МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ВІСНИК ВІННИЦЬКОГО ПОЛІТЕХНІЧНОГО ІНСТИТУТУ

Науковий журнал

Засновник і видавець: Вінницький національний технічний університет

Виходить 6 разів на рік Заснований у грудні 1993 року

№ 2 (167) 2023

Схвалено Вченою радою
Вінницького національного технічного університету,
протокол № 12 від 4.05.2023 р.

Вінниця · ВНТУ · 2023

Журнал «Вісник Вінницького політехнічного інституту» є виданням, яке входить до Переліку наукових фахових видань України у галузі технічних наук (**категорія Б**) за спеціальностями: 121, 122, 123, 124, 125, 126, 131, 132, 133, 141, 144, 151, 152, 163, 172, 183, 275, а також 01.05.00, 05.02.02, 05.02.10, 05.03.05, 05.09.03, 05.11.00, 05.13.05, 05.13.06, 05.12.13, 05.12.20, 05.14.02, 05.14.06, 05.22.20, 05.23.02, 05.23.05 (накази Міністерства освіти і науки України: від 11.07.2019 р. та № 975, від 15.10.2019, № 1301);

Журнал входить у міжнародні наукометричні бази Index Copernicus International та Google Scholar і реферується в Українському реферативному журналі «Джерело».

Журнал публікує статті, які містять нові теоретичні та практичні результати в галузях технічних, економічних, природничих та гуманітарних наук. Публікуються також огляди сучасного стану розв'язання важливих наукових проблем, огляди наукових та методичних конференцій, які відбулися у ВНТУ, статті з педагогіки вищої освіти.

Розділи журналу:

- автоматика та інформаційно-вимірювальна техніка;
- будівництво;
- гуманізація і гуманітаризація технічної освіти;
- застосування результатів досліджень;
- екологія та екологічна безпека;
- економіка та менеджмент;
- енергетика, електротехніка та електромеханіка;
- інформаційні технології та комп'ютерна техніка;
- машинобудування і транспорт;
- радіоелектроніка та радіоелектронне апаратобудування;
- стратегія, зміст та нові технології підготовки спеціалістів з вищою технічною освітою;
- рецензії;
- ювілеї і ювіляри.

Сайт журналу https://visnyk.vntu.edu.ua/

DOI журналу https://doi.org/10.31649/1997-9266

Адреса редакції:
ВНТУ, к. 112 ГНК,
вул. Хмельницьке шосе, 95,
м. Вінниця, Україна, 21021

Контакти:

E-mail: visnykvpi@gmail.com

Відповідальний за випуск Дерібо О. В.

ЗМІСТ

DOI випуску https://doi.org/10.31649/1997-9266-2023-167-2

ЕКОЛОГІЯ, ЕКОЛОГІЧНА БЕЗПЕКА

ЕНЕРГЕТИКА, ЕЛЕКТРОТЕХНІКА ТА ЕЛЕКТРОМЕХАНІКА

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КОМП'ЮТЕРНА ТЕХНІКА

МАШИНОБУДУВАННЯ ТА ТРАНСПОРТ

РАДІОЕЛЕКТРОНІКА ТА РАДІОЕЛЕКТРОННЕ АПАРАТОБУДУВАННЯ

CONTENTS

Issue DOI https://doi.org/10.31649/1997-9266-2023-167-2

ECOLOGY AND ENVIRONMENTAL SECURITY

ENERGY GENERATION, ELECTRIC ENGINEERING AND ELECTROMECHANICS

INFORMATION TECHNOLOGIES AND COMPUTER ENGINEERING

MECHANICAL ENGINEERING AND TRANSPORT

RADIOELECTRONICS AND RADIOELECTRONIC EQUIPMENT MANUFACTURING

https://doi.org/10.31649/1997-9266-2023-167-2-102-111

УДК 004.056.523.052(045)

О. В. Салієва[1]
І. С. Зоря[1]
І. О. Бондаренко[1]
М. О. Берестенко[1]

ПІДВИЩЕННЯ ДОСТОВІРНОСТІ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА НА ОСНОВІ ЗАХИЩЕНОГО ЕЛЕКТРОННОГО КЛЮЧА ТА ПОВЕДІНКОВОЇ БІОМЕТРІЇ

