МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Методи й апаратно-програмні засоби захисту інформації в комп'ютерних системах

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 123 - "Комп'ютерна інженерія"

Науковий керівник роботи: _____ (підпис) Л.О. Шумова (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Я.О. Критська (ініціали, прізвище)

Студент: _____ (підпис) Ю.О.Лигін (ініціали, прізвище)

Група: КІ-17зм

Сєвєродонецьк 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки _____
(шифр і назва)
Спеціальність 123 Комп'ютерна інженерія
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____20____р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Лигін Юрій Олександрович
(прізвище, ім'я, по батькові)

1. Тема роботи Методи й апаратно-програмні засоби захисту інформації в комп'ютерних системах

керівник проекту (роботи) Шумова Лариса Олександрівна, канд. техн. наук
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "18" 10 2018 р. № ____
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи дані, зібрані під час проходження науково-дослідної практики
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1 Методи і алгоритми розпізнавання клавіатурного почерку в інформаційних системах інформаційної інфраструктури.

2 Розробка математичних і аналітичних моделей механізму розпізнавання клавіатурного почерку.

3 Розробка алгоритмів розпізнавання клавіатурного почерку оператора інформаційної системи.

4 Охорона праці та безпека в надзвичайних ситуаціях. Екологія

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронна презентація

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях. Екологія	Критська Я.О., ст.викладач		

7. Дата видачі завдання 18.10.2018 р.

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
	Аналітичний огляд літератури за темою роботи	1.09.18-10.10.18	
	Аналіз методів аутентифікації в інформаційних системах	11.10.18-18.10.18	
	Розробка математичних і аналітичних моделей механізму розпізнавання клавіатурного почерку	19.10.18-30.10.18	
	Розробка алгоритмів аутентифікації користувачів	30.10.18-14.11.18	
	Створення програмного засобу для аутентифікації за клавіатурним почерком	15.11.18-30.11.18	
	Розгляд питань з охорони праці	29.11.18 – 07.12.18	
	Оформлення пояснювальної записки	08.12.18 – 26.12.18	
	Оформлення презентації роботи	27.12.18 – 6.01.19	

Студент _____ Лигін Ю.О.
(підпис) (прізвище та ініціали)

Науковий керівник _____ Шумова Л.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Лигін Ю.О. Методи й апаратно-програмні засоби захисту інформації в комп'ютерних системах.

Проведено аналіз характеристик клавіатурного почерку оператора комп’ютерних систем. Запропоновано метод визначення клавіатурного почерку, в якому розпізнавання клавіатурного почерку відбувається за вільним текстом і отриманий шаблон почерку не залежить від набраного оператором тексту та порядку введення символів. Розроблено аналітичну модель клавіатурного почерку, що дозволяє порівняти два шаблони клавіатурного почерку. Створено алгоритм авторизації оператора за клавіатурним почерком та алгоритм постійного таємного клавіатурного моніторингу з метою виявлення підміни авторизованого оператора.

Ключові слова: клавіатурний почерк, аналітична модель, міра Евкліда, бімодальний розподіл, час утримання клавіши.

АННОТАЦИЯ

Лыгин Ю.А. Методы и аппаратно-программные средства защиты информации в компьютерных системах.

Проведен анализ характеристик клавиатурного почерка оператора компьютерных систем. Предложен метод определения клавиатурного почерка, в котором распознавание клавиатурного почерка происходит по произвольному тексту, и полученный шаблон почерка не зависит от набранного оператором текста и порядка ввода символов. Разработана аналитическая модель клавиатурного почерка, которая позволяет сравнить два шаблона клавиатурного почерка. Создан алгоритм авторизации оператора за клавиатурным почерком и алгоритм постоянного тайного клавиатурного мониторинга с целью выявления подмены авторизованного оператора.

Ключевые слова: клавиатурный почерк, аналитическая модель, мера Евклида, бимодальное распределение, время удержания клавиши.

ABSTRACT

Lyhin Y.A. Methods and hardware-software of information protection in computer systems.

An analysis of the characteristics of the keyboard handwriting of the computer system operator is carried out. The method of determining the keyboard handwritten in which the recognition of the keyboard handwriting occurs in arbitrary text is proposed, and the received handwriting pattern does not depend on the typed text operator and the order of the character input. The analytical model of keyboard handwriting is developed, which allows comparing two patterns of keyboard handwriting. An algorithm for authorizing the operator behind the keyboard and an algorithm for constant secret key monitoring was created in order to identify the replacement of the authorized operator.

Key words: keyboard writing, analytical model, Euclidean measure, bimodal distribution, key hold time.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ІС – інформаційна система

КС- комп’ютерна система

КП- клавіатурний почерк

ЧУК- час утримання клавіши

FAR- помилка першого роду

FRR- помилка другого роду

ERR – оптимальний порог доступу

ВСТУП

Життя сучасного суспільства неможливе без повсюдного застосування інформаційних технологій. Комп'ютери обслуговують банківську систему, контролюють роботу атомних реакторів, розподіляють енергію, стежать за розкладом потягів, керують літаками і космічними кораблями. Сьогодні комп'ютерні системи і телекомунікації визначають надійність систем оборони і безпеки країни, реалізують сучасні інформаційні технології, забезпечуючи зберігання інформації, її обробку, доставку і надання споживачам.

Однак саме висока ступінь автоматизації, до якої прагне сучасне суспільство, ставить його в залежність від рівня безпеки використовуваних інформаційних технологій. Від них залежить благополуччя і життя людей. Масове застосування комп'ютерних систем, що дозволило вирішити задачу автоматизації процесів обробки постійно зростаючих обсягів інформації, зробило ці процеси надзвичайно уразливими по відношенню до агресивних дій і поставило перед споживачами інформаційних технологій нову проблему - проблему інформаційної безпеки.

Захист інформації в комп'ютерних системах і мережах - це комплексне завдання, вирішення якого відбувається за допомогою впровадження різних систем безпеки. Одну з головних ролей у вирішенні даного завдання відіграє елемент, що забезпечує контроль доступу до ресурсів комп'ютерної системи. Такий елемент виконує свої функції за допомогою процедур ідентифікації і аутентифікації користувачів. Ці процедури є основними в будь-якій системі захисту від несанкціонованого доступу, тому що кожен користувач повинен бути однозначно визначений і має бути гарантована відповідність користувача і його ідентифікатора, так як подальша робота в системі ведеться тільки з ідентифікованими суб'єктами.

Аутентифікація особи в інформаційній системі – це перевірка відповідності суб’єкта і того, за кого він себе намагається видати, за допомогою деякої унікальної інформації. З позицій інформаційної безпеки аутентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації, та передує авторизації.

Одним з основних факторів, що визначають стан захищеності тієї чи іншої комп’ютерної системи інформаційної інфраструктури, є ефективність функціонування підсистеми управління доступом і захисту інформації. Парольні і за допомоги предмета(атрибутні методи) методи ідентифікації і аутентифікації мають ряд суттєвих недоліків. Головний з них - неоднозначність ідентифікації оператора інформаційної системи (ІС) і можливість обману системи захисту, наприклад, шляхом крадіжки або імітації атрибута або злому пароля. Другий недолік даних методів ідентифікації і аутентифікації - неможливість виявлення підміни законного авторизованого оператора. В даному випадку зловмисник може

завдати шкоди оброблюваної в КС інформації, коли оператор залишає без нагляду робоче місце з пройденої процедурою авторизації.

Методи аутентифікації по біометричними параметрами особистості, в тому числі і за клавіатурним почерком (КП), з огляду на невід'ємності біометричних характеристик від конкретної людини, здатні забезпечити підвищену, у порівнянні з іншими способами перевірки відповідності, точності, неможливість відмови від авторства і зручність для операторів автоматизованих систем. Методи постійного прихованого клавіатурного моніторингу дозволяють виявляти підміну законного оператора і блокувати КС від вторгнення зловмисника. Таким чином, задача дослідження моделей, методів і алгоритмів розпізнавання клавіатурного почерку операторів інформаційних систем є актуальною на даний момент.

У дослідженнях по біометрії ряду вчених, таких як А.І. Іванов [72], М.Н. Десятерик [69], В.В. Марченко [84] виділені характеристики клавіатурного почерку: час утримання клавіші при натисканні, інтервали між натисканнями клавіш, сила натискання на клавішу, швидкість натискання на клавішу і ін. В роботах вчених В.І. Волчихина [59], А.І. Іванова [73] запропоновано використовувати апарат штучних нейронних мереж для математичної обробки даних, отриманих в результаті експериментів з біометричними даними людини. А.Н. Лебедєв, В.Б. Дорохов, Т.Н. Щукін, Е.В. Луценко в своїх працях [81,82] довели наявність залежності між змінами клавіатурного почерку оператора і його психофізіологічним станом.

Проблема застосування клавіатурного почерку в системах ідентифікації і аутентифікації операторів досліджувалася в роботах таких вчених, як Dawn Song, Peter Venable, Adrian Perrig (Pittsburgh, PA, USA) [31]; R. Gaines, W. Lisowski, S. Press, N. Shapiro (Santa Monica, CA, USA) [11]; Alen Peacock, J. Leggett, D. Umphress, G. Williams (Texas, USA) [22, 30, 41]; M.S. Obaidat, B. Sadoun (New Jersey, USA) [28,35]; С.Н. Расторгуєв [89], Р.Н. Мінніханов [85] та ін. В їх працях була запропонована класична схема аутентифікації операторів КС. Достовірність аутентифікації з використанням методів, описаних в працях перерахованих вище авторів, має допустимі значення ймовірності виникнення помилок першого і другого роду тільки при визначенні клавіатурного почерку за ключовою фразою.

Представлені методи застосовуються в процесі авторизації операторів ключової системи і не можуть бути використані для прихованого клавіатурного моніторингу і виявлення підміни законного оператора. Це пов'язано з тим, що клавіатурний почерк - динамічна поведінкова біометрична характеристика людини. Нестабільність почерку операторів пояснюється зміною їх психофізіологічного стану. Існуючі програмні реалізації методів розпізнавання клавіатурного почерку характеризуються недостатньою достовірністю ідентифікації і аутентифікації і високою ймовірністю виникнення помилок першого і другого роду. Внаслідок цього актуальна розробка нових моделей, методів, алгоритмів розпізнавання

клавіатурного почерку і їх програмних реалізацій, що підвищують точність і якість функціонування систем ідентифікації і аутентифікації.

Таким чином, обґрунтовано необхідність використання апарату теорії ймовірностей і математичної статистики, зокрема теорії нормального розподілу, для оцінки математичного сподівання часу утримання клавіш (ЧУК) як характеристики клавіатурного почерку оператора. Обґрунтовано необхідність подання ЧУК у вигляді бімодального розподілу. Це дозволить досягти прийнятного рівня помилок першого і другого роду при ідентифікації оператора при малій кількості вимірювань і дасть можливість скоротити час як на створення шаблону клавіатурного почерку, так і на процедуру авторизації. В зв'язку з використанням методу визначення клавіатурного почерку на основі врахування часу утримання клавіш стає можливо визначення клавіатурного почерку по вільному тексту. Це в свою чергу дозволяє здійснювати прихований клавіатурний моніторинг клавіатурного почерку і виявляти підміну законного оператора. Запропоновано метод розпізнавання клавіатурного почерку по вільному тексту на основі механізму аналізу клавіатурного введення в ключовий системі. Даний метод реалізований в алгоритмі розпізнавання клавіатурного почерку за часом утримання клавіш і часу введення часто вживаних у мові послідовностей літер. Розроблено програмне забезпечення постійного прихованого клавіатурного моніторингу, що впроваджується в інтерфейс ключової системи. Розроблена система ідентифікації оператора ключової системи інформаційної інфраструктури має точність в 99% при кількості операторів, зареєстрованих в системі, що дорівнює 100.

Метою магістерської роботи є підвищення інформаційної безпеки КС.

Для досягнення поставленої мети в роботі сформульовані і вирішені **наступні завдання**:

- аналіз і дослідження характеристик КП, існуючих методів, алгоритмів, моделей і засобів визначення КП оператора КС;
- розробка математичних моделей розпізнавання КП оператора КС;
- розробка алгоритму розпізнавання КП по часу утримання клавіш;
- розробка способу зберігання і передачі даних про КП;
- розробка методу розпізнавання КП по вільному тексту;
- розробка та реалізація алгоритму розпізнавання КП по часу утримання клавіш;
- проведення експериментального дослідження підсистеми доступу до КС на основі аналізу КП оператора.

Об'єкт дослідження – процеси організації і управління доступом до системи інформаційної інфраструктури.

Предмет дослідження - методи і алгоритми розпізнавання КП оператора КС.

Методи дослідження. У роботі використані методи теорії ймовірностей і математичної статистики, системного аналізу, теорії множин, методи об'єктно-орієнтованого програмування, теорії захисту інформації.

Наукова новизна одержаних результатів.

Запропоновано метод визначення клавіатурного почерку оператора ключової системи, що відрізняється від існуючих тим, що розпізнавання клавіатурного почерку відбувається за вільним текстом і отриманий шаблон почерку не залежить від набраного оператором тексту і порядком введення символів, що забезпечує можливість застосування методу для задач постійного прихованого клавіатурного моніторингу з метою виявлення підміни авторизованого законного оператора.

Розроблено математичну модель клавіатурного почерку, яка відрізняється від існуючих тим, що ЧУК представляється у вигляді бімодального розподілу (перетину двох нормальних розподілів), що збільшить до двох разів кількість застосовуваних при розпізнаванні КП характеристик, розроблена модель застосовується в алгоритмах розпізнавання клавіатурного почерка.

Апробація результатів роботи. Основні результати магістерської атестаційної роботи докладалися на всеукраїнській науково-пркатичній конференції з міжнародною участю «Майбутній науковець 2018» [46], опубліковано наукова стаття у фаховому виданню [47].

Особистий внесок здобувача Виконано аналіз існуючих методів і алгоритмів розпізнавання клавіатурного почерку, і застосовуваних в них характеристик КП. Розроблено математичну модель КП, заснована на теорії нормального розподілу. Автором отримані всі виносяться на захист положення, сформульовані наукові висновки та положення. Досліджено причини виникнення помилок I і II роду, що виникають при розпізнаванні КП в процесі аутентифікації.

Структура та обсяг магістерської роботи

Магістерська робота складається зі вступу, 4 розділів, висновків на 93 сторінках, списку використаних джерел з 105 найменувань, додатків. В магістерській роботі міститься 3 таблиці, 13 рисунків.

РОЗДІЛ 1
МЕТОДИ І АЛГОРИТМИ РОЗПІЗНАВАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

1.1. Можливості ідентифікації оператора в сучасних інформаційних системах при виконанні завдань забезпечення захищеності ключових систем

Одним з основних факторів, що визначають стан захищеності тієї чи іншої системи інформаційної інфраструктури , є ефективність функціонування підсистеми управління доступом і захисту інформації. Захист секретної та цінної інформації від несанкціонованого доступу необхідна для запобігання істотного матеріального і нематеріального збитку. Головним завданням проблеми захисту інформації в ключовий системі від несанкціонованого доступу є завдання розмежування функціональних повноважень і доступу до інформації. Дане завдання спрямована на запобігання можливості зловмисника зчитувати або модифікувати інформацію, що зберігається в ЕОМ. Дії по захисту інформації від несанкціонованого доступу включають [98]:

– недопущення зловмисника до інформаційної системи, засноване на засобах розпізнавання оператора;

– створення спеціального забезпечення для захисту інформації в ключовий системі;

– використання спеціальних засобів захисту інформації від несанкціонованого доступу.

У роботі [55] проведено аналіз і виділені основні засоби забезпечення захисту інформації від несанкціонованого доступу. Нижче представлені ті засоби і результати аналізу.

Законодавчі, організаційні та морально-етичні засоби. Проведений аналіз даних засобів захисту показав, що вони мають низькою надійністю без підтримки фізичними, технічними та програмними засобами. Також виявлено, що вони володіють високою залежністю від суб'єктивних чинників, наприклад, від загальної організації роботи на підприємстві або в організації.

Фізичні та інженерно-технічні засоби. Виявленими недоліками є висока вартість, необхідність регулярного контролю і проведення регламентованих робіт, можливість подачі помилкових тривог.

Апаратні і програмні засоби. Виявлені переваги: надійність, незалежність від суб'єктивних чинників, здатність до модифікації і розвитку, універсальність. Виявлено такі

недоліки, які проявляються в різних видах даних засобів: висока вартість, залежність від типу ЕОМ, недостатня гнучкість.

Одним з напрямків застосування програмно-апаратних засобів є системи контролю та управління доступом. Для успішного функціонування системи контролю та управління доступом до КС необхідно вирішення двох завдань:

1) зробити неможливим обхід системи управління і розмежування доступу діями, що знаходяться в рамках існуючої моделі захисту інформації;

2) гарантувати ідентифікацію оператора, який здійснює доступ до інформації.

Зазначені завдання виконуються шляхом проведення наступних процесів контролю і управління доступом в ключовій системі, застосовуваних до оператора:

1. Ідентифікацію, тобто, з одного боку, привласнення суб'єктам доступу індивідуальних ідентифікаторів (текстових, числових або спеціальних пристроїв), а, з іншого боку, розпізнавання суб'єктів по привласненим їм унікальним ідентифікаторів [15]

2. Аутентифікацію, тобто підтвердження автентичності ідентифікації суб'єкта з метою докази того, що суб'єкт є саме тим, ким він представився. [6]

Таким чином зроблено висновок про те, що забезпечення інформаційної безпеки ключової системи залежить від якості функціонування процесів аутентифікації і ідентифікації операторів.

1.2. Сучасні системи контролю та управління доступом до інформації

Виявлено, що в сучасних ключових системах процеси аутентифікації і ідентифікації, доступу до інформації, пов'язані в основному з процесом авторизації, тобто надання авторизованому суб'єкту (оператору) законних прав доступу до інформації, її обробку і зберігання в ключовій системі. Виділено наступні методи авторизації операторів, що застосовуються в КС:

1. Парольні - завдяки контрольній парольний фразі або поєднанню букв і символів.

2. Атрибутні – за допомоги унікального предмета (магнітні картки, смарт-карти, USB-токени і т.і.).

3. Біометричні - за фізіологічними параметрами людського тіла або поведінки людини.

Проведено аналіз сучасної ситуації в області систем контролю і управління доступом. За даними компанії IDC системи управління ідентифікацією та доступом складають 59% від загального ринку засобів IT-безпеки [89]. Дослідження, проведене CSI / FBI Computer Crime and Security Survey в 2017 році, виявило, що 51% компаній для авторизації операторів застосовують парольні методи, 35% атрибутні методи і тільки 20% біометричні методи [1]. За

даними соціологічного дослідження компанії Unisys 68% клієнтів в світі воліють, щоб банки, платіжні системи, державні органи для ідентифікації використовували біометрію замість паролів і карт [49]. Компанія AtSecurity на початку 2013 року провела опитування серед європейських IT- фахівців з на предмет використання ними технологій авторизації в банківській сфері [75]. Низька популярність (рис 1.1.) біометричних методів пов'язана з високою вартістю і складністю налаштування біометричних систем захисту інформації.

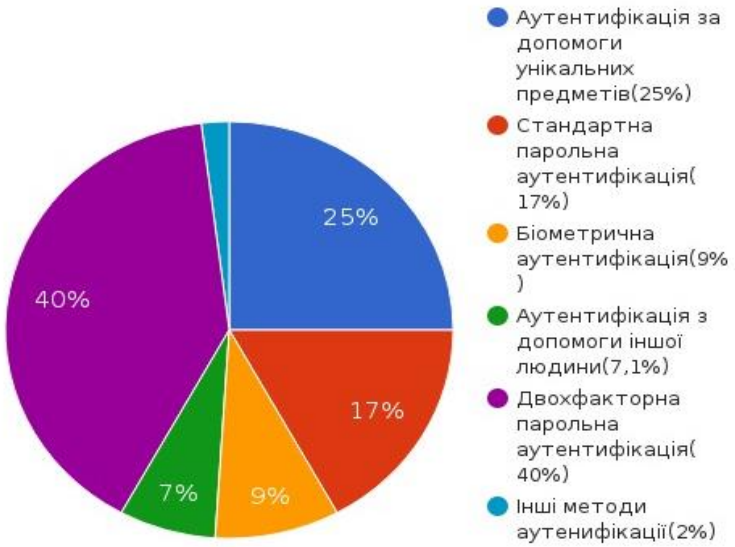


Рисунок 1.1 - Технології аутентифікації, які використовуються в європейських банках за даними опитування AtSecurity

За підсумками аналізу наведених вище фактів, можна зробити висновок про те, що найбільш поширені парольні і атрибутні (унікальні предмети) системи контролю і управління доступом. Але вони мають ряд суттєвих недоліків.

1.3. Переваги та недоліки парольних і атрибутних систем аутентифікаціїї

Парольні системи контролю та управління доступом є найбільш розповсюдженими засобами захисту інформації [1]. Перевагою таких систем є простота використання. Але подібні системи мають невисокий рівень безпеки, у зв'язку з великою кількістю недоліків. Виявлено такі недоліки парольних методів аутентифікації [91]:

– можливість підбору пароля;

– невиконання інструкцій по створенню безпечного пароля (недбале ставлення до процедури вибору пароля);

– існування і наявність у вільному доступі спеціалізованих утиліт для підпору і злому паролів;

– пароль може бути отриманий шляхом застосування фізичного та психологічного впливу на користувача;

– пароль може бути вкрадений (перехоплений при авторизації або бути візуально скомпрометований).

Проведено дослідження надійності застосування парольних методів ідентифікації і аутентифікації. Нижче перераховані виявлені факти, які підтверджують недоліки сучасних методів контролю та управління доступом. Згідно з даними, вказаними в звіті дослідницької лабораторії RSA [86]:

– 25% користувачів зберігають паролі у вигляді звичайного тексту на комп'ютері;

– 22% використовують для зберігання паролів мобільний телефон;

– 18% записують паролі облікових записів на листочках паперу.

