based on smart watches, 2023, DOI: https://doi.org /10.18372/2225-5036.29.17548.
[20]. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et. al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. doi: http: // doi.org/10. 15587/978-617-7319-57-2.

STUDY OF RESISTANCE TO ATTACKS OF REPRODUCING REMOTE CONTROL PROTOCOLS USING THE 433 MHz RADIO CHANNEL

This article identifies critical vulnerabilities in the EV1527 protocol that are widely used in remote control systems, particularly home automation systems. Focusing on a detailed analysis of the protocol structure and potential weaknesses, this study assesses the risks of replay attacks that can be carried out by intercepting and retransmitting radio signals. The results of the work demonstrate the significant vulnerability of this protocol to such attacks due to the lack of cryptographic protection of the transmitted data. As part of this work, experimental tests were conducted using the HackRF One software-controlled transceiver, which allowed to reproduction of the attack in controlled laboratory conditions. The experiments confirmed theoretical assumptions about the possibility of implementing such attacks, emphasizing the need to develop more secure communication protocols. HackRF One's application demonstrated how easily attackers can intercept and rebroadcast signals, gaining unauthorized access to remote control systems. This article highlights the importance of transitioning from legacy technologies to modern solutions that include dynamic codes and cryptography to increase security. The use of dynamic codes, such as the HCS301's moving code technology, greatly complicates the possibility of replay attacks because each code transmission is unique. This means that even if the signal is intercepted, an attacker will not be able to repeat it to gain access. The authors recommend the implementation of cryptographic methods, such as the HCS301 moving code technology, which greatly complicates the possibility of repeated attacks. The introduction of such technologies increases the level of security and makes remote control systems more resistant to malicious actions. In addition, the need for constant updating and improvement of security protocols to protect critical infrastructure is emphasized. Given these results, this work indicates an urgent need for updating and improving remote control systems, including the development of new, more attack-resistant protocols, especially in the context of ensuring the security of critical infrastructure facilities. The integration of modern cryptographic methods is a key step to protect against malicious attacks and ensure the reliable operation of remote-control systems.

Keywords: radio channel, interception, replay attack, physical security, PT2262, HackRF One, NanoVNA, EV1527.

Михайлова Ольга Олександрівна, доцент кафедри захисту інформації Національного університету «Львівська політехніка».

Olha Mykhaylova, associate professor of the Information Protection Department, Lviv Polytechnic National University.
E-mail: olha.o.mykhailova@lpnu.ua.
Orcid ID: 0000-0002-3086-3160.

Стефанків Артем Вікторович, студент кафедри захисту інформації Національного університету «Львівська політехніка».

Artem Stefankiv, student of the Information Protection Department, Lviv Polytechnic National University.
E-mail: artem.stefankiv.kb.2020@lpnu.ua.
Orcid ID: 0009-0006-8851-8358.

DOI: 10.18372/2410-7840.26.18838
УДК 004.056

СИМВОЛІКА БЕЗПЕКИ: ІНТЕГРАЦІЯ КРИПТОГРАФІЇ З КІБЕРБЕЗПЕКОЮ ДЛЯ ЗАХИСТУ ЦИФРОВИХ СИСТЕМ

Катерина Михайлишин, Іван Опірський

Кібербезпека виступає як комплекс процедур спрямованих на захист комп'ютерних систем, мереж та даних від несанкціонованого доступу. У теперішньому цифровому середовищі кібербезпека стала критично важливою для підприємницької діяльності, адміністрації та керівництва, а також для залучення приватних осіб, оскільки загрози від кібератак постійно зростають. Сучасний світ нерозривно пов'язаний з новітніми технологіями, які проникають в усі сфери нашого життя. Однак зростання залежності від цифрових технологій призводить до кіберзагроз, які можуть вплинути на безпеку та стабільність суспільства. Інтеграція криптографії з кібербезпекою є відповіддю на ці виклики. Стратегічний підхід до забезпечення безпеки інформаційної технології представляє інтеграція криптографії, що базується як забезпечення від несанкціонованого доступу і для забезпечення автентифікації та недоступності даних або систем. Злиття криптографії з кібербезпекою дозволяє створити комплексний підхід охорони цифрових систем враховуючи сучасні ризики й проблеми. Зростання кількості та складності загроз вимагає постійного вдосконалення методів, які в подальшому дозволять адаптуватися до сучасних і майбутніх атак, забезпечуючи ефективний захист цифрових систем та актуальність проблеми у сучасному цифровому світі. Дослідження в даній області стає

все більш потрібним у зв'язку із зростанням загроз у цифрових системам. Ця стаття вивчає можливості використання криптографічних методів для захисту інформації та забезпечення цілісності даних. Результати дослідження вказують на стратегічний потенціал інтеграції криптографії для створення комплексного підходу до захисту цифрових систем та ефективного управління кібербезпекою. Також у даній роботі проаналізується вплив інноваційних технологій, таких як блокчейн та квантова криптографія, на сферу кібербезпеки та їхні можливості. Розглянемо важливість ролі людського фактору у забезпеченні кібербезпеки та можливі підходи до врахування цього аспекту при розробці та впровадженні криптографічних рішень. Додатково проводиться аналіз українських кваліфікованих електронних підписів, що є вдосконаленою формою електронного підпису, забезпечуючи високий рівень захисту та автентичності електронних документів у технологічному середовищі.

