Encryption algorithms – Part 3: Block ciphers. 39. Горбенко И. Д., Долгов В. И., Олейников Р. В, Руженцев В. И., Михайленко М. С., Горбенко Ю. И., Тоцкий А. С., Казмина С. В. Перспективный блочный шифр "Калина" – основные положения и спецификация // Прикладная радиоэлектроника, 2007, №2. 40. IDEA NXT Technical Description, MediaCrypt, W W W. M E D I A C R Y P T. C O M, 2005 Надійшла до редколегії 2014 41. ISO/IEC 10116. Information technology – Security techniques – Modes of operation for an n-bit block cipher.

УДК 681.3

С. А. Лупенко, Н. Р. Шаблій, А. М. Лупенко
Тернопільський національний технічний університет імені Івана Пулюя

КОМПАРАТИВНИЙ АНАЛІЗ МОДЕЛЕЙ, МЕТОДІВ ТА ЗАСОБІВ АУТЕНТИФІКАЦІЇ ОСОБИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗА ЇЇ КЛАВІАТУРНИМ ПОЧЕРКОМ

Проаналізовано моделі, методи та засоби аутентифікації користувачів комп'ютерів за їх клавіатурним почерком. Виявлено недоліки наявних математичних моделей та методів опрацювання даних клавіатурного почерку. Сформульовано актуальні завдання подальших наукових досліджень у цій сфері інформаційної безпеки.

Ключові слова: біометрична аутентифікація, клавіатурний почерк, математичне моделювання.

COMPARATIVE ANALYSIS OF MODELS, METHODS AND TOOLS OF PERSONAL AUTHENTICATION IN INFORMATIONAL SYSTEMS AFTER KEYBOARD RHYTHM

The article analyzes the models, methods and means of authentication of computer users by their handwriting keyboard. Identified deficiencies of existing mathematical models and methods of data processing keyboard writing. Formulated topical problems of further research in the field of information security.

Key words: biometric authentication, computer handwriting, mathematical model.

Вступ

Інтенсивний розвиток засобів телекомунікацій, локальних та глобальних комп'ютерних мереж стимулює в останнє десятиліття інтенсивний розвиток технологій зберігання та опрацювання даних з використанням віддалених ресурсів – GRID та хмарних технологій, що, своєю чергою, призводить до того, що проблеми захисту інформації у цих системах виходять на перше місце. Захист інформації – це комплекс заходів, спрямованих на запобігання несанкціонованому витоку, модифікації та видаленню інформації, здійснюваним із застосуванням технічних, зокрема програмних, засобів. Враховуючи різноманіття потенційних інформаційних загроз, складність їх структури і функцій, а також участь людини в технологічному процесі опрацювання інформації, збереження і конфіденційності останньої можна досягти, лише створивши комплексну систему захисту інформації.

Одним із основних і невід'ємних елементів такої комплексної системи є підсистема управління доступом до інформаційних ресурсів, яка надає засоби реєстрації (ідентифікації) та аутентифікації користувачів, що уможливлює розмежування доступу кола осіб, які мають доступ до інформації та запобігання шкідливим впливам на роботу інформаційної системи загалом. Під *ідентифікацією* (лат. *identifico* – ототожнювати) розуміють процедуру розпізнавання користувача в системі, як правило, за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою. Ідентифікація використовується для отримання інформації про суб'єкт системи на основі наданого ним ідентифікатора. Є початковою процедурою надання доступу до системи. Після неї здійснюється аутентифікація та авторизація. *Аутентифікація* (з грец. *αυθεντικός* – реальний або істинний) особи в інформаційній системі – це перевірка відповідності суб'єкта і того, за кого він себе намагається видати, за допомогою деякої унікальної інформації (паролю, відбитка пальця, голосу тощо). З позицій інформаційної безпеки аутентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації, та передує авторизації.

