https://doi.org/10.31891/2307-5732-2025-357-65
УДК 621.391:004.056.5

РУДИЙ РОМАН
Чернівецький національний університет імені Юрія Федьковича
https://orcid.org/0009-0002-5161-5032
e-mail: rudyi.roman@chnu.edu.ua
ВОРОБЕЦЬ ГЕОРГІЙ
Чернівецький національний університет імені Юрія Федьковича
https://orcid.org/0000-0001-8125-2047
e-mail: g.vorobets@chnu.edu.ua

АПАРАТНІ ТА ПРОГРАМНІ РІШЕННЯ ЗАХИСТУ ПЕРСОНІФІКОВАНИХ ДАНИХ ТА ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

Розглянуто актуальні питання що стосуються організації та практичної реалізації захисту персоніфікованих даних у телекомунікаційних системах і мережах. Проведено аналіз типових кіберзагроз, які виникають на різних рівнях телекомунікаційної інфраструктури, включаючи кінцеві пристрої, мережеві протоколи та середовище Інтернету речей. Визначено ефективні апаратні рішення, зокрема апаратне шифрування, модулі безпеки, токени автентифікації, а також технології Secure Enclave і E-LUKS, що забезпечують високий рівень фізичної безпеки даних. Описано програмні рішення захисту, включаючи криптографічні алгоритми, засоби ідентифікації, автентифікації, авторизації, брандмауери, системи виявлення вторгнень та хмарні сервіси з підтримкою безпечного зберігання інформації.

Ключові слова: апаратні рішення, програмні рішення, телекомунікаційні системи та мережі, шифрування, захист інформації, персоніфіковані дані.

RUDYI ROMAN, HEORHII VOROBETS
Yuriy Fedkovych Chernivtsi National University

HARDWARE AND SOFTWARE SOLUTIONS FOR THE PROTECTION OF PERSONALLY IDENTIFIABLE DATA IN TELECOMMUNICATION SYSTEMS AND NETWORKS

This article presents a comprehensive study of hardware and software solutions aimed at securing personally identifiable information within modern telecommunication systems and networks. The increasing integration of digital technologies into all aspects of life—from healthcare and education to government administration—has intensified the demand for reliable and scalable data protection mechanisms.

The paper categorizes and analyzes hardware-based security solutions such as hardware encryption modules, secure enclaves, security tokens, and the E-LUKS encryption system, emphasizing their efficiency in providing physical isolation and cryptographic protection. These methods are particularly effective in environments with constrained resources, such as IoT devices, where traditional security measures may be impractical. The article also explores biometric authentication mechanisms, which enhance data security through the use of unique biological identifiers such as fingerprints and facial recognition.

On the software side, the study details solutions including encryption algorithms, data compression technologies, authentication and authorization systems, intrusion detection systems (IDS), firewalls, and secure cloud services. It highlights the adaptive capabilities of software measures in responding to rapidly evolving threats and managing access policies in virtualized or distributed environments.

The article concludes that neither hardware nor software security approaches are sufficient on their own. Instead, a hybrid security model that combines both is necessary for effective defense against modern cybersecurity challenges. This integrated approach ensures data confidentiality, integrity, and availability while supporting scalability and operational resilience. Recommendations are made for deploying layered security architectures that utilize the strengths of both hardware and software mechanisms to protect personal data in contemporary telecommunications infrastructure.

Keywords: hardware solutions, software solutions, telecommunication systems and networks, encryption.

Стаття надійшла до редакції / Received 28.06.2025
Прийнята до друку / Accepted 15.08.2025

Постановка проблеми

У сучасному цифровому середовищі телекомунікаційні системи та мережі стали невід'ємною частиною інфраструктури, що забезпечує передачу персоніфікованих даних у всіх сферах суспільного життя – від медицини до державного управління [1]. Разом із ростом обсягів та вартості переданої інформації зростають і ризики щодо можливостей несанкціонованого доступу, перехоплення чи модифікації трансльованої інформації. Кіберзлочинці використовують вразливості кінцевих пристроїв, мережевих протоколів, програмного забезпечення та інфраструктури для реалізації атак, включно з фішингом, DoS-атаками, компрометацією серверів та втручанням у канали зв'язку [3][4].

Дослідження [2][6] показують, що зростаюча кількість пристроїв Інтернету речей (IoT) створює додаткові виклики, адже більшість таких пристроїв мають обмежені ресурси й часто позбавлені базових механізмів безпеки, що робить їх ідеальними цілями для створення ботнетів і проникнення в мережеву інфраструктуру. Крім того, як свідчить робота [5], типові методи захисту даних в IoT-середовищі потребують адаптації через специфічні обмеження енерговитрат, пам'яті й

обчислювальних потужностей.

