https://doi.org/10.31891/2307-5732-2026-365-2
УДК 004.056.53(045)

САЛІЄВА ОЛЬГА
Вінницький національний технічний університет
https://orcid.org/0000-0003-2388-7321
e-mail: salieva8257@vntu.edu.ua
ПРИСЯЖНИЙ ДМИТРО
Вінницький національний технічний університет
https://orcid.org/0009-0000-8327-3183
e-mail: dimpris@gmail.com
БЕЗПАЛИЙ КИРИЛО
Вінницький національний технічний університет
https://orcid.org/0009-0008-0331-9312
e-mail: kyrylo.bezpalyi@vntu.edu.ua
ПУЗДРАНОВСЬКИЙ ІЛЛЯ
Вінницький національний технічний університет
https://orcid.org/0009-0004-1924-3261
e-mail: ilia.puzdranovskuy@gmail.com

УДОСКОНАЛЕННЯ МЕХАНІЗМІВ БЕЗПЕКИ DRM-СИСТЕМИ НА ОСНОВІ МОДИФІКОВАНОГО АЛГОРИТМУ HOTP ТА ІНТЕГРОВАНИХ ЗАСОБІВ БЛОКУВАННЯ ДОСТУПУ

У сучасних умовах динамічного розвитку інформаційно-комунікаційних технологій та інтенсивного зростання обсягів електронного контенту завдання забезпечення захисту авторських прав і управління доступом до цифрових ресурсів набуває особливої значущості. Поширення мережевих сервісів, хмарних платформ, мультимедійних систем і мобільних застосунків створює додаткові можливості для розповсюдження контенту, але одночасно – підвищує ризики його несанкціонованого копіювання, модифікації та використання. Серед можливих шляхів розв'язання виявлених проблем є використання систем DRM (Digital Rights Management), які забезпечують комплексний, багаторівневий механізм керування доступом до цифрового контенту, застосовуючи такі інструменти, як шифрування, токенізація, парольна автентифікація та ін. Проте кіберзлочинці постійно розробляють дедалі складніші способи обходу механізмів захисту DRM-систем, зокрема шляхом клонування апаратних ключів або компрометації програмних компонентів, що реалізують контроль доступу. У зв'язку з цим у роботі пропонується розробка ефективної DRM-системи, яка буде оперативно реагувати на новітні загрози, шляхом інтеграції з багаторівневими системами блокування доступу та використання одноразових паролів (OTP) для динамічно змінюваних USB-ключів безпеки на основі удосконаленого алгоритму Hashed-Based One-Time Password (HOTP). Запропонована система блокування доступу реалізуватиме багаторівневий механізм моніторингу, який забезпечує виявлення потенційно небезпечної активності та автоматичне припинення доступу у разі виявлення загрози. Її функціональність охоплюватиме захист від несанкціонованих спроб автентифікації, автоматичне блокування після перевищення допустимої кількості помилок входу, а також використання багатофакторної автентифікації для відновлення доступу. У свою чергу, удосконалений HOTP-алгоритм, інтегрований у роботу USB-ключів безпеки, забезпечуватиме суттєве підвищення рівня захищеності DRM-систем шляхом формування одноразових паролів під час кожної спроби доступу, що істотно знижує ймовірність їх перехоплення або повторного використання. Крім того, механізм динамічного оновлення секретного ключа після завершення кожної сесії створюватиме додатковий шар захисту, ускладнюючи реалізацію атак, спрямованих на компрометацію USB-ключів.