Існують різні метоти ідентифікації та аутентифікації користувачів інформаційної системи. Традиційні методи ідентифікації та аутентифікації ґрунтуються на використанні карток, електронних ключів, паролів і кодів доступу. Один зі способів аутентифікації в інформаційній системі полягає у попередній ідентифікації на основі користувацького ідентифікатора ("логіна" (англ. *login)* – реєстраційного імені користувача) і пароля – певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом у мережі. Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх з даними, які зберігаються в спеціальній захищеній базі даних і, у випадку успішної аутентифікації проводить авторизацію з подальшим допуском користувача до роботи в системі. Основний недолік таких методів ідентифікації та аутентифікації зумовлений неоднозначністю ідентифікованої особи. Передусім це пов'язано з тим, що для встановлення автентичності особи застосовують атрибутивні й основані на знаннях розпізнавальні характеристики. Іншим важливим недоліком традиційних методів ідентифікації та аутентифікації є відсутність можливості виявлення підміни ідентифікованого користувача, що дає змогу зловмисникові отримати доступ до ресурсів системи, який обмежений тільки правами ідентифікованого користувача.

Зазначені вище недоліки можна виправити, доповнивши систему захисту методами біометричної аутентифікації. Усі методи біометричної ідентифікації та аутентифікації поділяються на статичні та динамічні. Статичні методи ґрунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній властивості, вродженій і невід'ємній від неї (відбитки пальців, малюнок сітківки та райдужної оболонки ока, геометрія малюнка долоні). Динамічні методи ґрунтуються на поведінковій (динамічній) характеристиці людини, тобто враховують особливості, характерні для підсвідомих рухів у процесі відтворення якої-небудь дії. Серед цих методів біометричної аутентифікації значний інтерес викликають методи аутентифікації за динамічним підписом людини та за клавіатурним (комп'ютерним) почерком.

Для методу аутентифікації за клавіатурним почерком характерна можливість розпізнавання підсвідомих рухів людини під час введення нею тексту з клавіатури, що, своєю чергою, дає змогу вести прихований моніторинг роботи оператора та стежити за несанкціонованою підміною відповідальної особи чи її психофізичним станом. Сфера її застосування – системи, в яких існує клавіатурне введення інформації або управління через клавіатуру: це різні комп'ютерні системи та мережі, системи стільникового зв'язку та спецзв'язку.

Огляд літературних джерел

Проблеми застосування клавіатурного почерку в системах аутентифікації вивчались у роботах таких вчених, як Dawn Song, Peter Venable, Adrian Perrig (Pittsburgh, PA, USA); R. Gaines, W. Lisowski, S. Press, N. Shapiro (Santa Monica, CA, USA); Alen Peacock, J. Leggett, D. Umphress, G. Williams (Texas, USA); M. S. Obaidat, B. Sadoun (New Jersey, USA); С. Н. Расторгуев, Р. Н. Миниханов А. И. Иванов, Л. Е. Чала, Р. Р. Шарипов, М. Н. Казарин, А. Н. Савинов та інші.

Автором однієї з перших робіт у цій галузі є Гейнс (1980 р.) [1]. Його дослідження продовжені в роботах Леггета і Вільямса [2]. У своїй доповіді Леггет для характеристики достовірності (точності) біометричної аутентифікації навів такі дані своєї системи: FRR (помилка першого роду) – 5,5 %, FAR (помилка другого роду) – 5 % (помилка I роду (FRR) – помилкове відхилення справжніх користувачів (не впустити "свого") і помилка II роду (FAR) – помилкове прийняття зловмисників (впустити "чужого")). Коефіцієнт достовірності аутентифікації становив 89,5 %.

Дослідження біометричної аутентифікації за клавіатурним почерком також проводили такі вчені, як Гарсія, Янг та Хаммон. На відміну від попередників, Янг і Хаммон використали евклідову відстань між двома часовими векторами та час для набору заданої певної кількості слів. Однак не було надано даних про ефективність цієї системи, оскільки її розроблено в комерційних цілях.

Відомі роботи Ріка Джойса і Гупта Гопала [3]. Їх метод аутентифікації оснований на використанні інформації про часові затримки між натисканнями клавіш, отриманої під час введення логіна в модифікованій процедурі ідентифікації. Результати достовірності системи не наводяться.

