№ 8(36) 2024
НАУКА і ТЕХНІКА СЬОГОДНІ
серії: право, економіка, педагогіка, техніка, фізико-математичні науки

УДК 004.89:004.056.5

https://doi.org/10.52058/2786-6025-2024-8(36)-1089-1102

Лунгол Ольга Миколаївна кандидат педагогічних наук, доцент, доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, Донецький державний університет внутрішніх справ, вул. Велика Перспективна, 1, м. Кропивницький, https://orcid.org/0000-0001-8128-0072

ОЦІНКА ЗАСТОСУВАННЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В СИСТЕМАХ АВТЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

Анотація. У статті досліджуються сучасні біометричні технології, що використовуються у системах автентифікації, їх значення для забезпечення інформаційної безпеки та ідентифікації осіб. Зокрема, розглядаються криптографічні алгоритми, такі як Elliptic Curve Cryptography (ECC), Hash-based Message Authentication Code (HMAC), Secure Hash Algorithms SHA-2 і SHA-3, Advanced Encryption Standard-Galois/Counter Mode (AES-GCM). Ці алгоритми забезпечують високий рівень захисту біометричних даних, включаючи конфіденційність, цілісність та автентичність інформації. У статті детально аналізуються переваги біометричних технологій, такі як висока точність і надійність ідентифікації особи, відсутність можливості втрати або використання чужого ідентифікатора, а також зручність для користувачів. Водночас обговорюються потенційні ризики, пов’язані з використанням біометричних даних, включаючи можливість їх підробки, проблеми з приватністю та захистом особистої інформації, а також помилкові відмови при ідентифікації. Значну увагу приділено перспективам наукових досліджень у галузі біометричних технологій та криптографії. Постійний розвиток технологій дозволяє удосконалювати існуючі біометричні методи, розширювати їх застосування та інтегрувати з іншими інноваційними технологіями, зокрема штучним інтелектом. Також підкреслюється необхідність розвитку стандартів та законодавства щодо використання біометричних технологій для забезпечення захисту приватності та прав осіб. Окремо розглядається значущість інтеграції біометричних технологій із криптографічними методами для створення комплексних систем захисту. Порівняльний аналіз криптографічних алгоритмів демонструє їхні переваги та недоліки, а вибір конкретного алгоритму залежить від специфічних вимог і умов застосування. На основі проведеного дослідження, автор дійшов висновку, що біометричні технології та криптографічні методи є невід’ємними компонентами сучасних систем автентифікації, що забезпечують високий рівень захисту та надійності.

Подальший розвиток цих технологій сприятиме підвищенню безпеки інформаційних систем та захисту особистих даних користувачів.

Ключові слова: біометричні технології, інформаційна безпека, автентифікація, криптографічні алгоритми.

Lunhol Olha Mykolayivna PhD in Pedagogical Sciences, Docent, Associate Professor of the Department of Operational-search Activities and Information Security of Donetsk State University of Internal Affairs, Kropyvnytskyi, https://orcid.org/0000-0001-8128-0072

ASSESSMENT OF THE USE OF CRYPTOGRAPHIC ALGORITHMS IN BIOMETRIC DATA-BASED AUTHENTICATION SYSTEMS

Abstract. The article explores modern biometric technologies used in authentication systems, their significance in ensuring information security, and the identification of individuals. Specifically, it examines cryptographic algorithms such as Elliptic Curve Cryptography (ECC), Hash-based Message Authentication Code (HMAC), Secure Hash Algorithms SHA-2 and SHA-3, and Advanced Encryption Standard-Galois/Counter Mode (AES-GCM). These algorithms provide a high level of protection for biometric data, including confidentiality, integrity, and authenticity of information. The article provides a detailed analysis of the advantages of biometric technologies, such as high accuracy and reliability in person identification, the impossibility of losing or using someone else's identifier, and user convenience. It also discusses the potential risks associated with the use of biometric data, including the possibility of forgery, privacy issues, and personal information protection, as well as false rejections during identification. Significant attention is given to the prospects of scientific research in the field of biometric technologies and cryptography. The continuous development of technologies allows for the improvement of existing biometric methods, expansion of their applications, and integration with other innovative technologies, including artificial intelligence. The necessity of developing standards and legislation for the use of biometric technologies to ensure privacy protection and individual rights is also emphasized. The importance of integrating biometric technologies with cryptographic methods to create comprehensive security systems is separately considered. A comparative analysis of cryptographic algorithms demonstrates their advantages and disadvantages, with the choice of a specific algorithm depending on specific requirements and application conditions. Based on the conducted research, the author concludes that biometric technologies and cryptographic methods are integral components of modern authentication systems, providing a high level of security and reliability. The further development of these technologies will contribute to enhancing the security of information systems and the protection of users' personal data.

Keywords: biometric technologies, information security, authentication, cryptographic algorithms.