Фахівці компанії Індід (indeed-id.ru) наводять приклад зберігання паролів облікових записів користувачів в одній з банківських установ, де компанія проводила оцінку стану інформаційної безпеки перед розгортанням рішення Indeed-Id Enterprise ESSO - для оперативного доступу до власних паролів (від декількох інформаційних систем, які використовуються в банку) більшість співробітників використовували липкий листочок паперу як засіб зберігання. Вони приклеювали його до клавіатури знизу разом з паролем [64]. За підсумками дослідження методів парольної аутентифікації зроблений висновок про неможливість застосування парольних методів для виявлення підміни законного авторизованого оператора. Вводити пароль періодично під час роботи для підтвердження авторизації відволікає оператора від безпосереднього виконання призначених для нього робочих завдань. Відсутня можливість виявити мінімально і максимально допустимі часові інтервали між уведеннями пароля.

Дослідження методів атрибутної аутентифікації за допомогою унікального предмета дозволяє забезпечити більш надійний захист інформації, ніж парольна аутентифікація. Але атрибутна аутентифікація, як з «пасивними», так і з «активними» унікальними предметами володіє декількома виявленими недоліками [91]:

– можливість крадіжки предмета у оператора;

– необхідність в спеціальному обладнанні для роботи з магнітними картками, смарт-картами і т.і.;

– можливість виготовлення копії унікального предмета;

– можливість підробки унікального предмета.

Проведено аналіз програмного забезпечення, яке блокує доступ до ключової системі в разі вилучення ключа (спеціально-запрограмованого USB flash-накопичувача). Розробниками пропонується оператору забирати USB-ключ з собою, коли оператор відлучається від ЕОМ. В цьому випадку відбувається автоблокування комп'ютера до моменту подальшого підключення ключа. Прикладами даного програмного забезпечення являються: Predator (https://www.predator-usb.com/predator/en/index.php) і Rohos Logon Key (http://www.rohos.ru/products/rohos-logon-key/). Безпека ключа (неможливість підробки та копіювання) забезпечується застосуванням алгоритму шифрування AES-256 і захистом ключа PIN-кодом. Основний недолік даних систем для захисту від підміни законного оператора це людський фактор (оператор може відлучитися від КС при цьому не вийняти USB-ключ).

1.4. Сучасні біометричні системи аутентифікаціїї і можливість їх застосування для виявлення підміни авторизованого оператора.

Проведено дослідження біометричних систем контролю і управління доступом. Біометричні системи аутентифікаціїї засновані на розпізнаванні фізіологічних і поведінкових характеристик людини. Дані системи класифікуються в залежності від характеристики, за якою людина розпізнається [83] (рис 1.2.).

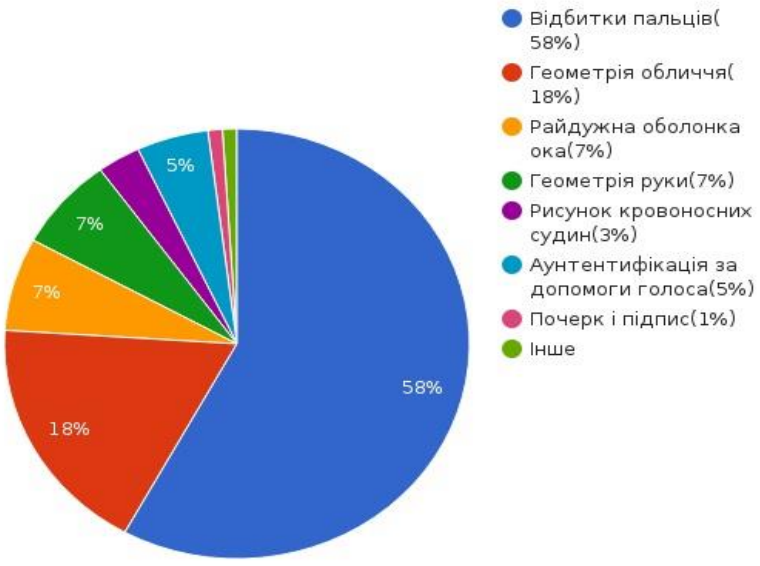


Рисунок 1.2 - Біометричні технології, які використовують для розпізнання

У процесі аутентифікації пред'явлений оператором зразок порівнюється з деякою погрішністю зі створеним раніше шаблоном. Похибка вибирається залежно від необхідного оптимального співвідношення помилок помилкового прийняття (FAR) і помилкового відмови (FRR), які відповідають точності і надійності роботи системи. Проведено дослідження та аналіз існуючих і активно експлуатованих біометричних систем ідентифікації і аутентифікації операторів [44, 72, 101] і проведена оцінка можливості їх застосування для виявлення підміни авторизованого законного оператора. Результати дослідження представлені в таблиці 1.1.

За підсумками проведеного аналізу зроблено висновок про те, що біометричні системи розпізнавання по відбитку пальця, райдужної оболонки ока, геометрії руки, вен руки, геометрії особи людини малозастосовні для виявлення підміни законного оператора, так як мають істотні обмеження у використанні і вимагають виконанню визначених умов при скануванні характеристик. Біометричні системи розпізнавання сітківки ока не дозволяють проводити постійний моніторинг особистості оператора, тому що вимагають виконання певних умов для сканування сітківки ока.

Таким чином, зроблено висновок про те, що для виявлення підміни законного оператора необхідно використовувати ті біометричні параметри, які проявляються при виконанні оператором завдань, пов'язаних безпосередньо з його роботою на КС. Найбільш часто зустрічаються завданнями, виконуваними оператором є робота з мишею і набір текстів на клавіатурі. Виходячи з даного припущення можна зробити висновок про те, що найбільш зручним для забезпечення процедури постійного таємного моніторингу з метою виявлення підміни оператора є клавіатурний почерк - динамічна поведінкова біометрична характеристика людини.

Таблиця 1.1 - Аналіз основних біометричних систем

Біометрич-ний параметр	Ціна пристрою (долл.)	Вірогід-ність помилки FAR, %	Переваги	Недоліки	Можливість застосування для виявлення підміни авторизованого оператора
1	2	3	4	5	6
Відбиток пальця	100	0,001	1. Висока достовірність. 2. Стійкість параметра. 3. Малий ідентифікаційний код. 4. Компактний зчитувач. 5. Низька вартість. 6. Застосування додаткових датчиків (Температури, сили натискання).	1. Безпосередній контакт з обладнанням. 2. Складність алгоритмів. 3. Легкість пошкодження папілярного візерунка пальців, що ускладнює ідентифікацію. 4. Сильна залежність якості зчитування від стану шкіри. 5. Можливість підробки відбитка пальця.	Проводиться впровадження сканерів відбитків пальців в мишки і клавіатури, в корпусу ноутбуків, але більшість з них служать тільки для забезпечення процесу авторизації (наприклад, BioLink U-Match Mouse компанії BioLink Technologies). Застосування з метою виявлення підміни оператора ускладнюється необхідністю постійного безпосереднього контакту пальців з зчитувачем, що є неможливим.

Продовження таблиці 1.1

1	2	3	4	5	6
Райдужна оболонка ока	>500	0.00001	1. Стійкість параметра. 2. Висока точність. 3. Надзвичайна складність підробки. 4. Відсутність безпосереднього контакту з обладнанням. 5. Висока швидкодія. 6. Сканування можна виробляти на відстані від декількох сантиметрів до декількох метрів.	1. Складність алгоритмів. 2. Висока вартість. 3. Низька доступність високих рішень.	Ускладнюється необхідністю постійного направленого погляду оператора в бік камери, володіє малими кутами сканування. Пристрій EyeLock компанії Hoyos Group розроблено для забезпечення процесу авторизації.
Геометрія руки(долоні)	>600	0.2	1. Стійкість параметра. 2. Простота алгоритмів.	1. Безпосередній контакт з обладнанням. 2. Незручна процедура сканування. 3. Великі розміри зчитувача.	Постійний моніторинг неможливий, якщо руки оператора розташовані поза зоною дії сканера.
Сітківка ока	4000	0.000001	1. Незмінність параметра з плином часу. 2. Висока точність. 3. Відсутність безпосереднього контакту з обладнанням.	1. Складність зчитування. 2. Складність алгоритмів. 3. Висока час обробки шаблону. 4. Висока вартість системи.	Відсутня, в зв'язку з необхідністю виконання визначених умов для зчитування характеристики.

Продовження таблиці 1.1

1	2	3	4	5	6
Геометрія обличчя	150	Від 5 до 0.0047	1. Можливість безперервної аутентифікації. 2. Відсутність безпосереднього контакту з обладнанням. 3. Низька вартість.	1. Залежність від умов освітлення, положення голови. 2. Залежність від міміки обличчя. 3. Залежність від перешкод (Окуляри, головний убір, зміна зачіски).	Можливість застосування для постійного моніторингу підміни оператора є, але присутній ряд обмежень, спричинених недоліками методу. Основне застосування - процес авторизації, наприклад, контролер-зчитувач STFR. 040EM марки Smartec.
Кровоносні судини руки(вени)	350	0.0008	.1. Висока точність. 2. Відсутність безпосереднього контакту з обладнанням. 3. Прихованість Характеристики.	1. Чутливість сканера до природного і штучного висвітлення. Характеристика залежить від стану здоров'я кровоносної системи людини.	Постійний моніторинг неможливий, якщо руки оператора розташовані поза зоною дії сканера. Біометричний зчитувач вен долоні PalmVein, представлений компанією Fujitsu застосовується для розпізнавання оператора в процесі авторизації.

1.5. Проблеми виявлення підміни законного оператора в інформаційній системі

Проведене дослідження загроз виявило, що найчастішими і небезпечними, з точки зору розмірів шкоди, є внутрішні загрози вихідні безпосередньо від співробітників, що мають доступ до ключової системі, а не від зовнішніх для організації зловмисників. До них відносяться (в порядку зменшення можливості зробити несанкціонований доступ до інформації): основний персонал, представники служби безпеки, допоміжний персонал, технічний персонал. Основними причинами незаконних дій персоналу є: образа, помста, бажання отримати матеріальну вигоду і так далі. Загроза несанкціонованого доступу до інформації внутрішніх суб'єктів ускладнюється тим, що вони знайомі зі структурою та основними функціями, принципами роботи засобів захисту інформації, що застосовуються на підприємстві, мають можливість доступу до КС.

У дослідженні приділено увагу небезпеки та ймовірності виникнення внутрішніх, інсайдерських, погроз інформаційної безпеки. Datapro Information Services Group провела поштовий опитування серед випадково обраних менеджерів інформаційних систем з метою з'ясування ситуації в області захисту інформації. Було отримано 1153 анкети, на основі яких отримані наведені нижче результати [76]:

- 3% зовнішні порушення (наприклад, атаки хакерів);
- 70-75% внутрішні порушення, з них:
  a) 10% здійснені скривдженими і незадоволеними працівниками;
  b) 10% здійснені з корисливих мотивів персоналом системи;
- 50-55% результат ненавмисних помилок персоналу та / або користувачів системи в результаті недбалості, халатності або некомпетентності.

Дослідження [58], проведене компанією InfoWatch в 2006 році, присвячене проблемам інформаційної безпеки російського держсектора охопило 191 державну організацію. даний проект уточнює результати третього щорічного дослідження «Внутрішні IT загрози 2006 », в ході якого було опитано 1450 російських організацій у всіх секторах економіки. Результати дослідження показали, що зовнішні загрози (45%) зустрічаються рідше, ніж внутрішні загрози (55%). Тільки 15% організацій уникли витоків інформації в плині року. Також компанія повідомляє про збільшення на 16% загального числа витоків інформації з організацій в порівнянні з 2011 роком [101]. Спеціалізований ресурс http://www.datalossdb.org/ прийшов до Аналогічних висновків, повідомляючи про зростання числа витоків інформації в 2012 році на 50% [10].

У звіті «Trends in IT Security Threats: 2007», підготовленому Computer Economics, перше місце по збитку (фінансових збитків від порушень інформаційної безпеки) займають загрози

інформаційної безпеки виходять від інсайдерів, випереджаючи інші види загроз [102]. За даними фахівців CSI в 2007 році з інсайдерськими погрозами зіткнулися 59% організацій [102]. Дослідження, проведене кадровим холдингом АНКОР, виявило, що 22% операторів користуються службовою інформацією для стороннього заробітку [74]. Аналіз інформаційної безпеки, проведений компанією Searchlnform в російських організаціях визначив наступні факти [74]:

– 19,2% співробітників готові відмовитися від пропозиції про продаж секретної інформації;

– 43,7% співробітників готові заробити на продажу важливою інформації;

– 12% про співробітників готові надати конфіденційну інформацію зловмисникам безкоштовно.

За даними опитування, проведеного в 2011 році фірмою Sailpoint Technologies [64] на території США, Великобританії та Австралії показало що з 3,5 тисячі опитаних співробітників (кожен з яких є по суті інсайдером) досить велика кількість готові вкрасти секретну інформацію у своїх компаній. 22% в США, 29%) в Австралії і близько 50% опитаних у Великобританії. 5% респондентів в США, 4% в Австралії і 24% у Великобританії продали б секретну інформацію своєї компанії з метою особистого збагачення. Схоже дослідження, проведене корпорацією Symantec спільно з спільнотою Профессіонали.ру на території Російської Федерації [64] показало, як співробітники компаній звертаються з внутрішньої інформацією. За результатами проведеного опитування, близько 70% працівників крадуть ділову інформацію, а 56%) готові вкрасти інформацію з атрибутами обмеженого доступу. У процесі дослідження аналітики виявили чотири типи співробітників-інсайдерів:

– 24% можуть піддати компрометації корпоративну обчислювальну мережу, не підозрюючи про це;

– 22% ігнорують базові вимоги безпеки, при цьому усвідомлюючи ступінь загрози;

– 7% увійшли до групи тих, хто переслідує власні корисливі мети;

– 47% опитаних службовців досить акуратно поводяться з комерційною таємницею.

Виявлено наступні факти про значний збиток, завданий інсайдерами:

– жителі Америки втратили $ 929 мільйонів через попадання паролів платіжних карт в руки третіх осіб [49];

– Жером Кервьєль завдав інвестиційному банку Societe Generale, в якому він працював трейдером, збиток в 5 млрд. євро, використовуючи в своїх махінаціях паролі колег [49];

– Джагмен Чан, співробітник банку HSBC, вкравши паролі колег, перевів 90 млн євро на рахунки інших банків [49];

– американська паливно-газова корпорація Enron Corporation оголосила про своє банкрутство через витік інформації, організованою її співробітниками [74].

За підсумками дослідження зроблено висновок про те, що внутрішні загрози є найнебезпечнішими для інформаційної безпеки та часто реалізованими при використанні парольних і атрибутних методів аутентифікації і авторизації в якості засобів захисту інформації. Рішення завдання виявлення підміни оператора є актуальним на сьогоднішній день.

Для захисту КС від несанкціонованого доступу винаходяться різні методи. Наприклад, USB-клавіатура KSI SonarLocID Keyboard, покликана забезпечити збереження важливої інформації. У клавіатуру вбудований радар, який автоматично визначає, чи знаходиться користувач за комп'ютером. Якщо оператор не заблокував доступ до системи, залишивши місце за комп'ютером. Така клавіатура за допомогою радара це визначить і сама заблокує систему. Мінусом цієї системи є те, що є можливість її обдурити (випадково або навмисно), наприклад, поставивши перед радаром якийсь предмет.

Таким чином, проблема виявлення підміни авторизованого оператора залишається актуальною і вимагає розробки нових варіантів розв'язання проблеми.

1.6 Аналіз клавіатурного почерку в процесах аутентифікації, ідентифікації та виявлення підміни оператора

Проведено дослідження методів ідентифікації і аутентифікації за клавіатурним почерком.

Використання методів поведінкової біометрії, заснованої на клавіатурному почерку, на відміну від методів фізіологічної біометрії не вимагає придбання додаткових біометричних пристроїв. Зразок клавіатурного почерку може бути отриманий за допомогою існуючих систем, таких як стандартна клавіатура. Це робить ці методи недорогими і ненав'язливими для оператора, і також може бути застосовано таємно, що дозволить поліпшити існуючі комп'ютерні системи забезпечення безпеки.

Відзначено, що основу дослідження клавіатурного почерку поклало дослідження роботи операторів телеграфу. В середині 19-го сторіччя, коли телеграф часто використовувався, було помічено, що оператори телеграфу могли ідентифікувати інших операторів по їх ритму набору.

Метод «Fist of the Sender» («Кулак відправника») використовувався під час Другої світової війни для ідентифікації відправника телеграфного повідомлення за ритмом, темпом і часу натискання телеграфного ключа [42].

Bryan і Harter [5] провели ряд експериментів на тридцяти семи телеграфних операторах, що мають різні ступені уміння набору. Вони відзначили, що телеграфні оператори могли дізнатися інших операторів по стилю набору.

На початку 80-их Національний науковий фонд і Національне Бюро Стандартів в Сполучених Штатах провели дослідження, встановлюють, що зразки клавіатурного почерку містять унікальні особливості, які можуть бути ідентифіковані [21].

Shaffer [39] показав, що набір тексту є запрограмованим умінням і, що руху при друку організовуються до їх фактичного виконання. Іванов А.І. в своїх працях показав, що при наборі тексту на клавіатурі однієї рукою виявляються задіяні близько 50 м'язів пальців руки і пальців передпліччя і ще приблизно 20 м'язів плеча і плечового пояса [72], тобто при друку двома руками людина управляє приблизно 140 м'язами. Тому зразок почерку людини є поведінкової особливістю, яка розвивається з плином часу і, таким чином, не може бути змінена, втрачена або забута.

У будь-поведінкової біометричної характеристиці можуть спостерігатися великі зміни в особливостях характеристики. Однак, вони повинні надати достатньо інформації, щоб ідентифікувати і визначати справжність особистості за шаблоном почерку [14].

Купер [8] був першим дослідником машинописного набору тексту, який розбив процес набору тексту на чотири стадії:

1) сприйняття людиною тексту;

2) збереження його в пам'яті;

3) переклад людиною збережених в його пам'яті символів в команди, передаються м'язам;

4) безпосередньо набір тексту з процедурою зворотного зв'язку, необхідної для перевірки точності набору тексту.

Salthouse [36] допрацював і поліпшив запропоновану Купером модель процесу набору тексту машиністом. Butsch [7] визначив, що «інтервал копіювання », тобто кількість тексту зберігається в пам'яті оператора при наборі залежить від досвідченості і умінь оператора. Використання пам'яті в як короткостроковий буферу перед друкуванням було доведено експериментами, проведеними Thomas і Jones [16]. Купер продемонстрував у своїх дослідженнях, що оператори розбивають текст на маленькі передбачувані групи, через обмеження на розмір буферної пам'яті. Verwey і Dronkert [43] в своїх експериментах довели, що процеси сприйняття читаного тексту і м'язових рухів при наборі тексту відбуваються

одночасно. У дослідженні, проведеному Shaffer [39], він запропонував, що існує внутрішній регулярний ритм набору визначених послідовностей символів. Він припустив, що клавіатурний почерк не є фіксованою характеристикою людини, а постійно змінюється. Він також зауважив, що процес набору заснований на знанні переходів і рухів між клавішами, і, що рухи м'язів при натисканні на клавіші організовані до їх фактичного виконання [38]. Інтервали між послідовними натисканнями клавіші для досвідчених операторів, як показали спостереження, були меншими, ніж в операторів з низької кваліфікації. R. S. Gaines, W. Lisowski, S. J. Press and N. Shapiro довели, що швидкість, з якою переміщаються пальці вдвічі швидше у досвідчених машиністів, ніж у недосвідчених [11]. Ostry [29] в своєму дослідженні часу переміщень рук при друку показав, що організація руху пов'язана з поточним психофізіологічних станом людини.

На підставі проведеного аналізу перерахованих вище досліджень запропоновано вважати клавіатурний почерк індивідуальної та унікальною для кожної людини поведінкової біометричної характеристикою. Запропоновано використовувати шаблон клавіатурного почерку в якості ідентифікатора оператора ключової системи.

Rumelhart і Norman [34] провели комп'ютерне моделювання дій оператора, що працює з клавіатурою. Вони промоделювали час інтервалу між натискання клавіш і повторення помилок при введенні. Моделі Купера, Salthouse, Rumelhart і Norman є першими моделями, розробленими з метою аналізу властивостей і характеристик клавіатурного почерку оператора.

Виділено два метода розпізнавання клавіатурного почерку оператора:

– по заздалегідь відомій контрольної (парольній фразі). Даний метод використовується в процесах авторизації оператора. Метод вперше запропонований Spillane [40]. Шаблон почерку зберігається разом з парольною фразою, і при аутентифікації оператора шаблон почерку і пароль порівнюються з почерком і паролем оператора, який претендує на доступ до КС. Зроблено висновок, що даний метод не підходить для виявлення підміни авторизованого оператора, так як оператори КС рідко вводять фіксовані, заздалегідь відомі слова і фрази.

– по вільному контрольному тексту. Метод вперше запропонований Marsters [24]. Даний метод має на увазі безперервний контроль клавіатурного почерку оператора. Однак, Marsters пропонує спочатку визначити набір слів, які часто набирає оператор, і надалі ідентифікувати почерк по ним. Зроблено висновок, що даний метод дозволяє проводити постійний потайний клавіатурний моніторинг оператора з метою виявлення підміни оператора за умови незалежності шаблону почерку від набирається тексту.

Під час набору тексту оператором, можна відзначити три події: момент натискання клавіші, утримання, і момент відпускання клавіші. На основі вибірки моментів натискання і утримання клавіш розраховуються тимчасові характеристики почерку. Нижче виділено наступні характеристики клавіатурного почерку, які застосовуються в системах ідентифікації і аутентифікації оператора [106,107].