Ключові слова: *кібербезпека, DRM-система, USB-ключ, HOTP-алгоритм, система блокування доступу, автентифікація.*

SALIIEVA OLHA, PRYSIAZHNYI DMYTRO, BEZPALYI KYRYLO, PUZDRANOVSKYI ILLIA
Vinnytsia National Technical University

ENHANCING SECURITY MECHANISMS OF A DRM SYSTEM BASED ON A MODIFIED HOTP ALGORITHM AND INTEGRATED ACCESS BLOCKING TOOLS

In the context of the dynamic development of information and communication technologies and the intensive growth of electronic content volumes, the task of ensuring copyright protection and access control to digital resources has become particularly important. The widespread adoption of network services, cloud platforms, multimedia systems, and mobile applications creates additional opportunities for content distribution; however, it simultaneously increases the risks of unauthorized copying, modification, and use. Among the possible approaches to addressing these issues is the use of DRM (Digital Rights Management) systems, which provide a comprehensive, multi-layered mechanism for managing access to digital content by employing tools such as encryption, tokenization, password-based authentication, and others. However, cybercriminals continuously develop increasingly sophisticated methods to bypass DRM protection mechanisms, including cloning hardware keys or compromising software components responsible for access control. In this context, the present study proposes the development of an effective DRM system capable of promptly responding to emerging threats through integration with multi-level access-blocking systems and the use of one-time passwords for dynamically changing USB security keys based on an enhanced Hashed-Based One-Time Password (HOTP) algorithm. The proposed access-blocking system implements a multi-level monitoring mechanism to detect potentially dangerous activities and automatically terminate access upon threat detection. Its functionality includes protection against unauthorized authentication attempts, automatic blocking after exceeding a predefined number of failed login attempts, and the use of multi-factor authentication for access recovery. Furthermore, the enhanced HOTP algorithm integrated into the USB security keys significantly improves the security of the DRM system by generating one-time passwords for each access attempt, thereby greatly reducing the likelihood of interception or reuse. Additionally, the dynamic updating of the secret key after each session provides an extra layer of protection, complicating attacks aimed at compromising USB keys.

Keywords: *cybersecurity, DRM-system, USB-token, HOTP-algorithm, access blocking system, authentication.*

Стаття надійшла до редакції / Received 11.02.2026
Прийнята до друку / Accepted 11.03.2026
Опубліковано / Published 28.05.2026

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

На сучасному етапі DRM-системи виступають важливим засобом забезпечення контролю доступу до інформаційних ресурсів і захисту об'єктів інтелектуальної власності від несанкціонованого перегляду, копіювання, модифікації та інших дій, що виходять за рамки встановлених виробником правил або ліцензійних умов. Ключові функції DRM-системи забезпечують інтеграцію механізмів автентифікації, шифрування та блокування доступу, що дозволяє реалізувати комплексний захист цифрового контенту та мінімізації ризиків. Водночас стрімке зростання нових кіберзагроз обумовлює постійну необхідність удосконалення механізмів DRM-систем, впровадження сучасних методів захисту та адаптивних систем контролю доступу з метою підвищення стійкості платформи до новітніх типів атак. У зв'язку з цим особливої уваги потребують дослідження, спрямовані на створення нових або вдосконалення наявних алгоритмів роботи DRM-системи, що базуються на інтеграції сучасних методів багатофакторної автентифікації та систем блокування доступу. Таким чином, у межах цієї роботи доцільно проаналізувати наявні методи забезпечення захисту інформаційних ресурсів у DRM-системах, розглянути особливості використання USB-ключів безпеки та алгоритми генерації одноразових паролів, розробити алгоритм роботи динамічно змінюваних USB-ключів на основі удосконаленого алгоритму HOTP, створити адаптивну систему блокування доступу для протидії загрозам безпеці, та протестувати реалізовану систему для оцінювання її ефективності та відповідності вимогам.