Постановка проблеми. Біометрична автентифікація інтегрує різні технології, що дозволяють надійно ідентифікувати особу за її унікальними фізіологічними або поведінковими характеристиками. Основним компонентом цих технологій є сенсори, які зчитують біометричні дані, такі як відбитки пальців, малюнок райдужної оболонки ока, рисунок вен долоні, особливості голосу, риси обличчя тощо. Водночас використання біометричних даних для автентифікації створює значні виклики щодо забезпечення безпеки та конфіденційності. Оскільки біометричні дані є унікальними, їх важко або навіть неможливо замінити, як пароль чи PIN-код.

Згідно з інформацією, наданою Державною службою спеціального зв'язку та захисту інформації [1], однією з основних проблем, пов'язаних з використанням біометричних методів автентифікації, є ймовірність помилкового доступу та помилкової відмови. Помилковий доступ відбувається, коли система надає доступ випадковій особі через схожість її біометричних даних із даними користувача. Помилкова відмова, навпаки, означає, що легітимний користувач не може отримати доступ, оскільки система його не розпізнала. Також Державна служба спеціального зв'язку наводить якісні характеристики біометричних систем, вказуючи на ймовірність помилкового доступу та відмови (див. табл. 1.).

Таблиця 1.

Якісні характеристики біометричних систем [1]

Об'єкт біометричної ідентифікації	*Імовірність помилкового доступу*	*Імовірність помилкової відмови*
Відбиток пальця	0,001 %	0,6 %
2D розпізнавання обличчя	0,1 %	2,5 %
3D розпізнавання обличчя	0,0005 %	0,1 %
Райдужна оболонка ока	0,00001 %	0,016 %
Сітківка ока	0,001 %	0,4 %
Малюнок вен	0,0008 %	0,01 %

Основною причиною таких помилок є недосконаліть сканерів та біометричних датчиків, особливо тих, що вбудовані в споживчі пристрої. Хоча ймовірність таких помилок є незначною, існує також ризик, що система може бути обманута «муляжем» або «обманкою» [1]. Отже, компрометація біометричних даних може мати серйозні наслідки як для окремої особи, так і для організації або навіть держави.

Залишається актуальним питання усунення ризику компрометації біометричних даних шляхом розробки новітніх методів захисту, що запобігають викраденню біометричних даних або використанню підроблених даних для

обходу системи. Важливим також є аналіз розвитку стандартів зберігання та обробки біометричних даних з метою забезпечення їхньої конфіденційності та недоступності для несанкціонованого доступу. Безперервні дослідження в галузі шифрування, захисту від перехоплення та злому, а також аналіз можливих ризиків і вразливостей біометричних систем є невід'ємною складовою забезпечення безпеки персональних даних користувачів та організацій.

Аналіз останніх досліджень і публікацій. Питання удосконалення та захисту біометричних технології в системах автентифікації є актуальним питанням сьогодення і активно досліджується вітчизняними та зарубіжними науковцями. Так, роботи Салієва О., Бондаренка І., Берестенка М., Габорець О., Томчука М., Цимбала В., Константинової Л., Норова А., Копача М., Пастушенка М., Білак В., Азарова А., Гудзя В., Блонського В., Сабодашка Д., Шепітька М. та ін. присвячені різним питанням удосконалення автентифікації на основі біометричних даних.

Константинова Л. та Норов А. [2] проводять порівняльний аналіз криптографії і стеганографії в інформаційній безпеці для захисту конфіденційності та цілісності даних. Науковці зазначають, що криптографія фокусується на перетворенні відкритого тексту в зашифрований, щоб забезпечити доступ до інформації лише уповноваженим особам, тоді як стеганографія фокусується на приховуванні існування інформації. Обидва методи мають різні підходи та застосування в інформаційній безпеці, і розуміння їх відмінностей та переваг є важливим для розробки безпечних систем зв'язку [2]. Ці методи часто використовуються разом для забезпечення більш високого рівня безпеки.

Про нову та революційну технологію, яка має значний потенціал для забезпечення безпечного зв'язку в майбутньому – квантову криптографію, описує в своїх досліженнях Шепітько М. [3]. Головна ідея квантової криптографії полягає в тому, що квантові властивості частин, таких як фотони, можуть бути використані для створення засобів забезпечення конфіденційності та виявлення будь-яких неупереджених спроб перехоплення інформації [3]. Переваги квантової криптографії включають її потенційну стійкість до квантових обчислень, які можуть ефективно розгадати багато сучасних криптографічних алгоритмів. Проте, важливо відзначити, що ця технологія все ще знаходиться на етапі досліджень і впровадження, існують технічні та практичні виклики, які потрібно вирішити перед широким застосуванням в реальних системах.