Час інтервалу між натисканнями клавіш [3] (час від натискання однієї клавіші до моменту натискання наступної клавіші або час від моменту відпускання однієї клавіші до моменту натискання наступної). Використання цієї характеристики вимагає довгого збору статистичних даних. Розраховано, що для збору даних про час між натисканнями 33 клавіш, відповідним буквах українського алфавіту (кожній клавіші відповідає 33 самостійних вибірки для комбінацій «АА», «АБ», «АВ» ... «АЯ» і т.д.) з розміром вибірки в 30 елементів потрібно 32670 елементів вхідних даних. Таким чином, обгрунтовано, що дана характеристика почерку не може бути застосована для виявлення підміни законного оператора.

Час введення двограмм [22] (наприклад, «АА», «ОЕ», «ЯЯ»), триграм [4] (наприклад, «ААА», «МАМ», «ЕЮЯ»), тобто час від натискання першої клавіші, до моменту відпускання останньої клавіші N-грами. Метод аналізу даної характеристики, так само як і попередній, вимагає збору великої кількості статистичних даних. Цим обґрунтована непридатність даної характеристики для виявлення підміни оператора.

Час утримання клавіш [25,33] (час від натискання до відпускання клавіші). Кількість вибірок статистичних даних часу утримання відповідає кількості натискає оператором клавіш, тобто 33 букв українського алфавіту відповідає 33 вибірки часу утримання клавіш. Запропоновано використовувати дану характеристику почерку для організації процедури постійного таємного клавіатурного моніторингу особистості оператора ключової системи з метою виявлення підміни.

Сила тиску, прикладеного до клавіші під час набору [2,23]. Вимагає установки додаткових датчиків (по одному на кожну клавішу) в клавіатурі. Це призводить до збільшення складності розробки клавіатур, збільшення їх вартості, і зростанню ймовірності виходу з ладу клавіатури.

Швидкість [19, 26] (кількість набраних оператором символів в відрізок часу) і ритм-поміж [18]. Виявлено, що дана характеристика почерку залежить від психофізіологічного стану оператора і, тому, дуже мінлива . Цим обґрунтована складність застосування даних характеристик в процесі виявлення підміни законного оператора. У загальному вигляді, функція A(t), що описує процес набору тексту оператором на клавіатурі, може бути записана наступним чином:

$$\boldsymbol{A(t) = B(t) + C(t) + D(t)}, \text{де}, \qquad (1.1)$$

B (t) - складова, що характеризує підсвідомі процеси мислення при наборі тексту;

C(t) - складова свідомих процесів мислення;

D(t) - механічні характеристики клавіатури, що впливають на процес набору тексту.

Основним завданням системи біометричної ідентифікації оператора за особливостями клавіатурного почерку є завдання виділення і подальшої ідентифікації компоненти B(t) з функції A(t), яка визначає вихідні дані для системи ідентифікації після вимірювання тимчасових характеристик клавіатурного почерку оператора. Для цього відповідно необхідно виділити компоненти C(t) і D(t) з вихідної функції A(t). Очевидно, що через неможливість побудови механічної моделі рухів людини при наборі тексту єдиним прийнятним рішенням є збір статистичних даних про клавіатурному почерку великої кількості операторів і побудова емпіричних залежностей C(t) і D(t).

Імовірність аутентифікації оператора за часом утримання клавіш в залежності від довжини ключової фрази є значно більш стабільної характеристикою клавіатурного почерку оператора, ніж час між натисканнями клавіш (пауз), яке збільшується з ростом довжини ключовий фрази. Це пояснюється тим, що процес натискання клавіші на клавіатурі є істинно підсвідомим процесом мислення. Характер даної функції практично не змінюється для широкого кола операторів незалежно від їх кваліфікації та досвіду роботи з клавіатурою. Звідси випливає, що складова B (t) найбільш точно характеризується часом утримання клавіш при введенні тексту оператором. Час утримання клавіші розраховується за формулою (1.2).

$$T_i^{\text{утрим.клав}} = T_i^{\text{відпускання}} - T_{\text{i}}^{\text{натискання}}, \qquad (1.2)$$

де:

$T_{\text{i}}^{\text{утримання}}$ - час утримання клавіші;

$T_{\text{i}}^{\text{відпускання}}$ - час відпускання клавіші;

$T_{\text{i}}^{\text{натискання}}$ - час натискання клавіші.

За підсумками аналізу характеристик клавіатурного почерку запропоновано використовувати час утримання клавіш в процесі виявлення підміни законного оператора [99,101]. У шаблон почерку оператора запропоновано зберігати усереднені значення часу утримання клавіш. маючи такий шаблон, стає можливо ідентифікувати і аутентифікувати оператора ключової системи. Далі наведено аналіз відомих методів ідентифікації і

аутентифікації операторів по клавіатурного почерку: статистичних методів, методів заснованих на застосуванні нейронних мереж, розпізнаванні образів і генетичних алгоритмах.

Статистичні методи полягають в обчисленні відхилень характеристик поточного почерку оператора, який претендує на доступ до КС і характеристик почерку в шаблоні, збереженого в системі для даного оператора. Для порівняння можуть використовуватися t-тести, відстань Евкліда, відстань Хеммінга і т.д. Joyce і Gupta [17] використовуючи статистичні методи отримали точності аутентифікації оператора досягли частоти помилкових прийомів (FAR) 0.25% і частоти помилкових відмов (FRR) 16.36%. У своїй роботі вони використовували відстань Хеммінга (1.3) і відстань Махаланобіса (1.4).

$$\mathrm{M} = \sum_{i=1}^{N} (|A_i| - |B_i|) \tag{1.3}$$

$$\mathrm{M} = \sqrt{\sum_{\mathrm{i}=1}^{\mathrm{N}} \frac{(\mathrm{A_I} - \mathrm{B_I})}{\sigma_{\mathrm{i}}^2}} \tag{1.4}$$

де:

i- номер клавіші;

N - кількість аналізованих клавіш;

A_i - тимчасова характеристика для клавіші з шаблону оператора, претендує на доступ;

B_i - тимчасова характеристика для клавіші з шаблону, що зберігається в базі шаблонів для конкретного оператора;

σ- середньоквадратичне відхилення A_i, від B_i.

Guven і Sogukpinar [13] грунтуючись на векторному аналізі досягли точності ідентифікації оператора в 95%. Аналіз робіт зазначених дослідників дозволив зробити висновок, що головною проблемою статистичних методів є недолік даних на стадії навчання, тобто при отриманні шаблону почерку оператора.

Нейромережеві методи, вперше даний метод був застосований Obaidat і Macchiarolo [28] для аутентифікації і ідентифікації операторів за часом між натисканнями клавіш. Вони досягли точності ідентифікації оператора в 96.8%, використовуючи нейронну мережу, засновану на сумі творів. Yong і ін. [45] запропонували використовувати динамічну нейронну мережу. За аналізом даних досліджень зроблено висновок про те, що головна перевага нейронних мереж полягає в тому, що вони можуть обробляти відразу декілька параметрів почерку. Виділено основні недоліки застосування нейронних мереж при розпізнаванні

клавіатурного почерку: потрібно чимало часу для процедур навчання і аутентифікації, присутність ситуацій, коли нейронна мережа не може навчиться через особливості вхідний вибірки. Так як даний метод використовується тільки в якості «чорного ящика», неможливо визначення достатнього для отримання шаблону почерку і подальшої успішної роботи обсягу і складу вхідних вибірки. Також, у разі додавання шаблону нового оператора ключової системи доведеться перенавчати всю нейронну мережу.

Розпізнавання образів - Giot і ін. [12] запропонували використовувати метод опорних векторів для розпізнавання клавіатурного почерку. Вони досягли рівня ідентифікації в 95%. Виявлено головна перевага даного методу - висока точність, обгрунтована ігноруванням помилок і похибок вимірювань часу утримання клавіш. Недоліком методу є те, що ідентифікація проводиться не за всіма шаблонами, а лише по тій частині шаблонів, яка знаходиться на кордонах.

Генетичні алгоритми - Revett і ін. [32] використовуючи генетичні алгоритми досягли ймовірності виникнення помилок FAR в 0.43% і FRR в 4.75%. Виявлено основна перевага використання генетичних алгоритмів - вони можуть легко звертатися з великими базами даних і можуть обробляти багатовимірні, не диференціальні, безперервні, і навіть непараметричні дані. виділено головні недоліки генетичних алгоритмів - висока трудомісткість, що обмежує сферу застосування, низька стійкість до відхилень тимчасових характеристик почерку, даний метод не гарантує знаходження оптимального рішення. Проведений аналіз методів аутентифікації і ідентифікації операторів за клавіатурним почерком дозволив вибрати в якості основи для подальших досліджень ймовірносно-статистичні методи. В як запобіжний схожості двох клавіатурних почерків вибрано Евклидову відстань. Евклідова відстань має ту перевагу, що вона обчислюється за вихідними даними і не зміниться при введенні нового елемента в вибірку, який є викидом.

1.7 Реалізація механізмів підсистеми постійного таємного клавіатурного моніторингу з метою виявлення підміни законного оператора

На основі зробленого аналізу пропонується наступна архітектура біометричної підсистеми виявлення підміни законного оператора (рис. 1.3.), що забезпечує процес отримання шаблону почерку і порівняння почерків. Дана архітектура відображає логічну декомпозицію системи на підсистеми.

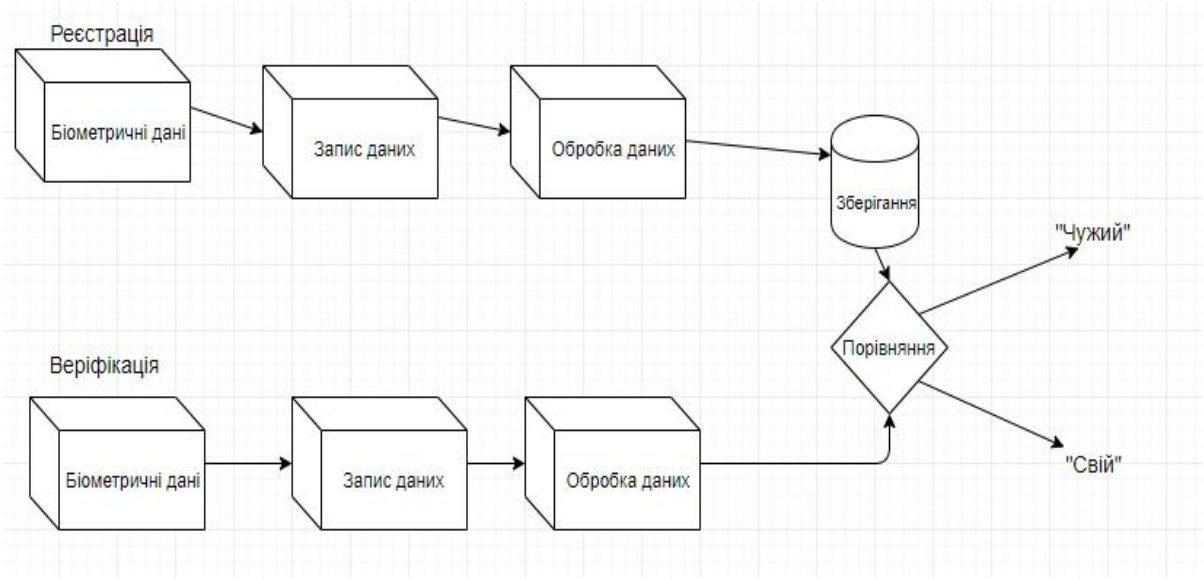


Рисунок 1.3 - Спрощена архітектура біометричної системи виявлення підміни законного оператора

Як видно на рисунку, підсистема складається з декількох блоків, описаних нижче.

Блок отримання і запис клавіатурного почерку оператора. Відповідає за отримання тимчасових міток подій натискання і відпускання клавіш, і зазначає, до якої клавіші відносяться ці події. Для отримання часу виникнення подій використовується таймер з високою роздільною здатністю, вбудований в сучасні ЕОМ. Даний блок містить так само фільтр довгих натискань на клавіші, які є викидами для вибірки часу утримань клавіш. Важливим моментом є точність визначення моменту виникнення подій клавіатури. Killourhy і Maxion [20] проводили експерименти по дослідженню впливу дозволу годин при аналізі клавіатурного почерку. Вони помітили, що EER збільшується приблизно на 4.2% при використанні дозвілу таймера 15 мс замість дозволу таймера 1 мс. Системна похибка викликає проблеми, що призводять до похибок підрахунку часу. Отже, системи повинні бути зроблені стійкими до похибок вибірки часу.

Блок обробки вибірки подій клавіатури. Відповідає за обчислення усереднених значень часу утримання клавіш. В якості усередненого значення вибрано математичне сподівання часу утримання клавіші.

Блок зберігання клавіатурного почерку. дозволяє зберегти шаблонні значення клавіатурного почерку операторів в базу шаблонів.

Блок порівняння поточного клавіатурного почерку і шаблонного. Служить для порівняння почерків, заснованому на розрахунку Евклідової відстані і прийняття рішення про аутентифікації і ідентифікації оператора за результатами порівняння. Для оцінки точності розпізнавання оператора в розробленій підсистемі розраховуються помилки першого (FRR) і

другого роду (FAR). FRR (1.5) характеризує ймовірність того, що законний оператор не буде упізнаний підсистемою. FAR (1.6) характеризує ймовірність того, що оператор, який не зареєстрований в системі, буде визнаний як законний.

$$FRR = \frac{\text{Кількість\_помилкових \_відмов}}{\text{Загальна\_кількість\_спроб\_доступу}} \quad (1.5)$$

$$FAR = \frac{\text{Кількість\_помилкових \_спроб\_доступу}}{\text{Загальна\_кількість\_спроб\_доступу}} \quad (1.6)$$

Процес постійного таємного клавіатурного моніторингу вимагає динамічного надходження і поновлення даних про клавіатурний почерк оператора. Для цього запропоновано при виникненні події клавіатури додавати до вибірки отримане нове значення часу утримання клавіші і видаляти першу подію, яка зберігалась у вибірці. Потім, на основі зміненої вибірки знову відбувається порівняння клавіатурних почерків, що дозволяє оперативно відреагувати на зміни клавіатурного почерку, наприклад, в випадку, якщо зловмисник отримав доступ до КС.

Проведено дослідження відомих систем контролю і управління доступом, заснованих на аутентифікації і ідентифікації оператора за клавіатурним почерком. Програмне забезпечення, яке випускається компаніями AdmitOneSecurity Inc. (Вашингтон) і Authenware Corp. (Флорида), BioChec (Нью-Йорк) включає в себе алгоритми аутентифікації по клавіатурного почерку, як характеристики почерку використовується час між натисканнями клавіш. Почерк визначається під час введення оператором пароля до системи. Біометричні системи Behaviometric (BehavioSec, Швеція), TypeSense (Deepnet Security, Лондон), DSGatewayTM (Delfigo Security, Бостон), KeystrokelD (ID Control, Нідерланди), Trustable Passwords (iMagicSoftware, Каліфорнія) засновані на рішенні доповнити парольну авторизацію розпізнаванням за клавіатурним почерком.

1.8 Висновки до розділу

1. На основі проведеного дослідження доведено, що застосовувані зараз парольні, атрибутні (предметні) і біометричні методи захисту інформації не забезпечують захисту інформації, що обробляється в ключовий системі від загроз інсайдерства.

2. Запропоновано використовувати метод аутентифікації і ідентифікації за клавіатурним почерком інформації від загроз інсайдерства.

3. Проведено аналіз властивостей і характеристик клавіатурного почерку. Запропоновано використовувати час утримання клавіш в якості параметра, що дозволяє проводити постійний потайний клавіатурний моніторинг з метою виявлення законного оператора.

4. Проведено аналіз моделей, методів, алгоритмів і засобів розпізнавання клавіатурного почерку оператора. запропоновано використовувати метод вільного контрольного тексту і ймовірносно-статистичні методи з метою розпізнавання клавіатурного почерку оператора.

РОЗДІЛ 2
РОЗРОБКА МАТЕМАТИЧНИХ І АНАЛІТИЧНИХМОДЕЛЕЙ МЕХАНІЗМУ РОЗПІЗНАВАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ

2.1 Розробка математичної моделі часу утримання клавіш, яка заснована на нормальному розподілі

Аналіз клавіатурного почерку ґрунтуються на припущенні, що клавіатурний почерк представляється у вигляді усереднених значень подій клавіатури. У системах Microsoft Windows виділяють три види подій клавіатури:

– подія KeyDown, яка відбувається один раз. Спрацьовує у час натискання фізичної клавіші. Подія нижчого рівня реагує на натискання будь-якої клавіші на клавіатурі. Повертає код натиснутою клавіші;

– подія KeyUp, яка виникає один раз після того, як оператор відпускає фізичну клавішу. В іншому подія аналогічно KeyDown;

– подія KeyPress, яка може виникати кілька разів, коли оператор утримує натиснуту клавішу. Ця подія виникає при натисканні клавіші, яке призвело до введення знаку.

Для виявлення усереднених значень запропоновано використовувати статистичний метод, який представляє собою сукупність взаємопов'язаних прийомів дослідження масових об'єктів і явищ з деякою внутрішньою неоднорідністю з метою отримання кількісних характеристик і виявлення загальних закономірностей шляхом усунення випадкових особливостей окремих одиничних спостережень. У системах розпізнавання клавіатурного почерку статистичними даними є значення часу подій клавіатури. Обраним ознакою клавіатурного почерку є час утримання клавіш, який відповідає часовому інтервалу між подіями KeyDown (A) і KeyUp (A), де A - одна з клавіш клавіатури. У зв'язку з використанням даного методу необхідний збір статистики, що складається з вибірки тимчасових значень, де елементом вибірки буде час утримання клавіші.

У ймовірносно-статистичному формулюванні виникає необхідність побудови середньостатистичних шаблонів на основі зразків, пред'явлених системі в режимі навчання. Припущено, що значення подій клавіші розподілені по нормальному закону. При цьому слід враховувати, що на характеристики клавіатурного почерку людини впливає безліч факторів: програмні і апаратні затримки (які теж є випадковими величинами), рух нервового імпульсу по нейронам, час відгуку м'язів людини на сигнал посланий мозком і т.і. Значить, на клавіатурний почерк впливає безліч незалежних випадкових величин. Ефект їх складання

описується формулою Гаусса [77]. Відповідно для зменшення впливу випадкових помилок необхідно уможливити відбір проб досліджуваної величини кілька разів.

Розглянемо застосування формули Гаусса [95] в процесі обробки результатів вимірювання характеристик клавіатурного почерку. Припустимо, що ми вимірюємо час утримання якийсь конкретної клавіші, позначимо цю величину **X**. В результаті проведених вимірювань ми отримали вибірку значень величини (2.1).

$$X_1, X_2, X_3 \ldots . X_N \qquad (2.1)$$

Цей ряд значень величини **X** складе нашу вибірку часу утримання клавіші. По даній вибірці дається оцінка результату вимірювань, тобто усереднене значення ЧУК клавіші, в яке прагне укластися «натреновану» руку при натисканні на клавішу. Величину, яка буде такою оцінкою, ми позначимо $\bar{A}$. Але так як це значення оцінки результатів вимірів не буде являти собою істинного значення вимірюваної величини часу утримання клавіші, необхідно оцінити помилку вимірювання. Припустимо, що ми зуміємо визначити оцінку помилки ΔX. У такому випадку ми можемо записати результат вимірювань у вигляді (2.2).

$$\mu = \bar{A} \pm \Delta X \qquad (2.2)$$

Таким чином необхідно, маючи вибірку (2.1), знайти оцінку результату вимірювань $\bar{A}$, її помилку ΔX і надійність **P**. Така задача вирішується застосуванням теорії ймовірностей і математичної статистики. У задачі вимірювання ЧУК виникаючі помилки підкоряються нормальному закону розподілу. Запропоновано в якості оцінки результатів вимірювань ЧУК розраховувати середнє значення всіх елементів зібраної для конкретної клавіші вибірки (2.3).

$$\bar{A}=\frac{\sum_{i=1}^{N} X_i}{N} \qquad (2.3)$$

де N - число вимірювань.

Значить, для вибірки в N вимірювань часу утримання, найбільш вірогідним значенням вимірюваної величини буде її середнє значення (арифметичне). Отримане середнє значення ЧУК прагне до істинного значення μ вимірюваної величини $\bar{A}$ при збільшенні числа вимірювань, тобто при $N \to \infty$.

Середньоквадратичної помилкою середнього арифметичного називається величина (2.4).

$$S_{\bar{A}} = \sqrt{\frac{\sum(\bar{A} - X_i)^2}{N(N-1)}} = \frac{S}{\sqrt{N}} \quad (2.4)$$

Точність оцінки зростає при збільшенні числа вимірювань. Помилка $S_{\bar{A}}$ дозволяє оцінити точність, з якою розраховано середнє значення ЧУК [94]. Обґрунтовано, що запропонований спосіб розрахунку помилок має надійність 0,68, коли величина часу утримання клавіш вимірюється не менше 30 разів.

При малій кількості вимірювань вводиться спеціальний коефіцієнт Стьюдента t [90] для розрахунку абсолютної помилки, який залежить від надійності P і числа вимірювань N (2.5).

$$\Delta X = S_{\bar{A}} * t, \quad (2.5)$$

де ΔX - абсолютна помилка для даної ймовірності попадання в довірчий інтервал.

Обґрунтовано, що величина середньоквадратичної помилки може бути застосована для розрахунку ймовірності, з якою справжнє значення ЧУК знаходиться в заданому інтервалі поблизу середнього арифметичного.

При N→ ∞ $S_{\bar{A}}$→0, тобто розмір інтервалу, в якому із заданою довірчою ймовірністю знаходиться істинне значення часу утримання клавіші ц, прагне до нулю зі збільшенням числа вимірювань.

В результаті проведеного дослідження показано, що, збільшуючи п, можна отримати результат з будь-яким ступенем точності, коли ймовірність виникнення помилок буде прагнути до нуля. Однак неможливо домогтися стовідсоткової точності, так як при досягненні рівня випадкових помилок, рівного рівня систематичних помилок, точність перестане збільшуватися зі збільшенням числа вимірювань.