***Ключові слова**: символіка безпеки, криптографія, кібербезпека, автентифікація, цифровий підпис, шифрування, безпека мережевого зв'язку, цифрові системи, хеш-функція, конфіденційність.*

ВСТУП

Обмін даними та власна інформація стали невід'ємною складовою сучасного суспільства. Безпека цифрових систем перетворилась на проблему першочергового значення. Порушення конфіденційності, кібератаки та крадіжки даних – це поширені загрози, від яких користувачі потребують надійного захисту. Поряд із швидким розвитком технологій з'являються нові виклики для кібербезпеки, такі як атаки на цифрові підписи й зловживання даними. У цьому контексті криптографія відіграє ключову роль у захисті конфіденційності та цілісності інформації. Роль криптографії постає як перспективний напрямок в розробці нових методів захисту від потенційних атак, які можуть стати загрозою для сучасних засобів й технології, що використовуються для забезпечення безпеки й автентичності інформації в цифровому середовищі. Аспекти предмету «Символіка безпеки» включають використання криптографічних протоколів для шифрування даних, розробку електронних підписів та захист від кіберзагроз мережевого зв'язку. Крім того, розглядаються типи цифрових підписів, як RSA, DSA, ECDSA, EdDSA, AES, SHA-2, SHA-3, Curve-25519, Blake2, ZKP, SPHINCS та XMSS (табл. 1).

Авторами дослідження встановлено, що:

• RSA [11] – криптографічний алгоритм з відкритим ключем, став першим придатним і для шифрування, і для цифрового підпису;

• DSA [12] створює електронний підпис, але не для шифрування, проте з відкритим ключем$

• ECDSA [6] та EdDSA [13] є корисними, адже використовують еліптичні криві для створення цифрових підписів;

• AES [9] симетричний блоковий шифр, що може зашифровувати та розшифровувати дані$

• SHA-2 [14] та SHA-3 [16] криптографічні хеш-функції, що призначені для обчислення унікального фіксованого хеш-значення з будь-яких вхідних даних. Переваги – безпечне зберігання паролів, перевірка цілісності даних та підтвердження автентичності повідомлень;

• Curve25519 [10] – сімейство криптографічних хеш-функцій. Висока швидкість та ефективність робить його популярним в широкому спектрі криптографічних застосувань, хешування паролів та контролі цілісності;

• Blake2 [15] криптографічна хеш-функція, що забезпечує стійкість до атак другого роду та захист від колізій;

• SPHINCS [2] вирізняється високим рівнем безпеки та ефективністю порівняно з іншими типами. Перевага – похідна стійкість, що робиться надзвичайно витривалим до квантових обчислень та атак шляхом знаходження приватних ключів за допомогою квантових комп'ютерів;

• XMSS [7] – схема, яка базується на деревах хешування Меркла. Відома своєю високою стійкістю до квантового обчислення і забезпечує велику кількість підписів з одного приватного ключа;

• ZKP [8] являється категорію схем цифрового підпису, які використовують протоколи нульзнання для створення цифрових підписів. Ключове – довести автентичність підпису без розкриття самого підпису.

Важливим аспектом є надати переваги й недоліки кожного випадку конкретних застосувань цифрових систем, а саме у безпеці, ефективності, масштабованості та відкритості. Дослідження криптографічних протоколів у мережі Інтернет [3] вже було предметом численних досліджень та наукових публікацій. Проводився детальний аналіз, порівняння та оцінка криптографічних протоколів захисту інформації в мережі Інтернет. У даному дослідженні криптографічних атак на схеми електронного цифрового підпису в фактор-кільцях зрізаних поліномів [4] було наведено практичні приклади моделі атаки підробки електронного цифрового підпису й шифрування та ефективності підробки підпису, де на решітках криптосистем є низка переваг, серед яких основ-

ним є стійкість від криптоаналізу. Тому питання безпеки підписів тут детально вивчається. Експериментальні дані показали, що алгоритм підпису при тестуванні стійкості та вразливості не покращує захисту від досліджуваного виду підробки.

Таблиця 1

Розміри ключів типів цифрового підпису

Назва	Розмір публічного ключа	Розмір приватного ключа
Advanced Encryption Standard	128/192/256	128/1925/256
Blake2 (хеш-функція)	Залежить від використаної конфігурації	Залежить від використаної конфігурації
Curve25519	256	256
Digital Signature Algorithm	2048	1024/2045
Edwards-curve Digital Signature Algorithm	256/448	256/448
Extended Merkle signature scheme	Генерується з приватного ключа	256/512
Elliptic Curve Digital Signature Algorithm	256	192/512
Rivest, Shamir & Adleman	2048/4096	2048/4096
Secure Hash Algorithm Version 2 (хеш-функція)	Залежить від рівня безпеки та вимог застосування	Залежить від рівня безпеки та вимог застосування
Secure Hash Algorithm Version 3 (хеш-функція)	Залежить від потреб застосування та рівня безпеки	Залежить від потреб застосування та рівня безпеки
Stateless hash-based signatures	Генерується з приватного ключа	256/512
ZKP-based signatures	256	256

Мета нашої статті – розгляд важливості та переваг сучасного цифрового середовища як символіка інтеграції у кібербезпеці, де загрози постійно зростають. Ми ставимо перед собою завдання розкрити стратегічний потенціал взаємодії криптографії з цифровим захистом для створення комплексного підходу до цифрових систем, який забезпечуватиме високий рівень конфіденційності, цілісності та доступності інформації. Для виконання даної роботи будуть виконані такі завдання:

- аналіз поточного стану, дослідження ролі інформаційної безпеки та визначення стратегічної можливості взаємодії – криптографії з кібербезпекою;
- розгляд ключових аспекти інтеграції, включаючи застосування криптографічних протоколів та цифрових підписів для забезпечення безпеки автентифікації користувачів, а також шифрування й застосування хеш-функцій;
- оцінювання різних факторів кожного алгоритму, де порівняння слугуватиме освітньою ціллю для тих, хто бажає зрозуміти різні аспекти криптографічних алгоритмів підпису та їх вплив на безпеку і ефективність системи.

