УДК 004.056

О. В. Лесько
В. В. Лукічов

МЕТОД ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З АПАРАТНОЮ ПРИВ'ЯЗКОЮ ДО USB-НОСІЇВ

Вінницький національний технічний університет

Анотація
Запропоновано метод захисту програмного забезпечення з використанням апаратної прив'язки до USB-носіїв у поєднанні з криптографічними механізмами та багатофакторною автентифікацією. Метод передбачає динамічне визначення рівня довіри (Trust Score) та адаптивне відновлення доступу за схемою поділу секрету Шаміра з порогом k, що змінюється від 2 до 5. Наведено принципи формування та розподілу часток секрету, фактори ризику та підходи до відновлення доступу без компрометації головного ключа.
Ключові слова: захист програмного забезпечення, USB-прив'язка, автентифікація, Trust Score, схема Шаміра, криптографія.

Abstract
A method for protecting software using hardware USB-binding combined with cryptographic protection and multi-factor authentication is proposed. The approach includes adaptive trust evaluation (Trust Score), dynamic threshold selection for Shamir Secret Sharing, and secure recovery mechanisms without compromising the master key. Principles of key generation, share storage and recovery scenarios are analyzed.
Keywords: software protection, USB binding, authentication, Trust Score, Shamir secret sharing, cryptography.

Вступ

У сучасних інформаційних системах усе більшого поширення набувають комбіновані методи захисту програмного забезпечення, спрямовані на протидію реверс-інжинірингу, підробці та несанкціонованому використанню [1]. Особливу увагу привертають рішення, що поєднують криптографічні механізми, багатофакторну автентифікацію та апаратні компоненти, оскільки такі системи забезпечують підвищену стійкість до аналізу й обходу захисту [2].

Апаратні рішення, зокрема USB-ключі, забезпечують значно вищий рівень захисту, однак їх використання потребує додаткових механізмів контролю довіри, особливо у контексті зростання кількості атак на автентифікаційні системи.

Сучасні системи захисту програмного забезпечення потребують адаптивних механізмів, які:

- комбінують кілька факторів автентифікації;
- враховують контекст використання (час, місце, історію доступів);
- дозволяють відновити доступ без створення нових ризиків;
- використовують криптографічно стійкі методи формування головного ключа.

Актуальною задачою є розроблення методу захисту програмного забезпечення з апаратною прив'язкою до USB-носіїв, який поєднує криптографічні методи (AES-256, SHA-256), адаптивну багатофакторну автентифікацію та динамічний поріг доступу у схемі Шаміра.

Результати дослідження

Запропонований метод базується на формуванні майстер-ключа S розміром 256 біт та його розподілі між п'ятьма факторами автентифікації: USB-носій, Hardware ID, пароль, TOTP та Recovery-фраза. Розподіл здійснюється за схемою секрет-шерингу Шаміра з поліномом ступеня 4:

$$f(x) = S + a^1x + a^2x^2 + a^3x^3 + a^4x^4 (mod\ p), \qquad (1)$$

де S – головний криптографічний ключ (256 біт); a_1, a_2, a_3, a_4 – випадкові коефіцієнти полінома; x – ідентифікатор фактора автентифікації; p – просте число, що визначає модуль арифметики.

Метод дозволяє встановлювати k у діапазоні від 2 до 5, що забезпечує гнучкість у нормальних умовах та підвищений рівень захисту в ризикованих сценаріях.

При втраті USB або пароля доступ може бути відновлено за рахунок використання мнемонічної фрази (BIP-39) та додаткового фактора (TOTP або HWID) без компрометації майстер-ключа.

Для оцінки ефективності запропонованого методу було проведено порівняльний аналіз його характеристик із поширеними системами апаратного захисту програмного забезпечення. Основні результати наведено в таблиці 1.

Таблиця 1. Порівняння традиційних USB-рішень та запропонованого методу

Система	Характеристика
Dinkey Pro	USB-донгли, захист ПЗ (Windows/Linux)
CodeMeter	Ліцензування + токен, фіксований набір факторів
Matrix Dongle	Класична апаратна прив’язка, без Trust Score
Запропонований метод	Адаптивний поріг k, 5 факторів, Recovery Flow

Аналіз показав, що традиційні USB-донгли забезпечують лише базовий рівень захисту і не враховують поведінкові фактори, контекст доступу чи можливість гнучкого відновлення секрету. На відміну від них, запропонований метод використовує адаптивний поріг k, п’ять незалежних факторів автентифікації та механізм Recovery Flow, що суттєво підвищує стійкість до компрометації USB-носія і до атак, пов’язаних із реверс-інжинірингом.

Висновки

Запропонований метод захисту програмного забезпечення з використанням апаратної прив’язки до USB-носіїв забезпечує підвищений рівень безпеки завдяки поєднанню криптографічного розподілу секрету, багатофакторної автентифікації та адаптивної оцінки рівня довіри. Реалізація схеми Шаміра у поєднанні з динамічним порогом k дозволяє гарантувати, що навіть у разі компрометації окремих факторів отримання майстер-ключа залишається неможливим без достатньої кількості часток. Використання Trust Score мінімізує ризики несанкціонованого доступу, оскільки система автоматично підвищує вимоги автентифікації у потенційно небезпечних ситуаціях.

На відміну від традиційних рішень на основі USB-донглів, запропонований метод не обмежується одним апаратним фактором, а формує багаторівневий механізм перевірки користувача та середовища, що значно ускладнює обхід захисту шляхом реверс-інжинірингу чи підробки пристрою. Наявність Recovery Flow забезпечує можливість безпечного відновлення доступу без розкриття головного ключа, що підвищує надійність системи при реальній експлуатації.

Перспективними напрямами подальших досліджень є розробка гібридних моделей захисту з використанням поведінкової аналітики, а також інтеграція апаратної прив’язки з розподіленими інфраструктурами для підвищення масштабованості та гнучкості системи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Malware Analysis and Reverse Engineering: Unraveling the Digital Threat Landscape [Електронний ресурс] // SSRN. – 2023. (дата звернення: 12.09.2025).

2. Максимець Д. В. Розробка комбінованого методу захисту програмного забезпечення від несанкціонованого використання: Магістерська дисертація. – Київ: КПІ ім. І. Сікорського, 2018. (дата звернення: 14.09.2025).

Лесько Олексій Віталійович — студент групи 1БС-24м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: leskoalesa7@gmail.com

Лукічов Віталій Володимирович – к. т. н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Lesko Oleksii V. — student of 1БС-24м group, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: leskoalesa7@gmail.com.

Lukichov Vitalii V. – Ph.D., Associate Professor, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: lukichov.vitalyi@vntu.edu.ua.