Таким чином, поточний стан наукових досліджень у сфері вдосконалення та захисту біометричних технологій для систем автентифікації демонструє значний прогрес і активний інтерес з боку наукової спільноти. Актуальність питань безпеки та надійності біометричних систем підтверджується численними дослідженнями, які зосереджені на розробці динамічних біометричних методів, багатофакторної автентифікації та інтеграції крипто-

графічних технологій. Розвиток сенсорних технологій, алгоритмів обробки даних та методів машинного навчання сприяє підвищенню точності ідентифікації та захищеності біометричних систем. Водночас перспективні напрямки, такі як квантова криптографія, відкривають нові можливості для забезпечення безпеки в майбутньому, хоча вони потребують подальших досліджень та вирішення технічних викликів. Наукова діяльність у цій галузі спрямована на створення більш ефективних, надійних та захищених біометричних систем, які можуть бути успішно впроваджені в різні сфери життя.

Мета статті полягає у проведенні детального аналізу і порівняння сучасних криптографічних алгоритмів, що застосовуються в системах автентифікації на основі біометричних даних, задля визначення їх ефективності, безпеки й подальшої розробки більш надійних і захищених методів автентифікації.

Виклад основного матеріалу. Біометрична автентифікація набуває все більшої популярності завдяки своїй зручності та високому рівню надійності. Проте, як будь-яка технологія, вона стикається з викликами, пов’язаними із забезпеченням безпеки та конфіденційності. У цьому контексті криптографія відіграє ключову роль у захисті біометричних даних.

Біометричні дані, такі як відбитки пальців, зображення обличчя, райдужка ока тощо, є унікальними для кожної людини і, на відміну від паролів, не можуть бути змінені. Це робить їх особливо цінними і водночас вразливими до атак. Криптографія забезпечує шифрування цих даних як під час зберігання, так і під час передачі, що запобігає несанкціонованому доступу або крадіжці.

При зборі біометричних даних одразу відбувається їх шифрування за допомогою криптографічних алгоритмів. Це гарантує, що навіть у разі компрометації системи або перехоплення даних, зловмисники не зможуть отримати доступ до справжніх біометричних даних без відповідного ключа розшифрування. Типовими алгоритмами для цього є AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-Adleman).

У біометричній автентифікації шаблони зберігаються у зашифрованому вигляді. Під час автентифікації користувача нові зібрані біометричні дані також шифруються і порівнюються зі збереженими шаблонами. Процес відбувається без розшифрування оригінальних шаблонів, використовуючи криптографічні протоколи, такі як гомоморфне шифрування або захищене обчислення.

Криптографія дозволяє додавати додаткові рівні безпеки, такі як цифрові підписи та сертифікати, для верифікації автентичності біометричних даних. Це гарантує, що дані не були змінені або підроблені під час передачі між різними компонентами системи. Крім того, криптографія сприяє збереженню конфіденційності користувачів. Наприклад, використання псевдонімів або біометричних токенів дозволяє здійснювати автентифікацію без розкриття особистих даних. Збереження конфіденційності користувачів

особливо важливе в умовах підвищеної уваги до захисту персональної інформації та дотримання нормативних вимог, таких як GDPR (General Data Protection Regulation).

Ефективне управління ключами є критично важливим аспектом використання криптографії у біометричних системах. Даний процес включає генерацію, зберігання, розподіл та відновлення криптографічних ключів. Надійні методи управління ключами гарантують, що доступ до біометричних даних мають лише авторизовані особи або системи.

Використання криптографії у біометричній автентифікації також стикається з певними викликами. Одним із них є обробка великих обсягів даних у реальному часі, що вимагає значних обчислювальних ресурсів. Проте розвиток квантових обчислень і нових криптографічних алгоритмів відкриває нові можливості для підвищення безпеки біометричних систем. Криптографія є невід'ємною складовою біометричної автентифікації, забезпечуючи захист біометричних даних від несанкціонованого доступу, підробки та крадіжки. Вона сприяє підвищенню загальної безпеки системи, забезпечує конфіденційність користувачів та додає додаткові рівні захисту. Завдяки постійному розвитку криптографічних технологій, біометричні системи стають ще більш надійними та ефективними у протистоянні сучасним загрозам.

Розглянемо більш детально криптографічний алгоритм AES (Advanced Encryption Standard) та його використання в біометричній ідентифікації. Advanced Encryption Standard (AES) [5 – 6] – це симетричний алгоритм блочного шифрування, який був прийнятий як стандарт шифрування урядом США у 2001 році. AES використовується для захисту електронних даних і став заміною алгоритму DES (Data Encryption Standard). Основні характеристики AES наведено у табл 2.

Таблиця 2.

Характеристика	*Тлумачення*
Блочний алгоритм	AES шифрує дані блоками по 128 біт
Довжина ключа	Підтримує ключі довжиною 128, 192 та 256 біт
Симетричний алгоритм	Один і той самий ключ використовується для шифрування та розшифрування даних
Структура	Заснований на підстановках та перестановках, що робить його стійким до різних видів криптоаналітичних атак

Процес шифрування в AES складається з кількох основних кроків, які включають:

1. Ініціалізацію ключа – процес генерації та розширення початкового ключа.