Аналіз досліджень та публікацій

Упродовж останніх років активно здійснюються дослідження, спрямовані на зміцнення безпеки DRM-систем та оптимізацію їх функціонування. Так, у роботі [1] автори запропонували протокол узгодження автентифікованих ключів для DRM-систем, який забезпечує анонімне та захищене встановлення сесій у DRM-системах із низькими комунікаційними витратами. У дослідженні [2] проаналізовано сучасні підходи до побудови DRM-систем та здійснено критичне оцінювання їх технічних можливостей, рівня гнучкості та обмежень щодо незмінності. Автори роботи [3] здійснили опис різних типів DRM-систем, а також навели приклади їх використання. У рамках дослідження [4] авторами було розроблено ефективний механізм розподілу ключів для DRM-систем, що враховує вимоги до безпеки та не призводить до зростання загальних витрат. У роботі [5] проаналізовано особливості функціонування DRM-систем, розглянуто механізми забезпечення захисту цифрового контенту від актуальних кіберзагроз та запропоновано підхід до побудови DRM-рішень, що ґрунтується на використанні методів штучного інтелекту у поєднанні з алгоритмами AES та ECC для формування ліцензійних ключів. Автори праці [6] розробили підхід до розповсюдження цифрового контенту в портативних DRM-системах із використанням смарт-карт, який забезпечує реалізацію взаємної автентифікації та встановлення захищеного сеансу обміну даними. У роботі [7] представлено автентифікований протокол контролю доступу, який зберігає право користувача на авторизоване розповсюдження контенту для системи управління цифровими правами – DRM. Автори праці [8] запропоновали надійну схему автентифікації з використанням біометричних даних для DRM-систем. У дослідженні [9] продемонстровано розроблений анонімний протокол автентифікації Eland, який ефективно інтегрований у DRM-системи та забезпечує оптимальний баланс між рівнем безпеки та продуктивністю роботи системи. Автори праці [10] здійснили криптоаналіз протоколу автентифікації для DRM-систем, що базується на використанні біометричних даних. На підставі отриманих результатів представлено порівняльний аналіз, який охоплює оцінювання обчислювальних витрат та показників безпеки, що надає змогу встановити оптимальне співвідношення між продуктивністю та рівнем захисту системи.

Незважаючи на велику кількість досліджень, спрямованих на підвищення безпеки DRM-систем, сучасні кіберзловмисники продовжують використовувати широкий спектр складних атак, серед яких – підроблення апаратних ключів, компрометація програмних модулів керування доступом та інші методи нейтралізації захисних механізмів. За таких обставин ефективна DRM-система повинна демонструвати високу гнучкість та здатність до швидкої адаптації, впроваджуючи більш прогресивні механізми захисту. З огляду на це, у роботі пропонується підвищити рівень захищеності DRM-системи керування доступом шляхом використання динамічно змінюваних USB-ключів на основі модернізованого HOTP-алгоритму в поєднанні з розширеною системою блокування доступу.

Формулювання цілей статті

Метою роботи є: розробка комплексного рішення, що поєднує використання динамічно змінюваних USB-ключів із вдосконаленим алгоритмом HOTP, забезпечуючи підвищений рівень захищеності DRM-системи.

Виклад основного матеріалу

Сучасні загрози для DRM-систем формують потребу в застосуванні розгорнутих та гнучких підходів до побудови архітектури їхнього захисту, а також у постійному вдосконаленні механізмів протидії кіберризикам. Використання одноразових динамічних паролів у поєднанні з апаратними засобами автентифікації, зокрема USB-ключами на основі алгоритму HOTP, є перспективним напрямом, що створює передумови для підвищення рівня безпеки DRM-систем.

Алгоритм HOTP є одним із базових механізмів генерування одноразових паролів, що формуються шляхом застосування хеш-функції до секретного ключа та значення лічильника автентифікації. Для інтеграції HOTP в USB-ключі безпеки, які застосовуються в DRM-системах, необхідно адаптувати алгоритм до умов динамічної аутентифікації, забезпечивши підтримку змінюваних ключів та стійкість до спроб їхнього клонування.

Модифікований алгоритм HOTP для апаратних токенів безпеки передбачає, що при кожній спробі доступу до DRM-системи USB-ключ генерує одноразовий пароль та передає його для проходження аутентифікації, характеризуючись при цьому такими ключовими особливостями:

– автоматичне формування одноразових аутентифікаційних токенів в режимі реального часу. Кожен запит на проходження автентифікації з використанням USB-ключа ініціює процедуру формування нового одноразового пароля за допомогою протоколу HOTP. Генерація OTP здійснюється шляхом застосування унікального значення лічильника у поєднанні з секретним ключем, який зберігається в захищеному сегменті пам'яті апаратного токена;

– механізм автоматичної ротації секретного ключа, що використовується для генерації OTP. Реалізація запропонованого оновлення може здійснюватися з регулярною періодичністю або після досягнення визначеної кількості успішних аутентифікаційних запитів, що підвищує загальний рівень криптографічної стійкості системи;

– захист від несанкціонованого копіювання. Кожен USB-токен має унікальний секретний ідентифікатор, що пов'язаний із його апаратною архітектурою та унеможливлює створення точних копій і застосування ключа на іншому обладнанні.