Апаратні рішення, такі як Secure Enclave [10], E-LUKS [11] та токени YubiKey [9], демонструють високу ефективність завдяки фізичній ізоляції та криптографічному захисту. Водночас програмні рішення — зокрема брандмауери [17], системи виявлення вторгнень [18], хмарні сервіси з підтримкою шифрування [19] — відіграють ключову роль у динамічному реагуванні на нові загрози та моніторингу мережевої активності. Однак у реальному середовищі жодне з рішень не є універсальним або достатнім самостійно.

Класичні програмні методи захисту даних, незважаючи на свою гнучкість, часто не гарантують достатнього рівня безпеки через вразливість до помилок конфігурації, обхідних атак і атак нульового дня. З іншого боку, апаратні рішення забезпечують вищий рівень фізичного захисту, але мають обмежену масштабованість і складні у впровадженні. Існує потреба у комплексному підході, який поєднує переваги як апаратних, так і програмних засобів, для протидії загрозам несанкціонованого доступу, витоку інформації та зловживання персональними даними.

Таким чином, постає актуальна проблема: необхідність системного аналізу та інтеграції апаратних і програмних рішень для ефективного захисту персоніфікованих даних у телекомунікаційних системах і мережах. Це вимагає поєднання високої надійності апаратного захисту із гнучкістю й масштабованістю програмних підходів.

Аналіз досліджень та публікацій

При аналізі сучасних наукових публікацій [1–19] можна зробити висновок, що дослідження охоплюють широкий спектр питань щодо забезпечення захисту персоніфікованих даних та інформації в телекомунікаційних системах і мережах. Зокрема, у статті [1] наводиться огляд комп'ютерних телекомунікаційних мереж, аналізуються їхні архітектури, протоколи і надаються рекомендації з питань безпеки та ефективності. У публікації [2] розглядаються загрози бездротовим мережам, аналізуються архітектури та протоколи безпеки, з особливим акцентом на проблемах та рішеннях, пов'язаних з атаками на такі мережі.

У дослідженнях [3, 4] здійснюється детальний аналіз кібербезпекових загроз, зокрема описуються сучасні шаблони атак, вразливості та стратегії протидії у критичній інфраструктурі. Особлива увага приділяється захисту мережевої інфраструктури від перехоплення трафіку, атак на протоколи, а також проблемам забезпечення надійності сервісів.

У публікаціях [5, 6] висвітлюються проблеми безпеки Інтернету речей (IoT). Автори описують специфічні вразливості IoT-пристроїв, такі як їх залучення до ботнетів, а також пропонують методи виявлення таких загроз за допомогою алгоритмів машинного навчання.

Роботи [7–11] присвячені апаратним рішенням захисту інформації. Зокрема, аналізується ефективність спеціалізованих апаратних модулів безпеки, технологій шифрування та автентифікації, включаючи використання модулів Secure Enclave, E-LUKS для IoT-пристроїв, та апаратних токенів для генерації одноразових паролів.

У дослідженнях [12, 13] розглядаються можливості застосування біометричних технологій для захисту персоніфікованих даних, акцентуючи на їх високій ефективності завдяки унікальним біологічним характеристикам користувачів.

У публікаціях [14–19] описуються програмні рішення, зокрема алгоритми шифрування для захисту даних у хмарних сервісах, технології стиснення даних для оптимізації зберігання та передачі інформації, а також системи управління доступом і виявлення вторгнень для забезпечення комплексної кібербезпеки. Окремий акцент зроблено на використанні брандмауерів та інших мережевих засобів захисту в критичних інфраструктурах, включаючи медичні інформаційні системи.

Метою роботи є: аналіз та систематизація сучасних апаратних і програмних рішень захисту персоніфікованих даних у телекомунікаційних системах і мережах.

Виклад основного матеріалу

Телекомунікаційні системи та мережі у сучасному світі мають широкий плив на промисловість, бізнес, освіту, медицину та соціальні сфери. Вони в себе включають різні компоненти та їх поділяють за різними критеріями: за масштабністю топологією, стандартами протокольних моделей, каналами зв'язку[1,2].

Телекомунікаційні системи та мережі складаються з численних компонентів, кожен з яких вразливий до певних типів атак. Наприклад, кінцеві пристрої, такі як користувацькі пристрої, можуть бути атаковані через шкідливе програмне забезпечення чи фішинг, коли користувачів обманом змушують розголошувати конфіденційну інформацію [3]. Телекомунікаційні мережі можуть піддаватися атакам шляхом перехоплення мережевого трафіку, або глушіння сигналу.

