НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ
Кафедра кібербезпеки та застосування автоматизованих інформаційних систем і технологій

Система захисту комп'ютерних даних від несанкціонованого доступу на основі використання біометричних характеристик користувачів

Виконав:
старшина С3 магістерського курсу
старшина ***Горнійчук Іван Вікторович***

Керівник:
доцент СК№5,
кандидат технічних наук, доцент ***Євецький Віктор Леонідович***

Київ – 2018

Актуальність роботи

Звична для користувачів комп'ютерних систем парольна аутентифікація, є досить вразливою до компрометації шляхом впровадження кейлогерів, та підбору паролю методом грубої сили (brute force). В той час як для біометричних систем аутентифікації ці вразливості відсутні, адже ідентифікатор користувача нерозривно з ним пов'язаний і скористуватись ним несанкціоновано практично неможливо.

Клавіатурний почерк та рукописний підпис як біометричні характеристики користувача

Клавіатурний почерк або ритм друкування – біометрична характеристика, що відображає притаманний конкретному кристувачеві спосіб друкування того чи іншого тексту.

Рукописний підпис – біометрична характеристика, що відображає індивідуальну манера підписування; заснована на письмово-руховій навичці користувача система рухів, за допомогою якої виконуються певні умовні графічні знаки (підпис).

Переваги використання зазначених біометричних характеристик

- відносно легкі в реалізації;
- використовують динамічні характеристики притаманні конкретній особі;
- мають високу швидкість прийняття рішення про істинність користувача;
- системи на основі клавіатурного почерку не вимагають використання додаткових апаратних засобів.

Недоліки існуючих систем

- Як комерційні так і наукові рішення не надають вихідний код, тому неможливо:
  1) перевірити їх на наявність вразливого чи шкідливого програмного коду;
  2) використовувати їх у подальших дослідженнях;
- В наукових роботах відсутні дані про дослідження сталості характеристик клавіатурного почерку на протязі тривалого часу.
- Існуючі системи автентифікації за рукописним підписом вимагають наявності спеціалізованих апаратних засобів, що робить їх дорогими, та незручними в експлуатації.

Наукова задача

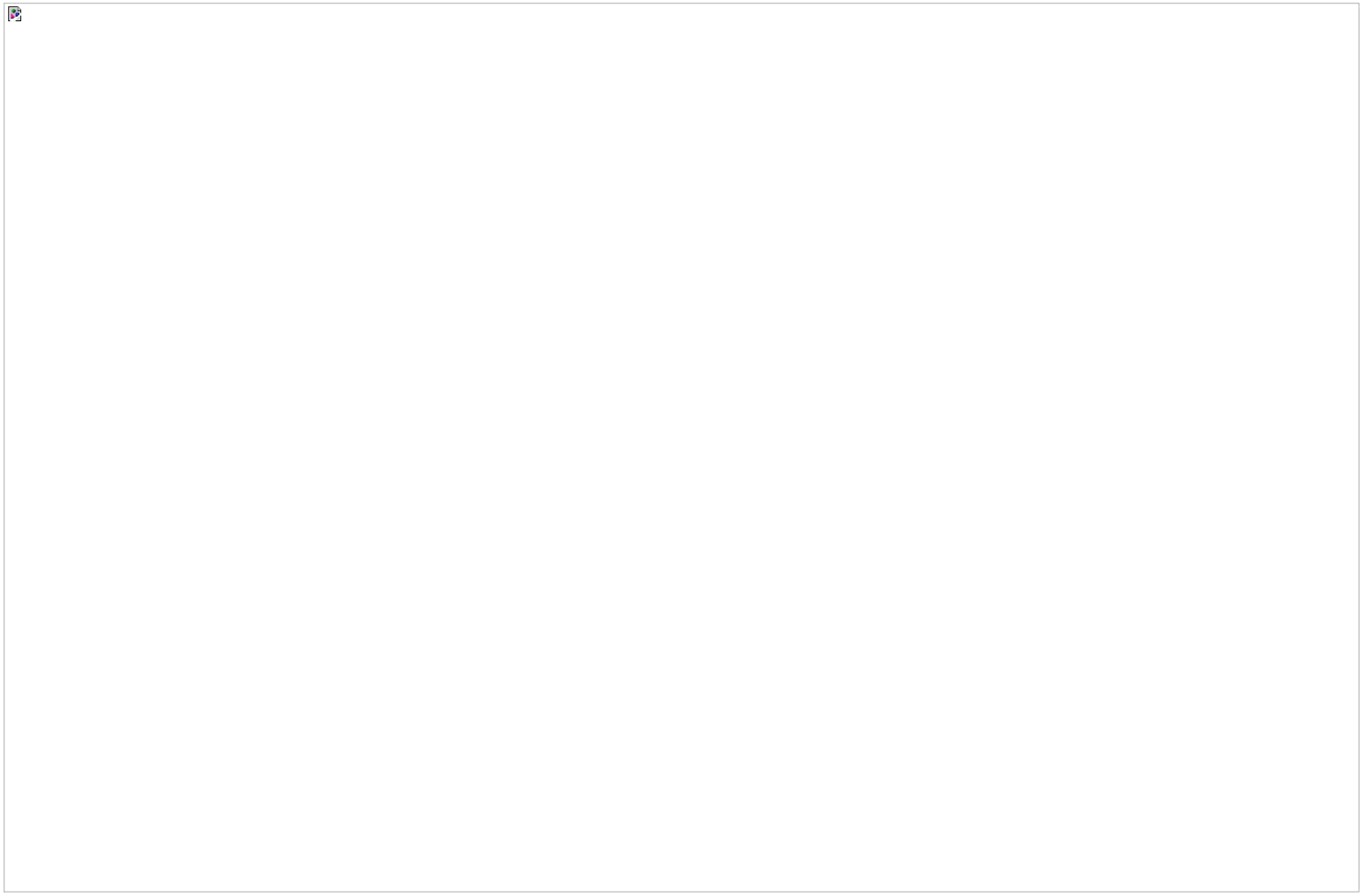
Розробка науково-методичних рекомендацій щодо застосування клавіатурного почерку та рукописного підпису в системах захисту даних від несанкціонованого доступу.