2. Перестановку, коли початковий ключ «XOR'иться» з першим блоком даних.

3. Основні раунди, під час яких відбувається виконання серії раундів шифрування, кожен з яких складається з операцій, представлених на рис. 1.

4. Фінальний раунд – відбувається повторення кроків SubBytes, ShiftRows та AddRoundKey без MixColumns.

Рис. 1 Схематичне зображення шифрування в AES (Advanced Encryption Standard)

AES використовує процес розширення ключа для генерування раундових ключів з початкового ключа. Даний процес включає застосування фіксованих таблиць підстановок (S-box) та лінійних перетворень для кожного раунду.

Оскільки біометрична ідентифікація потребує надійного захисту біометричних даних, то AES досить добре підходить для цього завдяки своїм високим стандартам безпеки та ефективності.

Процес використання AES в біометричній ідентифікації включає наступні етапи: збір біометричних даних за допомогою відповідних пристроїв; попередню обробку зібраних даних; генерацію шаблонів, під час якої з біометричних даних виділяються унікальні характеристики і перетворюються у шаблони; шифрування шаблонів (ініціалізація ключа, шифрування, зберігання); автентифікацію користувача. Більш детально процес використання AES в біометричній ідентифікації представлено на рис. 2.

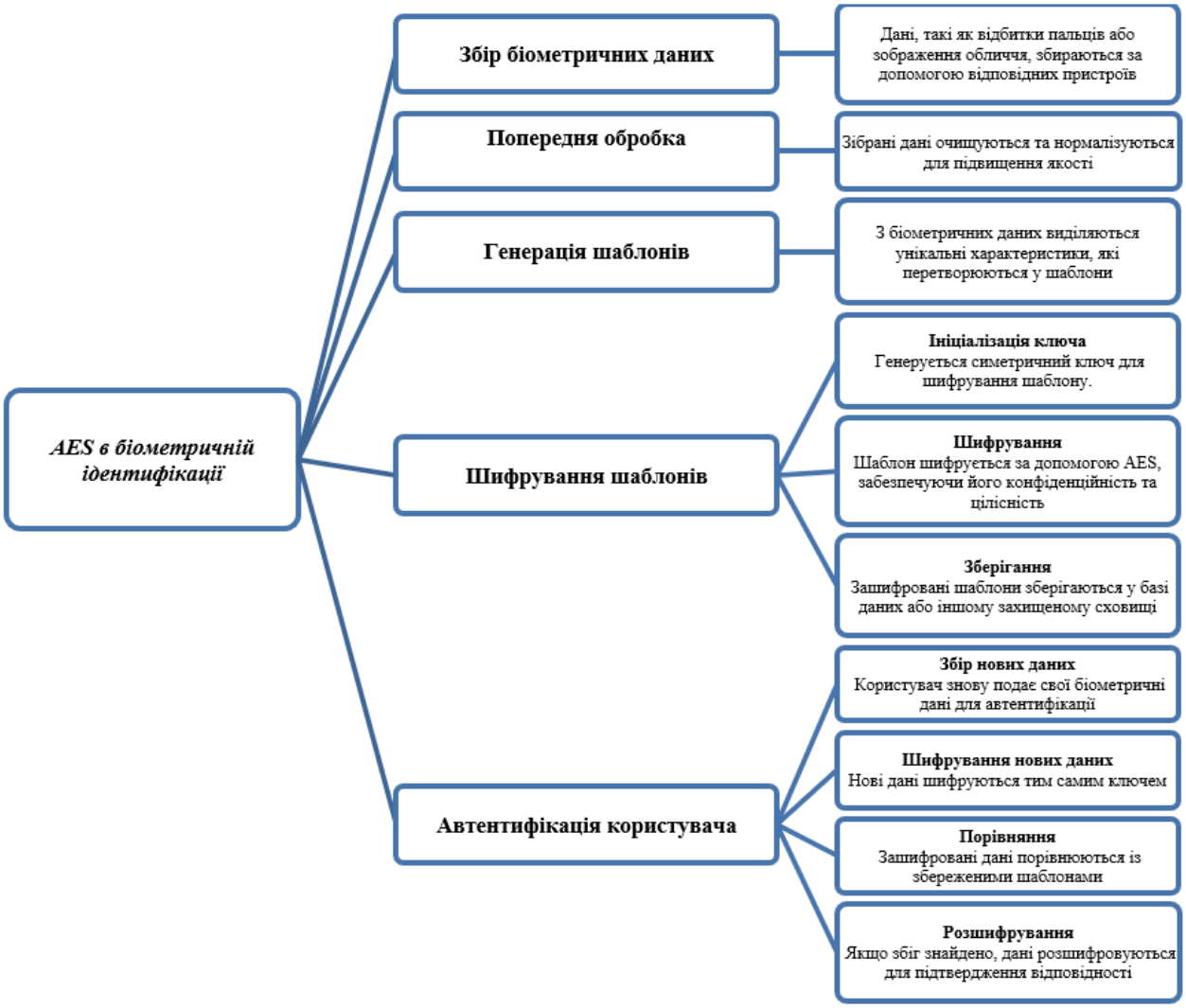

Рис. 2 Етапи процесу використання AES в біометричній ідентифікації

До переваг використання AES у біометричній ідентифікації можна віднести: високий рівень захисту біометричних даних завдяки стійкості до криптоаналітичних атак; швидке шифрування та розшифрування, що є важливим для систем реального часу; стійкість (підтримка різних довжин ключів дозволяє налаштувати рівень безпеки відповідно до потреб системи); універсальність (AES можна використовувати для захисту будь-яких типів біометричних даних, що робить його універсальним інструментом для різних додатків).

AES є одним з найпоширеніших та найбільш надійних криптографічних алгоритмів, який широко використовується для захисту біометричних даних. Висока швидкість, ефективність та стійкість до атак роблять AES зручним для забезпечення безпеки у системах біометричної ідентифікації. Використання AES забезпечує конфіденційність та цілісність біометричних даних, знижуючи ризики несанкціонованого доступу та підробки.

Розглянемо принцип роботи криптографічного алгоритму RSA (Rivest-Shamir-Adleman) в біометричній ідентифікації. RSA (Rivest-Shamir-Adleman) [7 – 9] – це криптографічний алгоритм з відкритим ключем, який був розроблений у 1977 році Рональдом Рівестом, Аді Шаміром та Леонардом Адлеманом. RSA використовується для захисту даних, цифрових підписів та забезпечення конфіденційності і автентичності повідомлень.

Основні характеристики RSA представлені у табл 3.