Інфраструктура мережі, включаючи маршрутизатори та комутатори, може бути скомпрометована для перенаправлення, перехоплення або порушення трафіку, тоді як атаки типу "відмова в обслуговуванні" (DoS) можуть перевантажити ресурси мережі, що робить сервіси недоступними [4].

Серверна інфраструктура та центри обробки даних зазнають впливу численних кіберзагроз, серед яких – цілеспрямовані атаки на інтернет-орієнтовані сервіси, прикладні та системні сервери з метою несанкціонованого вилучення інформації або порушення стабільності функціонування. Крім

того, існує ризик витоку даних внаслідок доступу сторонніх осіб до конфіденційної інформації, що зберігається у цифрових сховищах.

Пристрої Інтернету речей (IoT) стають все більш поширеними цілями, часто скомпрометованими для формування ботнетів для масштабних атак, або через експлуатацію вразливостей в програмному забезпеченні пристроїв [5,6].

Апаратні рішення

Апаратні рішення захисту даних включають в себе використання спеціалізованих пристроїв та модулів безпеки, таких як апаратні генератори випадкових чисел, апаратні модулі безпеки, а також спеціалізовані чіпи для шифрування даних т(рис 1). Такі пристрої забезпечують високий рівень безпеки завдяки фізичній ізоляції та спеціалізованій архітектурі, яка ускладнює несанкціонований доступ.

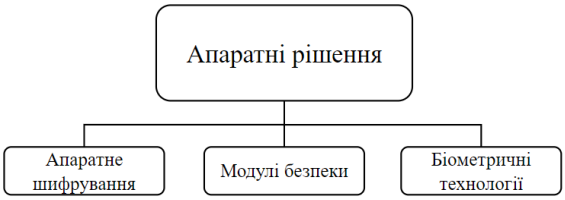

Рис.1. Основні види апаратних рішень захисту

Апаратне шифрування є основоположним, воно використовує спеціальні апаратні пристрої для шифрування даних безпосередньо на рівні пристрою. Це захищає дані від несанкціонованого доступу, навіть якщо отримано фізичний доступ до пристрою [7].

Модулі безпеки забезпечують фізично ізольовані простори для обробки конфіденційних даних, зберігання криптографічних ключів чи виконання криптографічних операцій, таким чином запобігаючи витоку через уразливості програмного забезпечення. До таких модулів можна віднести наступні підходи:

Токен автентифікації – це унікальний ідентифікатор, який використовується для підтвердження ідентичності користувача під час доступу до системи або ресурсу[8]. Він може бути випадково згенерованим рядком символів або числовим кодом, що дозволяє здійснювати безпечну автентифікацію без необхідності передачі пароля. Токени часто використовуються в системах двофакторної аутентифікації для забезпечення додаткового рівня безпеки. До пристроїв, що використовують такий підхід належать ключі базпеки Yubico[9]. Вони використовують спеціальні ізольовані елементи безпеки для генерації та зберігання даних, що використовуються для генерації токенів.

Secure enclaves, є технологією, що забезпечує високий рівень захисту конфіденційної інформації на комп'ютерних системах[10]. Вони дозволяють ізолювати важливі процеси і дані від зовнішніх втручань і навіть від самого операційного середовища. Ці контейнери використовують апаратну підтримку для забезпечення непошкоджуваності даних і їх конфіденційності.

E-LUKS (Embedded LUKS) пропонує апаратне рішення безпеки[11], спеціально розроблене для пристроїв Інтернету речей, враховуючи їхні унікальні обмеження ресурсів. Він розширює налаштування уніфікованого ключа Linux (LUKS), додаючи полегшені алгоритми шифрування та хешування для забезпечення конфіденційності, цілісності та автентичності даних. Реалізований на мікросхемах FPGA, E-LUKS забезпечує прозорий рівень безпеки між вбудованою системою та пам’яттю, що робить його високоефективним і дієвим засобом безпеки для середовищ Інтернету речей.

Yubico використовує токен автентифікацію для генерації одноразових паролів OTP. Він працює на основі симетричної криптографії, використовуючи шифрування AES-128. Одноразовий пароль, згенерований YubiKey, містить ідентифікатор пристрою та зашифровані дані. Індентифікатор пристрою є унікальним для кожного ключа, у свою чергу зашифровані дані містять: унікальний ключ, лічильник використання, внутрішній таймер та контрольна сума CRC-16.

Процес аутентифікації відбувається наступним чином. Користувач підключає YubiKey до пристрою та натискає кнопку, після чого YubiKey використовує свій секретний ключ разом з іншими параметрами. Всі ці дані шифруються за допомогою AES-128. Згенерований OTP вводиться на сайті чи в додатку для аутентифікації.