Є необхідність у дальшому дослідженні, адже варто розкрити нові можливості та переглянути конкретні випадки перевірки підпису, а саме шифрування та застосування хеш-функцій, особливо з урахуванням постійно зростаючих загроз й швидкого розвитку цифрових технологій. Для проведення досліджень буде також використовуватись порівняльна таблиця українських кваліфікованих електронних підписів, яка слугує як забезпечення надійності аутентифікації електронних документів в умовах, коли звичайні криптографічні протоколи можуть бути порушені за допомогою квантових обчислювальних атак.

Підписи, згенеровані за допомогою типу XMASS, залишаються безпечними навіть у випадку, якщо в майбутньому будуть розроблені квантові комп'ютери, які можуть ламати традиційні криптографічні алгоритми. Він відповідає вимогам сучасного цифрового світу і може бути використаний у спектрі безпеки мережі та даних. Враховуючи зазначене, напрямком подальших досліджень проводитиметься синтез результатів досліджень. Будуть викладені основні принципи цифрового підпису та його значення в контексті сучасного світу для перспективи подальшого розвитку та удосконалення заходів захисту інформації в цифровій області.

ОСНОВНА ЧАСТИНА

Дослідження впливу та інтеграції криптографії в кібербезпеці

Інформаційна безпека являється однією з найактуальніших проблем в сучасному цифровому світі. Вона охоплює не лише захист від несанкціонованого доступу до даних, а й забезпечення методів конфіденційності, цілісності та доступності інформації.

У цьому контексті, інтеграція криптографії з кібербезпекою стає ключовим напрямком досліджень для ефективного захисту цифрових систем. Вивчення в цій області спрямоване на розробку нових криптографічних методів, вдоскона-

лення існуючих алгоритмів та підвищення рівня захисту в цифровому просторі.

Пов'язаністю криптографії з кібербезпекою є: методи захисту даних, ідентифікація й аутентифікація, а також цифровий підпис. Методи безпеки конфіденційної інформації використовуються для захисту шляхом їх шифрування. Дослідження в цій області спрямовані на вдосконалення криптографічних алгоритмів, збільшення їх ефективності та стійкості до атак. Перевірка особи, пристрою чи програми використовуються для підтвердження ідентичності. Аналіз в цій області спрямований на розробку безпечних методів ідентифікації та аутентифікації з використанням шифрування. Щодо криптографічних методів у цифровому підписі, то це являється важливим складовим кібербезпеки, адже забезпечує можливість перевірки цілісності та автентичності даних, створюється за допомогою криптографічних алгоритмів і ключів. При цьому найбільша увага приділяється розвитку нових технологій, що враховує сучасні виклики й включає в себе пошук нових алгоритмів з вищою стійкістю до атак, також впровадження нових протоколів інформаційного обміну з метою забезпечення максимальної безпеки в цифровому середовищі (рис. 1).

Дослідження впливу й взаємозв'язку впровадження криптографії в сфері кібербезпеки може бути успішним лише в разі глибокого розуміння стану взаємодії кодування у кіберпросторі. Тісна взаємодія між цими двома аспектами створює підґрунтя для ефективного застосування криптографії у сфері інформаційної безпеки.

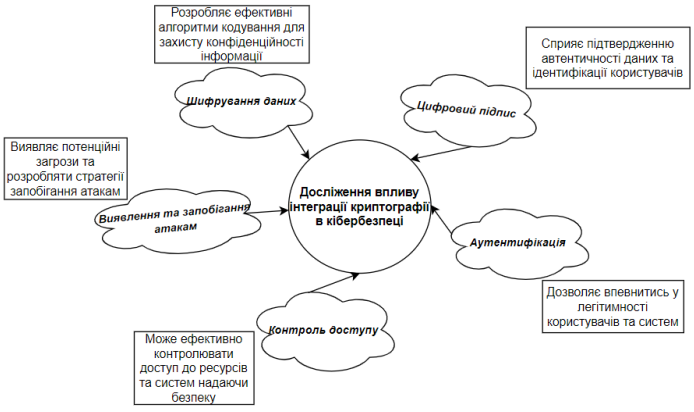

Рис. 1. Як кібербезпека впливає на сферу дослідження інтеграції криптографії

Аналіз сучасного стану і взаємодія кодування в контексті кібербезпеки

Криптографія виступає основним інструментом забезпечення конфіденційності та цілісності інформації, займається захистом даних шляхом перетворення її в зашифрований формат, що непридатний для розуміння без спеціального ключа або алгоритму, де лише уповноважені користувачі можуть отримати доступ. Ця галузь виникла з потреби вирішення проблем забезпечення приватності інформації та безпеки комунікацій. Розвиватись почала й ставати ще більш актуальною в епоху розвитку електронних технологій, де відбулось зростання обсягів обміну даними через мережу Інтернет. Кіберзлочинці постійно вдосконалюють свої методи, тому криптографія стає ключовим інструментом для захисту від різноманітних загроз таких як нижче (рис. 2).

Рис. 2. Аспекти кодування

Аналіз поточного стану може включати в себе перегляд різних методів кодування, їхні переваги та недоліки, а також огляд сучасних тенденцій і напрямків розвитку. Дослідження ролі кодування у кібербезпеці дозволяє визначити його важливість та вплив на загальний рівень захисту даних та інформаційних систем.