[1]Вінницький національний технічний університет

Стрімке поширення програмних додатків у всіх сферах людської діяльності зумовлює потребу забезпечення захисту даних, що містяться у них. Тому, наразі актуальними є питання, що стосуються вдосконалення методів автентифікації для запобігання несанкціонованого доступу до програмних ресурсів. Для розв'язання цих задач важливо врахувати, що різні типи систем висувають свої унікальні вимоги до підсистем автентифікації. До того ж, активний розвиток обчислювальної техніки обумовлює можливість зламу алгоритмів автентифікації, які ще декілька років тому вважалися надійними. У зв'язку з цим, у роботі пропонується підвищити достовірність автентифікації користувача на основі захищеного електронного ключа з використанням алгоритму AES та аналізу ентропії рухів мишки, що є індивідуальною характеристикою для кожної особи. Реалізація електронного ключа визначена такими його перевагами: зменшення витрат, підвищення зручності користування, зниження ймовірності втрати чи крадіжки та зменшення ризику атак через посередника. Аналіз ентропії рухів мишки дозволить здійснити автентифікацію користувача на основі біометричних поведінкових характеристик, які є універсальними, унікальними та постійними. Описуючи алгоритм процесу аналізу ентропії мишки, варто зауважити, що особливістю відстежування динамічних поведінкових характеристик є те, що користувач переміщає курсор мишки по складній кривій зі швидкістю, що змінюється у процесі переміщення. Форма кривої лінії і швидкість руху курсора обумовлені низкою фізіологічних та психологічних чинників, зокрема таких як: розмір й маса руки, положення руки і всього тіла, стан нервової системи, звичок користувача тощо. Для удосконалення алгоритму автентифікації користувача розроблено електронний ключ з використанням технології JSON Web Tokens, яка дозволяє уникнути помилок автентифікації, збільшити продуктивність та масштабованість додатку. Тестування розробленого програмного продукту буде виконано на основі unit-тестів та дослідження показників FAR та FRR.

Ключові слова: інформаційна система, двофакторна автентифікація, електронний ключ, ентропія рухів мишки.

Вступ

Широке розповсюдження електронних ресурсів в сучасних інформаційних системах (ІС) стимулює інтенсивний розвиток методів та засобів забезпечення їхньої захищеності. Одним з основних і невід'ємних елементів системи безпеки є процедура автентифікації користувача, яка полягає у перевірці відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи щодо належності його цьому об'єкту; встановлення або підтвердження автентичності [1].

На сьогодні спостерігається активне використання систем автентифікації у різних сервісах та порталах. Найпоширенішою є двофакторна автентифікація, яка є технологією, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів, зокрема таких як: електронні ключі, біометричні характеристики, паролі, коди доступу, магнітні карти та ін.

Особливий інтерес викликає біометрична автентифікація, яка поділяється на статичну та динамічну/поведінкову, і є прогресивним методом захисту облікових записів користувачів та підтвердження їхньої автентичності. У разі вдалої комбінації біометрії з іншими факторами, система

здатна захистити інформацію як від внутрішніх загроз, так і від зовнішніх вторгнень, оскільки використання кількох незалежних факторів значно зменшує ймовірність, що вони будуть використані одночасно.

Двофакторна автентифікація є додатковим бар'єром захисту доступності, цілісності та конфіденційності даних, що циркулюють в ІС.

Аналіз проблеми та постановка задачі

Дослідження питань щодо удосконалення методів автентифікації проведено у безлічі наукових праць. Так, у [2] запропоновано модель автентифікації користувачів ІС, яка ґрунтується на використанні поведінкової біометрії та математичного апарату теорії нечіткої логіки. Автори роботи [3] здійснили аналіз наявних методів автентифікації та зазначили переваги методу з використанням тесту Люшера. У науковій праці [4] представлено удосконалений метод автентифікації користувачів ІС за їхнім рукописним почерком, який за рахунок автоматизації процесу відбору контрольних точок у зразках та використання ймовірнісної нейронної мережі, збільшує імовірність правильного розпізнавання користувачів ІС. Щодо біометричної автентифікації, то у роботі [5] проаналізовано наявні методи захисту біометричного шаблону, розглянуто різноманітні атаки на системи біометричного розпізнавання, а в [6] розглядаються сучасні підходи до розробки схеми захисту для біометричних шаблонів.

На основі аналізу додатків двофакторної автентифікації [7]—[11] виявлено такі недоліки як використання одного набору генерації для всіх підключень, можливість контролю та доступу до інформації фірмою розробником. Тому актуальною є розробка програмного додатку з модифікованими засобами реалізації двофакторної автентифікації. Для вирішення цього завдання доцільно використати біометричну поведінкову систему на основі аналізу ентропії мишки як одного з факторів підвищення достовірності автентифікації користувача. Як інший фактор автентифікації варто вибрати електронний ключ, суть роботи якого базується на ефективному, гнучкому та безпечному використанні програмних токенів.

Таким чином, *метою роботи* є розробка вдосконаленого методу для підвищення достовірності автентифікації користувача на основі захищеного електронного ключа та аналізу ентропії рухів мишки.

Удосконалення алгоритму автентифікації користувача

Удосконалення алгоритму автентифікації користувача у захищеному додатку полягає у реалізації двофакторної автентифікації та застосуванні захищеного електронного ключа з використанням алгоритму AES та аналізу ентропії рухів мишки, що є індивідуальною характеристикою для кожного користувача.

Пропонується такий алгоритм автентифікації користувача у захищеному додатку.

Крок 1. Запуск виконуваного файлу додатку.

Крок 2. Здійснення процесу автентифікації користувача.

Крок 2.1. Якщо користувач вже має обліковий запис у системі — перехід до кроку 6.

Крок 2.2. Якщо користувачеві необхідно отримати доступ до системи — перехід до кроку 3.

Крок 3. Реєстрація користувача.

Крок 3.1. Заповнення користувачем персональних даних.

Крок 3.2. Здійснення процесу аналізу рухів мишки.

Крок 3.3. Підтвердження процесу реєстрації.

Крок 4. Перевірка форм заповнених користувачем.

