DOI 10.20535/2411-1031.2020.8.2.222592
УДК 004.056.53

ВІКТОР ЄВЕЦЬКИЙ,
ІВАН ГОРНІЙЧУК,
ГАННА НАКОНЕЧНА

ВПЛИВ ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ НА СТІЙКІСТЬ ОЗНАК РУКОПИСНОГО ПІДПИСУ КОРИСТУВАЧА

Розглянуто питання інформативності та сталості біометричних ознак користувача при автентифікації. Ідентифікатор, що використовує біометричні характеристики, нерозривно пов'язаний з користувачем, і скористатися ним несанкціоновано практично неможливо. Запропоновано використовувати динамічні біометричні характеристики користувачів. Їх перевагою є те, що завдяки наявності динамічної складової імовірність їх підроблення зловмисником дуже мала. Як біометричну характеристику користувача використано рукописний підпис. Він є суспільно і законно визнаною біометричною характеристикою, за якою автентифікується людина. Рукописний підпис має достатньо складну структуру і високу деталізацію, що ускладнює розв'язання проблеми автентифікації математичними методами і потребує великих обчислювальних затрат. Також недоліком є те, що існуючими системами автентифікації з використанням рукописного підпису вимагається встановлення додаткового спеціалізованого обладнання. Тому наявність сьогодні практично у всіх користувачів мобільних пристроїв, дозволила сформувати ідею використання їх як засобів автентифікації. Завдяки цьому запропоновано систему захисту комп'ютерних даних від несанкціонованого доступу на основі рукописного підпису з використанням мобільних пристроїв під управлінням операційної системи Android для введення підпису. Допуск користувача реалізується за алгоритмом на основі відстані Хемінга. Відповідно до обраного алгоритму розроблено метод формування біометричного вектору. Досліджено оптимальні характеристики та оцінено ефективність використання вектору біометричних характеристик запропонованої форми. Як ознаки рукописного підпису обрано швидкість руху на визначених проміжках, та кут нахилу вектору проміжку. Запропоновано оцінити сталість у часі та залежність обраних біометричних ознак від таких факторів: емоційного та фізичного стану користувача, а також часу доби в момент автентифікації. Розроблено програмний застосунок для операційної системи Android, яким збираються часові характеристики та значення запропонованих факторів для векторів часових характеристик з можливістю експортування накопичених даних.

Ключові слова: автентифікація, біометрична автентифікація користувача, біометрична характеристика, біометричний вектор, рукописний підпис, система біометричної автентифікації.

Постановка проблеми. Однією з актуальних задач розвитку інформаційних технологій на сучасному етапі є забезпечення надійного захисту інформації. Важливою та ще не розв'язаною проблемою є ефективна ідентифікація користувача, який отримує доступ до конфіденційної інформації. Традиційний парольний захист має ряд недоліків [1], [2]. Наприклад, у разі порушення конфіденційності пароля, це часто може залишитися непоміченим його власником, відразу порушується захист всієї інформації, до якої він має доступ. Як альтернатива парольній системі або її доповнення може розглядатися автентифікація користувачів за біометричними характеристиками [3], [4]. Такі технології мають низку переваг перед традиційними і знаходять все більше застосування в комп'ютерних системах.

Як біометричну характеристику доцільно використовувати рукописний підпис. Він є суспільно і законно визнаним та використовується для автентифікації людини. В зв'язку з

цим актуальним є його використання в системах автентифікації користувачів комп'ютерних систем. Перевагою динамічних систем розпізнавання підпису є те, що завдяки наявності динамічної складової зловмиснику практично неможливо підробити підпис "жертви" [5], [6].