Основні етапи роботи вдосконаленого алгоритму включають:

– встановлення початкового значення лічильника та секретного ключа, який застосовується для створення одноразових паролів;

– генерацію одноразових паролів шляхом обчислення хешу від значень лічильника та секретного ключа;

– передачу одноразових паролей для автентифікації: USB-ключ передає згенерований одноразовий пароль на сервер DRM-системи для його верифікації;

– оновлення параметрів безпеки. Після кожної успішної аутентифікації приватний ключ і поточне значення лічильника змінюються відповідно до визначених правил. Зокрема, приватний ключ може оновлюватися із застосуванням алгоритму HMAC або на основі хеш-функції, що обробляє його попереднє значення.

Важливо підкреслити, що коректне використання динамічних USB-ключів у DRM-середовищі можливе лише за умови синхронної роботи ключа та сервера, на якому зберігаються дані для верифікації одноразових паролів.

На основі наведеної концепції опишемо основні етапи роботи алгоритму функціонування динамічно змінюваних USB-ключів безпеки, що функціонують із використанням покращеного алгоритму HOTP.

Крок 1. Початкове налаштування та активація USB-ключа.

При першому підключенні USB-ключ проходить процедуру ініціалізації, під час якої генерується початкове значення секретного ключа та лічильника. Ці дані зберігаються у захищеній пам'яті ключа і передаються на сервер для подальшої синхронізації.

Крок 2. Вибір хеш-функції для HOTP.

На апаратному носії обирається тип хеш-функції, яка трансформує вхідні дані в одноразовий пароль. Важливою умовою функціонування є встановлення аналогічного алгоритму на боці DRM-сервера, що гарантує цілісність процесу автентифікації та сумісність обох компонентів системи.

Крок 3. Проходження парольної аутентифікації користувача.

Надання доступу до DRM-системи здійснюється після успішного проходження аутентифікації, що дозволяє розблокувати USB-ключ та запустити процес генерації OTP.

Крок 4. Генерація одноразового пароля.

Після успішного проходження автентифікації USB-ключ запускає алгоритм генерації одноразового пароля з використанням поточного значення секретного ключа (K) та лічильника (C).

Крок 5. Визначення актуального значення лічильника.

Апаратний токен зчитує зі своєї внутрішньої пам'яті значення лічильника (C), що дозволяє визначити поточну сесію доступу.

Крок 6. Визначення унікального значення секретного ключа.

Апаратний токен зчитує зі своєї внутрішньої пам'яті унікальне значення секретного ключа (K), що змінюється після кожного використання.

Крок 7. Формування одноразового пароля за алгоритмом HOTP.

У алгоритмі HOTP одноразовий пароль формується шляхом хешування значення лічильника (C) із секретним ключем (K), приміром: $OTP = HMAC - SHA - 256(K \,||\, C)$.

Крок 8. Надсилання одноразового пароля до DRM-системи.

Сформований одноразовий пароль передається на DRM-сервер через захищений канал зв'язку або спеціалізований програмний інтерфейс, що мінімізує ризики компрометації під час передачі.

Крок 9. Верифікація одноразового паролю на сервері.

Після отримання одноразового паролю DRM-система ініціює процедуру його верифікації шляхом зіставлення із значенням, сформованим на сервері на основі секретного ключа (K) та значення лічильника (C).

Крок 10. Проходження успішної автентифікації.

У разі успішної перевірки сервер виконує оновлення значення лічильника (C) та секретного ключа (K), закріплених за конкретним USB-токеном, що забезпечує подальший доступ користувача до захищених DRM-ресурсів.