Крок 4.1. Якщо усі дані введені правильно та сформовано зразок рухів мишки, то запит на реєстрацію підтверджується.

Крок 4.2. Якщо форма реєстрації заповнена неправильно, користувачеві виводиться на екран відповідне сповіщення, а форма реєстрації потребує повторного заповнення.

Крок 5. Підтвердження реєстрації користувача з боку адміністратора.

Крок 5.1. Адміністратор перевіряє нового користувача за його обліковими даними.

Крок 5.2. Якщо такому користувачу необхідно надати доступ до системи — ставить відповідну відмітку для розмежування доступу.

Крок 5.3. Адміністратор формує електронний ключ, що надсилається користувачу.

Крок 5.4. Збереження внесених змін.

Крок 6. Здійснення процесу автентифікації користувача.

Крок 6.1. Заповнення користувачем поля для введення логіну.

Крок 6.2. Завантаження електронного ключа.

Крок 6.3. Здійснення процесу аналізу рухів мишки.

Крок 6.4. Підтвердження процесу автентифікації.

Крок 7. Перевірка надання користувачеві доступу до системи.

Крок 7.1. Якщо логін та ключ користувача коректні, зразок ентропії рухів мишки відповідає зареєстрованому — користувач отримує доступ.

Крок 7.2. Якщо один із факторів не відповідає вимогам — користувачу виводиться на екран сповіщення про невдалу спробу автентифікації. У випадку, якщо користувач тричі здійснюватиме некоректний вхід — доступ до облікового запису заблоковується, електронний ключ буде недійсним. Для його поновлення потрібно звернутись до адміністратора та отримати новий електронний ключ на основі refresh-токену.

Крок 8. Після успішної автентифікації користувачеві надається доступ до системи.

Алгоритм формування захищеного електронного ключа

Першим етапом автентифікації користувача у захищеному додатку є застосування електронного ключа, розробка якого здійснюється з використанням технології JSON Web Tokens (JWT), що дозволяє уникнути помилок автентифікації, збільшити продуктивність та масштабованість додатку.

Структурно JWT складається з трьох частин: header (заголовок), payload (корисне навантаження), signature (підпис).

Після формування стрічки токену відбувається її шифрування за алгоритмом AES та передавання користувачеві, який пройшов етап реєстрації.

У межах роботи механізм формування токену вбудовуваний в основний програмний додаток.

Алгоритм формування електронного ключа за технологією JWT показано на рис. 1.

Опишемо використання електронного ключа на основі технології JWT.

Крок 1. Застосування даних користувача для запиту на формування токену.

Крок 2. Перевірка інформації користувача.

Крок 3. Формування електронного ключа та його шифрування.

Крок 4. Надання ключа користувачу.

Крок 5 Зберігання користувачем токену та прикріплення його значення до кожного запиту.

Крок 6. Надання доступу користувачеві після перевірки ключа системою.

Крок 7. Можливість відновлення доступу на основі електронного ключа з використанням refresh-токену.

На відмінну від класичної схеми [12], запропонований алгоритм дозволяє не зберігати інформацію про всі видані токени. Для входу в систему користувач передає свій токен, а додатку потрібно лише перевірити підпис і скористатися необхідними полями з розділу «Корисне навантаження».

Алгоритм процесу аналізу ентропії рухів мишки

Для визначення ентропії рухів комп'ютерної мишки здійснимо аналіз таких показників:

– траєкторія руху комп'ютерної мишки;

– відхилення руху комп'ютерної мишки від зафіксованої траєкторії;

– швидкість руху комп'ютерної мишки;

– прискорення руху комп'ютерної мишки;

– нетипові рухи комп'ютерної мишки;

– кліки комп'ютерної мишки.