- **Метою** дослідження є підвищення ефективності захисту комп'ютерних даних від несанкціонованого доступу
- **Об'єктом** дослідження є процес автентифікації користувача на основі біометричних характеристик
- **Предметом** дослідження є моделі, методи та методики автентифікації користувача за його біометричними характеристиками

Часткові задачі дослідження

1. Проаналізувати існуючі підходи, останні дослідження і публікації.
2. Отримати статистичний експериментальний матеріал використання клавіатурного почерку, на його основі оцінити сталість характеристик клавіатурного почерку протягом тривалого періоду часу.
3. Розробити методику формування вектора біометричних характеристик для рукописного підпису, та дослідити його оптимальні параметри.
4. Розробити схему реалізації системи автентифікації користувачів за їх рукописним підписом без використанням спеціалізованих пристроїв введеня та дослідити її ефективність.

Узагальненна схема роботи біометричних систем автентифікації



Розпізнавання користувачів на основі відстані Хеммінга

Відстань Хеммінга – число позицій, в яких відповідні символи двох слів однакової довжини є різними. В більш загальному випадку відстань Хеммінга застосовується для рядків (векторів) однакової довжини і служить метрикою відмінності (функцією, що дозволяє визначити відстань в метричному просторі) об’єктів однакової розмірності.

Вектор біометричних характеристик

- $$v = (p_1, p_2, p_3, \ldots, p_n)$$

де p_i - i-ий параметр біометричного вектора , n – загальна кількість параметрів вектора, його розмір.

Еталон біометричних характеристик

- Еталон біометричних характеристик має вигляд:

$$V_e = (\min(p_1), \max(p_1), \min(p_2), \max(p_2), \ldots, \min(p_n), \max(p_n), E_p),$$

$$\min(p_i) = m(p_i) - T[L,(1-P)] \cdot \sigma(p_i),$$

$$\max(p_i) = m(p_i) + T[L,(1-P)] \cdot \sigma(p_i),$$

$$E_p = m(E_v) + C[L,(1-P)] \cdot \sigma(E_v)$$

де $\boldsymbol{m(p_i)}$ - математичне очікування і-го часового параметра, $\boldsymbol{\sigma(p_i)}$ - його середнє квадратичне відхилення, $\boldsymbol{m(E_v)}$ і $\boldsymbol{\sigma(E_v)}$ - відповідно математичне очікуванні і середнє квадратичне відхилення для відстані Хеммінга по кожному вектору, $\boldsymbol{T[L,(1-P)]}$, $\boldsymbol{C[L,(1-P)]}$ - коефіцієнти Стьюдента, при $\boldsymbol{L}$ – степенів свободи і $\boldsymbol{P}$ – імовірність помилки 1 роду.

Прийняття рішення про істиність користувача

- Користувач визнається істинним якщо:

$$E_v \leq E_p,$$

де E_v - відстань Хеммінга від наданого вектору, до еталону,

E_p - порогове значення міри Хеммінга для даного користувача

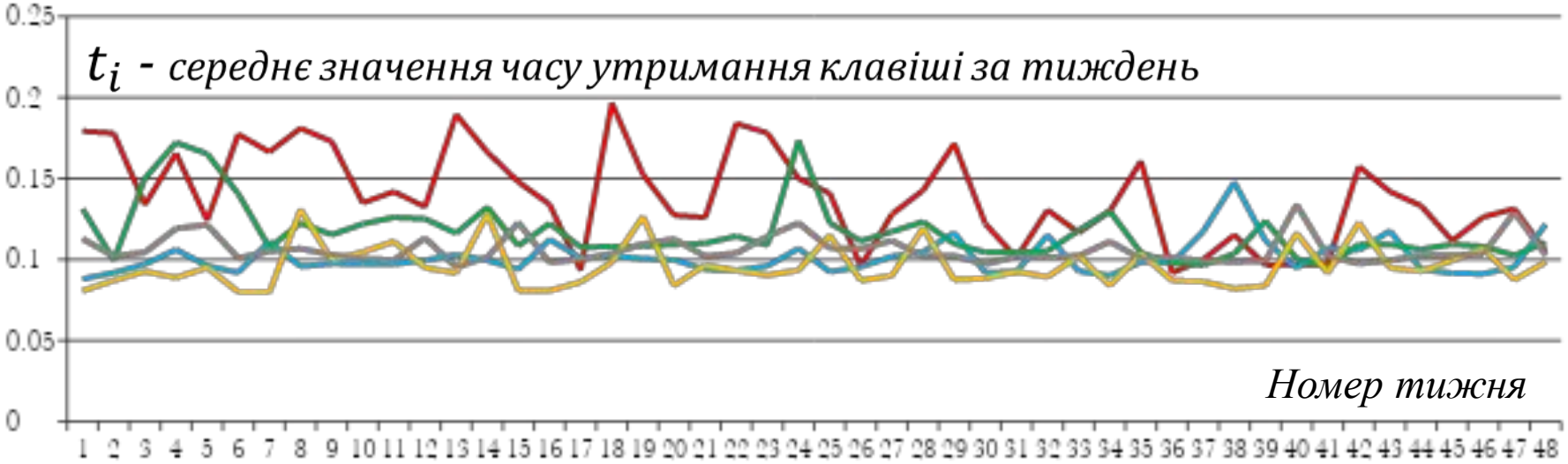
$$E_v = \sum_{i=1}^{N} e_i,$$

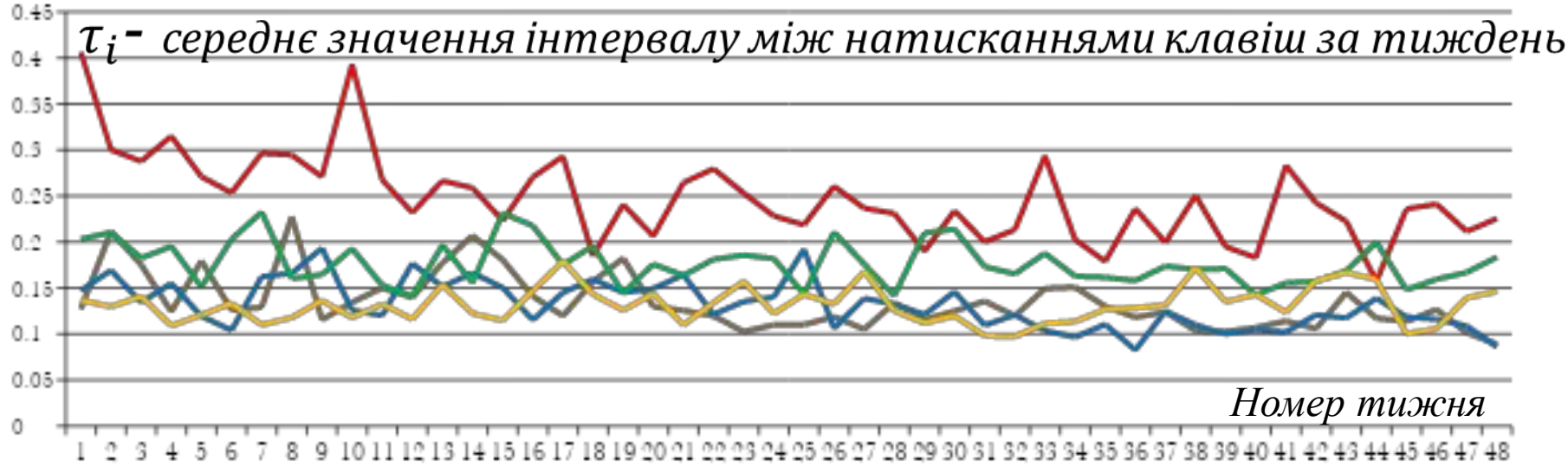
$$E = (e_1, e_2, e_3, \ldots, e_N),$$

$$e_i = \begin{cases} 0, t_i \in [\min(t_i), \max(t_i)] \\ 1, t_i \notin [\min(t_i), \max(t_i)] \end{cases}$$

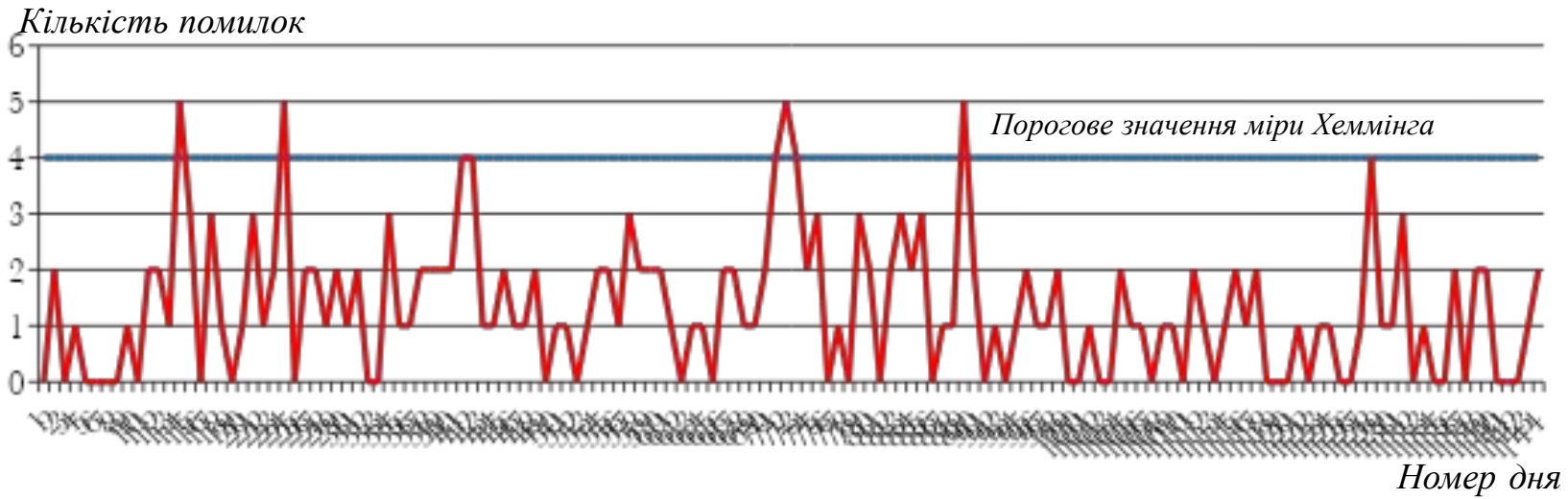
де $\boldsymbol{E}$ – вектор Хеммінга, $\boldsymbol{e_i}$- відстань між відповідними параметрами наданого часового вектора і еталону користувача, $\boldsymbol{t_i}$ - і-тий часовий параметр вектора біометричних характеристик.