Наявність сьогодні практично у всіх користувачів мобільних пристроїв, спонукала до ідеї використання їх в системах автентифікації, що може дозволити замінити ними спеціалізоване апаратне забезпечення. У попередніх роботах запропоновано схеми встановлення каналу зв'язку між мобільним пристроєм та комп'ютером, а також схема реалізації системи автентифікації користувачів за їх рукописним підписом з використанням мобільних пристроїв [7]. Запропоновано метод формування біометричного вектору для використання в динамічних біометричних системах автентифікації користувачів. Досліджено оптимальні характеристики та оцінено ефективність використання вектору біометричних характеристик запропонованої форми [8].

Аналіз останніх досліджень і публікацій. Рукописний підпис в умовах сьогодення використовується частіше для підписання електронних документів уповноваженими особами, ніж в системах автентифікації. Саме тому існує великий спектр програмного забезпечення, що дозволяє виконувати функцію підписання [9], [10], [11]. Таке програмне забезпечення орієнтоване на використання спеціалізованих графічних планшетів, більшість яких обладнанні спеціалізованим електронним пером. А також володіють власним інструментарієм розроблення застосунків для оброблення даних, отриманих в процесі розписування [12], [13], [14].

У подібних системах в ході підписання збирається інформація про різноманітні складові процесу підпису. Така інформація може містити такі характеристики [15], [16]:

- просторові координати кінця пера;
- тиск кінця пера на планшет;
- азимутальний кут пера;
- кут нахилу пера.

Існує багато підходів до обирання ознак рукописного підпису із отриманих при введені характеристик. Це робить можливим застосування великої кількості методів прийняття рішення для автентифікації користувачів за їх рукописним підписом [9] - [16].

Проте відсутні дослідження про сталість ознак рукописного підпису користувача протягом тривалого часу та їх стійкість до впливу інших дестабілізуючих факторів. Існуючі дослідження не акцентують на цьому увагу. Проте без цього складно зробити конструктивні рекомендації щодо їх ефективного використання в системах автентифікації.

Метою статті є аналізування стійкості ознак рукописного підпису для їх використання в системах динамічної біометричної автентифікації користувачів.

Виклад основного матеріалу дослідження. У дослідженнях описується залежність динамічних біометричних характеристик від наступних дестабілізуючих факторів [1], [5], [6]:

- емоційний стан користувача;
- фізичний стан користувача;
- час доби;
- плин часу в цілому.

Для отримання значення перших двох факторів, використано методику "Самооцінки емоційних станів" [17]. Базову розмірність шкал спрощено з 10 до 5 для уникнення надмірної детальності та полегшення самооцінки користувачами.

Емоційний стан користувача $EmSt = \{EmSt_1,\ EmSt_2,\ EmSt_3,\ EmSt_4,\ EmSt_5\}$, представлений за шкалою "піднесення-пригніченість", де його станам відповідають наступні оціночні твердження [17]:

- дуже пригнічений (-а). Відчуваю себе просто жахливо;
- настрій пригнічений і трохи сумно;
- відчуваю себе досить добре, "в порядку";
- відчуваю себе дуже добре. Життєрадісний (-а);

– сильний підйом, захоплення, веселощі.

Фізичний стан користувача $PhSt = \{PhSt_1,\ PhSt_2,\ PhSt_3,\ PhSt_4,\ PhSt_5\}$, представлений шкалою "жвавість-втома", де станам відповідають наступні оціночні твердження [17]:

– жахливо стомлений (-а). Майже виснажений (-а) і практично не здатний (-а) до дії. Майже не залишилося запасів енергії;
– досить втомлений (-а). В запасі не дуже багато енергії;
– відчуваю себе досить свіжим (-ою), в міру бадьорий (-а);
– відчуваю себе свіжим (-ою), в запасі значна енергія;
– порив, що не знає перешкод. Життєва сила вихлюпується через край.