Відомо що подальше збільшення числа вимірювань не матиме результату, тому що остаточна точність результату буде вимірюватися рівнем систематичної помилки. Визначивши значення систематичної помилки, вибирають прийнятний рівень випадкових помилок. Показано, що вибір порога надійності здійснюється виходячи з практичних міркувань тієї відповідальності, з якою робляться висновки про параметрах. Зазвичай в системах біометричної ідентифікації використовують 99,9% -й поріг ймовірності попадання в довірчий інтервал. Рівень ймовірності попадання в довірчий інтервал показує, яку максимальну ймовірність виникнення помилки першого роду система вважає допустимою.

Зменшення рівня ймовірності попадання в довірчий інтервал, інакше кажучи, жорсткість умов тестування гіпотез, збільшує ймовірність помилок другого роду.

Отже, вибір рівня ймовірності попадання в довірчий інтервал повинен здійснюватися з урахуванням можливого збитку від виникнення помилок першого і другого роду. З огляду на, що вибіркове розподіл деякої статистики, наприклад середньої арифметичної величини, при досить великих обсягах вибірок (наприклад, 100 і більше елементів) має нормальну форму, можна записати вираз:

$$-t \leq \frac{\bar{A} - \mu}{S_{\bar{A}}} \leq t \tag{2.6}$$

Цей вислів означає, що ймовірність того, що середня X, знайдена за вибіркою, відхилиться випадковим чином від центру ц на яку- то частку квадратичної помилки Sx, може бути оцінена через нормоване значення за таблицями нормального розподілу. Звідси можна стверджувати, що середня ц знаходиться з цієї ймовірністю в інтервалі (2.7).

$$\bar{A} - tS_{\bar{A}} \leq \mu \leq \bar{A} + tS_{\bar{A}} \tag{2.7}$$

Для кожної вибірки введення конкретного символу будуть матися два таких рівняння в зв'язку з бімодальне розподілу часу утримання клавіш. Величини $\bar{A}$ і $S_{\bar{A}}$ визначають за вибіркою, а t залежить тільки від одного з трьох значень ймовірності попадання в довірчий інтервал 0,95; 0,99; 0,999, приймаючи величини 1,96; 2,58; 3,29. Таким чином, задавши для обраного довірчого інтервалу певне значення Р, обчислюють необхідну кількість вимірювань часу утримання клавіш, що забезпечує мінімальний вплив випадкових помилок на точність результату. Отже, можна визначити, скільки разів повинна бути натиснута конкретна клавіша, для того щоб зібрати статистику, що характеризує усереднене ЧУК. Відповідно, для того щоб визначити клавіатурний почерк оператора КС, потрібно зібрати дані про середні значення часу утримання всіх використовуваних клавіш (наприклад, 26 клавіш, які відповідають літерам англійського алфавіту).

Таким чином, коли система працює в режимі навчання, необхідно отримати 26 вибірок, які складаються з N елементів. У зв'язку з бімодальне розподілу клавіатурного почерку Кожна вибірка ЧУК розділяється на дві підвибіркі, в залежності від присутності або відсутності накладення при натисканні клавіші. Середні значення кожної з підвибірок будуть збережені в шаблоні почерку оператора. Але таке припущення відповідає деякому ідеальному випадку, коли розподіл літер, які вносить оператор, підпорядковується рівномірному розподілу.

2.2 Розробка математичної моделі часу утримання клавіш, заснованої на бімодальному розподілі

Аналіз процесу набору тексту операторами ключових систем показав, що час утримання клавіш підпорядковується не нормальному, а бімодальному закону розподілу. Тобто перетину двох нормальних розподілів. Причиною бімодальності часу утримання клавіши є присутність накладень (одночасне натискання) клавіш при наборі. Це викликано одночасними рухами кількох пальців у операторів, які впевнено володіють методом друку. Накладення натискань клавіш відбувається, коли одна клавіша ще не відпущена, а інша вже натискається. Спостерігається тенденція до підвищення кількості накладень з підвищенням швидкості набору.

Переважна більшість накладень відбувається, коли клавіші сусідніх літер в слові натискаються різними пальцями. Накладення відбуваються з наступних причин:

• висока швидкість друку, при якій складач не встигає відпускати попередні клавіші до натискання наступних;

• великий час утримання клавіш натиснутими;

• поєднання першого і другого факторів.

Можна розрізнити три види накладень[46]:

1. В момент утримання першої клавіші відбувається натискання другої. Кнопка «К1» натискається. Далі відбувається натискання клавіші «К2», але «К1» ще не відпущена. Потім відбувається відпускання клавіші «К1», далі відпускається клавіша «К2» (рис 2.1).

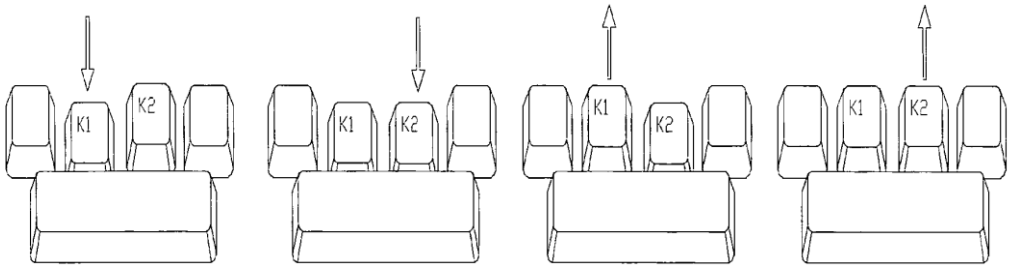


Рисунок 2.1 - Перший вид накладення клавіш

2. У момент утримання однієї клавіші відбувається відпускання іншої клавіші, тобто перша клавіша була натиснута в момент утримання другої. «К2» натиснута. «К1» натискається. Після цього відбувається відпускання клавіші «К2» і потім «К1». Є зворотним типом для першого виду.

3. Натискання і відпускання клавіші відбувається під час утримання іншої клавіши. Натиснута кнопка «К2», відбувається натискання і відпускання «К1» і потім відпускання «К2» (рис 2.2).

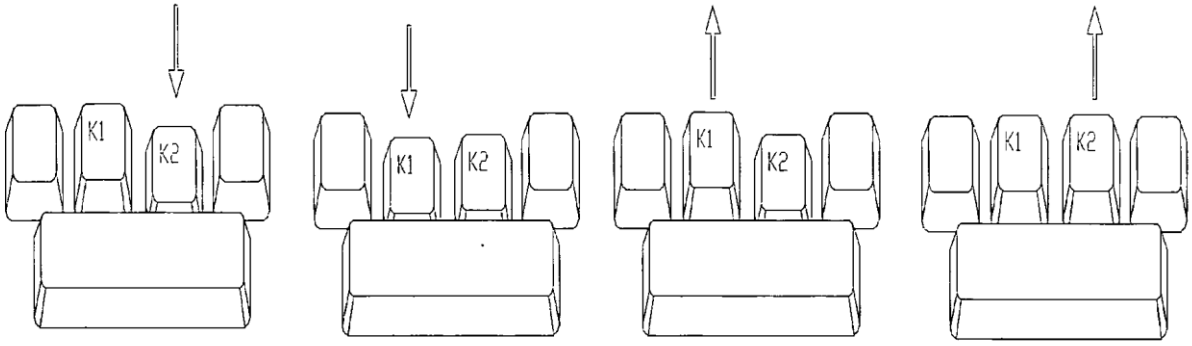


Рисунок 2.2 - Третій вид накладення клавіш

Емпіричні дослідження клавіатурних почерків оператора показали, що ЧУК при наборі тексту є бімодальним розподілом (перетином двох нормальних), а не розподілом Гауса (рис. 2.3.). Таким чином, методи і моделі, пропоновані для визначення ЧУК як математичне сподівання для нормального розподілу, мають значну похибку і не відображають реальних залежностей процесу набор тексту.

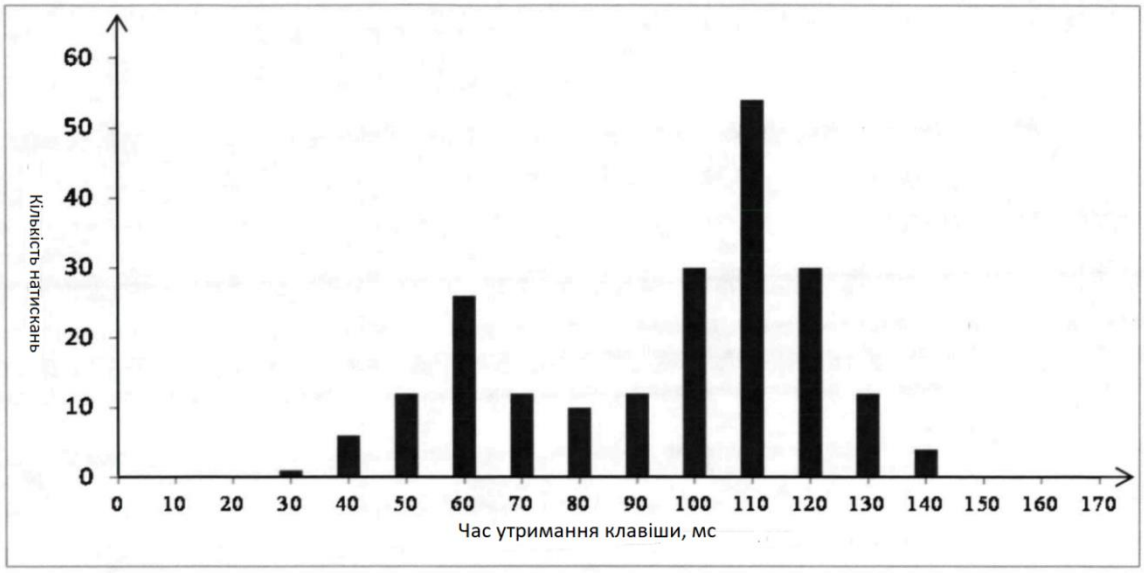


Рисунок 2.3 - Приклад бімодального розподілу часу утримання клавіши

Як приклад наведемо аналіз вибірки ЧУК «А» при наборі випадкового фрагмента тексту відображений в таблиці 2.1. Під час набору тексту клавіша «А» була натиснута 90 разів.

Якщо припустити, що ЧУК підпорядковується законам нормального розподілу, то можна розрахувати математичне сподівання як середнє ЧУК. При такому підході отримаємо математичне сподівання 96 мс. Але з таблиці 2.1 видно, що пік розподілів припадає на 35-37мс, 68-72мс і 104-108мс. Розраховане математичне сподівання для двох підвибірок, значення яких складають 86 і 106 мс. Тобто відхилення від розрахованого раніше математичного сподівання – 10 сек, що становить від 7 до 30% від вимірюваної величини.

Як роздільник вибірок можна використовувати математичне сподівання нормального розподілу, але цей підхід не відображає причини виникнення бімодального розподілу. З таблиці 2.1 видно, що до другого нормального розподілу потраплять елементи, якщо набір відбувався з накладеннями клавіш.

Маючи початкову вибірку (2.1), розподілену по бімодальному закону необхідно розділити її на 2 підвибірки, що мають властивості нормального розподілу (2.8).

$$\begin{aligned} &\boldsymbol{X_1, X_2, X_3, \dots X_j,} \\ &\boldsymbol{X_1, X_2, X_3, \dots X_k,} \end{aligned} \tag{2.8}$$

Критерієм поділу є наявність накладення в момент натискання клавіші, якому відповідало би поточне значення часу утримання клавіші з вибірки (2.1). Суть процесу розбиття вхідних даних на 2 підвибірки зведена до наступного:

ЯКЩО для поточного елемента вхідний вибірки часу утримання клавіш при наборі було накладення, **ТО** поточний елемент додається в вибірку часів утримання клавіш з накладеннями ЧУК-2,

ІНАКШЕ поточний елемент додається в вибірку часів утримання клавіш без накладень ЧУК-1.

Таким чином, використовуючи простий механізм визначення наявності накладення клавіш при наборі поділяються на дві незалежні вибірки і дві величини математичного сподівання ВУК для кожної клавіші, характеризують КП оператора ІС, що в свою чергу збільшить точність ідентифікації оператора, тобто знизить ймовірність виникнення помилок 1 і 2 роду. При цьому кожна з вибірок підпорядковується нормальному закону розподілу, а значить, до неї може бути застосована математична модель ЧУК, розроблена в розділі 2.1. Запропонована модель описується системою рівнянь (2.9).

$$\begin{aligned} &\bar{А}_{\text{ЧУК}-1} - \text{t}S_{\bar{А}_{\text{ЧУК}-1}} \le \mu \le \bar{А}_{\text{ЧУК}-1} + \text{t}S_{\bar{А}_{\text{ЧУК}-1}} \\ &\bar{А}_{\text{ЧУК}-1} - \text{t}S_{\bar{А}_{\text{ЧУК}-2}} \le \mu \le \bar{А}_{\text{ЧУК}-1} + \text{t}S_{\bar{А}_{\text{ЧУК}-2}} \end{aligned} \tag{2.9}$$

Таблиця 2.1 - Вибірка часу утримання клавіші «А»

ЧУК клавіши, мс	Кількість значень даного ЧУК вибірці	Ймовірність зустрічі ЧУК в вибірці,%	Кількість зареєстрованих накладень
32	2	7,14	0
35	2	7,14	0
36	5	17,86	0
37	2	7,14	0
38	1	3,57	0
67	1	3,57	0
68	3	10,71	0
69	1	3,57	0
70	3	10,71	0
71	2	7,14	0
72	4	14,29	0
73	1	3,57	0
74	1	3,57	0
102	1	3,57	1
103	1	3,57	1
104	4	14,29	3
105	13	46,43	13
106	10	35,71	10
107	10	35,71	10
108	8	28,57	8
109	1	3,57	1
110	1	3,57	1
140	1	3,57	1
141	1	3,57	1
142	3	10,71	3
143	3	10,71	3
144	4	14,29	4
145	2	7,14	2

2.3 Розробка аналітичної моделі клавіатурного почерку

Маючи шаблон клавіатурного почерку оператора стає можливо провести аутентифікацію та ідентифікацію оператора. Для цього необхідно провести процедуру порівняння поточного зразка почерку і збереженого раніше шаблона. Запропоновано використовувати відстань Евкліда для порівняння часу утримання клавіш поточного зразка і шаблону (2.10).

$$M = \sqrt{\sum_{i=1}^{V} (A_i - B_i)^2} \text{ , де} \tag{2.10}$$

M - розраховане значення відстані Евкліда,

V - кількість вибірок часу утримання клавіші, що відповідає кількості аналізованих клавіш

A_i - час утримання клавіші і з поточного зразка клавіатурного почерку оператора, який претендує на доступ,

B_i - час утримання клавіші і, що зберігається в шаблоні почерку.

Для бімодального розподілу часу утримання клавіш запропоновано грунтуючись на формулі 2.10 знаходити для кожної вибірки відповідне їй значення відстані Евкліда (2.11):

$$\begin{cases} \text{M}_{\text{ЧУК}-1} = \sqrt{\sum_{i=1}^{V_{\text{ЧУК}-1}} (A_i - B_i)^2} \\ \text{M}_{\text{ЧУК}-2} = \sqrt{\sum_{i=1}^{V_{\text{ЧУК}-2}} (A_i - B_i)^2} \end{cases} \tag{2.11}$$

Оператор буде успішно аутентифікований, ідентифікований, або його особистість буде підтверджена, якщо розраховані значення Евклидової відстані менші від встановленого в системі порога доступу. Поріг доступу підбирається в залежності від вимог до розроблюваної системі. Основними вимогами для систем захисту інформації є ймовірності виникнення помилок першого і другого роду. Суть процесу порівняння почерків і прийняття рішення про аутентифікації зведена до наступного правила:

ЯКЩО відстань Евкліда вибірки ЧУК-1 і вибірки ЧУК-2 поточного зразка почерку менше встановленого порогу доступу

$$\boldsymbol{IF}((\boldsymbol{M}_{\text{ЧУК}-\mathbf{1}} < \text{ПОРІГ\_ДОСТУПУ})\boldsymbol{AND}\ \boldsymbol{IF}(\boldsymbol{M}_{\text{ЧУК}-\mathbf{2}} < \text{ПОРІГ\_ДОСТУПУ}))$$

ТО оператор успішно пройшов аутентифікацію,

ІНАКШЕ оператор вважається невпізнаним підсистемою управління доступом і отримує відмову на доступ до інформаційної системи.

2.4 Розробка методу розпізнавання клавіатурного почерку оператора

Запропоновано метод розпізнавання клавіатурного почерку за часом утримання клавіш. Це дозволить отримати шаблон почерку, яка не залежить від тексту, що набирається і порядку вводяться оператором символів. Таким чином стає можливо визначення клавіатурного почерку оператора інформаційної системи по вільному контрольному тексту. Це забезпечує можливість застосування методу для задач постійного прихованого клавіатурного моніторингу з метою виявлення підміни авторизованого законного оператора, визначення відхилення психофізіологічного стану оператора комп'ютерної системи від нормального.

Проведений частотний аналіз російськомовних текстів показує (рис 2.3.), що букви в російськомовних текстах зустрічаються з різною ймовірністю і відповідно метод отримання шаблону клавіатурного почерку є залежним від цієї властивості [100].

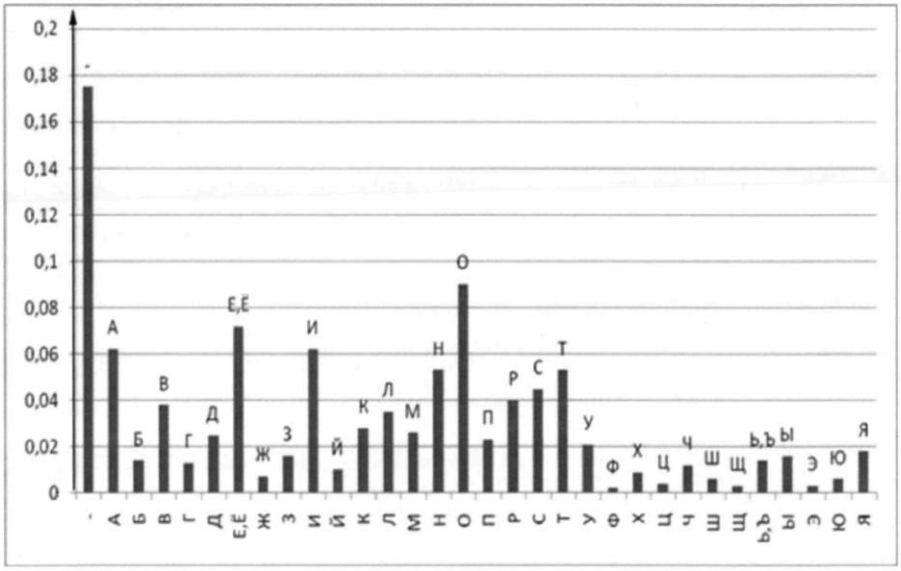


Рисунок 2.3 - Частота використовування букв в російськомовних словах

Наприклад, сама «популярна» буква «О» зустрічається з ймовірністю 0.090, а сама «рідкісна» буква «Ф» зустрічається з ймовірністю 0.002. Припустимо встановивши значення N = 10, тоді для збору статистичних даних по букві «О» знадобиться ввести текст довжиною

111 символів. А для отримання вибірки ЧУК «Ф» доведеться ввести текст що складається з 5000 символів, що відповідає 3 сторінок тексту формату А4 або близько 30 хвилин безперервного друку тексту.

Таким чином, отримання шаблону клавіатурного почерку стає довгим і трудомістким процесом, що не є бажаним в системах, які забезпечують безпеку інформації.

Виходячи з вищесказаного, запропоновано доповнити метод отримання шаблону клавіатурного почерку визначенням часу утримання клавіш для незавершених вибірок під час функціонування постійного таємного клавіатурного моніторингу. Як тільки вибірка для конкретної клавіші буде повністю зібрана, розраховується математичне сподівання часу утримання клавіші для цієї вибірки. Застосування бімодального розподілу, що збільшує кількість параметрів почерку, дозволить використовувати для аутентифікації і ідентифікації в повному обсязі сформований шаблон почерку.

2.5 Висновки до розділу 2

1. Проведено синтез і аналіз математичної моделі часу утримання клавіш(ЧУК), що представлена нормальним розподілом. Виявлено суттєвий недолік даної моделі - це її невідповідність процессам, що відбуваються при наборі тексту оператором.

2. Запропоновано математичну модель клавіатурного почерку, яка відрізняється від існуючих тим, що ЧУК представляється у вигляді перетину двох нормальних розподілів. Це збільшить до двох разів кількість застосовуваних при розпізнаванні КП характеристик.

3. Запропоновано аналітичну модель клавіатурного почерку, яка заснован на відстані Евкліда і дозволяє порівняти два шаблони почерку.

РОЗДІЛ 3
РОЗРОБКА АЛГОРИТМІВ РОЗПІЗНАВАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ ОПЕРАТОРА ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1 Розробка способу представлення часу утримання клавіш

Для обробки і зберігання клавіатурного почерку оператора представленого у вигляді бімодального розподілу запропонований спосіб зберігання і обробки почерку в ЕОМ. Розроблений спосіб складається з способу зберігання даних про події клавіатури (див. таблицю 3.1.) і способу зберігання шаблону клавіатурного почерку (див. таблицю 3.2.).

Таблиця 3.1 - Структура способу зберігання даних про події клавіатури

Клавіша 1	…	Клавіша N
Подія KeyUp або KeyDown	…	Подія KeyUp або KeyDown
Тік лічильника на якому відбулася подія	…	Тік лічильника на якому відбулася подія

Даний спосіб дозволяє послідовно розібрати всю послідовність подій клавіатури. При цьому будуть розраховані часи утримання клавіш і буде зазначено, чи відбувалися при цьому накладення клавіш. Якщо накладення були відсутні, то час утримання клавіші буде занесено до вибірки ЧУК-1, якщо присутні, то в вибірку ЧУК-2 шаблони.