На сервері здійснюється перевірка отриманого OTP (рис. 2). Спочатку сервер розділяє OTP на дві частини: ідентифікатор пристрою та зашифровані дані. Використовуючи ідентифікатор, сервер знаходить відповідний ключ AES-128, що був заздалегідь збережений. Потім сервер розшифровує OTP і перевіряє лічильник використання, дані з внутрішнього таймеру та контрольну суму CRC-16, щоб переконатися в його коректності та унеможливити повторне використання. Якщо всі перевірки успішні, сервер надає доступ до сервісу.

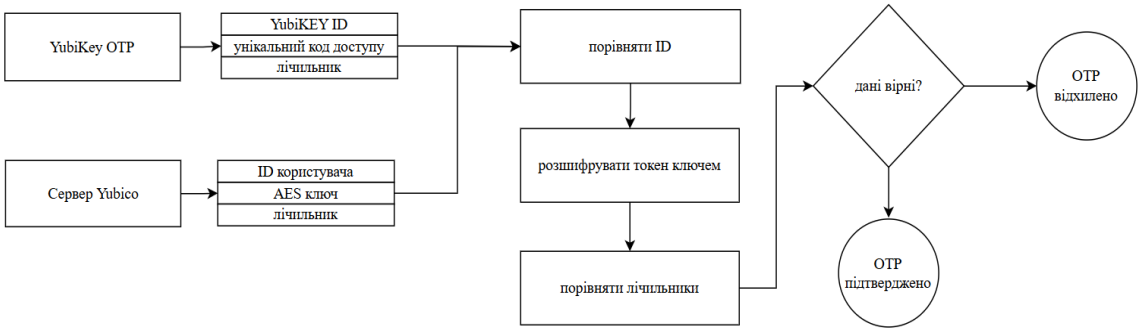

Рис.2. Схема перевірка OTP в Yubico [12]

Зауважимо, що термін «апаратне шифрування» часом можна трактувати неоднозначно: 1) пристрій який реалізовано на окремому апаратному ресурсі у вигляді схемотехнічного рішення; шифрування тут дійсно реалізовується на апаратному рівні у форматі побітового перетворення коду за відповідним алгоритмом, який формується і прошивається в апаратний модуль (мікросхему) у процесі його виготовлення; 2) пристрій у вигляді окремого апаратного ресурсу, який є носієм відповідного алгоритму/програмного коду шифрування записаного в пам'ять модуля. Перший варіант реалізується, наприклад, в MAC системах під керуванням macOS для сучасних процесорів Intel та Apple Silicon у вигляді спеціалізованих мікросхем захисту Apple T2. У другому випаду це можуть бути флеш пристрої які мають певні апаратні можливості обробки вхідних даних, зокрема відбитків пальців користувача, але підтримують відкритий бездрайверний протокол для двофакторної аутентифікації при підключенні до системи.

Перший варіант є більш захищеним, але при шифруванні файлів вони будуть дешифруватися тільки на базовому ресурсі. Тому актуальною є задача розширення можливостей даної технології та застосування в ній переваг другого варіанту, тобто можливостей перенесення модулів захисту між ресурсами і забезпечення захисту тих ресурсів, до яких вони підключені. У цьому плані перспективними ї технології реалізовані на програмованих логічних середовищах з можливістю реконфігурування апаратних рішень як на рівні реалізовуваних алгоритмів, так і на рівні архітектури функціональних модулів системи захисту даних.

Біометричні технології використовують апаратні пристрої для захоплення та обробки біометричних даних, таких як відбитки пальців або розпізнавання обличчя, забезпечуючи суворий контроль доступу до конфіденційної інформації на основі унікальних біологічних характеристик[13,14].

Програмні рішення

Програмні рішення включають в себе широкий спектр методів і технологій, таких як програмні криптографічні бібліотеки, системи управління доступом, а також програмні платформи для моніторингу та виявлення загроз (рис.3).

У сучасних телекомунікаційних системах програмні рішення відіграють ключову роль у формуванні адаптивної та багаторівневої стратегії захисту інформації. Вони надають можливість оперативного реагування на зміну загрозового середовища, дозволяють швидко впроваджувати оновлення безпеки та забезпечують централізоване управління політиками доступу. На відміну від апаратних методів, які переважно орієнтовані на фізичну ізоляцію та захист, програмні засоби більш гнучкі, масштабовані та придатні для розгортання у віртуалізованих та хмарних середовищах (рис.3).