Час доби *ToD* визначається за фактичним часом *ts* отримання вектору часових характеристик та набуває наступних значень:

$$ToD = \begin{cases} ToD_1,\ \text{"Ранок"},\ 5^{00} \le ts < 12^{00}; \\ ToD_2,\ \text{"День"},\ 12^{00} \le ts < 17^{00}; \\ ToD_3,\ \text{"Вечір"},\ 17^{00} \le ts < 00^{00}; \\ ToD_4,\ \text{"Ніч"},\ 00^{00} \le ts < 5^{00}. \end{cases}$$

Плин часу виражає сталість ознаки біометричного вектору протягом певного періоду часу.

У біометричних системах автентифікації на основі розпізнавання рукописного підпису претендентом на допуск за допомогою спеціалізованого графічного планшету або іншого пристрою введення вводиться фіксований рукописний підпис (пред'явлений на етапі навчання). У запропонованій системі використовуються лише значення просторових координат *x* та *y* кінця пера, та наявність контакту з дисплеєм – *p* в різні моменти часу *t* [7], [8]. Саме такі характеристики дає можливість отримати дисплей будь-якого сучасного мобільного пристрою. При цьому відрізок часу Δt, після якого будуть отримані координати повинен бути сталим і достатньо малим, для точності розрахунків. Мінімальна частота оновлення зображення на дисплеях сучасних мобільних пристроїв становить 60 Гц. Оскільки координати пера можна отримати тільки після реакції дисплею на команду сенсорної панелі, то мінімальну частоту оновлення даних можна вважати рівною частоті оновлення дисплею – 60 Гц. Для системи, що розробляється:

$$\Delta t = \frac{1}{60} \approx 0{,}0167\,c \approx 16\,мс.$$

Після введення підпису отримаємо наступні часові характеристики [8]:

$$\{(x_1; y_1; p_1),\ (x_2; y_2; p_2), ..., (x_N; y_N; p_N)\},\ N = T / \Delta t, \qquad (1)$$

де N – загальна кількість точок, що отримані під час підпису;

T – загальний час введення підпису.

Розширивши часові характеристики (1) значеннями дестабілізуючих факторів, та відміткою часу, отримаємо вектор часових характеристик v_τ такого виду:

$$v_\tau = (ts,\ EmSt,\ PhSt,\ ToD,\ (x_1; y_1; p_1),\ (x_2; y_2; p_2), ..., (x_N; y_N; p_N)). \qquad (2)$$

На основі вектору часових характеристик (2) можемо розрахувати значення біометричного вектору v:

$$v = \Phi_v(v_\tau),$$

де $\Phi_v(v_\tau)$ – функція розрахунку біометричного вектору на основі вектору часових характеристик.

Загальна форма біометричного вектору матиме такий вид:

$$v = (ts,\ EmSt,\ PhSt,\ ToD,\ I_1,\ I_2, ..., I_M), \qquad (3)$$

де I – ознака рукописного підпису користувача;

M – кількість ознак рукописного підпису користувача, що задається формою біометричного вектору.

Для оцінки впливу дестабілізуючих факторів на стійкість ознак необхідно на основі множини векторів часових характеристик V_τ сформувати множину біометричних векторів V:

$$V_\tau = \{\bigcup_{i=1}^{g} v_{\tau i}\},\ i = \overline{1, g},$$

$$V = \{\bigcup_{i=1}^{g} v_i\},\ i = \overline{1, g},$$

де g – кількість векторів часових характеристик наданих користувачем.

Стійкість ознаки до дестабілізуючого фактору можна відобразити наступним чином:

$$StI(Df) = \Phi_{st}(V', Df),$$

$$V' = \{v \in V \mid Df(v) = Df\},$$

де Df – один з описаних вище дестабілізуючих факторів;

$StI(Df)$ – функція стійкості ознаки I до дестабілізуючого фактору Df;

$\Phi_{st}(V', Df)$ – функція розрахунку значення стійкості ознаки на множині векторів V';

V' – множина біометричних векторів v, які належать множині V, і для яких значення відповідного дестабілізуючого фактору $Df(v)$ відповідає значенню Df.