Таблиця 3.

Характеристика	*Тлумачення*
Асиметричний алгоритм	Використовує два ключі – відкритий (public key) для шифрування і закритий (private key) для розшифрування
Базується на математичних «труднощах»	Безпека RSA базується на складності факторизації великих простих чисел
Широке використання	Використовується у різних додатках, включаючи SSL/TLS для захисту інтернет-трафіку, цифрових підписів та шифрування електронної пошти

Етапи процесу шифрування в RSA (Rivest-Shamir-Adleman) включають:

1. Генерацію ключів. Вибір двох великих простих чисел (p та q), які мають бути випадковими і приблизно однаковими за розміром. Обчислення модуля (n): $n=p\times q$. Обчислення функції Ейлера ($\varphi(n)$): $\varphi(n)=(p-1)\times(q-1)$. Вибір відкритого ключа (e): $1<e<\varphi(n)$, причому e та $\varphi(n)$ повинні бути взаємно простими. Обчислення закритого ключа (d): $d\equiv e-1 (\mathrm{mod}\ \varphi(n))$. Відкритий ключ складається з (e, n), закритий ключ – з (d, n).

2. Шифрування. Повідомлення M перетворюється на числове значення m, де $0\le m<n$. Шифротекст C обчислюється за формулою: $C=m^e (\mathrm{mod}\ n)$.

3. Розшифрування. Розшифроване повідомлення m обчислюється за формулою: $m=C^d \pmod n$. Отримане числове значення зворотньо перетворюється на повідомлення M.

Біометрична ідентифікація потребує надійного захисту даних, зібраних у процесі автентифікації користувачів. RSA підходить для цього завдяки своїй здатності забезпечувати безпечну передачу та зберігання біометричних даних.

Процес використання RSA в біометричній ідентифікації включає етапи збору біометричних даних, попередню обробку, генерацію та шифрування шаблонів, генерацію ключів, шифрування, зберігання та автентифікацію користувача. До переваг використання RSA у біометричній ідентифікації можна віднести високий рівень захисту біометричних даних завдяки асиметричній природі алгоритму; конфіденційність, оскільки використання відкритого ключа для шифрування гарантує, що лише власник закритого ключа зможе розшифрувати дані; забезпечення аутентичності даних за допомогою

цифрових підписів, що підтверджує їх цілісність та достовірність; незалежність, бо система може безпечно передавати біометричні дані через незахищені канали зв'язку, оскільки розшифрувати їх може лише володар закритого ключа.

Отже, RSA є одним із найбільш популярних асиметричних криптографічних алгоритмів, що забезпечує надійний захист біометричних даних. Здатність до забезпечення конфіденційності, аутентичності та цілісності даних робить RSA зручним для систем біометричної ідентифікації. Використання RSA гарантує, що біометричні дані залишаються захищеними від несанкціонованого доступу та підробки, забезпечуючи високий рівень безпеки та довіри до біометричних систем автентифікації.