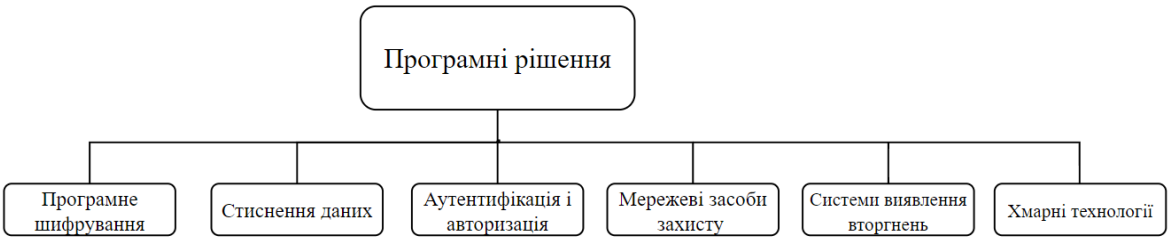

Рис.3. Основні види програмних рішень захисту

Програмне шифрування даних використовується для захисту інформації [15] на різних рівнях, включаючи дискове, файлове та мережеве шифрування, цим забезпечуючи, що тільки авторизовані користувачі можуть отримати доступ до даних.

Стиснення даних використовується для зменшення обсягу інформації, що зберігається або передається, зберігаючи при цьому її цілісність. Це зменшує час передачі та обсяг пам'яті, що потрібен

для зберігання. Стиснення не є формою шифрування, але може використовуватися разом із шифруванням для зменшення обсягу даних, які потрібно шифрувати та передавати[16].

Ідентифікація, аутентифікація і авторизація є іншим важливим компонентом програмних рішень безпеки[17], що забезпечують перевірку ідентичності користувачів і управління їхнім доступом до ресурсів, використовуючи різні методи(рис. 4).

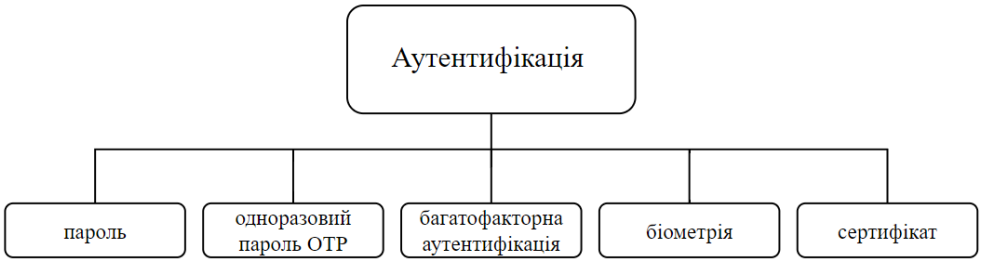

Рис.4. Види аутентифікація

Мережеві засоби захисту такі як брандмауери [18] є важливою частиною мережевої безпеки, забезпечуючи фільтрацію та контроль трафіку в мережі. Вони дозволяють встановлювати правила доступу та блокувати небажані з'єднання або потенційно небезпечні запити.

Системи виявлення вторгнень виявляючи аномальні або підозрілі активності[19], які можуть свідчити про можливі вторгнення. Ці системи використовують різноманітні методи, включаючи сигнатурний аналіз, аналіз зміни поведінки та машинне навчання для ідентифікації потенційно небезпечних подій. Після виявлення вторгнення системи виявлення вторгнень можуть автоматично або за допомогою адміністратора приймати заходи для блокування атаки або сповіщення про неї, що дозволяє оперативно реагувати на загрози та зменшувати потенційний ризик для мережевої інфраструктури.

Хмарні технології включають в себе віртуалізацію ресурсів, що дозволяє ефективно використовувати обчислювальні потужності та забезпечувати масштабованість. Зберігання даних в хмарних сервісах також відбувається з високим рівнем захисту[20], включаючи шифрування, резервне копіювання і захист від витоку інформації. Це дозволяє підприємствам зосередитися на безпеці даних, використовуючи спеціалізовані хмарні рішення без необхідності власної інфраструктури.

Висновки

Захист персоніфікованих даних в телекомунікаційних системах і мережах є критично важливим завданням у сучасному цифровому світі. Апаратні і програмні рішення грають вирішальну роль у забезпеченні безпеки цих даних. Апаратні рішення, такі як апаратне шифрування, модулі безпеки та біометричні технології, забезпечують фізичну ізоляцію і високий рівень захисту від несанкціонованого доступу. Програмні рішення, зокрема програмне шифрування даних, системи виявлення вторгнень і брандмауери, забезпечують комплексний захист на рівні програмного забезпечення, контролюючи доступ і виявляючи потенційні загрози. Ці рішення формують комплексний підхід проти різних кіберзагроз, забезпечуючи захист приватності та конфіденційності користувачів. Актуальним залишається питання розвитку технологій та засобів апаратного шифрування інформації та захисту комп’ютерних систем від несанкціонованого доступу на основі сучасних реконфігуровних програмованих логічних інтегральних середовищ. Це дозволить реалізовувати алгоритми різного рівня складності не тільки на етапі компоновки комп’ютерних систем, а й на рівні користувачів високої кваліфікації.