Крок 11. Оновлення криптографічного ключа на USB-токені.

Після підтвердження автентичності USB-ключ генерує нове значення секретного ключа (K) за допомогою стійкого криптографічного механізму, наприклад алгоритму HMAC. Так, новий ключ може бути сформованим наступним чином: $K' = HMAC - SHA - 256(K \,||\, OTP)$.

Крок 12. Оновлення лічильника.

Значення лічильника (C) інкрементується, що забезпечує унікальність наступного одноразового пароля та запобігає повторному використанню OTP.

Крок 13. Передача оновлених значень на сервер.

Сервер DRM зберігає оновлені значення секретного ключа та лічильника для синхронізації з USB-ключем.

Крок 14. Механізм відновлення після втрати синхронізації.

У випадку розсинхронізації між USB-ключем і сервером (наприклад, через невдалу автентифікацію) сервер може виконати перевірку кількох можливих значень лічильника $(C \pm n)$, щоб визначити відповідний OTP та синхронізуватися з USB-ключем.

Крок 15**.** Запобігання повторному використанню одноразових паролів.

DRM-система забезпечує блокування будь-яких спроб повторного застосування OTP, що унеможливлює використання перехоплених паролів та мінімізує ризик компрометації системи.

Крок 16. Захист від клонування USB-ключів.

Кожен USB-ключ містить інтегрований апаратний ідентифікатор, який використовується під час формування значення K для генерації унікальних OTP. Завдяки цьому використання підроблених або скопійованих носіїв з іншим ідентифікатором стає неможливим.

Крок 17. Блокування USB-ключа після кількох невдалих спроб автентифікації.

У разі, якщо OTP не проходить перевірку протягом визначеної кількості спроб, доступ до USB-ключа тимчасово призупиняється, що мінімізує ризики атак типу brute-force.

Крок 18. Регулярне оновлення секретного ключа.

DRM-система разом із USB-ключем періодично ініціює генерацію нового секретного ключа (K) для кожної користувацької сесії, забезпечуючи додаткову стійкість до компрометації та запобігаючи повторному використанню застарілих OTP.

Крок 19. Скидання параметрів у випадку виявлення потенційної загрози.

Якщо виявлено ознаки компрометації USB-ключа або несанкціонованого втручання, секретний ключ і значення лічильника скидаються до початкового стану, або USB-ключ переходить у заблокований режим до завершення повторної процедури активації.

Крок 20. Журналювання сесій та контроль безпеки.

DRM-система здійснює реєстрацію всіх сесій доступу, використаних OTP та операцій USB-ключа з метою виявлення аномальної активності, яка може вказувати на можливі спроби несанкціонованого доступу. Аналіз сформованих журналів сприяє зміцненню надійності та підвищенню стійкості алгоритму HOTP.

Додатковим компонентом DRM-рішень є система контролю доступу, яка забезпечує протидію несанкціонованому використанню захищених цифрових ресурсів. Її функціональність передбачає не лише обмеження доступу, а й своєчасне виявлення та реагування на спроби порушення безпеки або зловживання правами.

Здійснимо покроковий опис роботи розробленого алгоритму системи блокування доступу, який охоплює моніторинг аутентифікаційних запитів, управління поточними сеансами та механізми протидії компрометації системи.

Крок 1. Запуск модуля блокування.

На етапі запуску DRM-системи відбувається ініціалізація модуля блокування, який забезпечує відстеження спроб доступу та ведення журналу дій користувачів.

Крок 2. Моніторинг спроб доступу до системи.

Усі запити до модуля автентифікації підлягають автоматичній реєстрації, включно з успішними та невдалими входами, що дозволяє здійснювати подальший аналіз стану безпеки.

Крок 3. Встановлення межі некоректних запитів на автентифікацію.

Для захисту від несанкціонованого доступу задається максимальна кількість допустимих невдалих спроб входу в систему. Після перевищення цього порогу система автоматично блокує доступ.

Крок 4. Аналіз аномальної активності.