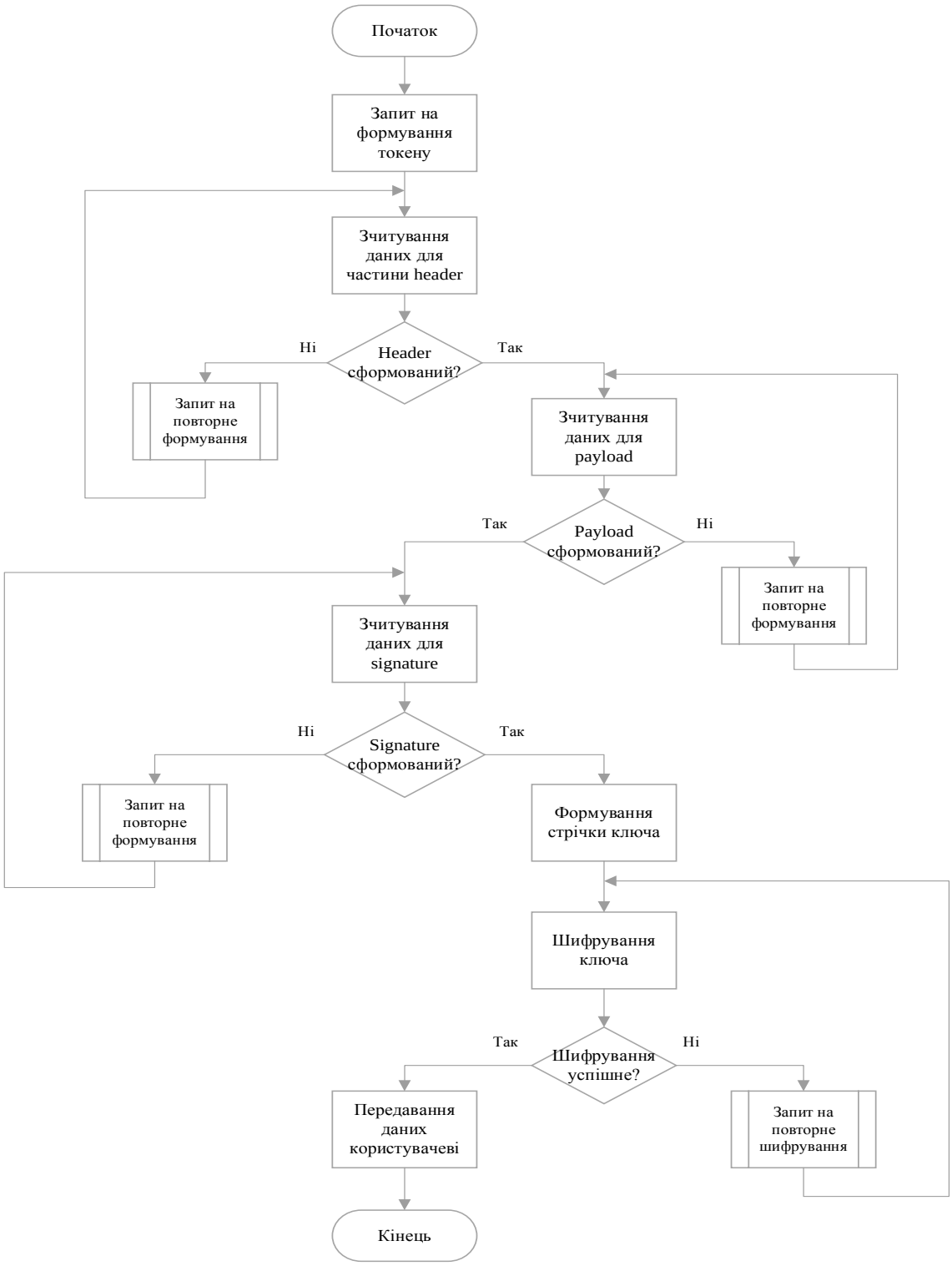

Рис. 1. Алгоритм формування електронного ключа

Щоб дослідити траєкторію руху комп'ютерної мишки застосуємо метод відслідковування кривих та розбиття їх на окремі вектори.

Алгоритм дослідження цього показника складається з п'яти кроків.

Крок 1. Спрощення траєкторії, за якою рухалась мишка та розбиття її на окремі вектори на основі алгоритму Дугласа–Пекера [13].

Крок 2. Обчислення довжини векторів

$$b = \frac{d\left(P_{0,}P(b)\right)}{d\left(P_{0,}P_1\right)} = \frac{|w|\cos\theta}{v_1} = \frac{w \cdot v_1}{|v_1|^2} = \frac{w \cdot v_1}{v_1 \cdot v_1},$$

де P_0, P_1 проекція вектора P_0, P на відрізок P_0, P_1, $v_1 = (P_1 - P_0)$, $w = (P - P_0)$.

Крок 3. Перетворення векторів в косинус кута нахилу відносно осі x та y

$$< L = (\cos\alpha, \cos\beta).$$

Це перетворення дозволить отримати набір даних в діапазоні [–1; 1].

Крок 4. Розпізнавання образу за допомогою багатошарового персептрона

$$f_n = \frac{\left|\frac{g_1}{a_1}\right| + \left|\frac{g_2}{a_2}\right| + |\ldots| + \left|\frac{g_m}{a_m}\right|}{m},$$

де m — кількість параметрів образу, g — параметри оброблюваного образу, a — параметри еталонних образів.

Варто зазначити, що в цій операції кількість входів в багатошаровий персептрон дорівнює кількості образів у програмі.

Крок 5. Виконання дій, асоційованих з розпізнаним образом.

Якість розпізнавання за цим алгоритмом залежить від ступеня відмінності використовуваних зразків, тобто чим менша кількість схожих зразків у програмі, тим вища якість розпізнавання.

Для дослідження відхилення руху комп'ютерної мишки від зафіксованої траєкторії застосуємо формулу для розрахунку евклідової відстані: $length((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - by_2)^2}$, де x_1 та y_1 — координати курсора, які потрібно врахувати для дослідження горизонтальних та вертикальних відхилень; x_2 та y_2 — координати точки.

Пропорційна близькість обчислюється за формулою $proximity = 1 - length / max(length)$.

Отримані показники надають можливість відстежувати відстань мишки від еталонної точки до отриманої в кожному коректному випадку.

Відносна різниця між довжиною траєкторії, пройденої курсором комп'ютерної мишки та довжиною лінії, що поєднує початкову та кінцеву точки переміщення курсора мишки, позначається δD та розраховується за формулою

$$\delta D = \frac{D - D_{min}}{D_{min}}.$$

Показники горизонтальної, вертикальної та загальної швидкості переміщення курсора обчислюються за формулами

$$V_{X_i} = \frac{\delta x_i}{\delta t_i}; \quad V_{Y_i} = \frac{\delta y_i}{\delta t_i}; \quad V_i = \sqrt{V_{X_i}^2 + V_{Y_i}^2}, \quad i = 2\ldots n,$$

де $\delta t_i = t_i - t_{i-1}$; $t_1 = 0$; $V_{X_1} = 0$; $V_{Y_1} = 0$; $V_1 = 0$.