Література

1. Тимошенко М. Огляд комп’ютерних телекомунікаційних мереж та технологій / М. Тимошенко // ADED-2024. – 2024. – № 1. – С. 12–17.

2. Nazir R., Laghari A.A., Kumar K., David S., Ali M. Survey on Wireless Network Security / R. Nazir, A.A. Laghari, K. Kumar, S. David, M. Ali // Archives of Computational Methods in Engineering. – 2022. – Vol. 29, No. 1. – P. 1591–1610. – DOI: https://doi.org/10.1007/s11831-021-09631-5.

3. Aslan Ö., Aktuğ S.S., Ozkan-Okay M., Yilmaz A.A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions / Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz, E. Akin // Electronics. – 2023. – Vol. 12, No. 6. – Article 1333. – DOI: https://doi.org/10.3390/electronics12061333.

4. Riggs H., Tufail S., Parvez I., Tariq M., Khan M.A., Amir A., Vuda K.V., Sarwat A.I. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure / H. Riggs, S. Tufail, I. Parvez, M. Tariq, M.A. Khan, A. Amir, K.V. Vuda, A.I. Sarwat // Sensors. – 2023. – Vol. 23, No. 8. – Article 4060. – DOI: https://doi.org/10.3390/s23084060.

5. Ramadan R. Internet of Things (IoT) Security Vulnerabilities: A Review / R. Ramadan // PAI. –

2021. – Vol. 2, No. 1. – [Електронний ресурс]. – Режим доступу: https://plomscience.com/journals/index.php/PLOMSAI/article/view/14

6. Hamza W.S., Ibrahim H.M., Shyaa M.A., Stephan J.J. IoT Botnet Detection: Challenges and Issues / W.S. Hamza, H.M. Ibrahim, M.A. Shyaa, J.J. Stephan // Test Engineering and Management. – 2020. – Vol. 83. – P. 15092–15097.

7. Visconti P., Velazquez R., Del-Valle Soto C., de Fazio R. FPGA-Based Technical Solutions for High Throughput Data Processing and Encryption for 5G Communication: A Review / P. Visconti, R. Velazquez, C. Del-Valle Soto, R. de Fazio // Telecommunication Computing Electronics and Control. – 2021. – Vol. 19, No. 4. – P. 1291–1306. – DOI: https://doi.org/10.12928/telkomnika.v19i4.18400.

8. Das S., Russo G., Dingman A.C., Dev J., Kenny O., Camp L.J. A Qualitative Study on Usability and Acceptability of Yubico Security Key / S. Das, G. Russo, A.C. Dingman, J. Dev, O. Kenny, L.J. Camp // Proceedings of the 7th International Workshop on Socio-Technical Aspects in Security and Trust (STAST). – 2018. – P. 28–39.

9. Garcia Cano-Quiveu P., Ruiz-de-Clavijo-Vazquez P., Bellido M.J., Juan-Chico J., Viejo-Cortes J., Guerrero-Martos D., Ostua-Aranguena E. Formal Verification of the YubiKey and YubiHSM APIs in Maude-NPA / P. Garcia Cano-Quiveu, P. Ruiz-de-Clavijo-Vazquez, M.J. Bellido, J. Juan-Chico, J. Viejo-Cortes, D. Guerrero-Martos, E. Ostua-Aranguena // ResearchGate. – 2018. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.325869307.

10. Secure Enclave [Електронний ресурс] // Apple Support. – Режим доступу: https://support.apple.com/uk-ua/guide/security/sec59b0b31ff/web (дата звернення: 12.10.2023).

11. Cano-Quiveu G., Ruiz-de-Clavijo-Vazquez P., Bellido M.J., Juan-Chico J., Viejo-Cortes J., Guerrero-Martos D., Ostua-Aranguena E. Embedded LUKS (E-LUKS): A Hardware Solution to IoT Security / G. Cano-Quiveu, P. Ruiz-de-Clavijo-Vazquez, M.J. Bellido, J. Juan-Chico, J. Viejo-Cortes, D. Guerrero-Martos, E. Ostua-Aranguena // Electronics. – 2021. – Vol. 10, No. 23. – Article 3036. – DOI: https://doi.org/10.3390/electronics10233036.

12. Що таке YubiKey? Зовнішній пристрій, що використовується для автентифікації [Електронний ресурс]. – Режим доступу: https://www.gate.com/uk/learn/articles/what-is-yubikey/280 (дата звернення: 06.06.2025).