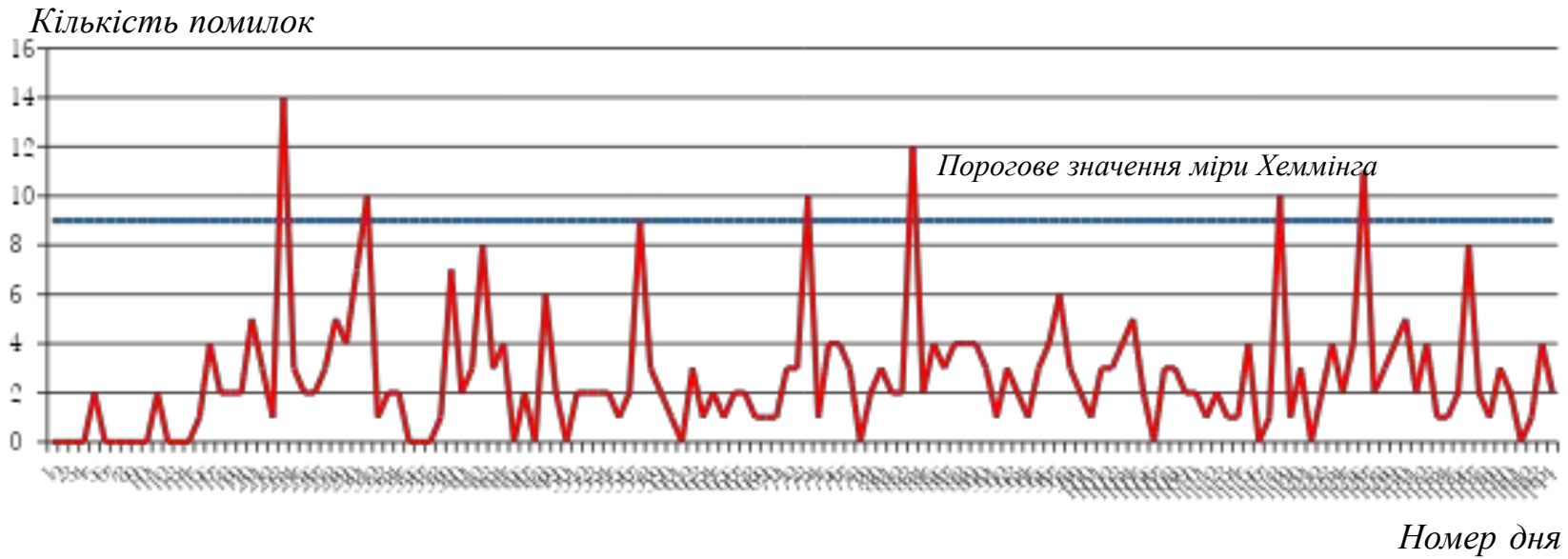
Результати дослідження сталості клавіатурного почерку





Результати дослідження сталості клавіатурного почерку





Імовірність вірного розпізнання користувача за його клавіатурним почерком

№	Кількість хибних відмов в автентифікації за час досліду	Частота хибної відмови	Частота надання допуску
1	4	0,027778	0,972222
2	6	0,041667	0,958333
3	4	0,027778	0,972222
4	6	0,041667	0,958333
5	3	0,020833	0,979167

$$p = \frac{p^* + \frac{1}{2}\frac{t_\beta^2}{n} \pm t_\beta \sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n}};$$

$p \in [0{,}95; 0{,}99]$

де $\boldsymbol{p}$ – імовірність вірного розпізнавання користувача,
$\boldsymbol{p}^*$ - частота вірного розпізнавання користувачів,
$\boldsymbol{n}$ – кількість дослідів,
$\boldsymbol{\beta}$ – довірча імовірність,
$\boldsymbol{t_\beta}$ - число середніх квадратичних відхилень, для досягнення імовірності потрапляння в інтервал β

Біометричний вектор рукописного підпису

$$\{(x_1; y_1), (x_2; y_2), \dots, (x_N; y_N)\}, N = T/\Delta t$$

де $(x_i; y_i)$ - координати, N – загальна кількість точок, що було отримано під час підпису, T – загальний час введення підпису, Δt – проміжок часу через який отримуються координати.

$$v = (s_1, s_2, \dots s_n, d_1, d_2, \dots d_n)$$

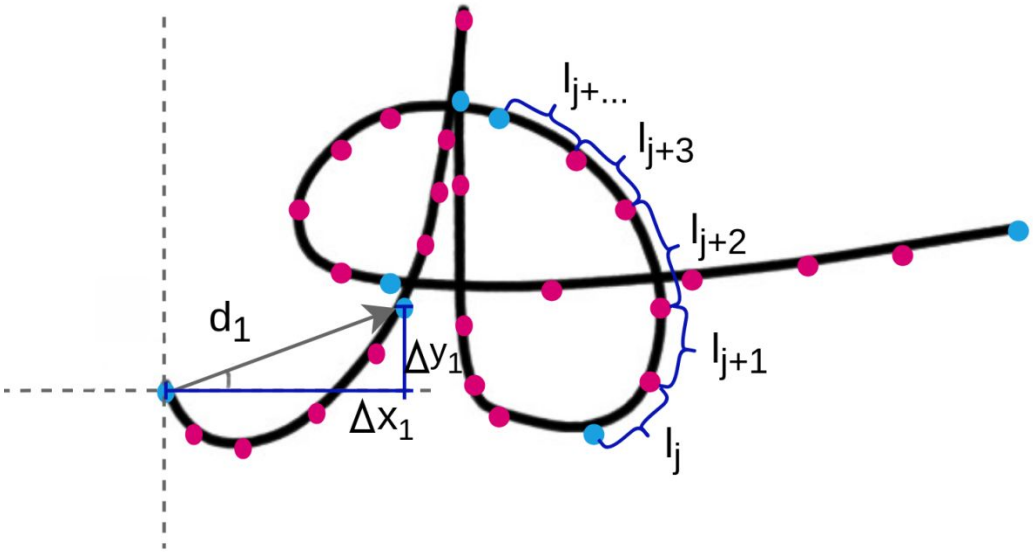
де n - фіксована кількість проміжків однакової довжини k $(k=N/n)$, на які розбивається досліджувана часова послідовність, s_i - середню швидкість введення проміжку, d_i - кут нахилу вектора, що з'єднує початок та кінець досліджуваного проміжку