Слід зауважити, що окрім трьох вищезазначених дестабілізуючих факторів доцільно оцінити стійкість до їх комбінацій. Множина таких факторів матиме такий вид:

$$\{EmSt,\ PhSt,\ ToD,\ EmSt \times PhSt,\ EmSt \times ToD,\ PhSt \times ToD,\ EmSt \times PhSt \times ToD\}.$$

А множина значень кожного з комбінованих факторів визначатиметься як декартів добуток підмножин.

Для оцінки впливу дестабілізуючих факторів на стійкість ознак рукописного підпису необхідно мати статистичні дані, накопичені протягом тривалого періоду часу кількома користувачами. Для реалізації цього було розроблено мобільний застосунок для операційної системи Android.

Застосунок розроблено з використанням Firebase. Firebase це хмарна платформа, яка надає ряд сервісів, SDK (Software Development Kit), API (Application Programming Interface) для розроблення мобільних та веб-застосунків [18]. Зокрема було використано можливості служб Firebase Authentication та Firebase Realtime Database.

Firebase Authentication надає серверні служби, прості у використанні SDK і готові бібліотеки користувацького інтерфейсу для автентифікації користувачів в застосунках. Ним підтримується автентифікація за допомогою паролів, телефонних номерів та популярних сервісів таких як Google, Facebook, Twitter.

Для реєстрації користувача в застосунку, спочатку від нього отримуються облікові дані для автентифікації. Ці дані містять адресу електронної пошти та пароль. Після цього вони відправляються до SDK Firebase Authentication.

Після успішного входу можна отримати доступ до основної інформації профілю користувача, і контролювати доступ до даних, які зберігаються в інших продуктах Firebase.

Firebase Realtime Database – це NoSQL база даних, що розташована в хмарі. Дані в ній зберігаються в форматі JSON та синхронізуються в реальному часі.

База даних забезпечує роботу в автономному режимі. Realtime Database SDK зберігає інформацію про всі операції та транзакції локально на диску, а після відновлення підключення здійснює синхронізацію даних з поточним станом серверу.

Доступ до бази даних можна здійснювати безпосередньо з клієнтського застосунку, без необхідності розробляти сервер. В той час безпека та валідація даних забезпечуються правилами безпеки самої бази даних. Вони дозволяють керувати доступом на основі ідентифікаторів користувача, які надає Firebase Authentication.

Проте Realtime Database має і свої недоліки. Оскільки це NoSQL база даних, то вона відрізняється низькою оптимізацією та функціональністю у порівнянні з реляційними базами даних, бо призначена перш за все для виконання великої кількості швидких операцій. Через це важливим є розроблення правильної структури бази даних.

У базі даних зберігається інформація про:

– пристрій, необхідна для подальшого нормування вектору часових характеристик (модель, висота, ширина дисплею в пікселях, його щільність, розмір діагоналі в дюймах);

– користувача (ідентифікатор Firebase Auth, ім'я, прізвище, електронна пошта, дата народження, дата реєстрації, дата останньої активності, кількість днів, коли користувач відправляв вектори, кількість записаних векторів, роль доступу);

– вектори часових характеристик (ідентифікатор Firebase Auth, дата та час створення вектору, пристрій з якого відправлено, $EmSt$, $PhSt$, ToD та власне вектор з часовими характеристиками за (1)).

Інтерфейс розробленого застосунку. Після запуску застосунку користувач потрапляє на екран автентифікації (див. рис. 1). Для реєстрації, необхідно ввести адресу електронної пошти, на яку пізніше буде надіслано посилання для підтвердження реєстрації, та пароль користувача на екрані реєстрації (див. рис. 2).