У системах біометричної автентифікації використовуються різні криптографічні алгоритми для забезпечення безпеки даних. Окрім AES та RSA існує кілька інших сучасних криптографічних алгоритмів, які часто застосовуються для захисту біометричної інформації. Серед них виділяємо Elliptic Curve Cryptography (ECC) [10 – 11], в якому еліптичні криві використовуються для побудови криптографічних алгоритмів на основі алгебраїчних структур еліптичних кривих над скінченними полями. ECC може використовуватися для безпечного шифрування біометричних шаблонів та цифрових підписів у системах біометричної автентифікації. ECC забезпечує високу безпеку завдяки складності проблеми дискретного логарифму на еліптичних кривих. ECC забезпечує той самий рівень безпеки з меншими ключами порівняно з RSA. Наприклад, ECC з ключем у 256 біт еквівалентний за безпекою RSA з ключем у 3072 біти. До переваг ECC можна віднести високу стійкість до криптоаналітичних атак завдяки складності проблеми дискретного логарифму на еліптичних кривих. Ефективність ECC полягає в тому, що менші розміри ключів знижують обчислювальні витрати та підвищують швидкість операцій. Менші ключі знижують вимоги до апаратного забезпечення, що є важливим для мобільних пристроїв та інших фізично або технічно обмежених середовищ.

Особливістю Hash-based Message Authentication Code (HMAC) [12 – 13] є використання криптографічних хеш-функцій в поєднанні з секретним ключем для забезпечення цілісності та автентичності повідомлення. HMAC може використовуватися для перевірки цілісності та автентичності біометричних даних, що зберігаються або передаються між компонентами системи. HMAC обчислюється шляхом застосування хеш-функції (наприклад, SHA-256) до комбінації повідомлення та секретного ключа. Даний криптографічний алгоритм забезпечує цілісність даних, оскільки будь-яка зміна даних призведе до зміни HMAC. Також він може підтверджувати автентичність даних, оскільки тільки сторони, які мають секретний ключ, можуть обчислити правильний HMAC.

Secure Hash Algorithms SHA-2 і SHA-3 – це криптографічні хеш-функції, які генерують унікальні хеші (дайджести) для будь-якого вхідного повідомлення. SHA-2 включає такі варіанти, як SHA-256 і SHA-512, які генерують хеші довжиною 256 і 512 біт відповідно. SHA-3 є новішою хеш-функцією з додатковими властивостями безпеки. Дані криптографічні алгоритми характеризуються високою стійкістю до колізій, тобто до ситуацій, коли два різних повідомлення генерують однаковий хеш. Ефективні обчислювальні алгоритми забезпечують швидку генерацію хешів. Хеш-функції можуть використовуватися для зберігання біометричних даних у формі хешів, що забезпечує їхню цілісність і унікальність. Крім того, використання хеш-функцій дозволяє зберігати біометричні дані у захищеному вигляді, що знижує ризик компрометації.

Advanced Encryption Standard-Galois/Counter Mode (AES-GCM) [14] – це режим роботи алгоритму AES, який забезпечує як шифрування, так і автентифікацію даних. Даний криптографічний алгоритм використовує Galois/Counter Mode для шифрування і забезпечення автентичності даних одночасно. Має високу швидкість шифрування і розшифрування. Забезпечує автентифікацію даних, що знижує ризик підробки або зміни даних. AES-GCM може використовуватися для забезпечення конфіденційності та цілісності біометричних даних під час їх зберігання та передачі.

Сучасні криптографічні алгоритми, такі як ECC, HMAC, SHA-2/3 та AES-GCM, забезпечують високий рівень безпеки, конфіденційності та автентичності біометричних даних, тому відіграють ключову роль у забезпеченні безпеки біометричних даних у системах автентифікації. Використання цих алгоритмів у системах біометричної автентифікації дозволяє захистити біометричні дані від несанкціонованого доступу, зміни та підробки, забезпечуючи надійну та безпечну автентифікацію користувачів.

Висновки. Біометричні технології в системах автентифікації відіграють важливу роль у забезпеченні інформаційної безпеки та ідентифікації осіб. Дослідження сучасних можливостей застосування біометричних методів для підтвердження особи в інформаційних системах є актуальним завданням сьогодення. Застосування біометричних технологій у системах автентифікації є одним з основних напрямків вирішення цієї проблеми. Ці технології базуються на унікальних фізіологічних або поведінкових характеристиках особи, таких як відбитки пальців, розпізнавання обличчя, сканування райдужки ока, голосові дані, дані ходи людини, відбитки долоні, венозна ідентифікація, серцевий ритм та генетичні дані.