Після завершення кожного циклу аутентифікації, система здійснює аналіз активності з метою виявлення аномальних патернів, що можуть включати використання нетипових мережевих ідентифікаторів (IP-адрес) або спроби підключення з несанкціонованих/невідомих пристроїв.

Крок 5. Автоматичне блокування облікового запису після досягнення максимально допустимої кількості невдалих спроб входу в систему.

У разі перевищення встановленої кількості невдалих спроб автентифікації обліковий запис блокується на деякий встановлений час.

Крок 6. Інформування користувача про блокування.

Користувачу надсилається відповідне повідомлення, у якому зазначаються причини обмеження доступу та надаються інструкції щодо подальших дій для відновлення роботи.

Крок 7. Верифікація користувача за допомогою багатофакторної аутентифікації під час відновлення доступу до системи.

По завершенні процедури блокування доступу система вимагає підтвердження особи за допомогою багатофакторної аутентифікації, наприклад, із залученням верифікаційних кодів, надісланих через альтернативні канали зв'язку.

Крок 8. Повторна перевірка автентичності після відновлення доступу до системи.

Після розблокування доступу до системи користувачеві необхідно знову пройти процедуру автентифікації, наприклад, із використанням одноразового пароля.

Крок 9. Журналювання подій доступу.

Система здійснює реєстрацію всіх сесій та ключових дій, що дозволяє проводити подальший аналіз активності та своєчасно виявляти можливі загрози безпеці.

Тестування є невід'ємним етапом життєвого циклу розробки системи, забезпечуючи її функціональну коректність, відповідність встановленим вимогам та стійкість до експлуатаційних навантажень.

У межах перевірки DRM-системи, що використовує динамічне оновлення USB-ключів, механізм HOTP-автентифікації та модуль блокування доступу, проведемо тестування, яке полягає у:

– перевірці правильності формування та валідації одноразових паролів;

– аналізу взаємодії з USB-ключами для зчитування секретних параметрів та підтримання синхронізації лічильників;

– дослідженні працездатності механізму блокування доступу в умовах перевищення допустимої кількості помилкових спроб;

– оцінюванні продуктивності системи за підвищених навантажень;

– аналізі користувацького інтерфейсу з метою забезпечення його зручності та коректної роботи.

Для підтвердження працездатності запропонованої DRM-архітектури та оцінювання її стійкості до актуальних кіберзагроз було проведено комплексне тестування ключових компонентів розробленої системи. Основна увага була приділена перевірці коректності роботи модифікованого алгоритму HOTP, аналізу часових характеристик процесу автентифікації, визначенню стійкості до таких атак як brute-force та replay, а також дослідженню ефективності модуля блокування доступу в умовах підвищеного навантаження. Експериментальне середовище включало сервер DRM-системи, апаратні USB-ключі з реалізованим удосконаленим алгоритмом HOTP та програмний модуль, який імітує користувацькі запити та потенційно шкідливу активність. Отримані результати дозволили всебічно оцінити поведінку систем.

На першому етапі було перевірено коректність генерації та валідації одноразових паролів при послідовному збільшенні значення лічильника. Отримані результати засвідчили стабільне формування OTP без випадків розсинхронізації між USB-ключем та сервером у межах тривалих сесій автентифікації. На рисунку 1 відображено залежність часу генерації одноразового пароля від кількості одночасних запитів: крива має майже лінійний характер із незначним зростанням затримки при збільшенні навантаження, а середній час формування OTP утримується в межах одиниць мілісекунд, що відповідає вимогам до інтерактивних систем керування доступом.