Визначення стратегічної можливості їх взаємодії дозволяє розробити рекомендації щодо оптимального використання кодування в цифрових системах з метою підвищення їх ефективності та надійності:

- використовуйте сучасні алгоритми шифрування, такі як AES (Advanced Encryption Standard), RSA (Rivest, Shamir & Adleman) та інші;
- забезпечте відповідний рівень ключа шифрування. До прикладу AES рекомендовано використовувати ключі довжиною 128, 192 або 256 біт;
- додайте до шифрування механізми аутентифікації та цифрового підпису для забезпечення цілісності даних;
- застосовуйте шифрування не лише для зберігання чутливої інформації, але й для захисту даних під час їх транспорту та обробки;
- періодично змінюйте ключі для запобігання можливого порушення безпеки в результаті атак методом перебору ключа.

Закріплення цих практик у стратегії кібербезпеки дозволить організаціям ефективно захищати свої цифрові ресурси від загроз і зберігати довіру користувачів до їхньої інформації. Використання сучасних алгоритмів шифрування, відповідний рівень ключа шифрування, а також додавання механізмів аутентифікації та цифрового підпису є критичними для забезпечення надійного захисту даних та інформаційних систем в сучасному цифровому середовищі. Застосування цих практик дозволяє підвищити ефективність та надійність захисту інформації, знизити ризик порушення безпеки та забезпечити високий рівень конфіденційності, цілісності та доступності даних для авторизованих користувачів.

Ключові аспекти інтеграції криптографічних протоколів: перевірка підпису, шифрування та застосування хеш-функцій

Під час переговорів визначаються три ключові параметри: алгоритм шифрування для безпосереднього захисту даних між кінцевими користувачами; алгоритм хешування для перевірки цілісності повідомлень та даних; а також алгоритм перевірки підпису для забезпечення автентичності даних, де документ підписується приватним ключем відправника, а потім перевіряється отримувачем за допомогою відповідного публічного ключа. Нижче (рис. 3) наведено схему перевірки:

- при використанні першого параметру дані перетворюються у незрозуміlу форму, що робить їх недоступними для несанкціонованого доступу. Це дозволяє забезпечити безпеку даних під час їх транспортування через непризначені для них мережі. І тільки авторизовані сторони можуть прочитати дані;
- при використанні другого параметру будь-які вхідні значення конвертуються в фіксований рядок певної довжини, відомий як хеш-значення, найменша модифікація вхідних даних призведе до значної зміни функцій, що робить його корисним для виявлення будь-яких змін в даних;
- при використанні третього алгоритму забезпечується надійна перевірку того, що дані були надіслані саме відправником, який претендує на авторство, і не були змінені під час передачі. Цей параметр дозволяє також відрізнити легітимні повідомлення від фальшивих.

Доречно буде розглянути детальніше ті три ключові параметри, які визначають безпеку та надійність системи обміну даними, які були наведені вище. Завдяки розумінню цих параметрів ми зможемо глибше вникнути в механізми захисту інформації та забезпечити високий рівень безпеки в процесі комунікацій. Далі подано (табл. 2-4) з переліком підтримуваних алгоритмів, що сприятиме зручності та ясності при виборі належних заходів забезпечення безпеки даних.

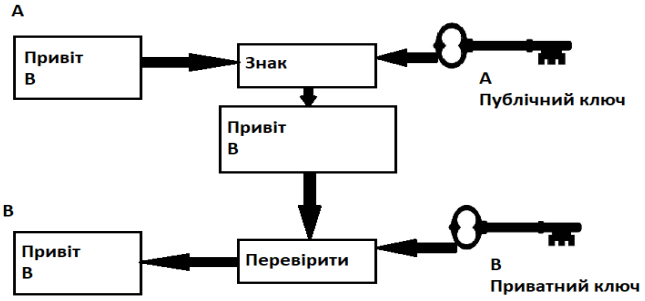

Рис. 3. Схема перевірки підпису

Таблиця 2

Параметр шифрування даних з описом

Алгоритм	Опис
Curve25519	Асиметричне шифрування. Заснований на криптографії кривих та розроблений для використання в протоколах обміну ключами
Blake2	Використовується для швидкого та безпечного обчислення контрольних сум та хеш-значень
Null (параметр)	Відсутність шифрування

Таблиця 3

Параметр застосування хеш-функцій з описом

Алгоритм	Опис
Blake2	Надає високу швидкість та стійкість
Null (параметр)	Відсутність алгоритму цілісності, тобто дані не перевіряються згідно цього фактору

NULL – параметр, що означає виконання лише перевірки цілісності, тобто дані не перевіряються.

Таблиця 4

Параметр застосування перевірки підпису з описом

Алгоритм	Опис
SPHINCS	Зберігає високий рівень безпеки та стійкості до квантових атак
XMSS	Базується на деревах підпису і має перевагу щодо високої стійкості та ефективності
Null (параметр)	Відсутність алгоритму перевірки підпису, тобто дані не перевіряються на автентичність

Розглянувши ключові аспекти інтеграції шифрувальних протоколів, зокрема перевірку підпису, криптографію та застосування хеш-функцій, можна визначити їхню важливість у забезпеченні безпеки інформаційних процесів. Надалі варто детальніше розглянути цифровий підпис як елемент, що аналізує найбільш використовувані криптографічні техніки кодування, їх основні принципи, адже це допоможе зрозуміти роль створення надійних заходів безпеки.

Цифровий підпис, як ключовий елемент, що розглядає найпоширеніші криптографічні методи шифрування. Основні принципи й відмінності, переваги та недоліки

Криптографічні методи забезпечують захищеність даних шляхом застосування різних алгоритмів й протоколів. Метою цих методів є забезпечення конфіденційності завдяки застосуванню різноманітних алгоритмів шифрувань та розшифрувань даних. Із загальною класифікацією криптографічних методів забезпечення інформації можна ознайомитися нижче (рис. 4).

