узагальнена оцінка складових криптографічних елементів, без прив'язки до їх реалізацій, розділення підходів оцінки методів та засобів є необхідним. Наведені пропозиції щодо створення такої узагальненої системи оцінювання можуть лягти в основу окремого методу.

1. Prvulovic P, Radosavljevic N, Babic D, Drajic D. HERMEES: A Holistic Evaluation and Ranking Model for Energy-Efficient Systems Applied to Selecting Optimal Lightweight Cryptographic and Topology Construction Protocols in Wireless Sensor Networks. Sensors. 2025; 25(9):2732.
2. The concept of nonlinear cryptographic primitives, their steganographic applications, and related areas of use / Volodymyr Anikin, Serhii Lienkov, Ihor Muliar, Volodymyr Dzhulii, Oleksandr Sieliukov, Yaroslav Melnyk. EUREKA: Physics and Engineering. 2025. № 5. P. 190-204.

Сучасні підходи до безперервної автентифікації користувачів на основі динаміки рухів комп'ютерної миші

УДК 004.056.5:57.087.1

Олександр Корченко[1], Антон Герасименко[2], Імад Ірейфідж[3]

Державний університет інформаційно-комунікаційних технологій,
[1]agkorchenko@gmail.com, [2]anton.hrsmnk@gmail.com,
[3]dr.imad.education@gmail.com

Традиційні методи автентифікації (паролі, токени) стають вразливими до методів соціальної інженерії та витоку даних. Поведінкова біометрія пропонує концепцію безперервної автентифікації (Continuous Authentication), яка дозволяє верифікувати особу не лише в момент входу в систему, а протягом усієї сесії роботи. Рух миші є унікальним для кожної людини через індивідуальні особливості нейромоторної координації, що робить його перспективним об'єктом дослідження.

Методологія вилучення ознак (Feature Extraction) при автентифікації користувачів за рухом миші. Для ідентифікації користувача координати курсора x та y перетворюються на набір статистичних та кінематичних ознак. Основні параметри включають: швидкісні показники (миттєва швидкість v та прискорення a), траєкторні ознаки (кривизна руху, кутова швидкість та "джиттер", тобто мікротремтіння), часові ознаки (час реакції між появою стимулу та початком руху, тривалість пауз - dwell time), операційні ознаки (частота кліків, швидкість подвійного натискання, манера прокручування коліщатка).

Основні алгоритми машинного навчання та класифікації при автентифікації користувачів за рухом миші. Сучасні дослідження фокусуються на двох підходах до навчання моделей:

Однокласова класифікація (One-Class Classification): Модель навчається лише на даних легітимного користувача (наприклад, алгоритм Isolation Forest або One-Class SVM). Система шукає аномалії, які свідчать про те, що за комп'ютером перебуває інша особа.

Глибоке навчання (Deep Learning): Використання рекурентних нейронних мереж (LSTM) та згорткових мереж (CNN). Ці архітектури здатні вловлювати складні часові залежності в послідовності рухів, які неможливо описати простими статистичними формулами.

За даними актуальних досліджень, показник помилкового відхилення (FRR) та помилкового допуску (FAR) у таких системах варіюється в межах 2–7%, що є достатнім для використання у ролі другого фактору захисту.

Проаналізуємо недоліки традиційної автентифікації та поведінкової біометрії.

Таблиця 1

Недоліки традиційної автентифікації та поведінкової біометрії

Аспект	Традиційний пароль	Поведінкова біометрія
Стійкість до фішингу	Низька (можна виманити)	Абсолютна (неможливо передати)
Час дії	Тільки при вході	Безперервно (кожні 10-30 секунд)
Зручність (UX)	Вимагає зусиль від користувача	Повністю прозоро (Zero Friction)
Спроба злому	Брутфорс або підбір	Вимагає робота-маніпулятора, що імітує людину

Але поведінкова біометрія має і недоліки. Попри високу ефективність, існують фактори, що знижують точність розпізнавання:

- Hardware-залежність: Зміна роздільної здатності екрана або перехід з миші на тачпад радикально змінює поведінковий профіль.
- Психофізіологічний стан: Стрес, втома або хвороба користувача впливають на мікромоторику.
- Контекст діяльності: Рухи миші під час гри суттєво відрізняються від рухів під час роботи в офісних програмах.

Висновки: Динаміка рухів миші є надійним та маловитратним методом біометричної ідентифікації. Найбільш перспективним напрямом розвитку є створення гібридних моделей, що поєднують аналіз рухів миші з динамікою натискання клавіш (Keystroke Dynamics), що дозволяє досягти майже нульового показника помилок у корпоративних мережах.

1. Antal, M.; Egyed-Zsigmond, E. Intrusion detection using mouse dynamics. IET Biom. 2019, 8, 285–294.
2. Siami-Namini, S.; Tavakoli, N.; Namin, A.S. The performance of LSTM and BiLSTM in forecasting time series. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 3285–3292.
3. Ahmed, A.A.E.; Traore, I. A new biometric technology based on mouse dynamics. IEEE Trans. Dependable Secur. Comput. 2007, 4, 165–179.