Таблиця 3.2 - Структура шаблону клавіатурного почерку оператора

Клавіша	$M_{ЧУК-1}$	$M_{ЧУК-2}$	Кількість $N_{ЧУК-1}$	Кількість $N_{ЧУК-2}$	Вибірка нормального розподілу ЧУК-1	Вибірка нормального розподілу ЧУК-2
А	44	98	!	!		
Б	56	106	!	!		116,108
…						
Ю	66		!	4		
Я	150	-				

У шаблон заноситься інформація про аналізованих клавішах, математичні сподівання вибірок утримання для кожної клавіші. Знак оклику заноситься в комірку в тому випадку, якщо для відповідної вибірки було зібрано достатню кількість вхідних біометричних даних і було розраховано математичне сподівання $M_{чук}$. Якщо триває збір статистики, то в шаблоні зазначається кількість вже зібраних елементів вибірки $N_{чук}$ і зберігається сама вибірка. По досягненні достатньої кількості даних вибірка видаляється. Приклад шаблону клавіатурного почерку оператора наведено у Додатку А. Так як вільний текст, за яким проводиться навчання або подальші процедури аутентифікації і ідентифікації, має різну ймовірність народження різних букв і символів, то збір достатньої для проведення ймовірносно-статистичного аналізу вибірки ЧУК вимагає введення дуже великого тексту (від 5000 символів і більше). Тому запропоновано ввести в інформаційний файл поля «кількість» і «вибірка».

В поле «вибірка» зберігаються ЧУК, що розділяються знаком «;», в поле «$N_{чук}$» заноситься кількість елементів у вибірці. при досягненні достатньої кількості елементів у вибірці підраховується ЧУК, вибірка очищається, в поле «$N_{чук}$» заноситься символ «!», який використовується для позначення факту закінчення підрахунку ВУК цієї клавіші. Далі елементи в цю вибірку заноситься не будуть. Якщо в процесі навчання достатню кількість елементів вибірки не зібрано, то буде розраховано тимчасове значення ВУК, а процес збору та розрахунку ВУК продовжиться при роботі алгоритмів авторизації та моніторингу, при підтвердженні, що текст набирає законний оператор, якому відповідав би даний шаблон. При аутентифікації і ідентифікації запропоновано ввести коефіцієнти впливу на підсумок розрахунку відстані Евкліда- більший вплив надавати закінченим вибіркам, незакінченими – менший вплив. Для введення коефіцієнтів запропоновано розділити абетку на кілька груп, в залежності від імовірності появи літер в текстах.

3.2 Розробка алгоритму отримання шаблону клавіатурного почерку оператора

Побудова систем біометричної ідентифікації засновано на створенні шаблонних уявлень ідентифікованих осіб. Шаблон створюється, тоді, коли система знаходиться в режимі навчання. Він є збережені в пам'яті системи, яка контролює доступ, біометричні характеристики людини, і використовується для порівняння з біометричними параметрами осіб, які претендують на доступ до ресурсів. У разі, коли виміряні системою значення параметрів оператора відрізняються від шаблону більше, ніж допускається порогом чутливості, він отримує відмову в доступі до ресурсів.

Розроблено алгоритм отримання і реєстрації шаблону клавіатурного почерку оператора [47]. Роботу алгоритму можна зобразити діаграмою діяльності (див. рис. 3.1). Для виявлення

усереднених значень часу подій клавіатури використовується ймовірносно-статистичний метод, тому необхідний збір статистики, що складається з вибірки тимчасових значень, де елементом вибірки буде час утримання клавіші. Алгоритм заснований на математичній моделі розробленої в розділі 2.2. В даному алгоритмі виконуються процес отримання інформаційного файлу - отримання шаблону КП оператора, який буде збережений в базі шаблонів. Для цього на початку виконання проводиться ідентифікація оператора за його унікальним ідентифікатором, наприклад, логіну.

Ініціалізується динамічний тривимірний масив KeyEventsArr, в якому зберігаються події клавіатури розробленим способом (рис 3.1.) Масив заповнюється, поки не буде натиснуто достатню (задається адміністратором або встановлену за замовчуванням) кількість клавіш.

На наступному етапі відбувається підрахунок часу утримання клавіш. Знаходиться подія натискання конкретної клавіші. Потім знаходиться подія відпускання цієї клавіші. З момента події відпускання віднімається момент події натискання і ділиться на частоту лічильника, для отримання значення ЧУК в мілісекундах. Моменти подій визначаються функцією QueryPerformanceCounter, частота лічильника функцією QueryPerformanceFrequency. На багатоядерних системах використовується функція SetThreadAffinityMask щоб вказати спорідненість процесора для системи.

Алгоритм має фільтр натискання системних клавіш (наприклад, BACKSPACE або ENTER), натискання яких не зберігається в шаблоні. Залежно від наявності або відсутності накладень при утриманні клавіші, значення ЧУК заноситься до вибірки першого (без накладання) або другого (з накладеннями) нормального розподілу. потім підраховується математичне сподівання кожної вибірки, і шаблон КП зберігається в облікового запису оператора.

Шаблонний інформаційний файл оператора має описану вище структуру (рис. 3.2.) отриманий шаблон застосовується в розроблених алгоритмі авторизації оператора за клавіатурним почерком і алгоритмі виявлення підміни законного оператора ключової системи.

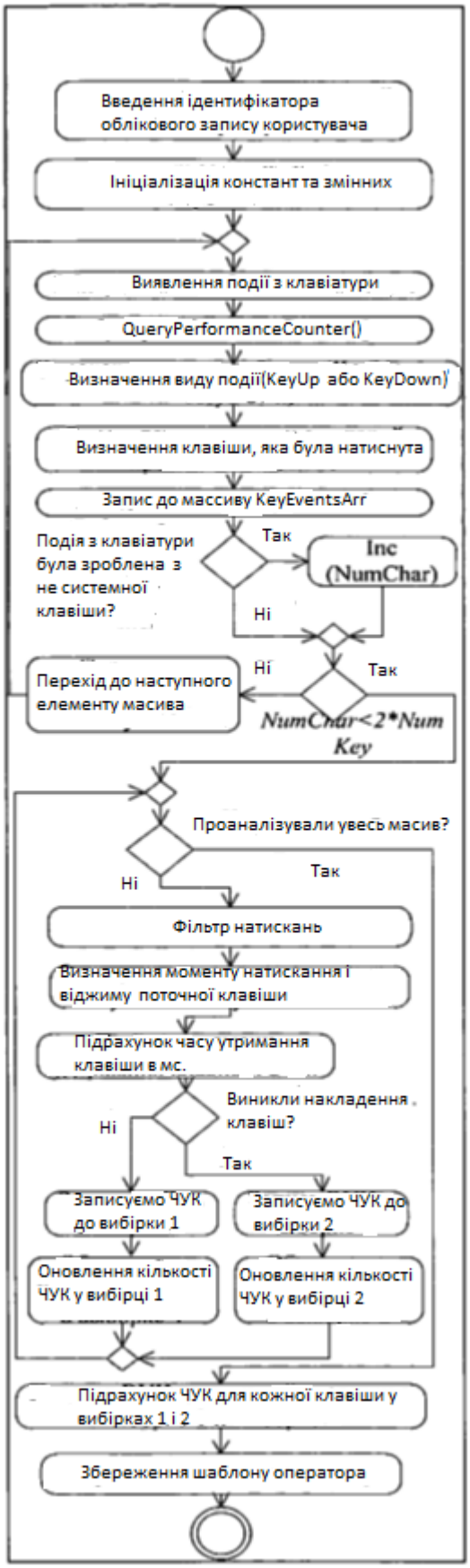


Рисунок 3.1 - Діаграма діяльності алгоритму отримання шаблону клавіатурного почерку

3.3 Розробка алгоритму авторизації оператора за клавіатурним почерком

Авторизація - це надання певній особі або групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій. Зазвичай процесу авторизації передує процес аутентифікації - підтвердження автентичності, відповідності оператора пред'явленому їм ідентифікатором. Запропоновано алгоритм аутентифікації і подальшої авторизації оператора ключової системи (рис. 3.2.). Алгоритм заснований на запропонованих у другому розділі моделях і методі. В даному алгоритмі порівняння відбувається за принципом «один до одного», тому завантажується шаблон конкретного оператора, ідентифікатором якого він представився. У разі успішної аутентифікації відбувається процес авторизації, а інакше - відмова.

Головна відмінність алгоритму авторизації [95] від алгоритму отримання шаблону почерку полягає в тому, що тут для визначення почерку використовується менша кількість натискань клавіш. Зазвичай пароль складається з 14-20 символів. Цей факт вимагає додаткової настройки порога доступу, для зменшення помилок першого і другого роду. поріг доступу налаштовується після аналізу локальної бази шаблонів клавіатурних почерків операторів, що мають доступ до конкретної ІС. Порівняння поточного зразка КП оператора з шаблонами відбувається шляхом розрахунку міри Евкліда [11] для кожної клавіші, при цьому ЧУК-1 і ЧУК-2 порівнюються як окремі елементи.

Отримане значення несхожості, розраховане як міра відстані Евкліда, порівнюється з порогом доступу. Якщо несхожість менше порога доступу, то оператор проходить процедуру авторизації, інакше отримує відмову.

Рисунок. 3.2 - Діаграма діяльності алгоритму аутентифікації і авторизації оператора

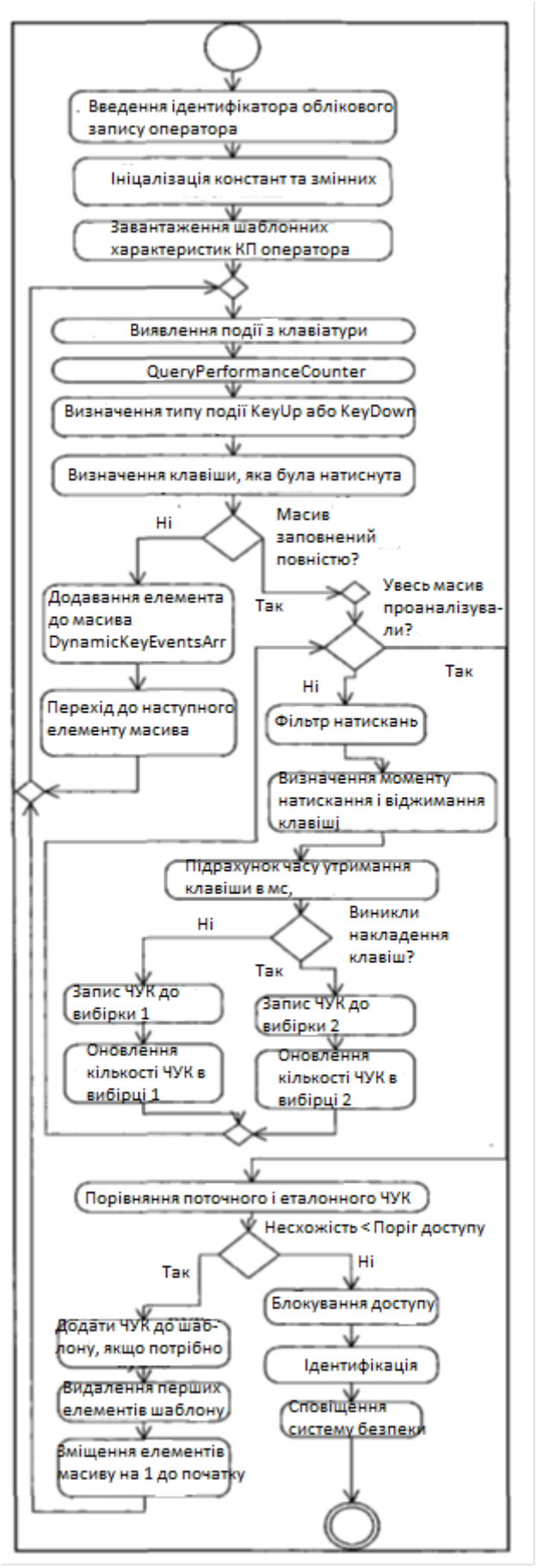


Рисунок 3.3 - Діаграма діяльності алгоритму виявлення підміни авторизованого оператора

3.4 Розробка алгоритму виявлення підміни авторизованого оператора

Був розроблений алгоритм виявлення підміни авторизованого оператора (рис. 3.3) [95]. Даний алгоритм методом постійного таємного моніторингу дозволяє виявити підміни зловмисником законного авторизованого оператора КС. Алгоритм заснований на запропонованих у другому розділі моделях і методі.

Масив DynamicKeyEvetsArr має невеликі розміри від 10 до 40 елементів і може бути обраний, наприклад залежно, від інтервал копіювання оператора. Інтервал копіювання - це число символів, які можуть бути надруковані в точності після однократного перегляду тексту. Лєбєдєв А.М встановив, що інтервал копіювання в звичайній ситуації передруку у досвідченого оператора склав в середньому 14,6 символів[81].

Поточні характеристики КП визначаються з цього масиву. Масив автоматично оновлюється при введенні тексту. Елементи, введені раніше, видаляються, і ЧУК розраховується автоматично, по доданим новим елементам. При виявленні підміни законного оператора вимірюється частота лічильника з високою роздільною здатністю, і якщо вона змінилася, то ЧУК вважається знову, і почерки порівнюються ще раз. Якщо частота не змінювалася або перерахований поточний почерк не збігається – ІС блокується. Система намагається ідентифікувати зловмисника по базі КП, що зберігаються в системі. Передається сигнал тривоги в службу безпеки. Якщо почерки збігаються і є введені символи, для яких підрахунок ЧУК не закінчений, то такі елементи додаються в відповідну вибірку, і відбувається перерахунок ЧУК. Якщо в цей момент зібрано достатньо для навчання кількість елементів у вибірці, то вибірка очищається і в поле «кількість» інформаційного файлу ставиться мітка «!». Даний метод можна так само використовувати і при перенавчанні всього шаблону почерку оператора, в разі змін клавіатурного почерку, наприклад, викликаних вдосконаленням оператором техніки друку.

3.5. Розробка архітектури та інтерфейсу підсистеми розпізнавання клавіатурного почерку оператора

Розроблено архітектуру підсистеми розпізнавання клавіатурного почерку оператора (рис. 3.4.). В архітектурі розробленої підсистеми виділені кілька блоків:

- блок збору біометричних характеристик,
- блок аналізу статистичних біометричних даних,
- блок збереження шаблонів КП,
- база шаблонів КП,
- блок порівняння шаблонних і поточних характеристик почерку

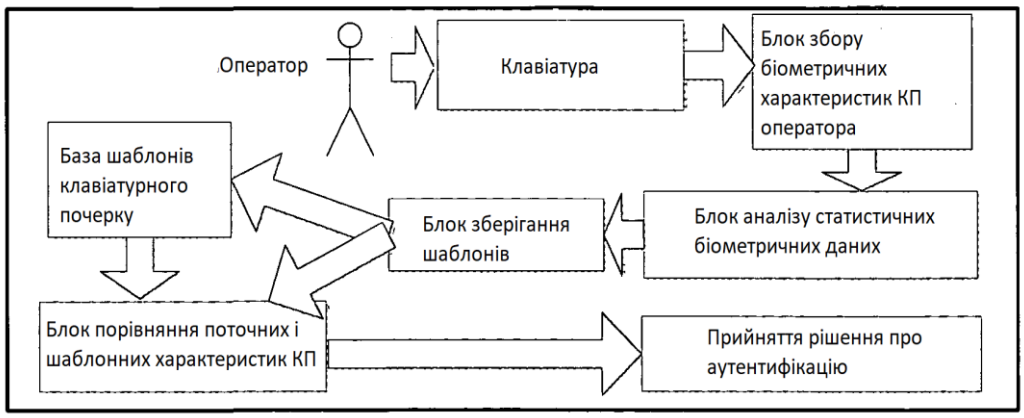


Рисунок 3.4 - Use Case діаграма підсистеми розпізнавання клавіатурного почерку

Блок збору біометричних характеристик заснований на розроблених моделі бімодального розподілу часу утримання клавіш і методі розпізнавання клавіатурного почерку. Даний блок функціонує у всіх трьох розроблених алгоритмах.

Програмно блок збору біометричних характеристик виглядає так:

Користувач авторизується в системі (рис 3.5)

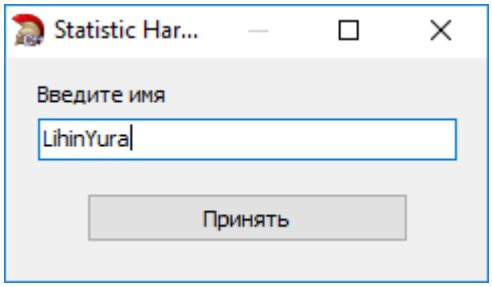


Рисунок 3.5 - Авторизація

Користувач переходить до вікна з текстом (рис 3.6).

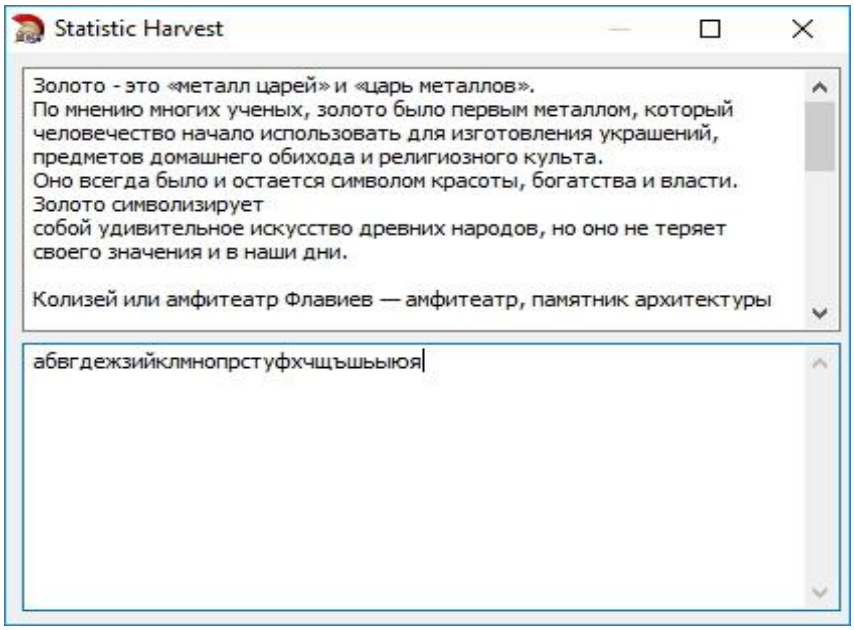


Рисунок 3.6 - Формування даних про оператора шляхом вільного тексту

Набравши цей текст, формується документ з унікальними характеристиками почерка користувача. Цей файл містить інформацію назву клавіши, статус натиснутої клавіши, час натискання і віджимання. Структура файлу на рисунку 3.7 та в Додатку А (Таблиця 2)

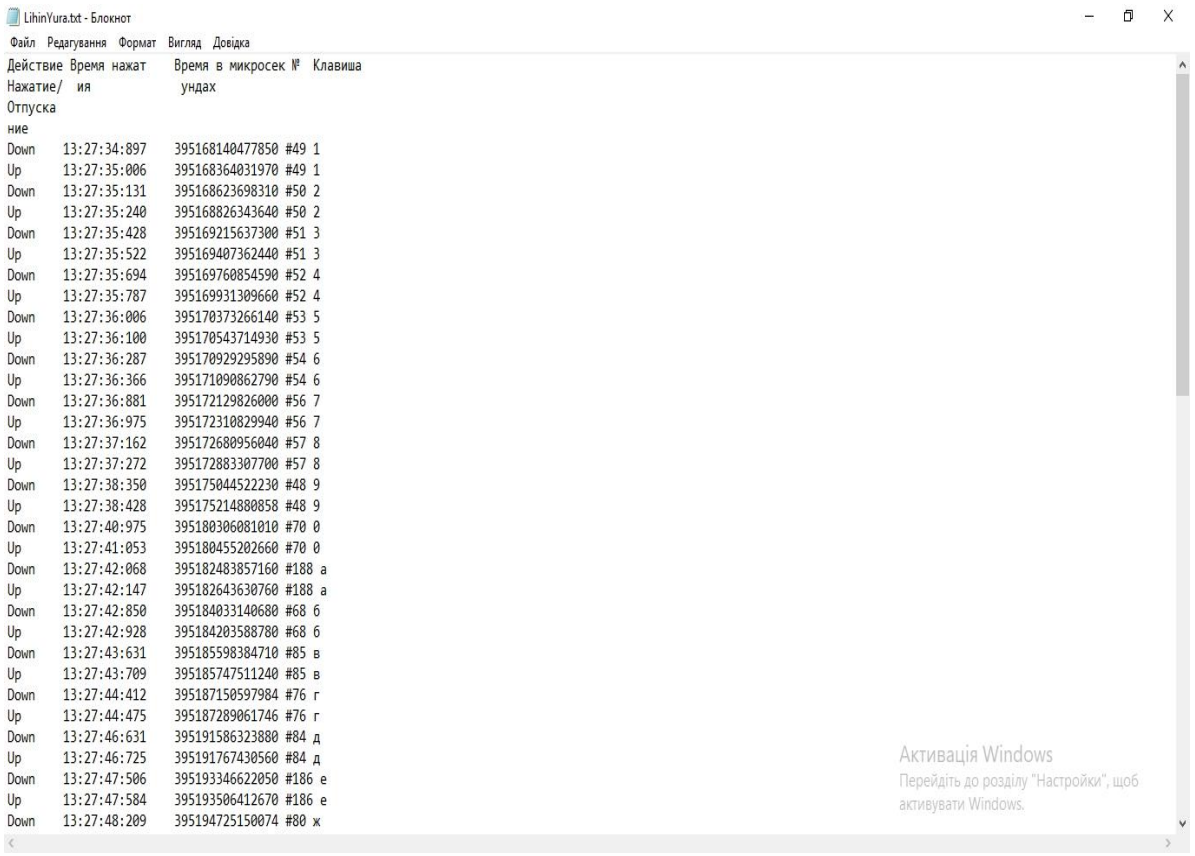


Рисунок 3.7 - Структура інформаційного файлу

Надалі цей файл передається до блоку аналізу статистичних даних, де формується до шаблон клавіатурного почерку оператора та до блоку збереження шаблонів

Блок аналізу статистичних біометричних даних включає в себе розроблений спосіб обробки клавіатурного почерку в ЕОМ, представлений у вигляді бімодального розподілу часу утримання клавіш..