Рис. 4. Класифікація криптографічних алгоритмів

Метод захисту інформації, а саме цифровий підпис, дає змогу забезпечити надійність та цілісність даних під час їх передачі. Використовуючи спеціальний алгоритм, має змогу зв'язати певний набір даних з унікальним цифровим підписом, який створюється за допомогою приватного ключа. Цей підпис може бути перевірений за допомогою відповідного публічного ключа, що дозволяє переконатися у недоторканності даних та їхньому походженні від певного джерела. Це забезпечує неспроможність інших осіб підробити або змінити підписані дані, оскільки тільки особа, яка володіє приватним ключем, може створити дійсний цифровий підпис.

Розрізняють чотири основні функції цифрового підпису:

1. Автентифікація. Дозволяє перевірити, що повідомлення або дані походять від конкретного відправника, це досягається за допомогою приватного ключа, доступ до якого має лише відправник, і публічного ключа, який перевіряє отримувач;

2. Цілісність. Цифровий підпис забезпечує засоби виявлення будь-яких змін або підробок у повідомленні під час транспортування. Якщо дані були змінені після підпису, перевірка підпису не буде успішною;

3. Невідмовність. Сторони можуть відмовитися від відповідальності за передачу або прийняття повідомлень, оскільки підпис не може бути згенерований або підроблений без приватного ключа, що належить конкретній стороні;

4. Конфіденційність. Хоч цифровий підпис не шифрує самі дані, проте може бути використаний разом з шифруванням для забезпечення конфіденційності повідомлень, дозволяючи лише відповідним сторонам розшифрувати та перевірити дані.

Розглянемо процес формування цифрового підпису, як важливий елемент сучасних систем криптографічного захисту. Детально розглянемо кожний крок процесу, починаючи з генерації хешу даних, і закінчуючи створенням унікального підпису за допомогою приватного ключа. Обговоримо значення та особливості кожного етапу, а також важливість цифрових підписів у сучасному цифровому світі.

1. Генерація хешу даних. Перед тим, як підписувати дані, варто, щоб вони обробились за допомогою хеш-функції → Хеш-функція отримує вхідні дані будь-якого розміру і обчислює фіксовані значення(унікальне для кожного набору даних та являються унікальним ідентифікатором);

2. Шифрування хешу приватним ключем відправника. Отриманий хеш-значення даних шифрується за допомогою ключа відправника → приватний ключ відомий тільки відправнику → надалі шифрування забезпечить унікальність підпису, адже тільки відправник має доступ до свого приватного ключа;

3. Утворення цифрового підпису. Після шифрування хеш-значення отримується цифровий підпис → унікальний та може бути перевірений за допомогою відповідного публічного ключа, який зазвичай розповсюджується разом з підписом.

Різні типи цифрових підписів мають на меті надати зручний та зрозумілий спосіб аналізу різних алгоритмів підпису для тих, хто зацікавлений у криптографії або в інших суміжних галузях. Порівняння надає можливість оцінити різні аспе-

кти кожного алгоритму та їх важливість. Дана таблиця (табл. 5) допоможе при виборі належного алгоритму підпису залежно від конкретних вимог і обмежень проекту. Порівняння може слугувати освітньою ціллю для тих, хто бажає зрозуміти різні аспекти криптографічних алгоритмів підпису та їх вплив на безпеку і ефективність системи.

Таблиця 5

Типи цифрових підписів та їх характеристики

Типи ЦП	**Принцип системи**	**Ключові характеристики**	**Приклади застосувань**	**Переваги**	**Недоліки**	**Криптогра-фія**
RSA	Алгоритм для формування й перевірки підпису	Розмір ключа, швидкість та безпека	Інтернет-банкінг, SSL/TLS, SSH	Висока безпека, широко підтримується	Обчислювально витратний	Симетричне
DSA	Криптографічний алгоритму для підписування та перевірки повідомлень	Довжина ключа, використання хеш-функцій	ЦП електронних документів, Ел.паспорт	Висока швидкість формування та перевірки підпису	Вимагає вибору безпечного хеш-алгоритму	Симетричне
ECDSA	Криптографії на еліптичних кривих для формування та перевірки підпису	Ефективність, безпека та розмір ключа	Bitcoin, Ethereum	Висока шв. формування та перевірки підпису	Вимагає правильного вибору еліптичної кривої	Асиметричне
EdDSA	Для підписування та перевірки повідомлень	Безпека, шв. та простота реалізації	Krypton, libsodium	Висока шв., легкість у використанні	Менш підтримується ніж RSA та DSA	Асиметричне
AES	Симетричний алгоритм, що не використовується для підпису	Надійність, швидкодія	Зашифрування файлів, сесійне шифрування даних	Висока шв. та безпека	Не призначений для підписування	Симетричне
SHA-2	Сімейство хеш-функцій для обчислення хешів даних	Односторонній алгоритм, шв. та безпека	Цифровий підпис документів, гешування паролів	Велика безпека та швидкість	Може бути вразливим до атак	Асиметричне
SHA-3	Сімейство хеш-функцій, стандартизований NIST	Відмінний від SHA-2, має високу безпеку	Захист паролів та ЦП даних	Велика безпека	Потребує додаткового обладнання для шв. обчислення	Асиметричне
Curve 25519	Криптографічний алгоритм, базується на еліптичних кривих	Шв., ефективність та безпека	Криптовалюти як Monero	Висока шв. та безпека	Може бути менш стійкий до атак	Асиметричне
Blake2	Криптографічний хеш-алгоритм, стійкий до колізійних атак	Висока шв., малий розмір хеш-значення	Хешування паролів, ЦП даних	Шв. та стійкість	Менш поширений ніж стандартні алгоритми	Симетричне
ZKP	Засновані на доказі знання	Конфіденційність та надійність	Криптовалюти, протоколи конфіденційності	Захист приватності та надійності	Не використовується для формування ЦП	Не використовує шифрування
SPHINCS	Схеми підпису на основі хеш-функцій	Безпека	Захист ідентифікації та аутентифікації	Велика стійкість до квантових атак	Обчислювальні витрати	Асиметричне
XMASS	Схема підпису на основі дерев Меркла	Велика стійкість до атак з викор. квантових комп'ютерів	ЦП для сенсорних мереж, блокчейн-технології	Висока стійкість до квантових атак, ефективне використання пам'яті	Потребує значних обчислювальних та пам'ятних ресурсів	Не використовує шифрування