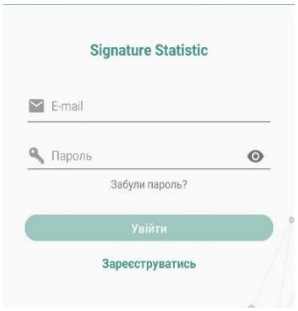

Рисунок 1 – Екран автентифікації

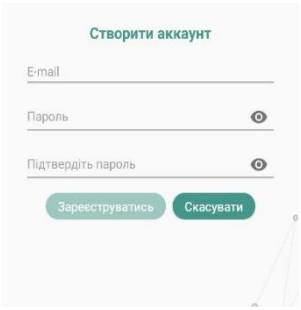

Рисунок 2 – Екран створення профілю

Після вдалої автентифікації користувача буде направлено на головний екран застосунку (див. рис. 3).

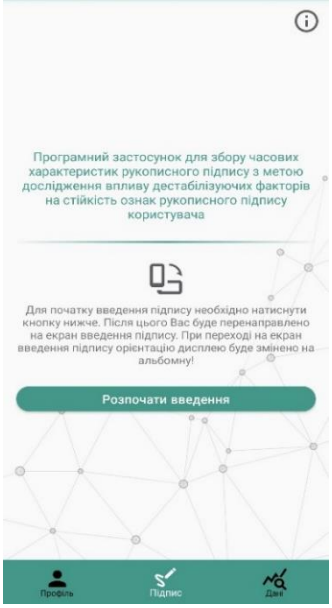

Рисунок 3 – Головний екран застосунку

Рисунок 4 – Екран з інформацією користувача

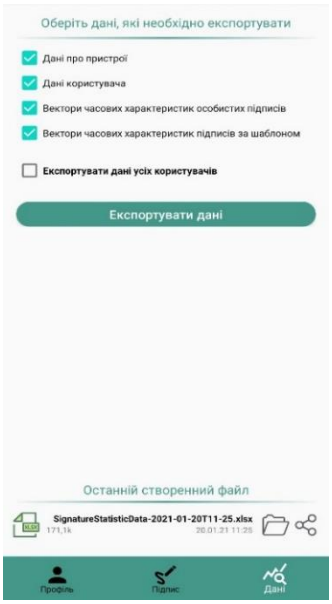

Рисунок 5 – Екран експорту даних

На рис. 4 демонструється екран з інформацією про користувача, а на рис. 5 показується екран експорту даних до файлу в форматі Microsoft Excel (.xlsx). Після успішного завершення операції внизу дисплею відображається панель з інформацією про створений файл. Після натискання клавіші “Розпочати введення”, на головному екрані, застосунок змінить орієнтацію дисплею на альбомну та відкриє екран введення підпису (див. рис. 6).

На ньому користувач розписується встановлену кількість разів, підтверджуючи збереження кожного натисканням клавіші “Відправити”. Якщо ж введений образ підпису не задовольняє користувача його можна очистити відповідною кнопкою.

Рисунок 6 – Екран введення підпису

Після введення останнього підпису користувач має оцінити свій емоційний (див. рис. 7) та фізичний стан (див. рис. 8).