Блок збереження шаблонів КП і база шаблонів КП так само використовують розроблений спосіб зберігання клавіатурного почерку в ЕОМ. В режимі навчання, відповідно до алгоритму реєстрації шаблону почерку, обчислюються значення математичного сподівання вибірок часу утримання клавіш. Отримані значення зберігаються в інформаційний файл-шаблон почерку оператора.

Блок порівняння шаблонних і поточних характеристик почерку використовується в процесі функціонування алгоритму аутентифікації і авторизації оператора КС, і алгоритму виявлення підміни законного оператора. Розраховується несхожість двох почерків, шляхом обчислення Евклидова відстані, а потім отримане значення порівнюється з порогом доступу. У разі виявлення підміни законного оператора КС блокується і подається сигнал тривоги.

3.6 Оцінка точності розпізнавання особистості оператора за клавіатурним почерком

При розгляді будь-яких систем прийняття рішень і (або) розпізнавання найважливішими показниками якості роботи таких систем є ймовірності помилок системи. Якщо система призначена для поділу всіх досліджуваних об'єктів на два класи (а саме таке поділ здійснюють системи аутентифікації операторів – вони повинні розділити на два класи «свій-чужий» всіх, хто намагається авторизуватись) то для неї актуальні два види помилок. Це так звані помилки першого роду, коли система приймає «свого» за «чужого». І помилки другого роду, коли, навпаки, «чужого» система приймає за «свого» [97,98].

Нехай дана вибірка $Y = \{Y_i \ \dots, Y_n\}$ з невідомого спільного розподілуP^Y, і поставлена бінарна задача перевірки статистичних гіпотез: H_0 - нульова гіпотеза, а H_1 - альтернативна гіпотеза. Припустимо, що вибірка відповідає клавіатурного почерку оператора, що проходить процес аутентифікації. Наприклад, вона представлена часом утримання
оператором клавіш клавіатури. Тоді нульова гіпотеза H_0 буде відповідати припущенням, що оператор, який аутентифікується, дійсно є зареєстрованим оператором системи (саме тим, ким він представився системі) і його можна авторизувати. Альтернативна гіпотеза H_1 матиме протилежне значення: зловмисник не є законним оператором системи і повинен отримати відмову в авторизації.

Припустимо, що задано статистичний критерій (3.1) сопоставляющий кожної реалізації вибірки $\boldsymbol{Y} = \boldsymbol{y}$ одну з наявних гіпотез.

$$f{:}R^n \rightarrow \{H_0, H_{1\}}, \tag{3.1}$$

Для прикладу з клавіатурним почерком як статистичного критерію візьмемо міру Евкліда (3.2) і поріг доступу PD підсистеми прийняття рішень, що визначає допустиме відхилення клавіатурного почерку від шаблону, для прийняття рішення про те, що почерк тестованого оператора збігається з шаблонним, збереженим в базі.

$$M{:=}M+sqr((Times\ [i,\ 0]\ -eTimes\ [i,\ 0])\ /\ eTimes\ [i,\ 0], \tag{3.2}$$

Тут s - значення міри Евкліда [74]. Times [i, 0] - час утримання конкретної клавіші з вибірки, що відповідає клавіатурному почерку тестованого оператора. eTimes [i, 0] - час утримання конкретної клавіші, що зберігається в шаблонному зразку клавіатурного почерку тестованого оператора. Згідно застосування даного критерію можливі 2 випадки:

• Якщо M <PD, то відхилення характеристик почерку поточного оператора ключової системи відповідає дозволеному діапазону. В цьому випадку приймається рішення про те, що оператор є законним і відбувається процес авторизації.

• Якщо M> PD, то відхилення характеристик почерку поточного оператора ключової системи не відповідає дозволеному діапазону. Значить, приймається рішення про те, що оператор не є законним і він отримує відмову в авторизації.

Можливі наступні чотири ситуації:

1. Розподіл P^Y вибірки Y відповідає гіпотезі H_0, і вона точно визначена статистичним критерієм, тобто $f(Y) = H_0$. значить, клавіатурний почерк оператора збігається з його шаблонним почерком по заданому критерію. Оператор є законним і успішно проходить авторизацію.

2. Розподіл P^Y вибірки Y відповідає гіпотезі H_0, але вона невірно відкинута статистичним критерієм, тобто $f(Y) = H_1$. значить, клавіатурний почерк оператора не збігається з його шаблонним почерком за заданим критерію. Оператор є законним, але система помилково приймає рішення про відмову в авторизації.

3. Розподіл P^Y вибірки Y відповідає гіпотезі H_1 і вона точно визначена статистичним критерієм, тобто $f(Y) = H_1$. значить, клавіатурний почерк оператора не збігається з його

шаблонним почерком по заданому критерію. Поточний оператор не є зареєстрованим оператором системи і справедливо отримує відмову в авторизації.

4. Розподіл P^Y вибірки Y відповідає гіпотезі H_1 але вона невірно відкинута статистичним критерієм, тобто $f(Y) = H_0$. значить, клавіатурний почерк оператора не збігається з його шаблонним почерком за заданим критерію. Оператор не є законним, але помилково отримує дозвіл на авторизацію.

У другому і четвертому випадку відбулися статистичні помилки, які і є помилками першого і другого роду відповідно.

Для розрахунку FAR запропоновано використовувати процедуру порівняння методом "чужий" до "чужому" зберігаються в базі даних "шаблонів" при варіації порога виявлення. Припустимо, що в базі зберігаються п шаблонів відповідно п операторів ключової системи. перший шаблон клавіатурного почерку оператора, що зберігається в базі даних, порівнюється з усіма іншими $n-1$ шаблонами клавіатурних почерків операторів з цієї ж бази. Відповідно для першого шаблону відбувається $\text{п}-1$ порівнянь. Другий шаблон вже порівнювався з першим шаблоном. значить, порівняння почнеться з третього шаблону і всього для нього станеться $\text{п}-2$ порівнянь. Зазначена процедура здійснюється до передостаннього шаблону бази. Це означає, що число можливих порівнянь VFAR "чужий" до
"чужого" в базі з п шаблонів буде (3.3):

$$VFAR = \frac{n(n-1)}{2} \tag{3.3}$$

Для оцінки FRR запропоновано використовувати відношення кількості відмов у доступі за критерієм "біометричний контроль не пройдений" до загальної кількості спроб пред'явлення біометричних параметрів (в спрощеному випадку - до загальної кількості проходів).

Таким чином, буде отримана самонавчається, яка встановлює поріг чутливості в залежності від варіацій зберігаються в базі почерків. Також система, після аналізу почерків співробітників-операторів інформаційної системи, запропонує адміністратору рекомендації по допустимим значенням порога із зазначенням ймовірностей FRR і FAR при відхиленні значення порога від нормальної величини. Природно при першому запуску системи дані для визначення FRR зазначеним методом або порівнянням "Свій" до "свого" (кілька зразків клавіатурного почерку одного і того ж оператора) в системі зі зрозумілих причин відсутні. Таким чином, пропонується вважати значення FAR обов'язковим для реалізації системним параметром. А параметр FRR будемо вважати допустимим, якщо він співмірний з ймовірністю

помилки помилкового спрацьовування для систем контролю і управління доступом (СКУД), яка не має біометричного контролю. Фактично FRR визначається інтенсивністю процесів авторизації операторів ключової системи: якщо їх мало, то FRR може бути відносно великим, а якщо багато, то повинен бути малим. Відповідно чим важливіше статус охороняється системи, тим менше. допущених осіб (менша кількість авторизації) і, отже, може бути задано більш високе значення FRR при зменшенні FAR.

3.7 Аналіз результатів використання алгоритму клавіатурного моніторингу та ідентифікації особистості при розпізнаванні операторів

Проведено аналіз результатів використання розробленого алгоритмупри розпізнаванні операторів ключових систем на основі зібраної бази шаблонів клавіатурних почерків.планування експериментальних досліджень полягала:

а) у виборі 10 операторів, зі стажем роботи на ЕОМ не менше 1 рік,

б) виборі контрольного тексту для експерименту об'ємом 1200 символів для реєстрації шаблонів клавіатурного почерку операторів,

в) отримання вибірки часу утримання клавіш при наборі операторами тексту,

г) обробці розробленою системою зібраних даних і аналізі результатів розпізнавання.

Проведено порівняння (4995 операцій порівняння) зібраних шаблонів операторів один з одним з різними значеннями порога доступу з метою обчислення ймовірності виникнення помилки FRR. Для розрахунку величини FAR було зібрано по 5 зразків почерку 10 чоловік, щоб виявити відхилення в клавіатурному почерку оператора один з одним. В результаті було обрано найкращий поріг доступу розраховану за допомоги відстані Евкліда, при процедурах порівняння шаблонів КП. (рис. 3.8). Оптимальний поріг доступу дорівнює = 0,8.

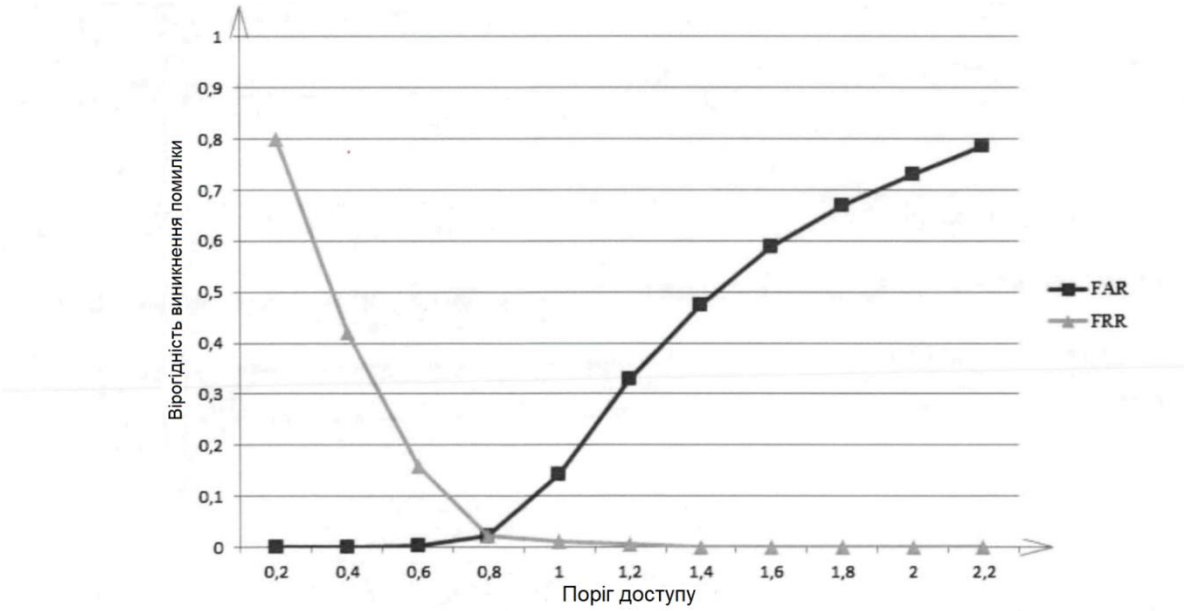


Рисунок 3.8 - Залежність рівня помилок першого і другого роду від встановленого порогу доступу

3.8 Висновки до розділу 3

1. Розроблено спосіб відображення і зберігання клавіатурного почерку в ЕОМ, який представлений у вигляді бімодального розподілу часу утримання клавіш.

2. Запропоновано алгоритм отримання шаблону клавіатурного почерку оператора інформаційної системи. Він відрізняється від існуючих алгоритмів тим, що при розпізнаванні клавіатурного почерку в якості характеристики почерку використовується час утримання клавіш, який представлений у вигляді перетину двох нормальних розподілів. Це забезпечує можливість визначення клавіатурного почерку оператора ключової системи по вільному контрольному тексту.

3. Запропоновано алгоритм авторизації оператора інформаційної системи за клавіатурним почерком, який представлений у вигляді бімодального розподілу часу утримання клавіш.

4. Запропоновано алгоритм постійного таємного клавіатурного моніторингу з метою виявлення підміни авторизованого оператора. Данний алгоритм базується на методі постійного таємного клавіатурного моніторингу часу утримання клавіш.

5. Розроблено архітектуру і інтерфейс підсистеми розпізнавання клавіатурного почерку оператора, що дозволяє організувати процес таємного клавіатурного моніторингу.

6. Розроблено комплекс програм, що реалізують алгоритми і методи розпізнавання клавіатурного почерку, які можуть використовуватися як системи контролю та управління доступом до інформаційної системи.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної магістерської роботи було дослідження методів й апаратно-програмні засобів захисту інформації в комп'ютерних системах, і як результат було створено прогромне забезпечення для аутентифікаціїї операторів. В подальшому розроблятиметься реальна система, яка значно полегшить процес аутентифікаціїї. Так як в процесі проектування використовувалося персональна ЕОМ, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера на якому буде розроблятися/використовуватися розроблена система.

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Обов’язки працівників щодо додержання вимог нормативно-правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені безпосередньо «Інструкцією на робоче місце № 1» або посадовою інструкцією з посадою

оператора ОЕМ, та іншими затвердженими власними нормативними актами з питань охорони праці (правилами, нормами, регламентами, положеннями, стандартами, інструкціями та іншими документами, обов'язковими до виконання), тобто тих, що діють на підприємстві/організації, і визначені НПАОП 0.00-6.03-93 «Порядок опрацювання та затвердження власником нормативних актів про охорону праці, що діють на підприємстві».

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою дипломного проекту регулюються Кодексом законів про працю (КЗпП) України, відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємства.

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [НПАОП 0.00-А.12-05].

Обов'язковими вимогами враховане наступне:

– не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.

– на підприємстві/організації, де експлуатуються ЕОМ з відео дисплейними терміналами (ВДТ) і периферійними пристроями (ПП), розробляється інструкція з охорони праці відповідно до Положення про розробку інструкцій з охорони праці, затвердженого наказом Держнаглядохоронпраці від 29.01.98 N 9, зареєстрованого в Міністерстві юстиції України 07.04.98 за N 226/2666 (НПАОП 0.00-4.15-98).

– ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

– перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов'язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:

1) вступного, який проводять працівники служби охорони праці об'єкта господарювання з усіма працівниками, яких приймають на роботу незалежно від їхньої освіти та стажу роботи за програмою, в якій подають загальні питання охорони праці із врахуванням її особливостей на об'єкті господарювання;

2) первинного, який проводять керівники структурних підрозділів на місці праці з кожним працівником до початку їхньої роботи на цьому робочому місці.

Проходження працівником цих інструктажів з питань охорони праці підтверджується записами у відповідних журналах обліку інструктажів і скріплюється підписами осіб, які проводили інструктажі та осіб, які отримали інструктажі.

3) Повторвий (не рідше одного разу в 6 місяців);

А) Позаплановий (при зміні правил охорони праці);

5) Поточний (проводять з працівниками перед виконанням робіт, на яких оформляється наряд-допуск)

4.2 Аналіз стану умов праці

Робота над створенням системи аутентифікації проходитиме в приміщенні СНУ ім.. Володимира Даля. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

4.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об'єм, $м^3$	75

Згідно з [ДСН 3.3.6.0А2-99 «Санітарні норми мікроклімату виробничих приміщень»] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	700	680 ÷800
Висота простору для ніг, мм	720	не менше 600
Ширина простору для ніг, мм	650	не менше 500
Глибина простору для ніг, мм	778	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	500	не менше 500
Глибина сидіння, мм	500	не менше 500
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	100	100
Відстань від очей до екрану дисплея, мм	900	700 ÷800

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

За ступенем пожежної безпеки приміщення належить до категорії В. Кабінет оснащений переносним вуглекислотним вогнегасником ВВК-5 .

Наявна аптечка для надання долікарської допомоги, а також у кабінеті роблять вологе прибирання та щоденно провітрюють приміщення.

4.2.3 Навантаження та напруженість процесу праці

Виконання магістерської роботи: за фізичним навантаженням відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав'язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м'язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Тобто наявне психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;
- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;
- монотонності праці;
- перенапруження аналізаторів;
- емоційних перевантажень.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також інші профілактичні заходи на ведені в ДСанПіН 3.3.2.007-98

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви для операторів комп'ютерного набору тривалістю 10 хв. через кожну годину роботи.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої.

За умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом, яких можуть бути: принтер, сканер та інші джерела виділення багатьох хімічних речовин - напр., озону, оксидів азоту та аерозолів високодисперсних частинок тонера), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3).

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
фізичні			
- підвищена температура поверхонь обладнання	експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи	2	ДСН 3.3.6.042-99
- підвищений рівень шуму на робочому місці	-//-	2	ДСН 3.3.6.037-99
- підвищений рівень іонізуючого випромінення в робочій зоні	-//-	2	ДСН 3.3.6.042-99 ГОСТ 12.1.006-84
- підвищений рівень електромагнітного випромінення	-//-	2	ГОСТ 12.1.006-84
- підвищений рівень статичної електрики	-//-	2	ГОСТ 12.1.030-81
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015
- підвищена яскравість світла	порушення умов праці (організації місця праці- налагодження моніторів)	1	ДСанПіН 3.3.2.007-98
- понижена контрастність	-//-	1	ДСанПіН 3.3.2.007-98
хімічні:			
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безпервна робота)	2	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання,. Небезпека загоряння пов'язана з особливістю комп'ютерів - із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,

2) системою протипожежного захисту,

3) організаційно-технічними заходами.

Запобігти утворенню горючого середовища (замінити горючі речовини і матеріали на негорючі і важкогорючі) не надається технічно можливим. Тому проектом передбачаються способи і засоби запобігання утворення (або внесення) в горюче середовище джерел запалювання, таких як:

1) застосування електроустаткування, відповідної пожежонебезпечної і вибухонебезпечної зонам відповідно до ПУЕ;

2) застосування в конструкції швидкодійних засобів захисного відключення можливих джерел запалення;

3) виключення можливості появи іскрового розряду в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення.

Згідно НАПБ Б.03.002-2007 таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт. або хімічний пінний ОХП-10 – 1 шт;
- повсть 1 1 м^2, кошму 2×1,5 м^2 або азбестове полотно 2×2 м^2 в кількості 1 шт.

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [ДСН 3.3.6.0А2-99 «Санітарні норми мікроклімату виробничих приміщень»]

4.4.2 Освітлення

Освітленість приміщення має велике значення при роботі на ПЕОМ. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5-1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає СНіП 11-4-79 [13]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє СНіП і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2 + b^2} \cdot S_b = (1/8 \div 1/10) \cdot S_n \quad (4.1)$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 5 = 25$ м^2

$S_{вік} = 1/8 \cdot 25 = 3{,}125$ м^2

Приймаємо 2 вікна площею $S = 1{,}6$ м^2 кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5А00 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *n* виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \quad (4.2)$$

де *E* – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 25 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5А00лм (для ЛБ-80).

Підставивши числові значення у формулу (А.2), отримуємо:

$$n = \frac{300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 2.$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

4.5 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп'ютерів (зумовлений як роботою системних блоків, клавіатури, так і друкуванням на принтерах, а також зовнішніми чинниками), коливається у межах 50–65 дБА [ДСН 3.3.6.037-99]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. Тому на практиці рекомендують знижувати фактичний рівень шуму у приміщеннях, де створюють комп'ютерні програми, виконують теоретичні та творчі роботи, проводять навчання до 40 дБА, а в приміщеннях, де виконують роботу, що потребує зосередженості, — до 55 дБА. У залах опрацювання інформації та комп'ютерного набору рівні шуму не повинні перевищувати 65 дБА.

4.6 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти) і установки в віконному отворі автономного кондиціонера БК-2000. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП (30 $м^3$ на годину на одного працюючого).

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.7 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

- експлуатацію сертифікованого обладнання;

- дотримання заходів електробезпеки;

- забезпечення оптимальних параметрів мікроклімату;

- забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);

- облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

а) якщо об'єм приміщення 20 м^3, то потрібно подати не менш як 30 м^3/год повітря;

б) якщо об'єм приміщення у межах від 20 до 40 м^3, то потрібно подати не менш як 20 м^3/год повітря;

в) якщо об'єм приміщення становить понад 40 м^3, допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;

- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;

- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

- не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

Вимоги безпеки при надзвичайних ситуаціях:

1) При раптовому припиненні подачі електричної енергії вимкнути всі пристрої ПК в такій послідовності: периферійні пристрої, ВДТ, системний блок, стабілізатор (або блок безперервного живлення). Витягнути вилки з розеток. При наявності ознак горіння (дим, запах горілого) необхідно вимкнути всі пристрої ПК, знайти місце загоряння і виконати всі можливі заходи для його ліквідації, попередивши терміново про це керівництво. У випадку виникнення пожежі негайно попередити про це пожежну частину та керівництво, виконати усі можливі

заходи по евакуації людей з приміщення і розпочати гасіння пожежі первинними засобами пожежогасіння.

2) При замиканні, перевантаженні електричного струму на електричному обладнанні, внаслідок ураження грозової блискавки та ймовірної небезпеки ураженням електричним струмом, приймають наступне:

- попередження замикання здійснюється правильним вибором, монтажем експлуатації мереж;

- застосування захисту схем у вигляді швидкодіючих реле, а також вимикачів, плавких запобіжників, автоматичних вимикачів.