У симетричному шифруванні використовується один і той же ключ для кодування та декодування даних згідно рисунку (рис. 5). Метод є швидким та ефективним, але вимагає безпечного обміну ключем між відправником та одержувачем. Там, де необхідно зашифрувати великий шматок даних, симетричне шифрування виявляється відмінним варіантом. В результаті алгоритми симетричного шифрування є значно швидшими ніж асиметричні, адже потребують менше обчислювальної потужності й не знижують швидкість інтернету.

Рис. 5. Симетричне шифрування

Асиметричне шифрування використовує два ключі – публічний та приватний, згідно наступного рисунку (рис. 6). Публічний ключ використовується для шифрування даних, тоді як приватний ключ застосовується для їх розшифрування. Найбільш очевидною перевагою цього типу шифрування є безпека, яку він надає. У цьому методі відкритий ключ є загальнодоступним, а закритий ключ варто надійно зберігати. Це гарантує, що дані залишаються захищеними від атак «людина посередині». Другою важливою особливістю, яку пропонує асиметричне шифрування – аутентифікація. Метод гарантує, що побачивши дані, він зможе дешифрувати тільки той об'єкт, який повинен їх отримати. Це підтверджує, що ви розмовляєте або обмінюєтеся інформацією з реальною людиною або організацією.

Рис. 6. Асиметричне шифрування

Основні дослідження принципів цифрового підпису: порівняння, переваги й недоліки – це важливий аспект, адже дає нам узагальнити наші знання та зрозуміти повну картину застосування цифрових підписів у сучасному інформаційному середовищі. Аналіз полягає в оцінці ефективності, де порівняння переваг та недоліків допомагає визначити результативність цифрового підпису у порівнянні з іншими методами аутентифікації. Недоліки допоможуть ідентифікувати можливі ризики та вразливості, які можуть бути використані для подальшого вдосконалення методів підпису та встановлення кращих практик використання. Розуміння цих принципів сприяє стимулюванню інновацій та розвитку нових технологій. Таким чином, дослідження, що зображене у таблиці (табл. 6) сприяє розширенню знань, визначенню оптимальних стратегій та розвитку сучасних практик в області кібербезпеки.

Таблиця 6

Важливі аспекти порівняння цифрового підпису

Аспекти	Переваги	Недоліки
Безпека	Високий рівень через викор. сильних криптографічних алгоритмів	Залежність від ключів, вразливість до атак
Ефективність	Перевірка автентичності та цілісності даних за допомогою швидких алгоритмів	Обчислювальні витрати при декількох одночасних перевірках
Масштабованість	Легко застосовується у різних масштабах, від індивідуальних повідомлень до великих транзакцій та документів, що робить його ідеальним для викор. В різних областях	Передача ключів, обчислювальні витрати
Відкритість	Стандарти та протоколи забезпечують доступність та сприяють широкому використанню	Недостатня конфіденційність, якщо алгоритм не вдається адекватно протестувати через відкритий доступ до них

Порівняльний аналіз українських кваліфікованих електронних підписів

Кваліфікований електронний підпис (КЕП) – являється удосконаленим електронним підписом, що створюється із використанням засобу кваліфікованого електронного підпису і ґрунтується на кваліфікованому сертифікаті відкритого ключа. Цінністю КЕПу виступає забезпечення надійної аутентифікації електронних документів в умовах, коли звичайні криптографічні протоколи можуть бути порушені за допомогою квантових обчислювальних атак.

Основні переваги цього підпису полягають у відповідності засадам криптографії, що надає високий рівень безпеки, не відтворюваність цифрового підпису та неможливість його підроблення за допомогою атак. Якщо цифровий підпис пройшов перевірку, що включає такі етапи проведені нижче, отримав підтвердження автентичності й надав правову значимість, тоді він стає кваліфікованим:

• підтверджено наявність дійсного кваліфікованого сертифіката електронного підпису або печатки на момент створення підпису;

• здійснено ідентифікацію підписанта або створювача печатки за допомогою кваліфікованого сертифіката;

• отримано підтвердження, що особистий ключ, що використовується для підпису або печатки, знаходиться в безпечному кваліфікованому пристрої;

• перевірено цілісність електронних даних, пов'язаних з цим підписом або печаткою.

Створення таблиці порівнянь сервісів українських кваліфікованих електронних підписів має значний практичний сенс. Це інструмент, що дозволяє користувачам отримати узагальнену інформацію про основні властивості та відомості послуг, що надаються різними провайдерами КЕП українського ринку. Розгляд даної таблиці (табл. 7) надає нам можливість об'єктивного вибору, ефективного аналізу та економії часу, а також швидко та ефективно проаналізувати основні показники і зробити зважений вибір серед запропонованого.