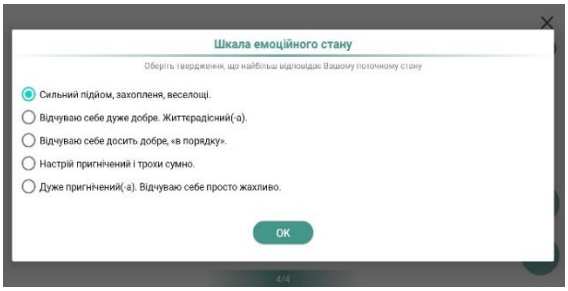

Рисунок 7 – Екран самооцінки емоційного стану

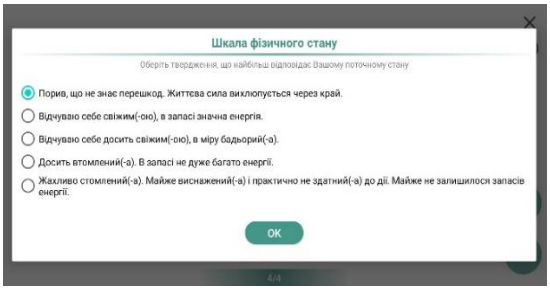

Рисунок 8 – Екран самооцінки фізичного стану

Висновки. В результаті проведеної роботи проаналізовано останні дослідження і публікації щодо стійкості ознак рукописного підпису для їх використання в системах динамічної біометричної автентифікації користувачів. Запропоновано перелік дестабілізуючих факторів, що можуть впливати на стійкість ознак рукописного підпису. Серед них: емоційний та фізичний стан користувача, час доби та плин часу в цілому. Наведено множину їх значень та спосіб визначення цих значень. Запропоновано метод оцінки впливу дестабілізуючих факторів на сталість ознак рукописного підпису.

Розроблено мобільний застосунок для операційної системи Android. Він призначений для збору часових характеристик рукописного підпису користувачів, а також значень запропонованих дестабілізуючих факторів. Ним забезпечується експорт накопичених статистичних даних до файлу в форматі Microsoft Excel (.xlsx) для його подальшої обробки.

У перспективах подальших досліджень планується накопичити статистичні дані, оцінити сталість ознак рукописного підпису та вплив на них запропонованих дестабілізуючих факторів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Э. Анисимова, “О проблеме верификации с использованием рукописных подписей”, *Современная техника и технологии*, №3, 2016. [Электронний ресурс]. Доступно: http://technology.snauka.ru/2016/03/9715. Дата обращения: Лип. 15, 2020.

[2] А. Скородумов, "Плюсы и минусы биометрической идентификации", *Information Security/ Информационная безопасность,* № 6, с. 31-33, 2018. [Электронний ресурс]. Доступно: http://lib.itsec.ru/articles2. Дата обращения: Лип. 20, 2020.

[3] І. Горнійчук, та В. Євецький, "Використання клавіатурного почерку в системах автентифікації користувача", *Information Technology and Security,* vol. 4, iss. 1 (6), pp. 27-33, 2016, doi: 10.20535/2411-1031.2016.4.1.95927.

[4] L. Irwin, "GDPR: Things to consider when processing biometric data", *IT Governance European Blog,* 2017. [Online]. Available: https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data. Accessed on: June 12, 2020.

[5] И. Смирнов, и С. Борисова, "Распознавание рукописного почерка при аутентификации пользователей ПЭВМ", *Успехи современного естествознания*, № 6, с. 99-100, 2012.

[6] Ю. Желудов, "Проблемы идентификации в системах распознавания рукописных подписей", *Научный журнал* "*Информатика*", № 9 (32), 2018. [Электронный ресурс]. Доступно: https://cyberleninka.ru/article/n/problemy-identifikatsii-v-sistemah-raspoznavaniya-rukopisnyh-podpisey. Дата обращения: June 20, 2020.

[7] І. Горнійчук, В. Євецький, та В. Кубрак, "Використання мобільних пристроїв в біометричних системах автентифікації користувача", *Information Technology and Security*, vol. 7, iss. 1 (12), pp. 14-24, 2019, doi: 10.20535/2411-1031.2019.7.1.184213.

[8] І. Горнійчук, та В. Євецький, "Вибір динамічних показників рукописного підпису для автентифікації користувачів", *Information Technology and Security*, vol. 8, iss. 1 (14), pp. 19-30, 2020, doi: 10.20535/2411-1031.2020.8.1.217994.

[9] SignToLogin – Products. Signtologin.com, 2020. [Online]. Available: https://signtologin.com/products. Accessed on: Aug. 01, 2020.

[10] DocuSign eSignature. DocuSign Inc., 2020. [Online]. Available: https://www.docusign.com/products/electronic-signature. Accessed on: Aug. 01, 2020.

[11] 3M™ Electronic Signature Authentication (ESA) Software. 3M.com, 2020. [Online]. Available: https://www.3m.com/3M/en_US/company-us/all-3m-products/~/3M-Electronic-Signature-Authentication-ESA-Software/?N=5002385+3290603306&rt=rud. Accessed on: Aug. 01, 2020.