Розрахунок параметрів біометричного вектору рукописного підпису

$$s_i = \frac{\sum_{j=ik}^{(i+1)k} l_j}{k}, i = (\overline{0,n}),$$

$$l_j = \sqrt{(x_{j+1} - x_j)^2 + (y_{j+1} - y_j)^2},$$

де l_j - відстань Евкліда між сусідніми точками проміжку



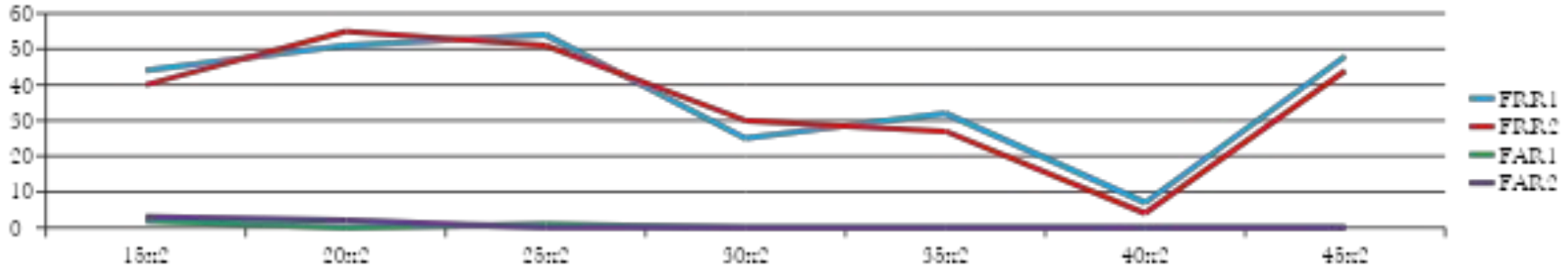
$$d_i = \begin{cases} \arccos(\cos\alpha_i), \Delta y_i > 0 \\ 360^{\circ} - \arccos(\cos\alpha_i), \Delta y_i < 0 \end{cases}$$

$$\cos\alpha_i = \frac{y_{i+1} - y_i}{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}}$$

де a_i - кут нахилу вектора проміжку та одиничного вектора $\bar{e}(0; 1)$, що обраховується із скалярного добутку цих векторів

Результати дослідження оптимальної довжини біометричного вектора

Довжина біометричного вектору	Учасник 1				Учасник 2			
		FRR		FAR		FRR		FAR
15*2	44	0,44	2	0,02	40	0,40	3	0,03
20*2	51	0,51	0	0	55	0,55	2	0,02
25*2	54	0,54	1	0,01	51	0,51	0	0
30*2	25	0,25	0	0	30	0,23	0	0
35*2	32	0,32	0	0	27	0,27	0	0
40*2	7	0,7	0	0	4	0,4	0	0
45*2	48	0,48	0	0	44	0,40	0	0



$$FRR = \frac{n_1}{n}; \qquad FAR = \frac{n_2}{n}$$

де FRR – імовірність помилкових відмов істинному користувачеві; FAR – імовірність надання доступу сторонньому користувачеві; n_1- кількість відмов істинному користувачеві, n_2 - кількість випадків хибного надання доступу, n – загальна кількість спроб.

Система захисту даних від НСД на основі використання рукописного підпису

Система складається з трьох окремих модулів:

- модуль реєстрації користувачів;
- модуль автентифікації користувачів;
- модуль Android.