13. Jain A.K., Kumar A. Biometric Recognition: An Overview / A.K. Jain, A. Kumar // In: Jain A.K., Flynn P., Ross A.A. (eds) Handbook of Biometrics. – Springer, 2007. – P. 49–79.

14. Rusyn V., Subbotin S., Aceng A. Simple Autonomous Security System Based on Arduino UNO Platform and Fingerprint Scanner Module: A Study Case / V. Rusyn, S. Subbotin, A. Aceng // Computer Modeling and Intelligent Systems. – 2021. – Vol. 2864. – P. 262–271.

15. Fatima S., Rehman T., Fatima M., Khan S., Ali M.A. Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing / S. Fatima, T. Rehman, M. Fatima, S. Khan, M.A. Ali // Engineering Proceedings. – 2022. – Vol. 20, No. 1. – Article 14. – DOI: https://doi.org/10.3390/engproc2022020014.

16. Jayasankar U., Thirumal V., Ponnurangam D. A Survey on Data Compression Techniques: From the Perspective of Data Quality, Coding Schemes, Data Type and Applications / U. Jayasankar, V. Thirumal, D. Ponnurangam // Journal of King Saud University – Computer and Information Sciences. – 2021. – Vol. 33, No. 2. – P. 119–140. – DOI: https://doi.org/10.1016/j.jksuci.2018.05.006.

17. Usmonov M. Authentication, Authorization and Administration / M. Usmonov // Science and Education. – 2021. – Vol. 2, No. 7. – P. 233–242.

18. Anwar R.W., Abdullah T., Pastore F. Firewall Best Practices for Securing Smart Healthcare Environment: A Review / R.W. Anwar, T. Abdullah, F. Pastore // Applied Sciences. – 2021. – Vol. 11, No. 19. – Article 9183. – DOI: https://doi.org/10.3390/app11199183.

19. Субач І., Фесьоха В., Фесьоха Н. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі / І. Субач, В. Фесьоха, Н. Фесьоха // Інформаційні технології та безпека. – 2017. – Т. 5, № 1(8). – С. 29–41.

20. Gupta I., Singh A.K., Lee C.-N. Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions / I. Gupta, A.K. Singh, C.-N. Lee // IEEE Access. – 2022. – Vol. 10. – P. 1–1. – DOI: https://doi.org/10.1109/ACCESS.2022.3188110.

References

1. Тимошенко М. Огляд комп'ютерних телекомунікаційних мереж та технологій / М. Тимошенко // ADED-2024. – 2024. – № 1. – С. 12–17.

2. Nazir R., Laghari A.A., Kumar K., David S., Ali M. Survey on Wireless Network Security / R. Nazir, A.A. Laghari, K. Kumar, S. David, M. Ali // Archives of Computational Methods in Engineering. – 2022. – Vol. 29, No. 1. – P. 1591–1610. – DOI: https://doi.org/10.1007/s11831-021-09631-5.

3. Aslan Ö., Aktuğ S.S., Ozkan-Okay M., Yilmaz A.A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions / Ö. Aslan, S.S. Aktuğ, M. Ozkan-Okay, A.A. Yilmaz, E. Akin // Electronics. – 2023. – Vol. 12, No. 6. – Article 1333. – DOI: https://doi.org/10.3390/electronics12061333.

4. Riggs H., Tufail S., Parvez I., Tariq M., Khan M.A., Amir A., Vuda K.V., Sarwat A.I. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure / H. Riggs, S. Tufail, I. Parvez, M. Tariq, M.A. Khan, A. Amir, K.V. Vuda, A.I. Sarwat // Sensors. – 2023. – Vol. 23, No. 8. – Article 4060. – DOI: https://doi.org/10.3390/s23084060.

5. Ramadan R. Internet of Things (IoT) Security Vulnerabilities: A Review / R. Ramadan // PAI. – 2021. – Vol. 2, No. 1. – [Електронний ресурс]. – Режим доступу: https://plomscience.com/journals/index.php/PLOMSAI/article/view/14

6. Hamza W.S., Ibrahim H.M., Shyaa M.A., Stephan J.J. IoT Botnet Detection: Challenges and Issues / W.S. Hamza, H.M. Ibrahim, M.A. Shyaa, J.J. Stephan // Test Engineering and Management. – 2020. – Vol. 83. – P. 15092–15097.

7. Visconti P., Velazquez R., Del-Valle Soto C., de Fazio R. FPGA-Based Technical Solutions for High Throughput Data Processing and Encryption for 5G Communication: A Review / P. Visconti, R. Velazquez, C. Del-Valle Soto, R. de Fazio // Telecommunication Computing Electronics and Control. – 2021. – Vol. 19, No. 4. – P. 1291–1306. – DOI: https://doi.org/10.12928/telkomnika.v19i4.18400.