Показники прискорення, ривка та кутової швидкості визначаються за такими формулами:

$$a_i = \frac{\delta V_i}{\delta t_i}; \quad j_i = \frac{\delta a_i}{\delta t_i}; \quad \omega_i = \frac{\delta \Theta_i}{\delta t_i}, \quad i - 2\ldots n,$$

де $a_1 = 0$; $j_1 = 0$; $\omega_1 = 0$.

Для знаходження загального прискорення переміщення курсора використовується формула

$$a(t) = \frac{a_x(t)}{\sqrt{1 + \left(\frac{a_y(t)}{a_x(t)}\right)^2}} + \frac{a_y(t)}{\sqrt{1 + \left(\frac{a_x(t)}{a_y(t)}\right)^2}}.$$

До того ж, для представлення даних потрібно знайти додаткові параметри

$$r = \sum_{i=1}^{n} \sqrt{\delta x_i^2 + \delta y_i^2},$$

де r — довжина траєкторії;

$$L = \sqrt{\left(x_n - x_1\right)^2 + \left(y_n - y_1\right)^2},$$

де L — довжина відрізка між двома кінцевими точками траєкторії;

$$s = \frac{L}{r},$$

де s — прямолінійність траєкторії;

$$T = t_n - t_1,$$

де T — час виконання дії.

Далі опишемо процес оцінювання нетипових рухів комп'ютерної мишки для визначення складності траєкторії. У випадку наявності усіх необхідних для обчислення параметрів x та y за певний час, можна розрахувати зрушення між кожним кроком за нормалізований час відповідно

$$\Delta x = x_{timestep+1} - x_{timestep};$$

$$\Delta y = y_{timestep+1} - y_{timestep}.$$

Наступним кроком є обчислення кількості однакових вікон *x*-зрушення розміром M_m та M_{m+1} та середньої кількості схожих вікон.

Ентропію можна розрахувати за формулою $\Delta S = In\left[M_m\right] - In\left[M_{m+1}\right].$

Застосуємо зональний клік-тест для дослідження кліків комп'ютерної мишки користувачем.

Алгоритм дослідження клік-тесту буде мати такий вигляд.

Крок 1. Здійснення користувачем кліків мишкою у певних зонах.

Крок 2. Фіксування параметрів кліків у вигляді карти координат.

Крок 3. Формування звіту характеру кліків для кожного користувача.

Крок 4. Зіставлення еталонних значень з отриманими під час кожного випадку автентифікації користувача.

Крок 5. Визначення ентропії.

Тестування та аналіз результатів розробки

Після розробки усіх необхідних алгоритмів, здійснено програмну реалізацію додатку у середовищі Visual Studio на мові C#.

Реалізуємо тестування створеного додатку за допомогою unit-тестів та показників *FAR* та *FRR*.

Застосуємо unit-тести [14] для перевірки таких сценаріїв:

– правильне введення логіну і неправильний ключ;
– правильне введення логіну і некоректна ентропія;
– некоректний логін, ключ та правильна ентропія;
– некоректний логін, ентропія рухів та правильний ключ;
– коректне введення пароля, ключа, рухів мишки.

Для забезпечення надійності аналізу на основі рухів мишки, протестуємо десятьох учасників, мета яких — повторити задані рухи мишкою еталонного користувача.

Досліджуватиметься шість показників, за якими здійснюється аналіз:

– траєкторія руху комп'ютерної мишки;
– відхилення руху комп'ютерної мишки від зафіксованої траєкторії;
– швидкість руху комп'ютерної мишки;
– прискорення руху комп'ютерної мишки;
– нетипові рухи комп'ютерної мишки;
– кліки комп'ютерної мишки.

На рис. 2 показано діаграму, яка відображає відмінність еталонного зразка користувача від показників, отриманих у результаті тестування десятьох учасників.

Аналізуючи цю діаграму, бачимо, що хоча й структура показників схожа, проте кількісні дані суттєво відрізняються, адже поведінкова біометрична характеристика на основі рухів мишки є індивідуальною для кожного користувача.