Основними перевагами використання біометричних технологій є висока точність і надійність ідентифікації особи, відсутність можливості втрати або використання чужого ідентифікатора та зручність для користувачів. Ці технології значно підвищують рівень безпеки в інформаційних системах,

знижують витрати на управління паролями, а також спрощують процес автентифікації.

Однак, слід зазначити потенційні ризики використання біометричних технологій, такі як можливість підробки біометричних даних, проблеми з приватністю та захистом особистої інформації, а також можливість виникнення помилкових відмов при ідентифікації. Перспективи наукових досліджень у галузі біометричних технологій у системах автентифікації є досить обширними. Постійний розвиток технологій дозволяє удосконалювати біометричні методи, розширювати область їх застосування, а також поєднувати наявні досягнення з іншими технологіями та інноваціями, включаючи можливості штучного інтелекту.

Важливо продовжувати дослідження щодо захисту біометричних даних від кіберзагроз. Необхідно розвивати стандарти та законодавство щодо використання біометричних технологій, що сприятиме уникненню можливих конфліктів щодо приватності та прав особи. Дослідження сучасних криптографічних алгоритмів, таких як AES, RSA, ECC, HMAC, SHA-2/3 та AES-GCM, демонструє їх високу ефективність у захисті біометричних даних. Використання криптографічних методів дозволяє забезпечити конфіденційність, цілісність та автентичність біометричної інформації. Ці алгоритми надають можливість шифрувати біометричні дані, захищати їх від несанкціонованого доступу та маніпуляцій, а також забезпечують захист під час передачі даних між компонентами системи.

Значущість інтеграції біометричних технологій із криптографічними методами для створення комплексних систем захисту є незаперечною. Наприклад, застосування алгоритму AES для шифрування біометричних шаблонів, алгоритму RSA для захисту ключів шифрування, а також ECC для автентифікації користувачів суттєво підвищує загальний рівень безпеки системи. Порівняльний аналіз криптографічних алгоритмів демонструє, що кожен із них має свої переваги та недоліки, а вибір конкретного алгоритму визначається специфічними вимогами та умовами застосування.

Перспективним напрямом подальших досліджень є розробка нових криптографічних методів, які здатні забезпечити ще вищий рівень захисту біометричних даних, а також удосконалення існуючих алгоритмів для підвищення їх ефективності та стійкості до нових видів небезпек. Крім того, необхідно проводити дослідження з інтеграції біометричних систем з іншими методами автентифікації для створення багатофакторних систем, які забезпечують максимальний рівень безпеки. Подальший розвиток цих технологій сприятиме підвищенню безпеки інформаційних систем та забезпеченню захисту особистих даних користувачів.

Література:

1. Державна служба спеціального зв'язку та захисту інформації України. Парольний захист обладнання. URL: https://cip.gov.ua/ua/faqs.

2. Константинова Л.В., Норов А.О. Криптографія та стеганографія: різниця та застосування в захисті інформації. 2023. Матеріали VI Міжнародної науково-практичної конференції «Інформаційна безпека та комп'ютерні технології». 20-21.04.2023 р. Кропивницький: ЦНТУ, 2023. С. 5-6.

3. Шепітько М.Т. Кібербезпека в епоху цифрової трансформації: новітні підходи та стратегії управління ризиками. Матеріали IV Всеукраїнської науково-практичної конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу». 28 лютого 2024 року. Навчально-науковий інститут захисту інформації ДУІКТ. Київ, 2024. С. 61-65.

4. Лунгол О.М. Удосконалення професійної підготовки майбутніх фахівців правоохоронної діяльності засобами інформаційних технологій. Наука і техніка сьогодні. № 7(7) 2022. С. 153 – 163.

5. Muttaqin K., Rahmadoni J. Analysis and design of file security system AES (advanced encryption standard) cryptography based. Journal of Applied Engineering and Technological Science (JAETS). 2020, 1(2). Pp. 113-123.

6. Teng L., Li H., Yin S., Sun Y. A Modified Advanced Encryption Standard for Data Security. Int. J. Netw. Secur. 2020. 22(1). Pp. 112-117.

7. Alhassan A. B., Mahama A. H., Alhassan S. Residue architecture enhanced audio data encryption scheme using the rivest, shamir, adleman algorithm. International Journal of Advanced Engineering and Technology. Volume 6, Issue 2, 2022, Pp. 21-29.

8. Tsurkan, O., Haborets, O., Lunhol, O. Innovative development of technologies in training future law enforcement specialists. Science and technology today. Issue № 12(12). Pp. 96 – 106.

9. Elumalai E., Muruganandam D. Secure and efficient data storage with Rivest Shamir Adleman algorithm in cloud environment. Bulletin of Electrical Engineering and Informatics, 2024, 13(4). Pp. 2659-2667.