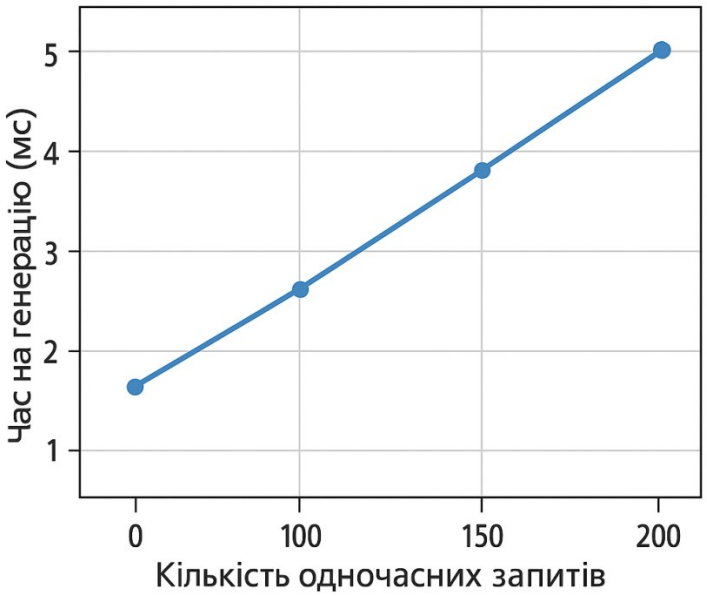

Рис. 1. Залежність часу генерації одноразового пароля (OTP) від кількості одночасних запитів

Оцінювання продуктивності роботи системи при зростанні кількості одночасних запитів користувачів показало, що інтеграція динамічно змінюваних USB-ключів безпеки не призводить до істотної деградації характеристик. На рисунку 2 відображено залежність середнього часу повного циклу автентифікації від кількості паралельних запитів.

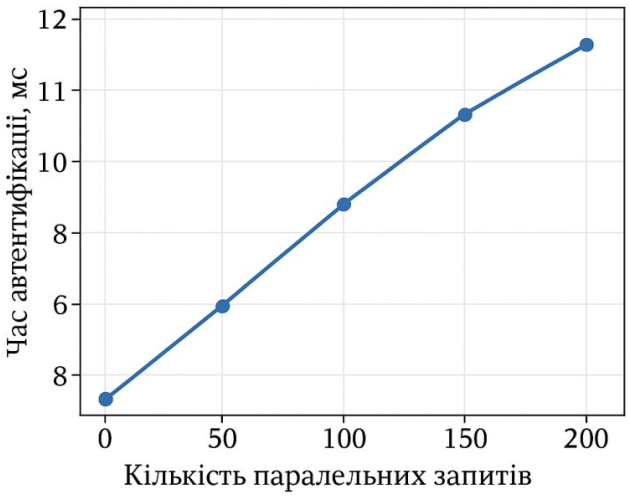

Рис. 2. Залежність середнього часу повного циклу автентифікації від кількості паралельних запитів

Зі зростанням навантаження до умовно граничних значень спостерігається плавне збільшення затримки, однак максимальний час відповіді залишається в межах, прийнятних для практичного використання в реальних DRM-системах.

Результати дослідження демонструють підвищення рівня захищеності DRM-систем управління доступом на основі модифікованого алгоритму динамічно змінюваних ключів безпеки та розробленої адаптивної системи блокування доступу. Проте актуальним є дослідження щодо використання криптографічних протоколів нового покоління, включаючи алгоритми на основі еліптичних кривих та квантово-стійкі схеми автентифікації. Їх інтеграція у структуру USB-ключів може забезпечити додатковий рівень захисту в умовах зростання обчислювальних можливостей зловмисників.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У даному дослідженні було запропоновано архітектуру захищеної DRM-системи, що базується на застосуванні динамічних USB-ключів безпеки з інтеграцією удосконаленого алгоритму HOTP та комплексної системи контролю й блокування доступу для запобігання неавторизованому отриманню доступу до конфіденційного контенту.

Впровадження модифікованого алгоритму HOTP у USB-ключі значно підвищує рівень захищеності DRM-архітектури. Це досягається шляхом динамічної генерації одноразових паролів, використання яких мінімізує ризик несанкціонованого перехоплення або повторного застосування облікових та автентифікаційних даних. Крім того, додатковий захисний ефект від атак на USB-ключі забезпечується динамічним оновленням секретного ключа після кожної завершеної сесії.