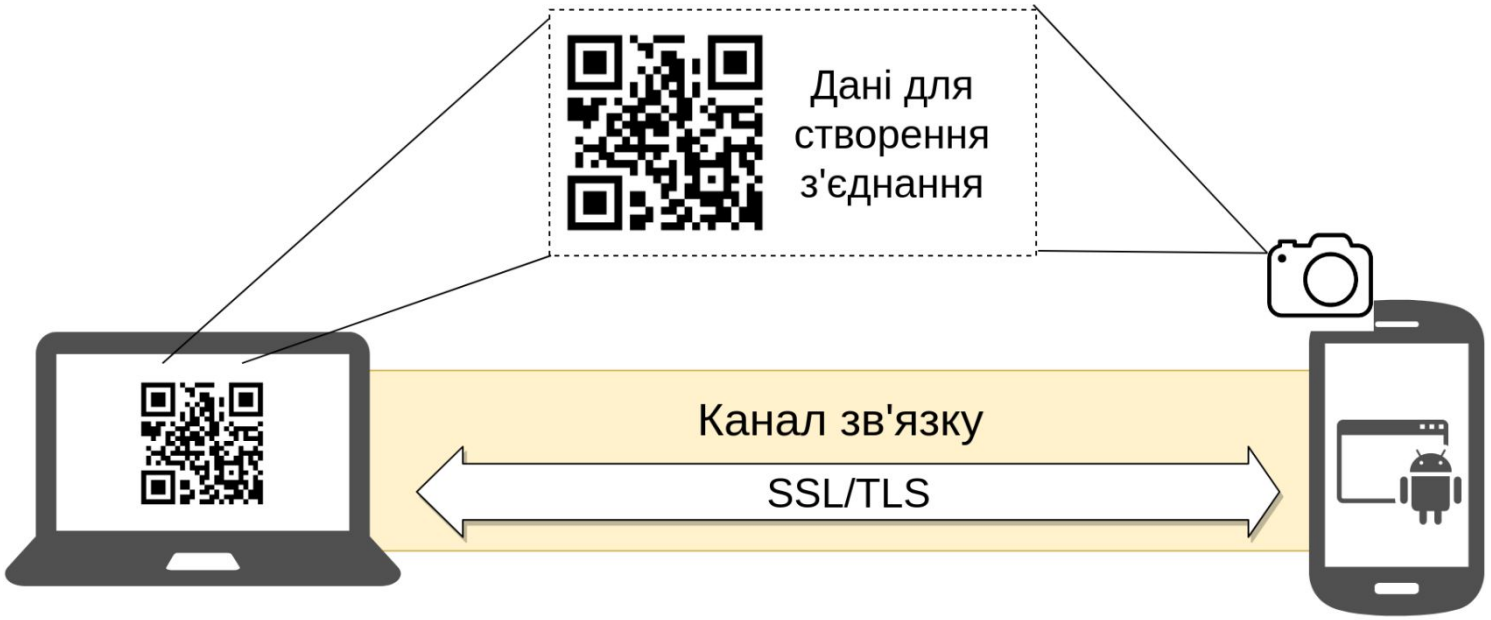


Схема взаємодії модуля реєстрації та модуля Android