а) У випадку дотику до корпусу та інших струмоведучих частин електроустановки, що опинилися під напругою використовують захисне заземлення - зниження до безпечних значень напруги дотику і кроку, обумовлених замиканням на корпус та ін. Це досягається шляхом, зменшення потенціалу заземленого обладнання (за рахунок підйому потенціалу підстави, на якому стоїть людина, до значення, близького до значення потенціалу заземленого обладнання) та відключення від загальної електромережі ураженого обладнання.

б) У випадку замикання фази на корпус, зниження ізоляції мережі нижче визначеної межі і, нарешті, в разі дотику людини безпосередньо до частини, що знаходиться під напругою. Основними елементами пристрою захисного відключення є прилад захисного відключення і автоматичний вимикач.

Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

Загальний опір захисного заземлення визначається за формулою:

$$R_{ззп} = \frac{R_з \cdot R_п}{R_п \cdot n \cdot \eta_з + R_з \cdot \eta_п}, \qquad (A.3)$$

де Rз - опір заземлення, якими когут бать труби, опори, кути і т.п., Ом;

Rш - опір опори, яке з'єднує заземлювачі, Ом;

п - кількість заземлювачів;

ηз - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; ηз = 0,7

ηш - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; ηш = 0,5;

Опір заземлення визначається за формулою:

$$R_з = \frac{\rho}{2\pi \cdot l} \cdot \left(\ln \frac{2 \cdot l}{d} + \frac{1}{2} \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right), \qquad (A.4)$$

де ρ - питомий опір ґрунту, залежить від типу ґрунту, Ом·м;

для піску - А00 ÷ 700 Ом·м; приймаємо ρ = А00 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l = 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_з = \frac{400}{2 \cdot 3{,}14 \cdot 3}\left(\ln\frac{2 \cdot 3}{0{,}05} + \frac{1}{2}\ln\frac{4 \cdot 2 + 3}{4 \cdot 2 - 3}\right) = 110, \text{ Ом}$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_ш = \frac{\rho}{2\pi \cdot L} \cdot \ln\frac{2 \cdot L^2}{b \cdot t^1}, \quad (А.5)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

t_1 - глибина заземлення від рівня землі, м; $t_1 = 0{,}5$ м.

$$R_п = \frac{400}{2 \cdot 3{,}14 \cdot 160} \cdot \ln\frac{2 \cdot 160^2}{0{,}03 \cdot 0{,}5} = 5{,}99, \text{ Ом}$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_з}{4 \cdot \eta_з}, \quad (А.6)$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ззп} = \frac{110 \cdot 5{,}99}{5{,}99 \cdot 79 \cdot 0{,}7 + 110 \cdot 0{,}5} = 1{,}7 \text{ Ом}$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{ззп} < 4$ Ом.

4.8 Охорона навколишнього природного середовища

4.8.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи, а саме: розробка програмного забезпечення в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища», Законом України «Про забезпечення санітарного та епідемічного благополуччя населення», Законом України «Про відходи», Законом України «Про охорону атмосферного повітря», Законом України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру», Водний кодекс України.

В процесі діяльності оператора виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

1 Змінні носії інформації - IV клас небезпеки

2 Відходи друкуючих пристроїв - IV клас небезпеки

4.8.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Наводяться вимоги зберігання виявлених за своєю роботою відходів відповідно до вимог Державних санітарних правил і норм ДСанПіН 2.2.7.029.

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення Зазначені для зберігання відходів місця чи об'єкти повинні використовуватися лише для заявлених відходів.

Відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і доставляють на місце утилізації або захоронення

4.8.3 Визначення впливу та заходів щодо поводження з відходами ІТ галузі

З метою визначення та прогнозування впливу відходів на навколишне середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно до Закону України

«Про відходи» повинен здійснюватися моніторинг місць утворення, зберігання, і видалення відходів

Відомості про місце утворення та місце розташування відходів зазначаються на «План схемі місці розміщення відходів організації / виробництва» та наводяться у таблиці 4.5

Таблиця 4.5 - **Відомості про місце утворення та місце розташування відходів**

№ з/п	Код та найменування відходів за ДК -005-96	Технологічний процес або виробництво, де утворюються відходи / клас небезпеки	Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху)	№ на схемі (додається масштабна схема місць розміщення відходів)
1	Змінні носії інформації	4	буд. 84, кім. 412 V=0,0005 м^3	8401-ТХ
2	Відходи системних блоків (в комплекті) Пакувальні матеріали батарейки Відходи друкуючих пристроїв. Акумулятор для джерел безперебійного харчування	4	буд. 84, кім. 412 m=5,0 кг.	8401-ТХ
3	Відходи друкуючих пристроїв.	4	буд. 84, кім. 412 V=1,0 м^3	8401-ТХ
4	Акумулятор для джерел безперебійного харчування	3	буд. 84, кім. 412 S =5,0 м.2	8401-ТХ

4.9 Висновки до розділу

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в дипломній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної

та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

А також визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

ВИСНОВКИ

1. Проведено аналіз характеристик КП, існуючих методів, алгоритмів, моделей і засобів визначення КП оператора КС.
2. Запропоновано метод визначення клавіатурного почерку оператора комп'ютерної системи, який відрізняється від існуючих методів тим, що розпізнавання клавіатурного почерку відбувається за вільним текстом і отриманий шаблон почерку не залежить від набраного оператором тексту та порядку введення символів, що забезпечує можливість застосування методу для задач прихованого клавіатурного моніторингу з метою виявлення підміни авторизованого законного оператора.
3. Запропоновано математичну модель клавіатурного почерку, яка відрізняється від існуючих моделей тим, що час утримання клавіши представляється у вигляді перетину двох нормальних розподілів. Це збільшує в два рази кількість застосовуваних при розпізнаванні КП характеристик.
4. Запропоновано аналітичну модель клавіатурного почерку, що дозволяє порівняти два шаблони клавіатурного почерку.
5. Запропоновано алгоритм отримання шаблону клавіатурного почерку оператора інформаційної системи. Він відрізняється від існуючих алгоритмів тим, що при розпізнаванні клавіатурного почерку в якості характеристики почерку використовується час утримання клавіш, який представлений у вигляді перетину двох нормальних розподілів.
6. Запропоновано алгоритм авторизації оператора інформаційної системи за клавіатурним почерком. Запропоновано алгоритм постійного таємного клавіатурного моніторингу з метою виявлення підміни авторизованого оператора.
7. Розроблено спосіб представлення і зберігання клавіатурного почерку в ЕОМ.
8. Розроблено комплекс програм, які реалізують алгоритми і методи розпізнавання клавіатурного почерку. Їх можна використовувати як системи контроля та управління доступу до інформаційної системи.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 2007 COMPUTER CRIME AND SECURITY SURVEY [Електронний ресурс] / Режим доступу: http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf, вільний - Яз. англ.

2. Allen, J. D. An Analysis of Pressure-Based Keystroke Dynamics Algorithms. / J. D. Allen - Master's thesis - Dallas, TX: Southern Methodist University, 2010-97 p.

3. Balagani, K. S. On the Discriminability of Keystroke Feature Vectors Used in Fixed Text Keystroke Authentication. / K. S. Balagani, V. V. Phoha, A. Ray, S. Phoha // - Pattern Recognition Letters - Vol. 32, 2011 - pp. 1070-1080.

4. Bergadano, F. User authentication through keystroke dynamics. / F.Bergadano, D. Gunetti, C. Picardi // ACM Transactions on Information and System Security, - Vol. 5 (4), 2002 -pp.367-397.

5. Bryan, W.L. Studies in the physiology and psychology of the telegraphic language. / W. L. Bryan, N. Harter.// Psychological Review -4 (1), 1987 -pp. 27-53.

6. Burr, W.E. Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology. / W. E. Burr, D. F. Dodson, W. T. Polk. // Technical Report 800-63, - National Institute of Standards and Technology (NIST), 2006 - 121 p.

7. Butsch, R. Eye movements and the eye-hand span in typewriting. / R. Butsch // Journal of Educational Psychology - 23 (2), 1932 - pp. 104 - 121.

8. Cooper, W.E. Studies of typing from the LNR research group / W.E. Cooper, D.A. Norman, D.E. Rumelhart // Cognitive aspects of skilled typing. –New York: Springer-Verlag; 1983. - pp. 45-65.

9. CreateWaitableTimer - [Електронний ресурс] / Режим доступу: http://msdn.iTiicrosoft.com/en-us/library/ms682492(VS.85).aspx, вільний - Яз. англ.

10. DataLossDB Open security foundation [Електронний ресурс] / Режим доступу: http://www.datalossdb.org/

11. Gaines, R. S. Authentication by Keystroke Timing: Some Preliminary Results. / R. S. Gaines, W. Lisowski, S. J. Press, N. Shapiro. // Technical Report R-2526-NSF, - Santa Monica, CA: Rand Corporation, 1980 -113 p.

12. Giot, R. GREYC keystroke: A benchmark for keystroke dynamics biometric systems. / R. Giot, M. El-Abed, C. Rosenberger // In IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems 2009 -pp. 1-6.

13. Guven, A. Understanding users 'keystroke patterns for computer access security. / A. Guven, I. Sogukpinar. // Computers & Security, - Vol. 22 (8), 2003 pp. 695-706.

14. Jain, A.K. An Introduction to Biometric Recognition / A.K. Jain, A. Ross, S. Prabhakar // IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics -Vol. 14, No. 1, January 2004 - pp. 4-20.

15. Jain, A.K. Biometrics: Personal Identification in Networked Society, chapter Introduction To Biometrics. / A.K. Jain, R. Bolle, S. Pankanti // Springer, 1 edition, January 1999 -pp. 1-41.

16. Jones, R.G. A model for subjective grouping in typewriting. / E. A. C Thomas, R. G. Jones. // Quarterly Journal of Experimental Psychology - 22 (3), 1970-pp. 353-367.

17. Joyce, R. Identity authentication based on keystroke latencies. / R.Joyce, G. Gupta. // Communications of the ACM, - Vol. 33 (2), 1990. - pp.168-176.

18. Kang, P. Improvement of keystroke data quality through artificial rhythms and cues. / P. Kang, S. Park, S. seob Hwang, H. joo Lee, S. Cho. // Computers & Security, 27 (l-2): 3 - 11, 2008.

19. Kaman, M. Biometric personal authentication using keystroke dynamics: A review. / M. Karnan, M. Akila, N. Krishnaraj // Applied Soft Computing, - 11 (2), 2011 - pp. 1565-1573.

20. Killourhy, K. The Effect of Clock Resolution on Keystroke Dynamics. / K. Killourhy, R. Maxion // In R. Lippmann, E. Kirda, and A. Trachtenberg, editors, Recent Advances in Intrusion Detection, - volume 5230 of Lecture Notes in Computer Science, Рік випуску 2008 - pp. 331-350.

21. L.F. Coppenrath and Associates Biometric Solutions By Classification. [Електронний ресурс] / Режим доступу: http://www.lfca.net/Reference%20Documents/Biometric%20Solutions%20By%20Classification.pdf, 2001., вільний - Яз. англ.

22. Leggett, J. Dynamic identity verification via keystroke characteristics. / J. Leggett, G. Williams, M. Usnick, M. Longnecker // International Journal of Man-Machine Studies, - Vol.35 (6), 1991 pp. 859 - 870.

23. Lv, H.-R. Emotion recognition based on pressure sensor keyboards. / H.-R. Lv, Z.-L. Lin, W.-J. Yin, J. Dong. // Multimedia and Expo, 2008 pp. +1089 -1092.

24. Marsters, J. D. Keystroke Dynamics as a Biometric. / J. D. Marsters // PhD thesis - University of Southampton 2009 - 56 p.

25. Monrose, F. Authentication via keystroke dynamics. / F. Monrose, A.Rubin // In Proceedings of the 4th ACM Conference on Computer andCommunications Security, 1997 pp. 48-56.

26. Monrose, F. Password hardening based on keystroke dynamics. / F Monrose, M. K. Reiter, S. Wetzel // International Journal of Information Security - Vol.1, 2002 pp. 69-83.

27. NtDelayExecution - RealCoding [Електронний ресурс] / Режим доступу: http://forums.realcoding.net/lofiversion/index.php/tl6146.html,

вільний - Яз. англ.

28. Obaidat, M. An online neural network system for computer access security. / M. Obaidat, D. Macchiarolo // IEEE Transactions on Industrial Electronics, - 40 (2), 1993 -pp.235 -242.

29. Ostry, D.J. Tutorials in Motor Behavior, chapter Execution-Time Movement Control. / D.J. Ostry // Elsevier Science Publishers B. V., 2 edition,1985-pp. 457

30. Peacock, A. Typing patterns: a key to user identification. / A. Peacock, X. Ke, M. Wilkerson // IEEE, Security Privacy, - 2 (5), 2004 - pp.40-47.

31. Perrig Adrian, Dawn Song, Peter Venable. «User Recognition by Keystroke Latency Pattern Analysis »[Електронний ресурс] / Режим доступу: http://paris.cs.berkeley.edu/perrig/projects/keystroke/file.ps вільний - Яз. англ.

32. Revett, K. A Bioinformatics Based Approach to Behavioural Biometrics. / K. Revett. // In Frontiers in the Convergence of Bioscience and Information Technologies, 2007 - pp. 665-670.

33. Robinson, J. A. Computer User Verification Using Login String Keystroke Dynamics. / J. A. Robinson, V. M. Liang, J. A. M. Chambers, C L. MacKenzie // IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, - Vol. 28 (2), 1998 - pp. 236-241.

34. Rumelhart, D. E. Simulating a skilled typist: a study of skilled cognitivemotor performance. / D. E. Rumelhart, D. A. Norman. // Cognitive Science-6 (1), 1982-pp. 1-36.

35. Sadoun, B. Verification of Computer Users Using Keystroke Dynamics. / M. S. Obaidat, B. Sadoun / ЯEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, - 27 (2), 1997 - pp. 261-269.

36. Salthouse, T.A. Perceptual, Cognitive, and Motoric Aspects of Transcription Typing. / T.A. Salthouse // Psychological Bulletin - 99 (3), 1986 - pp. 303-319.

37. Salthouse, T. A. Anticipatory processing in transcription typing. / T. A. Salthouse // J. Appl. Psychol. 70, 2, 264-271.

38. Shaffer, L. H. Latency mechanisms in transcription. / L. H. Shaffer // Attention and performance - Vol. 4 - New York: Academic Press, 1973 - pp. 435-446.

39. Shaffer, L.H. Timing in the motor programming of typing. / L.H. Shaffer // Quarterly Journal of Experimental Psychology, 1978- V. 30. N 2. - pp. 333-345.

40. Spillane, R. J. Keyboard Apparatus for Personal Identification. / R.J. Spillane. // Technical Disclosure Bulletin -17, 3346, - IBM, 1975 - 77 p.

41. Umphress, D. Identity verification through keyboard characteristics. / D. Umphress, G. Williams // International Journal of Man-Machine Studies, - 23 (3), 1985-pp. 263-273.

42. Vacca, J.R. Biometric Technologies and Verification Systems. / J.R. Vacca // Butterworth-Heinemann, 1 edition, 2007 - 656 p.

43. Verwey, W.B. Practicing a Structured Continuous Key-Pressing Task: Motor Chunking or Rhythm Consolidation? / W.B. Verwey, Y. Dronkert. // Journal of Motor Behavior - 28 (1), 1996. - pp. 71-79.

44. Wildes, R.P. Iris Recognition: An Emerging Biometric Technology / R.P. Wildes // Proceedings of The IEEE - USA: Institute of Electrical andElectronics Engineers, 1997 - vol. 85, no. 9. - pp. 1348-1363.

45. Yong, S. Weightless Neural Networks for Typing Biometrics Authentication. / S. Yong, W. K. Lai, G. Goghill // In Knowledge-Based Intelligent Information and Engineering Systems, volume 3214 of Lecture Notes in Computer Science, 2004 - pp. 284-293.

46 Лигін Ю.О. Аутентифікація користувачів комп'ютерних систем на основі аналізу їх клавіатурного почерку.//Майбутній науковець-2018: матеріали всеукр. наук.-практ.конф. 14 груд.2018 р.,м. Сєвєродонецьк .Ч.II./укладач В.Ю. Тарасов - Сєвєродонецьк: Східноукр.нац. ун-т ім. В.Даля, 2018 -332с. - С.18-20

47 Лигін Ю.О. Засоби аутентифікації користувачів комп’ютерних систем на основі інформаційниї моделей / Ю.О. Лигін, Л.О. Шумова // Вісник СНУ ім. В. Даля: науковий журнал – 2018. - №6[247] – с. 82-85.

48. Ахутин, В. М. О принципах построения комплексов для непрерывного контроля за организмом человека и автоматической нормализации его состояний Текст. / В.Н. Ахутин // Биоэлектрическое управление: Человек и автоматические системы. - М .: Наука, 1970. - С. 519.

49. Биометрические системы: новое слово в информационной безопасности бизнеса [Электронный ресурс] / Режим доступа: http://www.bioiTietrics.ru/news/biometricheskie_sistemi_novoe_slovo_v_informacionno ibezopasnostibiznesa /

50. Борзяк, Э.И. Анатомия человека / Э.И. Борзяк, В.Я. Бочаров, Л.И. Волкова и др .; под ред. М.Л. Сапин. - М .: Медицина, 1987. - Т. 1. - 109 с.

51. Брюхомицкий, Ю.А., Учебные Биометрические системы контроля доступа по рукописному и клавиатурному почеркам. / Ю.А. Брюхомицкий, М.Н. Казарин. // Научная сессия МИФИ-2006. XIII Всероссийская научная конференция. проблемы информационной безопасности в системе высшей школы, - Таганрог, ТРГУ, 2004, - С. 33-34.

52. Белов, Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов - М.: "Торячая линия- Телеком ", 2006.-544 с.

53. Бусленко, Н.П. Моделирование сложных систем /Н.П. Бусленко. - М.: Наука, 1978.- 400 с.

54. Вапник В.Н. В равномерной сходимости частот появления событий к их вероятность /В.Н. Вапник, А.Я. Червоненкис // Теория вероятностей и ее применения, 1971, Т. 16, № 2. С. 264-280.

55. Варфоломеев, А.А. Основы информационной безопасности: Учебное пособие. / А.А. Варфоломеев - М .: РУДН, 2008. - 412 с.

56. Вежневец, В. Оценка качества работы классификаторов. / В. Вежневец - Компьютерная графика и мультимедиа. - Выпуск №4 (1) / 2006 [Электронный ресурс] / Режим доступа: http://cgm.computergraphics.rU/content/view/l06 ..

57. Веитцель, Е.С. Прикладные задачи теории вероятностей. / Е.С. Вентцель, Л. А. Овчаров. - М .: Радио и связь, 1983. -416 с.

58. Внутренние ИТ-угрозы в госсекторе 2006 [Электронный ресурс] / Режим доступа: http://www.cnews.ru/reviews/free/gov2007/articles/inner_danger.shtinl

59. Волчихина В.И. Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации / В.И. Волчихина, А.И. Иванов, В.А. Фунтиков. - Пенза: Изд-во Пензе. гос. ун-та, 2005.-276 с.

60. Гайдамакин, Н.А. Автоматизированные информационные системы, базы и банки данных. / Н.А. Гайдамакин // Вводный курс: Учебное пособие. - М .: Гелиос АРВ, 2002.-415 с.

61. Гамбаров, М. Статистическое моделирование и прогнозирование / Г.М. Гамбаров, Н.М. Журавль, Ю.Г. Королев - М .: Финансы и статистика, 1990. -384 с.

62. Гатчина, Ю.А. Математические модели оценки инфраструктуры системы защиты информации на предприятии / Ю.А. Гатчина, И.О. Жаринов, А. Коробейников // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики, СПб: ИТМО, 2012, -№2, - с.92-95.

63. Гатчина, Ю.А. Основные аспекты создания системы защиты периметра корпоративной информационной системы. / Ю.А. Гатчина, Н.В. Ермаков, А. Коробейников, К.В. Строганов // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики, - СПб: ИТМО - 2007, - №40, - с.279- 283.

64. Глазырин, И. Персональные данные. будни банковской безопасности / И. Глазырин // Банковские технологии. - М .: Профи-Пресс, 2012. - №5.-С. 35-37

65. Голинкевич Т. А. Прикладная теория надежности / Т. А. Голинкевич - М .: Высшая школа, 1985.-475 с.

66. Горелик, А.Л. Методы распознавания / А.Л. Горелик, В. А. Скрипкин. - М .: Высшая школа, 1984. - 80 с.

67. ГОСТ Р 51241-98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

68. ГОСТ Р ИСО / МЭК 15408-2001 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий

69. Десятерик, М.Н. Биометрическая нейросетевая система идентификации пользователя по особенностям клавиатурного почерка / В.Ф. Гузик, Г. А. Галуев, М.Н. Десятерик // Нейрокомпьютеры. Разработка, применение. 2001. - № 7-8, - С. 104-118.

70. Задорожный, В. Обзор биометрический технологий / В. Задорожный // Защита информации. Конфидент. - 2003. - № 5. - С. 26-29.

71. Зильберман, П. Б. Эмоциональная устойчивость оператора / П.Б. Зильберман // Очерки психологии труда оператора. - М .: Наука, 1974. С. 138-172

72. Иванов, А.И. Биометрическая идентификация личности по динамике подсознательных движений. / А.И. Иванов - Пенза: Изд-во Пензе. гос. ун-та, 2000.-188 с.

73. Иванов, А.И. Нейросетевые алгоритмы биометрической идентификации личности. / А.И. Иванов // Серия «Нейрокомпьютеры и их применение ». Кн. 15. - М .: Радиотехника, 2004. - с. 22-50.

74. Идов, Р. Защititесь от инсайдера / Р Идов - ТЭК. Стратеги развития - М .: Богенпринт, 2012. - №5- С. 64-65

75. Исследование: самые популярные системы аутентификации в Европе [Электронный ресурс] / Режим доступа: http://blogerator.ru/page/issledovanie-populjarnye-sistemy-autentifikaciibiometricheskaia-autentifikacija-indeed-id-statistika

76. Киселев, Ю.Н. Электронная коммерция: Практическое руководство. / Ю.Н. Киселев - СПб .: ДиаСофтЮП, 2001. - С. 11-40.