Таблиця 7

Характеристика сервісів кваліфікованих цифрових підписів

ТИПИ	**Алгоритми підпису (RSA, DSA, ECDSA)**	**Можливість зміни підписанта**	**Ціна**	**Рівень підтримки**	**Опис рівня підтримки**	**Двофакторні перевірки**
ДП "УЦЕС"	✓	✓, безкоштовно	300 -1000 грн/рік, (обраний тарифний план, обсяг послуг та додаткові функції)	Високий	Обумовлений держ. статусом й великим командним складом, що забезп. оперативну тех. підтримку	Пароль чи PIN-код + фізичний токен/смарт-карта/біометричні дані
Е-СЕРТИФІКАТ	✓	✓, платно (варіюється 500-2500грн)	500-2000 грн/ рік, (обраний тарифний план та обсяг послуг)	Середній	Популярність серверів, проте невеликий командний склад	Пароль чи PIN-код + одноразовий код аутентифікації, який надсилається на телефон або іншим канал
АКЦЕПТ	✓	✕	300-1200 грн/рік	Середній	Задовільна тех. підтримка, але не має такої команди як державніустанови чи великі корпорації	Пароль або PIN-код + SMS-код чи фізичний токен
Приват-Банк	✓	✓, безкоштовно	Безкоштовно	Високий	Статус банку, розмір та наявність великого командного складу забезпечує ефективну та швидку підтримку	Комбінація - пароль + одноразовий код, отриманий через SMS або моб. додаток
EDS.UA	✓	✓, безкоштовно	250-1000грн	Низький	Обмежені ресурси та мала к-ть персоналу не може приділити вдосталь часу для тех. підтримки	Пароль + одноразовий код аутентифікації, отриманий через SMS або моб. додаток

Після розгляду порівняльного аналізу українського КЕПу стає очевидно, що область цифрового підписування є значною у сфері кібербезпеки та електронного документообігу. Кваліфікований електронний підпис, як важливий інструмент цифрової аутентифікації, надає надійність документів та має важливе значення в різних сферах діяльності. Результати порівняльного аналізу дозволяють нам зробити обгрунтований вибір серед різноманітних пропозицій ринку кваліфікованих електронних підписів, забезпечуючи високу безпеку та ефективність процесів електронного підписування.

ВИСНОВКИ

Загальною метою символіки безпеки є розгляд важливості та переваг сучасного цифрового середовища у контексті кібербезпека, де загрози постійно зростають. Для досягнення цієї мети використовуються дослідження впливу та інтеграція криптографії, де з'ясували, що впливають такі аспекти як – шифрування даних, автентифікація, контроль доступу та інші. Одним з важливих характеристик аналізу сучасного стану в інформаційній системі є дослідження ролі шифрування, адже воно дозволяє визначити важливість та вплив на загальний рівень захисту даних. Також важливо було розглянути детальніше ті три ключові параметри, які визначають безпеку та надійність системи обміну даними. Розуміння цих параметрів дозволяє глибше вникнути в механізми захисту інформації та забезпечити високий рівень безпеки в процесі комунікацій.

Нарешті ключовим елементом, що розглядає найпоширеніші криптографічні методи шифрування є цифровий підпис. Порівняння надало можливість оцінити різні аспекти кожного елементу та їх важливість. Таблиця порівнянь допоможе вам при виборі належного алгоритму підпису залежно від конкретних вимог і обмежень проекту, слугує освітньою ціллю для тих, хто бажає зрозуміти криптографічні алгоритми підпису та їх вплив на безпеку і ефективність системи.

Додатково, дослідження та процес перевірки кваліфікованих електронних підписів підкреслює важливість надання високого рівня безпеки у цифровому середовищі, сприяючи захисту конфіденційності, цілісності та достовірності даних та документів. Представлені результати аналізу вказують на важливість використання у сучасному інформаційному просторі КЕП, задля надійності електронних документів та забезпечування користувачів високою безпекою підписування.

ЛІТЕРАТУРА

[1]. Korneev M.E. (2020). "Investigation of the possibilities of applying cryptographic methods of protection in information networks" (http://surl.li/rkzuy).

[2]. Yakishin O., Onikiychuk O., Skrynnik V., Kuznetsova K. (2019). "The application of crypto-algorithms in decentralized networks and the prospects of their replacement for the post-quantum period" (http://surl.li/rlabk).

[3]. Kostyuk K.O. (2023). "Research of cryptographic protocols for information protection on the Internet" (https://elartu.tntu.edu.ua/handle/lib/41648).

[4]. Kuznetsov O.O., Horbenko Y.I., Kuznetsova T.Y (2016). "Investigation of cryptographic attacks on electronic digital signature schemes in factor rings of truncated polynomials" (http://surl.li/rlase).

[5]. «Bimodal Lattice Signature Scheme». Wikipedia, (2024), [Електронний ресурс] https://en.wikipedia.org/wiki/BLISS_signature_scheme. Дата доступу 2 березня 2024.

[6]. «Elliptic Curve Digital Signature Algorithm». Wikipedia, (2018), [Електронний ресурс] https://www.wikidata.uk-ua.nina.az/ECDSA.html. Дата доступу 28 лютого 2024.

[7]. "What is quantum blockchain", FutureNow – Technologies&ScienceBlog, (2023), [Електронний ресурс] http://surl.li/rmtsp. Дата доступу 3 березня 2024.

[8]. «What Is a Zero-Knowledge Proof?», Chainlink, (2023), [Електронний ресурс]. http://surl.li/rlksw. Дата доступу 10 березня 2024.

[9]. "What is AES encryption? Memory.net.ua., (2022), [Електронний ресурс]. https://memory.net.ua/info/aes-shifruvannja. Дата доступу 7 березня 2024.