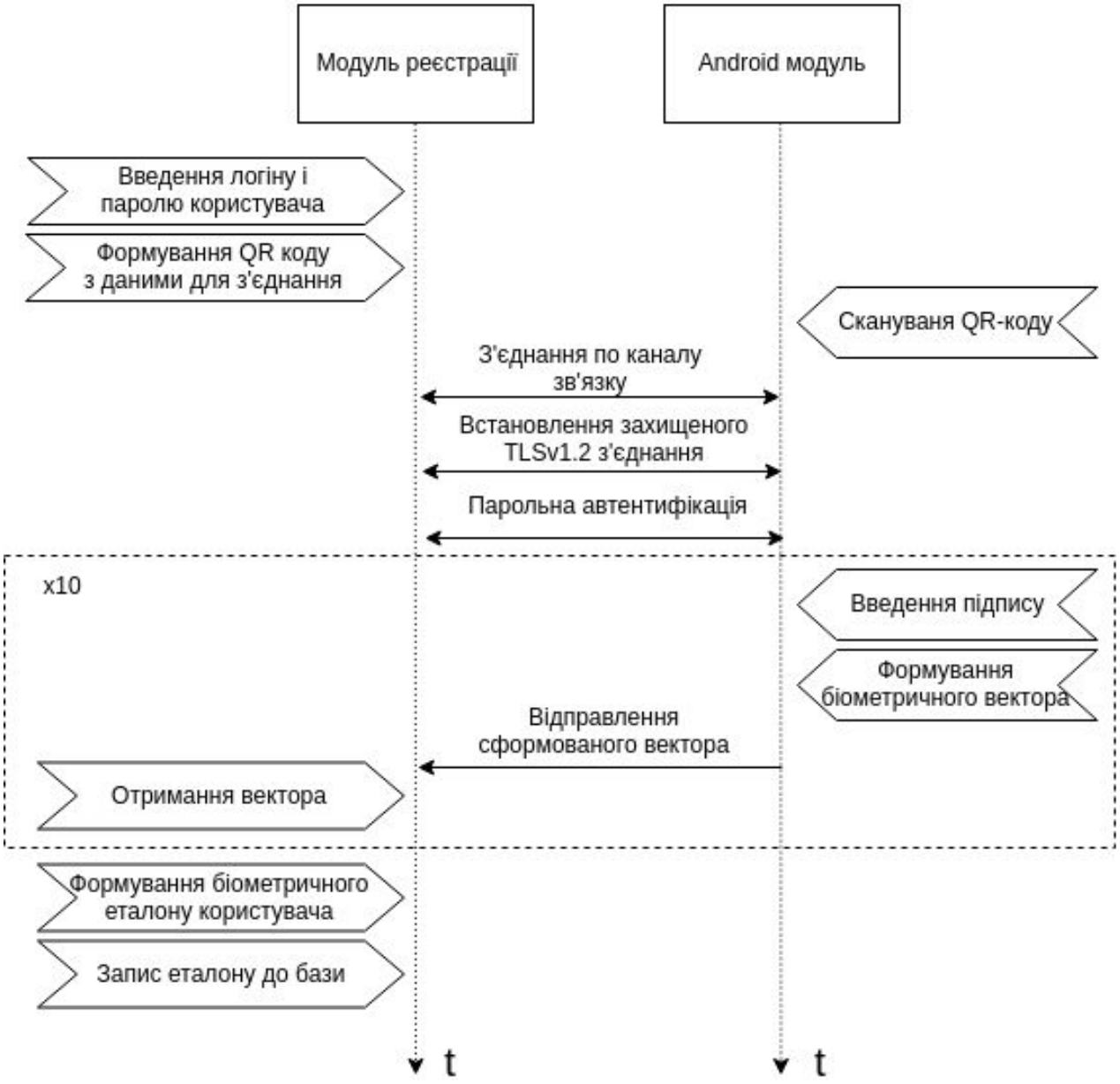
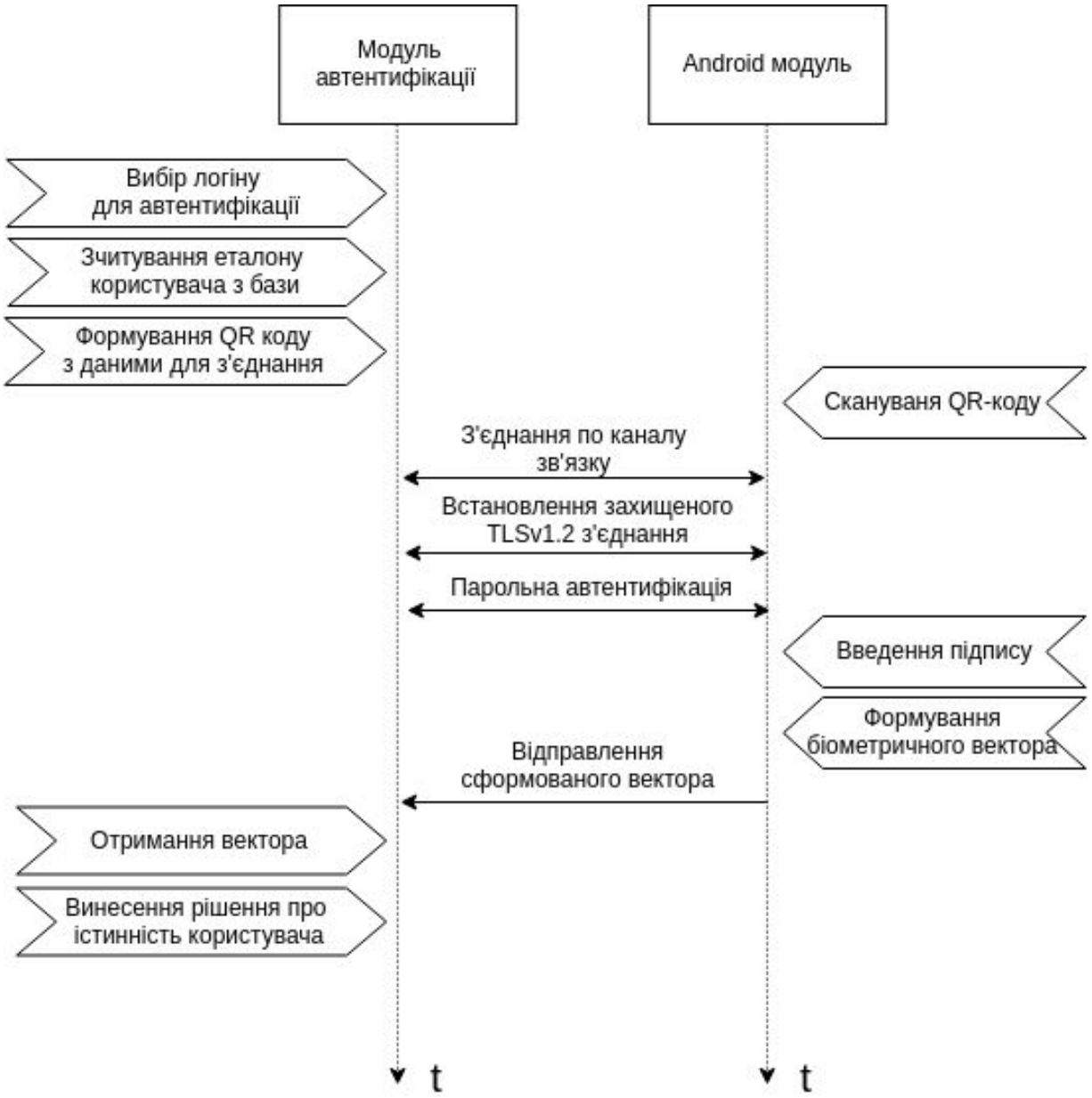
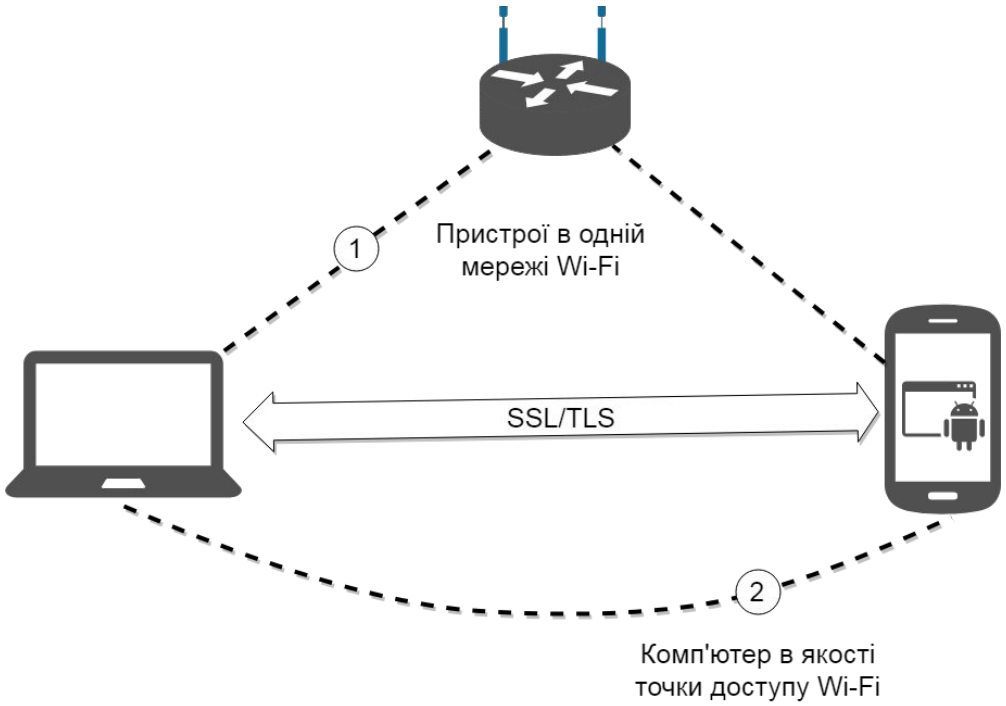