77. Колмогоров, А. Н. Теория вероятностей и математическая статистика. / А. Н. Колмогоров - М .: Наука, 1986 г. - 534 с.

78. Корнеева, А. П. Машинопись и основы современного делопроизводства / А.П. Корнеева, А.М. Амелина, А. П. Загребельный. - М .: Просвещение, 1979. - 212 с.

79. Коробейников, А. Алгоритм распознавания трехмерных изображений с высокой детализацией / А.Г. Коробейников, П.А. Кудрин, И.Г. Сидоркина // Вестник марийско государственного технического университета. Серия: Радиотехнические и Инфокоммуникационный системы - Йошкар-Ола: Марийско государственный технический университет, 2010. -№2 (9) .- С. 91-98.

80. Коробейников, А. Законодательные требования в области обеспечения информационной безопасности автоматизированных систем. / А. Коробейников, Ю. Гатчина,

А.Л. Липатов, Д.В. Осломенко // Сборник тезисов IV межвузовской конференции молодых ученых, -СПб: СПбГУ ИТМО, 2007. - с 165-169.

81. Лебедев, А. Н. ЭЭГ прогноз успешности выполнения психомоторного теста при снижение уровня бодрствования: постановка задачи. / Т.Н. Щукин, В. Б. Дорохов, Е.В. Луценко, А.Н. Лебедев // Научный журнал КубГАУ. - 2004.- №4 (6). - 9 с.

82. Лебедев, А. Н. ЭЭГ прогноз успешности выполнения психомоторного теста при снижение уровня бодрствования: анализ результатов исследования. / Т.Н. Щукин, В. Б. Дорохов, А. Н. Лебедев, Е. Луценко // Научный журнал КубГАУ. - 2004- №4 (6). - 17 с.

83. Лукашев, И. Биометрии в СКД: вызовы времени и новые возможности. / И. Лукашев - Системы безопасности - М .: Groteck, 2007. - №6.-С. 128-133

84. Марченко В.В. Динамическая аутентификация на основе анализа клавиатурного почерка / В.П. Широчин, А.В. Кулик, В.В. Марченко // Вестник Национального технического университета Украины «Информатика, управление и вычислительная техника». - 1999. - № 32. - С. 3-16.

85. Минниханов, Р.Н., Столов Е.Л. Аутентификация оператора на основе его работы с клавиатурой. / Р.Н. Минниханов, Е.Л. Столов // Тез. докл. третьей межд. конф. "Развитие и применение открытых систем". -М., 1996.-С. 159-162.

86. Можно ли сэкономить при помощи биометрии [Электронный ресурс] / Режим доступа: http://www.cnews.ru/reviews/free/securitv2010/articles/articlesl3.shtml

87. Музыкин, С. Н. Моделирование динамических систем. / С. Н. Музыкин, Ю. М. Родионова. - Ярославль: Верх.-волж. кн. изд-во, 1984. -245с.

88. Пятибратов, А.П. Человеко-машинные системы: эффект эргономического обеспечения. / А.П. Пятибратов - М.: Экономика, 1987.- 468с.

89. Расторгуев, С. П. Программные методы защиты информации в компьютерах и сетях. / С П . Расторгуев, - М.: Изд-во Агентства «Яхтсмен», 1993.- 188 с.

90. Розанов, Ю.А. Лекции по теории вероятностей. / Ю.А. Розанов - М. : Наука, 1968. - 120 с.

91. Романец, Ю.В. Защита информации в современных компьютерных системах. / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин // - 2-е издание: М.: Радио и связь, 2001. -376 с.

92. Руссинович, М. Внутреннее устройство Microsoft Windows. / М. Руссинович, Д. Соломон - СПб.: Питер, 2005. - 992 с.

93. Рыбченко, Д.Е. Критерии устойчивости и индивидуальности компьютерного почерка при вводе ключевых фраз. / Д.Е. Рыбченко — Специальная техника средств связи. Серия «Системы, сети и технические средства конфиденциальной связи».— Пенза, ПНИЭИ, 1997, вып.№2 - с. 104-107.

94. Савельева, А.И. Обработка результатов измерения при проведении физического эксперимента: Методические указания к лабораторной работе М-1 по курсу «Общая физика» / А.И. Савельева, И.Н. Фетисов // Под ред. СП. Ерковича. — М.: Изд-во МГТУ, 1990. -32 с.

95. Савинов, А.Н. Три алгоритма управления доступом к КСИИ на основе распознавания клавиатурного почерка оператора / А.Н. Савинов, И.Г. Сидоркина // Вестник Чувашского университета. - Чебоксары: ЧТУ им. И.Н. Ульянова, 2013. - № 3. - С. 293-301.

96. Сарбуков А.Е. Аутентификация в компьютерных системах / А.Е. Сарбуков, А.А. Грушо // Системы безопасности. - 2003. - № 5(53). - С. 118-122.

97. Симанков, В.С. Адаптивное управление сложными системами на основе теории распознавания образов: Монография (научное издание) / В. С. Симанков, Е. В. Луценко. - Краснодар: Техн. ун-т Кубан. гос. технол. ун-та., 1999.-318 с.

98. Синицын, И.Н. Метрологические и биометрические технологии и системы / И.Н. Синицын, А.В. Губин, О.С. Ушмаев // История науки и техники. - М.: НАУЧТЕХЛИТИЗДАТ, 2008 - №7. - С. 41-44.

99. Тыртышников, Е.Е. Методы численного анализа. / Е.Е. Тыртышников - М.: ИЦ Академия, 2007. - 317 с.

100. Фор, А. Восприятие и распознавание образов. / А. Фор - М. Машиностроение, 1989. - 103 с.

101. Шахлевич, А. Imperva. Решение File Activity Monitoring - друг и помощник Вашей DLP-системы. [Электронный ресурс] / Режим доступа: http://www.netwell.ru/press/smi_detail.php?aid=60&binn_rubrik_pl_articles=221

102. Шляхтина, С. ИТ-безопасность: сегодня и завтра / С. Шляхтина - КомпьютерПресс - М.: КомпьютерПресс , 2008 - №3 - С. 20-23.

103. Щупак Ю.А. Win32 API. Эффективная разработка приложений. - СПб.: Питер, 2007. - 572 с.

104. Яглом, А. М. Вероятость и информация / А. М. Яглом, И. М. Яглом // М.: Наука, 1973 -456 с.

105. Ясенев, В.Н. Информационная безопасность в экономических системах: Учебное пособие / В.Н. Ясенев - Н. Новгород: Изд-во ННГУ, 2006.-253 с.

Додаток А. Шаблони клавіатурного почерку оператора

Таблиця А.1 - Шаблон клавіатурного почерку оператора з розрахованими математичними сподіваннями

Login			LihinYura			
Клавіша	$M_{ЧУК-1}$	$M_{ЧУК-2}$	Кількість $N_{ЧУК-1}$	Кількість $N_{ЧУК-2}$	Вибірка нормального розподілу ЧУК-1	Вибірка нормального розподілу ЧУК-2
А	44	98	!	!		
А	56	106	!	!		
Б						
В	64	96	!	!		
Г	72	124	!			
Д	61	94				
Е	51	100				
Е	76	108		!		
Ж	54		!			
З	84	1	!			
И	62			!		
И	60	101				
К	62	108	!			
Л	61		!	!		
М	49		!			
Н	64	22	!			
О	62	63				
П	63	124				
Р	57	94	!			
С	70		!			
Т	90					
У	89			!		
ф	82		!			
Х	81	89	!			
ц	85		!			
ч	80	108	!			
ш	49	106	!	!		
щ	64	102				
ъ	72	90				
ы	61	96		!		
ь	51	124				
э	76	94	!			
ю	54	100	!			
я	84	108				

Таблиця А.2 - Інформаційний файл

Действие Клавиша Нажатие\Отпускание	Время нажатия	Время в микросек	№
Down	13:27:34:897	395168140477850	#49 1
Up	13:27:35:006	395168364031970	#49 1
Down	13:27:35:131	395168623698310	#50 2
Up	13:27:35:240	395168826343640	#50 2
Down	13:27:35:428	395169215637300	#51 3
Up	13:27:35:522	395169407362440	#51 3
Down	13:27:35:694	395169760854590	#52 4
Up	13:27:35:787	395169931309660	#52 4
Down	13:27:36:006	395170373266140	#53 5
Up	13:27:36:100	395170543714930	#53 5
Down	13:27:36:287	395170929295890	#54 6
Up	13:27:36:366	395171090862790	#54 6
Down	13:27:36:881	395172129826000	#56 7
Up	13:27:36:975	395172310829940	#56 7
Down	13:27:37:162	395172680956040	#57 8
Up	13:27:37:272	395172883307700	#57 8
Down	13:27:38:350	395175044522230	#48 9
Up	13:27:38:428	395175214880858	#48 9
Down	13:27:40:975	395180306081010	#70 0
Up	13:27:41:053	395180455202660	#70 0
Down	13:27:42:068	395182483857160	#188 а
Up	13:27:42:147	395182643630760	#188 а
Down	13:27:42:850	395184033140680	#68 б
Up	13:27:42:928	395184203588780	#68 б
Down	13:27:43:631	395185598384710	#85 в
Up	13:27:43:709	395185747511240	#85 в
Down	13:27:44:412	395187150597984	#76 г
Up	13:27:44:475	395187289061746	#76 г
Down	13:27:46:631	395191586323880	#84 д
Up	13:27:46:725	395191767430560	#84 д
Down	13:27:47:506	395193346622050	#186 е
Up	13:27:47:584	395193506412670	#186 е
Down	13:27:48:209	395194725150074	#80 ж
Up	13:27:48:287	395194884563110	#80 ж
Down	13:27:49:068	395196464473440	#66 з
Up	13:27:49:162	395196645556260	#66 з

ДОДАТОК Б. Електронна презентація

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені В.Даля

Методи й апаратно-програмні засоби захисту інформаціїї в комп'ютерних системах

Автор:
ст. групи КІ-17зм
Лигін Юрій Олександрович

Керівник дипломної роботи:
Шумова Лариса Олександрівна

2019

Рисунок Б.1 –Слайд №1

Актуальність теми і мета роботи

- Захист інформації в комп'ютерних системах і мережах - це комплексне завдання, вирішення якого відбувається за допомогою впровадження різних систем безпеки. Одну з головних ролей у вирішенні даного завдання відіграє елемент, що забезпечує контроль доступу до ресурсів комп'ютерної системи. Такий елемент виконує свої функції за допомогою процедур ідентифікації і аутентифікації користувачів. Тому стає **актуальною** проблема захисту інформаціїї від несанкціонованого доступу. Кожен користувач повинен бути однозначно визначений і має бути гарантова на відповідність користувача і його ідентифікатора
- **Метою дослідження** є підвищення інформаційної безпеки КС.

Рисунок Б.2- Слайд №2

Задачі дослідження

Для досягнення поставленої мети в роботі сформульовані і вирішені **наступні завдання**:

- аналіз і дослідження характеристик КП, існуючих методів, алгоритмів, моделей і засобів визначення КП оператора КС;
- розробка математичних моделей розпізнавання КП оператора КС;
- розробка алгоритму розпізнавання КП по часу утримання клавіш;
- розробка способу зберігання і передачі даних про КП;
- розробка методу розпізнавання КП по вільному тексту;
- розробка та реалізація алгоритму розпізнавання КП по часу утримання клавіш;
- проведення експериментального дослідження підсистеми доступу до КС на основі аналізу КП оператора.

Об'єкт дослідження – процеси організації і управління доступом до системи інформаційної інфраструктури

Предмет дослідження - методи і алгоритми розпізнавання КП оператора КС.

Рисунок Б.3 – Слайд №3

Технології аутентифікації, які використовують у світі

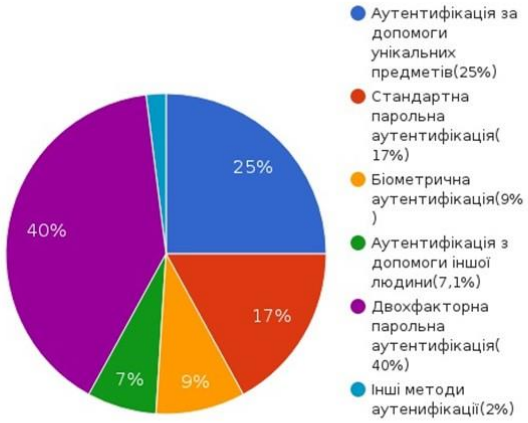


Рисунок Б.4- Слайд № 4

Недоліки парольних та атрибутних методів аутентифікації

Парольні аутентифікація є найбільш розповсюдженим засобам захисту інформації. Перевагою таких засобів є простота використання. Але подібні системи мають невисокий рівень безпеки, у зв'язку з великою кількістю недоліків. Виявлено такі недоліки парольних методів аутентифікації :

- можливість підбору пароля;
- невиконання інструкцій по створенню безпечного пароля (недбале ставлення до процедури вибору пароля);
- існування і наявність у вільному доступі спеціалізованих утиліт для підпору і злому паролів;
- пароль може бути отриманий шляхом застосування фізичного та психологічного впливу на користувача;
- пароль може бути вкрадений (перехоплений при авторизації або бути візуально скомпрометований).

Аутентифікація за допомогою унікального предмета дозволяє забезпечити більш надійний захист інформації, ніж парольна аутентифікація. Але атрибутна аутентифікація, як з «пасивними», так і з «активними» унікальними предметами володіє декількома виявленими недоліками:

- можливість крадіжки предмета у оператора;
- необхідність в спеціальному обладнанні для роботи з магнітними картками, смарт-картами і т.і.;
- можливість виготовлення копії унікального предмета;
- можливість підробки унікального предмета.

Рисунок Б.5 – Слайд №5

Спрощена архітектура біометричної системи виявлення підміни законного оператора

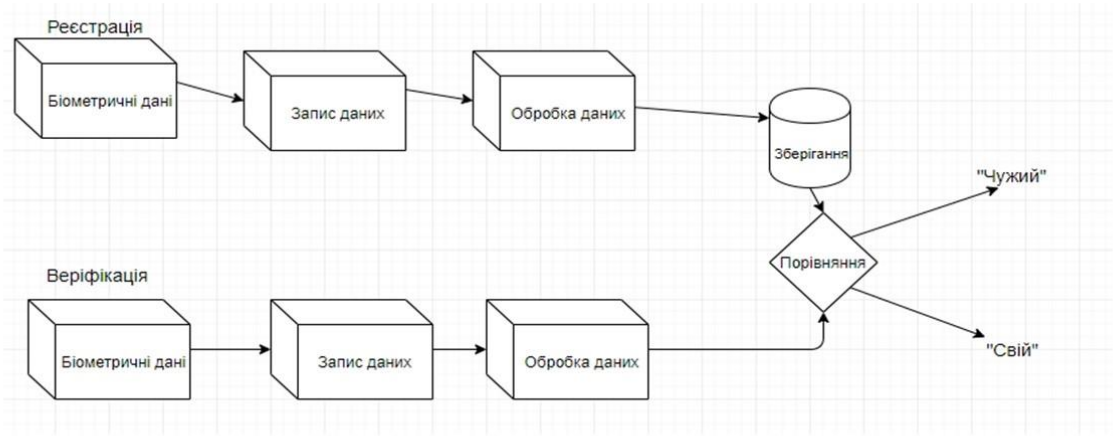
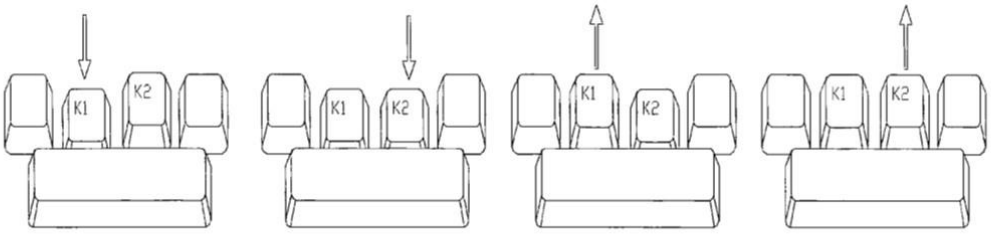


Рисунок Б.6 – Слайд № 6

Зразок ситуації накладення клавіш



В момент утримання першої клавіші відбувається натискання другої. Кнопка «К1» натискається. Далі відбувається натискання клавіші «К2», але «К1» ще не відпущена. Потім відбувається відпускання клавіші «К1», далі відпускається клавіша «К2»

Рисунок Б.7 – Слайд № 7

Алгоритм отримання клавіатурного почерку

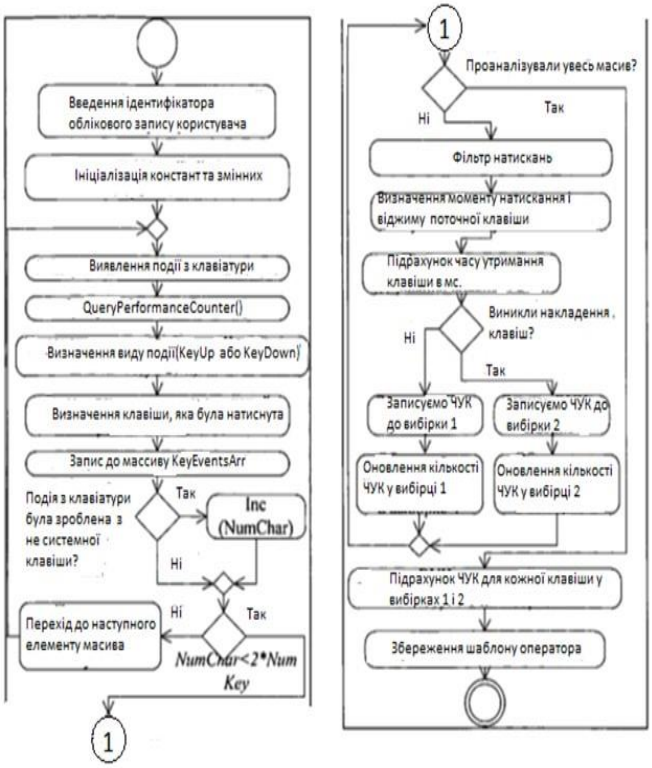


Рисунок Б.8 – Слайд № 8

Програмний інтерфейс блоку збору біометричних характеристик

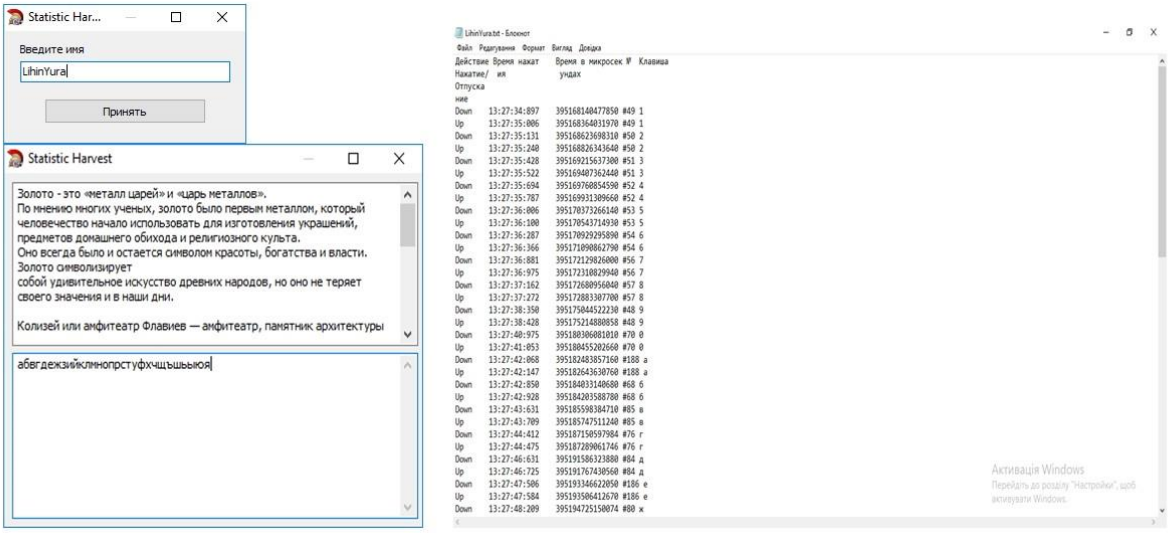


Рисунок Б.9 - Слайд № 9

Висновки

Проведено аналіз характеристик комп'ютерного почерку оператора комп'ютерної системи, а також існуючих методів, алгоритмів, моделей і засобів визначення комп'ютерного почерку.

Запропоновано метод визначення клавіатурного почерку, який відрізняється від існуючих такими характеристиками:

- розпізнавання клавіатурного почерку відбувається за довільним текстом,
- отриманий шаблон почерку не залежить від набраного оператором тексту та порядку введення символів, що забезпечує можливість застосування методу для задач прихованого клавіатурного моніторингу.

Запропоновано математичну модель клавіатурного почерку, яка відрізняється від існуючих моделей тим, що час утримання клавіши представляється у вигляді перетину двох нормальних розподілів. Це збільшує в два рази кількість застосовуваних при розпізнаванні КП характеристик.

Запропоновано аналітичну модель клавіатурного почерку, що дозволяє порівняти два шаблони клавіатурного почерку.

Розроблено алгоритм отримання шаблону клавіатурного почерку, в якому при розпізнаванні почерку як характеристика використовується час утримання клавіш, час утримання представлений у вигляді перетину двох нормальних розподілів.

Запропоновано алгоритм авторизації оператора за клавіатурним почерком. Запропоновано алгоритм постійного таємного клавіатурного моніторингу з метою виявлення підміни авторизованого оператора.

Розроблено спосіб представлення і зберігання клавіатурного почерку в ЕОМ.

Рисунок Б.10 – Слайд № 10