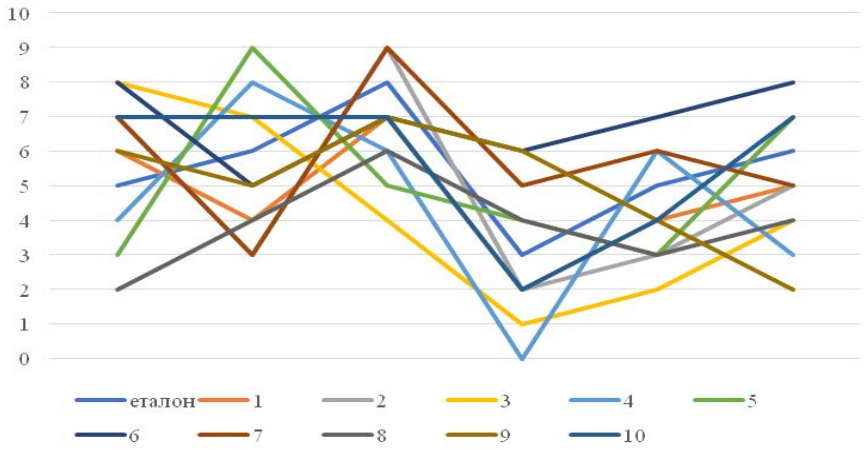

Рис. 2. Дослідження зміни показників

Для оцінювання запропонованого методу аналізу рухів мишки застосуємо показники біометричної ідентифікації [15]

$$FAR = \frac{NFA}{NIVA},$$

де FAR — ймовірність помилкового доступу, NFA — кількість фактів помилкового доступу, $NIVA$ — загальна кількість звернень до системи.

$$FRR = \frac{NFF}{NIVA},$$

де FRR — ймовірність помилкової відмови в доступі, NFF — кількість фактів відмови в доступі, $NIVA$ — загальна кількість звернень до системи.

Проаналізуємо роботу удосконаленого методу автентифікації у порівнянні з іншими методами.

У таблиці 1 наведено показники *FAR* і *FRR* автентифікації для п’яти користувачів, які здійснювали спробу входу по десять разів за кожним методом.

Таблиця 1

Порівняння розробки з існуючими методами (показники *FAR* і *FRR*, %)

Метод	*FAR*	*FRR*	*FAR*	*FRR*	*FAR*	*FRR*	*FAR*	*FRR*	*FAR*	*FRR*
Гістограмний метод	33	39	38	33	34	32	31	39	33	37
Метод на основі клавіатурного почерку	34	45	35	37	32	41	39	45	32	38
Запропонований метод	21	27	26	28	22	24	23	25	22	24

Далі проведемо дослідження для порівняння запропонованого методу та методу на основі нейронної мережі за участі десятьох учасників, які здійснювали спробу входу по десять разів за кожним методом. Результати проведеного дослідження показані на рис. 3 та 4.

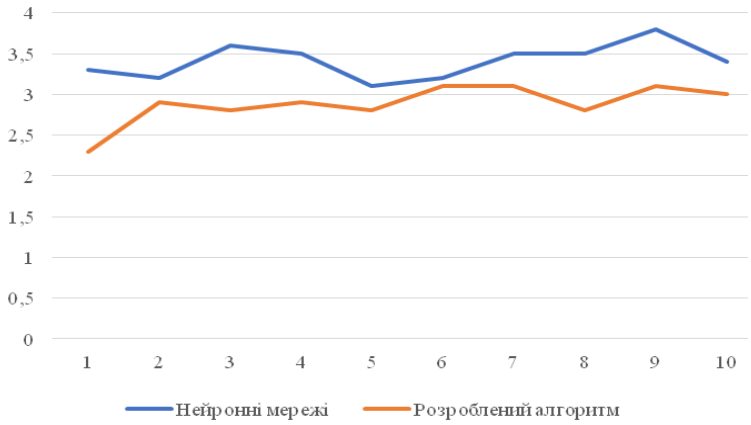

Рис. 3. Показники ймовірності помилкового доступу

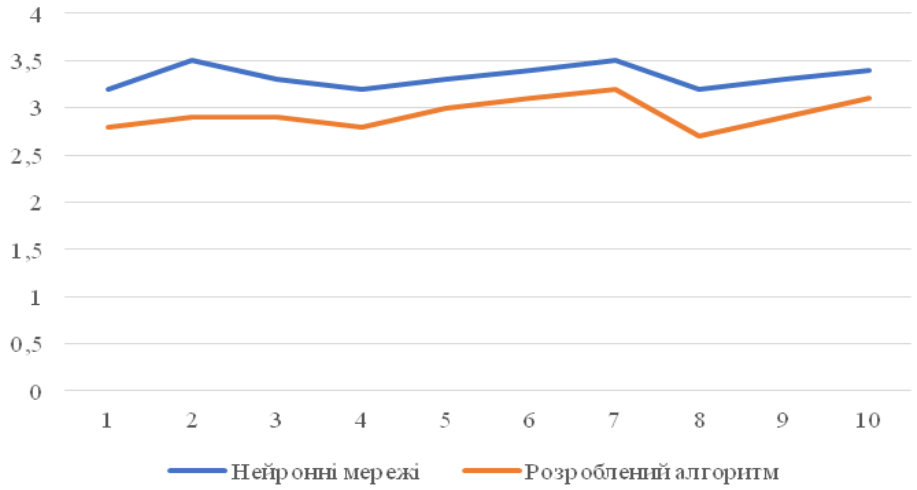

Рис. 4. Показники ймовірності помилкової відмови у доступі

Отримані результати тестування якості біометричних показників, стійкості токена та тестове практичне застосування розробленого додатку на основі запропонованого методу свідчить про те, що розроблений алгоритм біометричної автентифікації показав кращі результати.