[12] Wacom Inc. technology for Developers. Wacom Inc., 2020. [Online]. Available: https://developer.wacom.com/en-us. Accessed on: Aug. 01, 2020.

[13] Solutions: HUION. Shenzhen Huion Animation Technology Co., 2020. [Online]. Available: https://support.huion.com/support/solutions. Accessed on: Aug. 01, 2020.

[14] Download Developer Tools (API/SDK). Signotec GmbH, 2020. [Online]. Available: https://en.signotec.com/service/downloads/developer-tools-api-sdk-/. Accessed on: Aug. 01, 2020.

[15] И. Аникин, и Э. Анисимова, "Распознавание динамической рукописной подписи на основе нечёткой логики", *Вестник Казанского государственного энергетического университета,* № 3 (31), с. 48-64, 2016.

[16] В. Липский, "Идентификация рукописных подписей с использованием нейросетей", на *54-ой научной конференции аспирантов, магистрантов и студентов БГУИР*, Минск, 2018, с. 84-85.

[17] А. Карелин, *Большая энциклопедия психологических тестов*. Москва, Россия: ЭКСМО, 2005.

[18] Firebase by platform. Firebase, 2020. [Online]. Available: https://firebase.google.com/docs. Accessed on: July. 01, 2020.

Стаття надійшла до редакції 10.08.2020.

REFERENCE

[1] E. Anisimova, "About the verification problem using handwritten signatures", *Modern technology and technology*, no. 3, 2016. [Online]. Available: http://technology.snauka.ru/2016/03/9715. Accessed on: July 15, 2020.

[2] A. Skorodumov, "Pros and cons of biometric identification", *Information Security*, no. 6, pp. 31-33, 2018. [Online]. Available: http://lib.itsec.ru/articles2. Accessed on: July 20, 2020.
[3] I. Horniichuk, and V. Yevetskiy, "Use of keyboard handwriting in user authentication systems", *Information Technology and Security*, vol. 4, iss. 1, pp. 27-33, 2016, doi: 10.20535/2411-1031.2016.4.1.95927.
[4] L. Irwin, "GDPR: Things to consider when processing biometric data", *IT Governance European Blog*, 2017. [Online]. Available: https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data. Accessed on: June 12, 2020.
[5] I. Smirnov, and S. Borisov, "Handwriting recognition when authenticating PC users", *Succeeding in modern natural science*, no. 6, pp. 99-100, 2012.
[6] Y. Zheludov, "Identification problems in handwritten recognition systems", *Scientific journal* "*Informatics*", no. 9 (32), 2018. [Online]. Available: https://cyberleninka.ru/article/n/problemy-identifikatsii-v-sistemah-raspoznavaniya-rukopisnyh-podpisey. Accessed on: June 20, 2020.
[7] I. Horniichuk, V. Yevetskiy, and V. Kubrak, "Applying mobile devices in biometric user authentication systems", *Information Technology and Security*, vol. 7, iss. 1, pp. 14-24, 2019, doi: 10.20535/2411-1031.2019.7.1.184213.
[8] I. Horniichuk, and V. Yevetskiy, "Selection of handwritten signature dynamic indicators for user authentication", *Information Technology and Security*, vol. 8, iss. 1, pp. 19-30, 2020, doi: 10.20535/2411-1031.2020.8.1.217994.
[9] SignToLogin – Products. Signtologin.com, 2020. [Online]. Available: https://signtologin.com/products. Accessed on: Aug. 01, 2020.
[10] DocuSign eSignature. DocuSign Inc., 2020. [Online]. Available: https://www.docusign.com/products/electronic-signature. Accessed on: Aug. 01, 2020.
[11] 3M™ Electronic Signature Authentication (ESA) Software. 3M.com, 2020. [Online]. Available: https://www.3m.com/3M/en_US/company-us/all-3m-products/~/3M-Electronic-Signature-Authentication-ESA-Software/?N=5002385+3290603306&rt=rud. Accessed on: Aug. 01, 2020.
[12] Wacom Inc. technology for Developers. Wacom Inc., 2020. [Online]. Available: https://developer.wacom.com/en-us. Accessed on: Aug. 01, 2020.
[13] Solutions: HUION. Shenzhen Huion Animation Technology Co., 2020. [Online]. Available: https://support.huion.com/support/solutions. Accessed on: Aug. 01, 2020.
[14] Download Developer Tools (API/SDK). Signotec GmbH, 2020. [Online]. Available: https://en.signotec.com/service/downloads/developer-tools-api-sdk-/. Accessed on: Aug. 01, 2020.
[15] I. Anikin, and E. Anisimova, "Detection of dynamic handwritten signature based on fuzzy logic", *Bulletin of the Kazan State Energy University*, no. 3 (31), pp. 48-64, 2016.
[16] V. Lipsky, "Identification of handwritten signatures using neural networks", in *Proc. 54-th scientific conference of post-graduate students, masters and students of BSUIR*, Minsk, 2018, pp. 84-85.
[17] A. Karelin, *Great encyclopedia of psychological tests*. Moscow, Russia: EKSMO, 2005.
[18] Firebase by platform. Firebase, 2020. [Online]. Available: https://firebase.google.com/docs. Accessed on: July. 01, 2020.