Схема взаємодії модуля автентифікації та модуля Android



Реалізація системи за запропонованою схемою



Варіанти встановлення зв'язку чере
Wi-Fi:

1)обидва пристрої знаходяться в одній мережі Wi-Fi;

2)персональний комп'ютер виступає в ролі точки доступу для мобільного пристрою.

Переваги розробленої системи:

- кросплатформеність;
- відсутність додаткових апаратних засобів;
- зручність у використанні;
- одна і та ж клієнтська програма може використовуватись для автентифікації в різних системах;
- відкритий вихідний код.

Висновки

- В результаті проведеного дослідження було проаналізовано сталість характеристик клавіатурного почерку користувача протягом тривалого часу.
- На підставі отриманих даних було зроблено висновки про відносно високу сталість клавіатурного почерку користувачів із впевненим рівнем комп'ютерного набору, за тривалий періоду часу.
- Імовірність вірного розпізнавання користувачів за їх клавіатурним почерком, є не нижчою за 0,95.
- Розроблено методику формування вектора біометричних характеристик для рукописного підпису, та досліджено його оптимальну довжину.
- Запропоновано схему реалізації системи автентифікації користувачів за їх рукописним підписом з використанням мобільних пристроїв в якості пристроїв введеня, та здійсненно її реалізацію.
- Імовірність вірного розпізнавання користувачів за їх рукописним підписом, в розробленій системі є не нижчою за 0,91.
- Використання систем автентифікації на основі розглянутих біометричних характеристик рекомендується в якості додаткового засобу автентифікації завдяки їх високій надійності.

Апробація результатів дослідження

Результати дослідження було апробовано на наступних науково-практичних конференціях:

- «Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем» 15-17 травня 2018року;
- «Безпека інформації в інформаційно-телекомунікаційних системах», 22-24 травня 2018 року;
- «Сучасні інформаційні технології та кібербезпека» 15-16 листопада 2018;

Апробація результатів дослідження

Публікації за результатами досліджень:

- Євецький В., Горнійчук І., Використання клавіатурного почерку в системах автентифікації користувача. Information Technology and Security. 2016. Випуск 4. С.27-33.
- Горнійчук І., Аналіз сталості характеристик клавіатурного почерку користувача в системах біометричної автентифікації. Матеріали науково-практичної конференції «Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем». – К.:ІСЗЗІ КПІ ім.Ігоря Сікорського, 2018. С. 174-177.
- Євецький В., Горнійчук І., Використання клавіатурного почерку для підвищення ефективності автентифікації користувача. Безпека інформації в інформаційно-телекомунікаційних системах. Матеріали ювілейної науково-практичної конференції. – 2018. – Вип. 20
- Євецький В., Горнійчук І., Система автентифікації користувачів на основі розпізнання рукописного підпису. Матеріали науково-практичної конференції «Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем». – К.:ІСЗЗІ КПІ ім.Ігоря Сікорського, 2018. С. 197-199

Апробація результатів дослідження

Результати досліджень сталості характеристик клавіатурного почерку були відзначені дипломом І ступеню за перемогу в Всеукраїнському конкурсі студентських наукових робіт з галузей знань і спеціальностей 2017/2018 навчального року.

УКРАЇНА

ДЕРЖАВНА СЛУЖБА ВЛАСНОСТІ УКРАЇНИ ІНТЕЛЕКТУАЛЬНОЇ

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 71534

"Комп'ютерна програма реєстрації користувачів для авторизації засобами клавіатурного почерку "HandWriting"

(вид, назва твору)

Автор(и) Горнійчук Іван Вікторович, Євецький Віктор Леонідович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 19.04.2017

Державна служба інтелектуальної власності України Ідентифікаційний код 37552556 М.П.

Голова Державної служби інтелектуальної власності України

В.о. Голови А.А. Малиш

УКРАЇНА

ДЕРЖАВНА СЛУЖБА ВЛАСНОСТІ УКРАЇНИ ІНТЕЛЕКТУАЛЬНОЇ

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 71533

"Комп'ютерна програма авторизації користувачів засобами клавіатурного почерку "Login"

(вид, назва твору)

Автор(и) Горнійчук Іван Вікторович, Євецький Віктор Леонідович

(повне ім'я, псевдонім (за наявності))

Дата реєстрації 19.04.2017

Державна служба інтелектуальної власності України Ідентифікаційний код 37552556 М.П.

Голова Державної служби інтелектуальної власності України

В.о. Голови А.А. Малиш

Дякую за увагу!

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ
Кафедра кібербезпеки та застосування автоматизованих інформаційних систем і технологій

Система захисту комп'ютерних даних від несанкціонованого доступу на основі використання біометричних характеристик користувачів

Виконав:
старшина С3 магістерського курсу
старшина ***Горнійчук Іван Вікторович***

Керівник:
доцент СК№5,
кандидат технічних наук, доцент ***Євецький Віктор Леонідович***

Київ – 2018