Окрім цього, визначимо оцінку підвищення достовірності аутентифікації шляхом порівняння отриманих у ході тестування показників. За результатами першого досліду достовірності показників методу розпізнавання за клавіатурним почерком, гістограмним методом та розроблюваним методом, якість отриманих показників підвищена у середньому на 12 % (див. табл. 1). За результатами другого досліду показники ймовірності помилкового доступу та показники ймовірності помилкової відмови у доступі на основі аналізу ентропії рухів мишки нижчі ніж у протестованої нейронної мережі (див. рис. 3, рис. 4). Відсоток помилкового доступу для нейронної мережі становить 35 %, а для запропонованого методу — 26 %. Відсоток помилкової відмови у доступі для нейронної мережі становить 33 %, для запропонованого методу — 26 %.

Результати підвищення достовірності автентифікації на основі токену є якісною характеристикою запропонованого удосконалення. Зокрема, для дослідження отриманих результатів по роботі з токеном, застосовано платформу Postman [16], що дозволяє здійснити тестування розробки. Проведено такі перевірки:

1) надсилання запиту без JWT для перевірки того, що дані зможуть повернутися;

2) редагування/видалення одного символу з JWT, для перевірки того, що дані не повернуться під час використання такого токена всередині запиту;

3) декодування коректного JWT всередині налагоджувача, редагування даних в ньому з метою тестування того, чи зможе він функціонувати в запиті;

4) перевірка, коли закінчується термін дії JWT, і спроба надіслати запит із відповідним токеном, щоб протестувати, що надіслані дані не будуть повернуті;

5) розгортання нового JWT, термін дії якого почнеться в майбутньому, і тестування того, що дані не будуть повернуті;

6) декодування JWT і перевірка того, чи в його структурі не зберігаються персональні дані користувача.

Усі наведені тести для реалізованого токену пройдені успішно. Порівняно з класичною схемою [12], розроблений алгоритм токену мав кращі показники захищеності у разі здійснення декодування. Такий результат зумовлений тим, що у запропонованому алгоритмі токену не передбачено зберігання даних про попередні версії токену, а відповідно у разі його зламу зловмисник отримає менше суттєвих даних із персональною інформацією про користувача, що вплине на ефективність та результативність такого зламу, неможливість відновити дані токену та відповідно отримати доступ до системи на основі облікового запису власника цього токену.

Ще одним результатом запропонованого методу є зменшення часових витрат під час його реалізації. Адже за запропонованим методом двофакторної автентифікації завдяки використанню електронного ключа не виникає необхідності очікувати підтвердження автентифікації від адміністратора системи, а аналіз ентропії рухів миші не потребує довготривалого навчання нейронної мережі.

Таким чином, запропонований метод двофакторної автентифікації користувачів вирішує поставлене завдання роботи, а саме підвищення достовірності розпізнавання користувачів системи. Враховуючи кількісні та якісні дані наведених показників вважатимемо, що достовірність автентифікації за цим методом підвищена орієнтовно на 11 %.

Висновки

У роботі підвищено достовірність автентифікації користувача на основі захищеного електронного ключа та поведінкової біометрії.

Для досягнення мети удосконалено алгоритм автентифікації користувача у захищеному додатку. Для цього реалізовано двофакторну автентифікацію на основі аналізу ентропії рухів мишки, яка є індивідуальною характеристикою для кожного користувача. Окрім того, застосовано електронний ключ, який містить дані користувача та має відповідний захист криптографічним алгоритмом AES, що зумовлює його стійкість до зламу.

Застосування програмного електронного ключа зумовлено такими його перевагами: зменшення витрат, підвищення зручності користування, зниження ймовірності втрати чи крадіжки та зменшення ризику атак через посередника.

Аналіз ентропії рухів мишки дозволив здійснити автентифікацію користувача на основі біометричних поведінкових характеристик, які є універсальними, унікальними й постійними.

Проведений аналіз програмної розробки показав, що додаток працює коректно, unit-тести забезпечують позитивний результат, що підтверджує відсутність помилок у написаному коді. Результати тестування за показниками *FAR* та *FRR* свідчать про підвищення достовірності розпізнавання користувачів на 11 %. Стійкість до зламу електронного ключа зумовлена вибраною технологією JWT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу,» *НД ТЗІ 1.1-003-99*, чинний від 01.07.1999.

[2] В. В. Фесьоха, і Н. О. Фесьоха, «Модель нечіткої автентифікації користувачів інформаційних систем органів військового управління на основі поведінкової біометрії,» *Захист інформації,* т. 23, № 2, с. 116-123, 2021.

[3] О. В. Горбенко, Ю. Л. Горбенко, А. Ю. Горбенко, і О. М. Сівоха, «Захист інформаційних систем за допомогою використання методів автентифікації,» *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського*, с. 79-85, 2020.

[4] О. Г. Корченко, А. М. Давиденко, і О. О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних,» *Захист інформації*, т. 21, № 1, с. 40-51, 2019.

[5] P. Jayapriya, R. R. Manimegalai, and R. Kumar Lakshmana, "A Survey on Different Techniques for Biometric Template Protection," *Journal of Internet Technology*, vol. 21, no. 5, 2020.

[6] A. Sarkar, and Binod K. Singh, "A Review on Different Biometric Template Protec-tion Methods," *Recent Advances in Computer Science and Communications*, vol. 14, issue 5, pp. 1551-1572, 2021.

