбачають вдосконалення моделі для врахування ширшого спектру параметрів, таких як вплив різних типів атак на енергоспоживання та продуктивність пристроїв. Доцільно також дослідити інтеграцію моделей у реальні вбудовані платформи для їхньої верифікації в умовах експлуатації. Подальші роботи можуть включати адаптацію моделі до специфічних архітектур процесорів і використання штучного інтелекту для автоматизації вибору оптимальних рішень з точки зору безпеки та ресурсоємності.

Список бібліографічного опису

1. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In Proceedings of the 4th Edge Computing Workshop (doors 2024), Zhytomyr, Ukraine (pp. 85–96).
2. Aloseel, A., He, H., Shaw, C., & Khan, M. A. (2020). Analytical review of cybersecurity for embedded systems. IEEE Access, 9, 961-982.
3. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovsky P. Modern encryption methods in IoT: hardware solutions and cryptographic libraries for data protection. Розвитки інформаційно-керуючих систем та технологій: монографія / Н.М. Аксак, Д. Антонов та ін.; під наук. ред. проф. В. Вичужаніна. Львів-Торунь: Ліха-Прес, 2024. С. 28–45. https://doi.org/10.36059/978-966-397-422-4.
4. 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. https://doi.org/10.36910/6775-2524-0560-2024-55-24
5. Yarmilko, A., Rozlomii, I., & Naumenko, S. (2024, May). Dependability of Embedded Systems in the Industrial Internet of Things: Information Security and Reliability of the Communication Cluster. In International Scientific-Practical Conference «Information Technology for Education, Science and Technics» (pp. 235–249). Cham: Springer Nature Switzerland.
6. Saraiva, D. A., Leithardt, V. R. Q., de Paula, D., Sales Mendes, A., González, G. V., & Crocker, P. (2019). Prisec: Comparison of symmetric key algorithms for iot devices. Sensors, 19(19), 4312.
7. Perazzo, P., Righetti, F., La Manna, M., & Vallati, C. (2021). Performance evaluation of attribute-based encryption on constrained IoT devices. Computer Communications, 170, 151–163.
8. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177–28193.

9. Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. Wireless Personal Communications, 112(3), 1947–1980.
10. Marwedel, P. (2021). Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things (p. 433). Springer Nature.
11. Abella, C. S., Bonina, S., Cucuccio, A., D'Angelo, S., Giustolisi, G., Grasso, A. D. & Scuderi, A. (2019). Autonomous energy-efficient wireless sensor network platform for home/office automation. IEEE Sensors Journal, 19(9), 3501–3512.
12. Mahbub, M., Hossain, M. M., & Gazi, M. S. A. (2020). IoT-Cognizant cloud-assisted energy efficient embedded system for indoor intelligent lighting, air quality monitoring, and ventilation. Internet of things, 11, 100266.
13. Shah, Y., & Sengupta, S. (2020, October). A survey on Classification of Cyber-attacks on IoT and IIoT devices. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0406–0413). IEEE.
14. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2023). IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. In Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023) (pp. 145–146). Bratislava.
15. Frantz, M., Xiao, Y., Pias, T. S., Meng, N., & Yao, D. D. (2024). Methods and Benchmark for Detecting Cryptographic API Misuses in Python. IEEE Transactions on Software Engineering.

References

1. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In Proceedings of the 4th Edge Computing Workshop (doors 2024), Zhytomyr, Ukraine (pp. 85–96).
2. Aloseel, A., He, H., Shaw, C., & Khan, M. A. (2020). Analytical review of cybersecurity for embedded systems. IEEE Access, 9, 961-982.
3. Rozlomii I., Yarmilko A., Naumenko S., Mykhailovsky P. Modern encryption methods in IoT: hardware solutions and cryptographic libraries for data protection. Developments of information management systems and technologies: monograph / N.M. Aksak, D. Antonov and others; under the scientific editorship of prof. V. Vychuzhanin. Lviv-Torun: Likha-Press, 2024. P. 28–45. https://doi.org/10.36059/978-966-397-422-4.
4. Rozlomii, I., Symonyuk, V., Naumenko, S., & Mykhailovskyi, P. (2024). The security model of interconnected computing devices based on a lightweight encryption scheme for IoT. COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION, (55), 191–198. https://doi.org/10.36910/6775-2524-0560-2024-55-24
5. Yarmilko, A., Rozlomii, I., & Naumenko, S. (2024, May). Dependability of Embedded Systems in the Industrial Internet of Things: Information Security and Reliability of the Communication Cluster. In International Scientific-Practical Conference «Information Technology for Education, Science and Technics» (pp. 235–249). Cham: Springer Nature Switzerland.
6. Saraiva, D. A., Leithardt, V. R. Q., de Paula, D., Sales Mendes, A., González, G. V., & Crocker, P. (2019). Prisec: Comparison of symmetric key algorithms for iot devices. Sensors, 19(19), 4312.
7. Perazzo, P., Righetti, F., La Manna, M., & Vallati, C. (2021). Performance evaluation of attribute-based encryption on constrained IoT devices. Computer Communications, 170, 151–163.
8. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. (2021). Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities. IEEE Access, 9, 28177–28193.
9. Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. Wireless Personal Communications, 112(3), 1947–1980.
10. Marwedel, P. (2021). Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things (p. 433). Springer Nature.
11. Abella, C. S., Bonina, S., Cucuccio, A., D'Angelo, S., Giustolisi, G., Grasso, A. D. & Scuderi, A. (2019). Autonomous energy-efficient wireless sensor network platform for home/office automation. IEEE Sensors Journal, 19(9), 3501–3512.
12. Mahbub, M., Hossain, M. M., & Gazi, M. S. A. (2020). IoT-Cognizant cloud-assisted energy efficient embedded system for indoor intelligent lighting, air quality monitoring, and ventilation. Internet of things, 11, 100266.
13. Shah, Y., & Sengupta, S. (2020, October). A survey on Classification of Cyber-attacks on IoT and IIoT devices. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0406–0413). IEEE.
14. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2023). IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. In Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023) (pp. 145–146). Bratislava.
15. Frantz, M., Xiao, Y., Pias, T. S., Meng, N., & Yao, D. D. (2024). Methods and Benchmark for Detecting Cryptographic API Misuses in Python. IEEE Transactions on Software Engineering.