8. Das S., Russo G., Dingman A.C., Dev J., Kenny O., Camp L.J. A Qualitative Study on Usability and Acceptability of Yubico Security Key / S. Das, G. Russo, A.C. Dingman, J. Dev, O. Kenny, L.J. Camp // Proceedings of the 7th International Workshop on Socio-Technical Aspects in Security and Trust (STAST). – 2018. – P. 28–39.

9. Garcia Cano-Quiveu P., Ruiz-de-Clavijo-Vazquez P., Bellido M.J., Juan-Chico J., Viejo-Cortes J., Guerrero-Martos D., Ostua-Aranguena E. Formal Verification of the YubiKey and YubiHSM APIs in Maude-NPA / P. Garcia Cano-Quiveu, P. Ruiz-de-Clavijo-Vazquez, M.J. Bellido, J. Juan-Chico, J. Viejo-Cortes, D. Guerrero-Martos, E. Ostua-Aranguena // ResearchGate. – 2018. – [Електронний ресурс]. – Режим доступу: https://doi.org/10.325869307.

10. Secure Enclave [Електронний ресурс] // Apple Support. – Режим доступу: https://support.apple.com/uk-ua/guide/security/sec59b0b31ff/web (дата звернення: 12.10.2023).

11. Cano-Quiveu G., Ruiz-de-Clavijo-Vazquez P., Bellido M.J., Juan-Chico J., Viejo-Cortes J., Guerrero-Martos D., Ostua-Aranguena E. Embedded LUKS (E-LUKS): A Hardware Solution to IoT Security / G. Cano-Quiveu, P. Ruiz-de-Clavijo-Vazquez, M.J. Bellido, J. Juan-Chico, J. Viejo-Cortes, D. Guerrero-Martos, E. Ostua-Aranguena // Electronics. – 2021. – Vol. 10, No. 23. – Article 3036. – DOI: https://doi.org/10.3390/electronics10233036.

12. Що таке YubiKey? Зовнішній пристрій, що використовується для автентифікації [Електронний ресурс]. – Режим доступу: https://www.gate.com/uk/learn/articles/what-is-yubikey/280 (дата звернення: 06.06.2025).

13. Jain A.K., Kumar A. Biometric Recognition: An Overview / A.K. Jain, A. Kumar // In: Jain A.K., Flynn P., Ross A.A. (eds) Handbook of Biometrics. – Springer, 2007. – P. 49–79.

14. Rusyn V., Subbotin S., Aceng A. Simple Autonomous Security System Based on Arduino UNO Platform and Fingerprint Scanner Module: A Study Case / V. Rusyn, S. Subbotin, A. Aceng // Computer Modeling and Intelligent Systems. – 2021. – Vol. 2864. – P. 262–271.

15. Fatima S., Rehman T., Fatima M., Khan S., Ali M.A. Comparative Analysis of AES and RSA Algorithms for Data Security in Cloud Computing / S. Fatima, T. Rehman, M. Fatima, S. Khan, M.A. Ali // Engineering Proceedings. – 2022. – Vol. 20, No. 1. – Article 14. – DOI: https://doi.org/10.3390/engproc2022020014.

16. Jayasankar U., Thirumal V., Ponnurangam D. A Survey on Data Compression Techniques: From the Perspective of Data Quality, Coding Schemes, Data Type and Applications / U. Jayasankar, V. Thirumal, D. Ponnurangam // Journal of King Saud University – Computer and Information Sciences. – 2021. – Vol. 33, No. 2. – P. 119–140. – DOI: https://doi.org/10.1016/j.jksuci.2018.05.006.

17. Usmonov M. Authentication, Authorization and Administration / M. Usmonov // Science and Education. – 2021. – Vol. 2, No. 7. – P. 233–242.

18. Anwar R.W., Abdullah T., Pastore F. Firewall Best Practices for Securing Smart Healthcare Environment: A Review / R.W. Anwar, T. Abdullah, F. Pastore // Applied Sciences. – 2021. – Vol. 11, No. 19. – Article 9183. – DOI: https://doi.org/10.3390/app11199183.

19. Субач І., Фесьоха В., Фесьоха Н. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі / І. Субач, В. Фесьоха, Н. Фесьоха // Інформаційні технології та безпека. – 2017. – Т. 5, № 1(8). – С. 29–41.

20. Gupta I., Singh A.K., Lee C.-N. Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions / I. Gupta, A.K. Singh, C.-N. Lee // IEEE Access. – 2022. – Vol. 10. – P. 1–1. – DOI: https://doi.org/10.1109/ACCESS.2022.3188110.