[7] Google Authenticator. GooglePlay. [Electronic resource]. Available: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=uk&gl=US . Accessed: 15 March 2023.

[8] Duo Mobile. *GooglePlay*. [Electronic resource]. Available: https://play.google.com/store/apps/details?id=com.duosecurity.duomobile&hl=uk&gl=US. Accessed: 15 March 2023.

[9] Microsoft Authenticator. *GooglePlay*. [Electronic resource]. Available: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=uk&gl=US. Accessed: 15 March 2023.

[10] Free OTP. *GooglePlay*. [Electronic resource]. Available: https://play.google.com/store/apps/details?id=org.liberty.android.freeotpplus&hl=uk&gl=AZ. Accessed: 15 March 2023.

[11] Authy. *GooglePlay*. [Electronic resource]. Available: https://play.google.com/store/apps/details?id=com.authy.authy&hl=uk&gl=US. Accessed: 15 March 2023.

[12] *JSON Web Tokens*. [Electronic resource]. Available: https://auth0.com/docs/secure/tokens/json-web-tokens. Accessed: 15 March 2023.

[13] Douglas-Packer algorithm. *Towardsdatascience*. [Electronic resource]. Available: https://towardsdatascience.com/simplify-polylines-with-the-douglas-peucker-algorithm-ac8ed487a4a1. Accessed: 20 March 2023.

[14] Unit testing. *Techtarget.* [Electronic resource]. Available: https://www.techtarget.com/searchsoft warequality/definition/unit-testing#:~:text=Unit%20testing%20is%20a%20software,independently%20scrutinized%20for%20proper%20operation. Accessed: 20 March 2023.

[15] FAR and FRR: security level versus user convenience. *Recogtech*. [Electronic resource]. Available: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience. Accessed: 20 March 2023.

[16] Postman. *Офіційний сайт Postman.com* [Electronic resource]. Available: https://www.postman.com. Accessed: 20 March 2023.

Рекомендована кафедрою менеджменту та безпеки інформаційних систем ВНТУ

Стаття надійшла до редакції 24.04.2023

Салієва Ольга Володимирівна — д-р філософії з кібербезпеки (PhD), старший викладач кафедри менеджменту та безпеки інформаційних систем, e-mail: salieva8257@gmail.com ;

Зоря Ірина Сергіївна — асистент кафедри менеджменту та безпеки інформаційних систем, e-mail: iryna.zoria03@gmail.com ;

Бондаренко Ірина Олексіївна — асистент кафедри менеджменту та безпеки інформаційних систем, e-mail: fm.ub15b.bondarenko@gmail.com ;

Берестенко Михайло Олександрович — студент факультету менеджменту та інформаційної безпеки: e-mail: mberestenko7@gmail.com .

O. V. Saliieva[1]
I. S. Zoria[1]
I. O. Bondarenko[1]
M. O. Berestenko[1]

Increasing the Reliability of User Authentication Based on Protected Electronic Key and Behavioral Biometrics

Vinnitsa National Technical University

The rapid spread of software applications in all spheres of human activity necessitates the need to ensure the protection of the data contained in them. Therefore, currently, the issues related to the improvement of authentication methods to prevent unauthorized access to software resources are relevant. To solve these problems, it is important to consider that different types of systems have their own unique requirements for authentication subsystems. In addition, the active development of computer technology makes it possible to break authentication algorithms, which were considered reliable a few years ago. In this regard, the work proposes to improve the reliability of user authentication based on a protected electronic key using the AES algorithm and analysis of the entropy of mouse movements, which is an individual characteristic for each person. The implementation of the electronic key is due to its advantages, such as reduced costs, increasing the convenience of use, reducing the probability of loss or theft, and reducing the risk of attacks through an intermediary. Analyzing the entropy of mouse movements will enable to perform the user authentication based on biometric behavioral characteristics that are universal, unique and permanent. Describing the algorithm of the mouse entropy analysis process, it is worth noting that the feature of tracking dynamic behavioral characteristics is that the user moves the mouse cursor along a complex curve with a speed that changes during the movement. The shape of the curved line and the speed of the cursor movement are determined by a number of physiological and psychological factors, in particular, such as: the size and weight of the hand, the position of the hand and the whole body, the state of the nervous system, user habits, etc. To improve the user authentication algorithm in the protected application, an electronic key using the JSON Web Tokens technology, which allows you to avoid authentication errors, increase the performance and scalability of the application, has been developed. Testing of the developed application will be performed on the basis of unit tests and the study of FAR and FRR indices.

Keywords: information system, two-factor authentication, electronic key, entropy of mouse movements.

Saliieva Olha V. — Dr. of Philosophy in Cyber Security (PhD), Senior lecturer of the Chair of Management and Security of Information Systems, e-mail: salieva8257@gmail.com ;

Zorya Iryna S. — Assistant of the Chair of Management and Security of Information Systems, e-mail: iryna.zoria03@gmail.com ;

Bondarenko Iryna O. — Assistant of the Chair of Management and Security of Information Systems, e-mail: fm.ub15b.bondarenko@gmail.com ;

Berestenko Mykhailo O. — Student of the Department of Management and Information Security, e-mail: mberestenko7@gmail.com