Розроблена система блокування доступу передбачає багаторівневий контроль, виявлення підозрілої активності та автоматичне реагування на потенційні загрози. Вона включає механізми протидії несанкціонованим спробам автентифікації, автоматичне блокування після перевищення допустимої кількості невдалих спроб входу в систему, а також застосування багатофакторної автентифікації для безпечного відновлення доступу. Разом з тим, окрему увагу приділено аналізу поведінкових характеристик користувачів та динамічній адаптації порогів спрацювання системи.

Проведене тестування підтвердило ефективність запропонованих рішень: система демонструє стабільну роботу при збільшенні навантаження, мінімальні часові затримки під час генерації та перевірки одноразових паролів. Механізм блокування доступу коректно реагує на несанкціоновані дії, а процес ресинхронізації між сервером та USB-ключем відбувається швидко й без втрати працездатності системи.

Запропонований підхід до розробки DRM-систем із використанням адаптивних USB-ключів та інтелектуальної системи блокування підтверджує свою ефективність у підвищенні загального рівня безпеки, забезпеченні стійкості до атак на ключі та унеможливленні спроб обходу механізмів контролю доступу. Результати роботи можуть бути застосовані й у ширшому контексті, зокрема для систем, що потребують надійного та багаторівневого захисту даних або пристроїв.

References

1. Rewal P., Mishra D., Mishra A., & Rana S. Enhancing security of biometrics based authentication framework for DRM system. Multimedia Tools and Applications. 2023. Vol. 82, no. 26. P. 40857-40871. URL: https://doi.org/10.1007/s11042-023-14891-3

2. Hussain A., & Kiah M. L. M. Ethics, Digital Rights Management, and Cyber Security: A Technical Insight of the Authorization Technologies in Digital Rights Management and the Need of Ethics. In Applied Ethics in a Digital World. 2022. P. 25-44. IGI Global Scientific Publishing. URL: https://doi.org/10.4018/978-1-7998-8467-5.ch003

3. Coates S. K., & Abroshan H. Guideline for the production of Digital Rights Management (DRM). arXiv preprint arXiv:2311.06671. 2023. URL: https://doi.org/10.5121/ijsptm.2023.12403

4. Mishra D., Obaidat M. S., Kasi A., Rewal P., & Mishra A. Construction of a secure and efficient content key distribution framework for DRM systems. International Journal of Communication Systems. 2023. Vol. 36, no. 17, e5605. URL: https://doi.org/10.1002/dac.5605

5. Tiwari A., Shukla P. K., Sharma S., & Mishra N. Algorithms for DRM (Digital Right Management) of OTT (Over the Top) Platforms: A Survey. In 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS). P. 1-6. IEEE. URL: https://doi.org/10.1109/WorldSUAS66815.2025.11199256

6. Mishra D., Rana S. A provably secure content distribution framework for portable DRM systems. J Inform Secur Appl. 2021. Vol. 61. P. 102928. URL: https://doi.org/10.1016/j.jisa.2021.102928

7. Rana S., Mishra D. An authenticated access control framework for digital right management system. Multimed Tools Appl. 2021. Vol. 80. P. 25255-25270. URL: https://doi.org/10.1007/s11042-021-10813-3

8. Khan M.A, Ghani A, Obaidat M.S, Vijayakumar P, Mansoor K, Chaudhry S.A. A robust anonymous authentication scheme using biometrics for digital rights management system. In: 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI) IEEE. 2021. P. 1-5. URL: https://doi.org/10.1109/CCCI52664.2021.9583219

9. Fan Q., Chen J., Wen Y., Luo M. Eland: an efficient lightweight anonymous authentication protocol applied to digital rights management system. J Int Technol. 2022. Vol. 23, no. 2. P. 267-278. URL: https://doi.org/10.53106/160792642022032302007

10. Rewal P., Kasi A., Obaidat M. S., Mishra D., Mishra A., & Hsiao K. F. On the Security of Content key Distribution Framework for DRM systems. In 2022 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI). P. 1-7. IEEE. URL: https://doi.org/10.1109/CCCI55352.2022.9926727