[10]. «Curve25519». Wikipedia, (2024), [Електронний ресурс]. https: // en.wikipedia.org / wiki/Curve25519. Дата доступу 16 березня 2024.

[11]. RSA (Rivest–Shamir & Adleman). Wikipedia, (2024), [Електронний ресурс]. https: // en.wikipedia.org/wiki/RSA_(cryptosystem). Дата доступу 18 березня 2024.

[12]. «What is DSA | DSA Full Form». Geeksforgeeks, (2024), [Електронний ресурс]. https://www.geeksforgeeks.org/what-is-dsa-dsa-full-form. Дата доступу 18 березня 2024.

[13]. EdDSA. Wikipedia, (2024), [Електронний ресурс]. https://en.wikipedia.org/wiki/EdDSA. Дата доступу 20 березня 2024.

[14]. "Information about the need for the SHA-2 hash function". GoDaddy,(2021), [Електронний ресурс]. http://surl.li/rmggz. Дата доступу 25 березня 2024.

[15]. «BLAKE (hash function)». Wikipedia, (2023), [Електронний ресурс]. http://surl.li/rmtui. Дата доступу 16 березня 2024.

[16]. Grabovskyi Y. I., Sovin Y. R., Tyshik I. Y. (2015) "Comparison of Implementations of New SHA-3 Hashing Algorithms" (http://surl.li/rmtxz).

[17]. «Digital signature». Wikipedia, (2024), [Електронний ресурс]. https: // en.wikipedia.org / wiki/Digital_signature. Дата доступу 27 березня 2024.
[18]. Golub O.S., Grigorenko O.G., Repa F.M. (2023). "Data confidentiality in information communication networks and means of ensuring it" (https://ela.kpi.ua/ server / api / core / bitstreams/2c8ad1be-8812-4195-a5a5-f68ca0d5b974/content)

SECURITY SYMBOLS: INTEGRATING CRYPTOGRAPHY WITH CYBER SECURITY TO PROTECT DIGITAL SYSTEMS

Cyber security is a set of procedures aimed at protecting computer systems, networks and data from unauthorized access. In today's digital environment, cyber security has become critical for business, administration and management, as well as for private individuals, as threats from cyber-attacks are ever increasing. The modern world is inextricably linked with the latest technologies that permeate all spheres of our lives. However, the growing dependence on digital technologies leads to cyber threats that can affect the security and stability of society. Integrating cryptography with cybersecurity is the answer to these challenges. A strategic approach to ensuring the security of information technology is the integration of cryptography, which is based as security against unauthorized access and to ensure authentication and inaccessibility of data or systems. The merger of cryptography with cyber security allows to create a comprehensive approach to the protection of digital systems, taking into account modern risks and problems. The increase in the number and complexity of threats requires constant improvement of methods that will allow adapting to modern and future attacks, ensuring effective protection of digital systems and the relevance of the problem in today's digital world. Let's consider the importance of the role of the human factor in ensuring cyber security and possible approaches to take this aspect into account when developing and implementing cryptographic solutions. In addition, an analysis of Ukrainian qualified electronic signatures is conducted, which is an improved form of electronic signature, ensuring a high level of protection and authenticity of electronic documents in a technological environment.

Keywords: security symbols, cryptography, cyber security, authentication, digital signature, encryption, network security, digital systems, hash function, privacy.

Михайлишин Катерина Василівна, студентка кафедри захисту інформації Національного університету «Львівська політехніка».

Kateryna Mykhailyshyn, student at the Department of Information Security, Lviv Polytechnic National University.
E-mail: Kateryna.mykhailyshyn.kb.2022@lpnu.ua.
Orcid ID: 0009-0009-4835-6958.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.26.18839
УДК 681.3.06

МОДЕЛЬ ПРОЦЕДУРИ РОЗПІЗНАВАННЯ ОСОБИ ЗА ЗОБРАЖЕННЯМ ОБЛИЧЧЯ ТА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА ПРИ БІОМЕТРИЧНІЙ АВТЕНТИФІКАЦІЇ ПЕРСОНАЛУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ІЗ ЗАСТОСУВАННЯМ НЕЙРОМЕРЕЖЕВИХ ЗАСОБІВ

Олександр Корченко, Олег Терейковський

Виклики сьогодення визначають необхідність вдосконалення засобів біометричної автентифікації персоналу об'єктів критичної інфраструктури. Поширені засоби біометричної автентифікації, що як правило базуються на використанні нейромережевих технологій аналізу зображення обличчя, в багатьох випадках не достатньо адаптовані до умов розпізнавання під час виконання персоналом своїх функціональних обов'язків, що характеризуються впливом різноманітних завад при відеореєстрації та підвищенням ймовірності атак за допомогою муляжів. Ще один перспективний напрямок вдосконалення визначається доступністю сучасних засобів відеореєстрації, які забезпечують додаткову можливість розпізнавання особи за райдужною оболонкою ока та можливість розпізнавання емоцій, що дозволяє оцінити психоемоційний стан представників персоналу. Показано, що першим етапом вдосконалення нейромережевих засобів біометричної автентифікації є розробка формалізованого опису процедури розпізнавання, яка враховує перспективні напрямки вдосконалення. Запропоновано відповідну модель, що забезпечує формалізований опис і критерії оцінки ефективності кожної із операцій та процедури розпізнавання в цілому. При цьому вперше обґрунтовано перелік критеріїв оцінки якості попередньої обробки зображень, що підлягають нейромережевому аналізу в системі біометричної автентифікації та вперше запропоновано підходи до визначення параметрів завад та розпі-