10. Ullah S., Zheng J., Din N., Hussain M. T., Ullah F., Yousaf M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review, 47. 2023. https://doi.org/10.1016/j.cosrev.2022.100530

11. Hankerson D., Menezes A. Elliptic Curve Cryptography. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. 2021. https://doi.org/10.1007/978-3-642-27739-9_245-2

12. Kumar P.H., AnandhaMala G.S. HMAC-R: Hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment. The Journal of Supercomputing, 79(3), 2023. 3181-3209. https://doi.org/10.1007/s11227-022-04714-x

13. Nagasundharamoorthi I., Venkatesan P., Velusamy P. Hash message authentication codes for securing data in wireless body area networks. Concurrency and Computation: Practice and Experience, 36(5), 2024. https://doi.org/10.1002/cpe.7934

14. Alsobky W., Ismail A., Mohra A., Hassan A., Abdelaziem A. Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (28). International Journal of Telecommunications, 2(01). 2022. Pp. 1-11.

References:

1. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. Parolnyi zakhyst obladnannia . [State Service of Special Communications and Information Protection of Ukraine. Password protection of equipment]. *cip.gov.ua.* Retrieved from https://cip.gov.ua/ua/faqs [in Ukrainian].

2. Konstantynova, L.V., & Norov, A.O. (2023). Kryptohrafiia ta stehanohrafiia: riznytsia ta zastosuvannia v zakhysti informatsii [Cryptography and steganography: difference and application in information protection]. Proceedings from *VI Mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsiina bezpeka ta kompiuterni tekhnolohii» – VI International Scientific and Practical Conference "Information Security and Computer Technologies"*. (pp. 5-6). Kropyvnytskyi: TsNTU [in Ukrainian].

3. Shepitko, M.T. (2024) Kiberbezpeka v epokhu tsyfrovoi transformatsii: novitni pidkhody ta stratehii upravlinnia ryzykamy [Cybersecurity in the era of digital transformation: the latest approaches and strategies for risk management]. Proceedings from *IV Vseukrainskoi naukovo-praktychnoi konferentsii «Stratehii kiberstiikosti: upravlinnia ryzykamy ta bezperervnist biznesu» – IV All-Ukrainian scientific and practical conference "Cyber resilience strategies: risk management and business continuity"*. (pp. 61-65). Navchalno-naukovyi instytut zakhystu informatsii DUIKT. Kyiv [in Ukrainian].

4. Lunhol, O. (2022). Udoskonalennia profesiinoi pidhotovky maibutnikh fakhivtsiv pravookhoronnoi diialnosti zasobamy informatsiinykh tekhnolohii [Improving the Professional Training of Future Law Enforcement Specialists Using Information Technology Tools]. *Nauka i tekhnika sohodni – Science and Technology Today, 7, 152 – 162* [in Ukrainian].

5. Muttaqin, K., & Rahmadoni, J. (2020) Analysis and design of file security system AES (advanced encryption standard) cryptography based. *Journal of Applied Engineering and Technological Science (JAETS, 1(2), 113-123* [in English].

6. Teng, L., Li, H., Yin, S., & Sun, Y. (2020) A Modified Advanced Encryption Standard for Data Security. *Int. J. Netw. Secur*., 22(1), 112-117 [in English].

7. Alhassan, A. B., Mahama, A. H., & Alhassan, S. (2022) Residue architecture enhanced audio data encryption scheme using the rivest, shamir, adleman algorithm. *International Journal of Advanced Engineering and Technology*, 6/2, 21-29 [in English].

8. Tsurkan, O., Haborets, O., & Lunhol, O. (2022). Innovative development of technologies in training future law enforcement specialists. Science and technology today, 12(12), 96 – 106 [in English].

9. Elumalai, E., & Muruganandam, D. (2024) Secure and efficient data storage with Rivest Shamir Adleman algorithm in cloud environment. *Bulletin of Electrical Engineering and Informatics*, 13(4), 2659-2667 [in English].

10. Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2022) Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*, 47 [in English].

11. Hankerson, D., & Menezes, A. (2021) Elliptic Curve Cryptography. *Encyclopedia of Cryptography, Security and Privacy*. Retrieved from https://doi.org/10.1007/978-3-642-27739-9_245-2 [in English].

12. Kumar, P.H., & AnandhaMala, G.S. (2023) HMAC-R: Hash-based message authentication code and Rijndael-based multilevel security model for data storage in cloud environment. *The Journal of Supercomputing, 79(3), 3181-3209* [in English].

13. Nagasundharamoorthi, I., Venkatesan, P., & Velusamy, P. (2024) Hash message authentication codes for securing data in wireless body area networks. *Concurrency and Computation: Practice and Experience, 36(5)*. Retrieved from https://doi.org/10.1002/cpe.7934 [in English].

14. Alsobky, W., Ismail, A., Mohra, A., Hassan, A., & Abdelaziem A. (2022) Design and Implementation of Advanced Encryption Standard by New Substitution Box in Galois Field (28). *International Journal of Telecommunications, 2(01), 1-11* [in English].