VIKTOR YEVETSKYI,
IVAN HORNIICHUK,
HANNA NAKONECHNA

INFLUENCE OF DESTABILIZING FACTORS ON THE STABILITY OF USER'S HANDWRITTEN SIGNATURE INDICATORS

Consideration is given to the question of user`s handwritten signature parameters informativeness and stability during authentication. An identifier that uses biometric characteristics

is inextricably linked to the user and it is almost impossible to use it without authorization. It is proposed to use dynamic biometric characteristics of users. Their advantage is that due to the presence of a dynamic component, the probability of their forgery by an attacker is very low. A handwritten signature is used as a biometric characteristic of the user. A handwritten signature is a socially and legally recognized biometric characteristic used for human authentication. It has a rather complex structure and high detail - all this makes solving the problem of user identification by mathematical methods quite complex and requires high computational costs. Another significant disadvantage is that handwritten authentication systems require the installation of additional specialized equipment, which makes the use of such systems as an ordinary means of authentication very expensive. Nowadays the presence of mobile devices in almost all users has made it possible to form the idea of using them in authentication systems. Thanks to that a scheme for implementing a computer security system against unauthorized access based on handwritten signatures using Android-based mobile devices as signature input devices were proposed. An algorithm based on Heming's distance was chosen to implement user tolerance. According to the selected algorithm, a method for forming a biometric vector has been developed. The optimal characteristics are investigated and the efficiency of using the proposed form biometric characteristics vector is estimated. The speed of movement at certain intervals and the inclination angle of the vector interval were chosen as indicators of the handwritten signature. It is offered to estimate stability in time and dependence of the chosen biometric signs on the following factors: emotional and physical condition of the user, and also time of day at the moment of authentication. Developed a software application for the Android operating system, which collects the time characteristics and values of the proposed factors for time characteristics vectors, as well as allows to export the accumulated data.

Keywords: authentication, biometric user authentication, biometric characteristics, biometric vector, handwritten signature, biometric authentication system.

Євецький Віктор Леонідович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-5364-8076.

E-mail: viktorevetskv@gmail.com.

Горнійчук Іван Вікторович, аспірант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-6754-4764.

E-mail: horniychuk.ivan@gmail.com.

Наконечна Ганна Вікторівна, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0003-0200-9650.

E-mail: hanvik.nak@gmail.com.

Yevetskyi Viktor, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Horniichuk Ivan, postgraduate student, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Nakonechna Hanna, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.