Цю проблематику вивчав С. П. Расторгуєв [4]. У своїй монографії автор розділив процедуру аутентифікації на два види. Перший вид – це парольна аутентифікація (ґрунтується на способі введення пароля, а не лише на знанні останнього), де користувач за парольною фразою проходить процедуру аутентифікації. Другий вид – аутентифікація користувачів за набором випадкових фраз. Автор не наводить результатів достовірності методів аутентифікації.

Відома робота Р. Н. Мінніханова, в якій реєстровані параметри розділено на дві групи:

1. Параметри, пов'язані з часовими характеристиками введення тексту.

2. Параметри сполучення символів, в яких помилки під час введення заздалегідь заданого тексту трапляються найчастіше, а також швидкість реакції оператора на виявлення та виправлення помилки. Коефіцієнт достовірності аутентифікації у такій системі становить 80 %.

Постановка задачі

Незважаючи на значний інтерес до систем біометричної аутентифікації за клавіатурним почерком, ці системи характеризуються низькою достовірністю (точністю) аутентифікації особи. З метою виявлення причин, що зумовлюють низьку достовірність, на рис. 1 подано основні етапи розроблення та створення систем біометричної аутентифікації за клавіатурним почерком, а саме з виявленням на інтуїтивному феноменологічному рівні властивостей структури даних клавіатурного почерку, важливих для розв'язання задач дослідження, конструюється їх математична модель, яка, поряд із методами та алгоритмами опрацювання, становить математичне забезпечення проектованої системи [5]. Далі це математичне забезпечення втілюється у відповідні програмно-апаратні засоби.

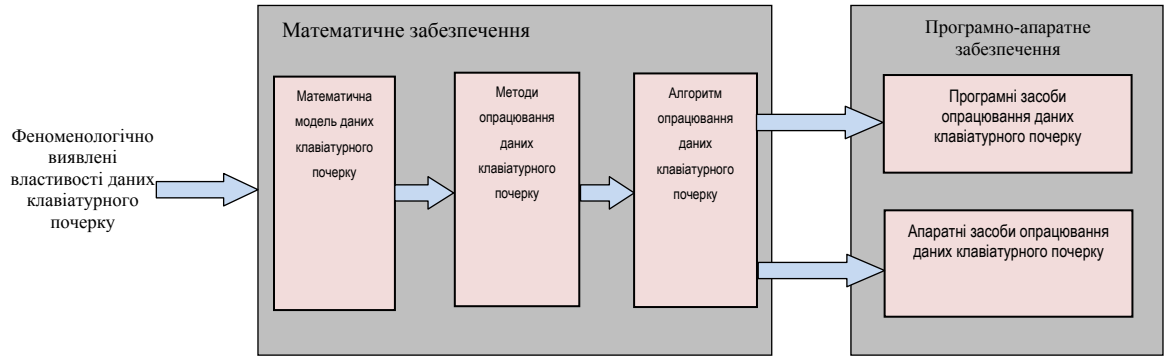

Рис. 1. Етапи розроблення та створення системи біометричної аутентифікації за клавіатурним почерком

Першим та визначальним етапом проектування систем біометричної аутентифікації за клавіатурним почерком є створення їх математичних моделей, які б адекватно відображали важливі, з погляду завдань дослідження, сторони часової структури даних, які надходять від клавіатури. Адже математична модель значною мірою задає потенціал та ефективність створюваних інформаційних технологій, зумовлює структуру програмної та апаратної складових проектованої інформаційної системи. Від якості математичної моделі даних (див. рис. 2) суттєво залежить точність та достовірність методів їх опрацювання системою біометричної аутентифікації, рівень інформативності та репрезентативності аутентифікаційних та ідентифікаційних ознак, достовірність прийнятих рішень.

Рис. 2. Причинно-наслідкові зв'язки стосовно якості системи біометричної аутентифікації за клавіатурним почерком

Як видно із проведеного аналізу, основною причиною такого стану справ є недостатня ефективність відповідного математичного забезпечення систем біометричної аутентифікації за клавіатурним почерком. Зважаючи на викладене вище, актуальним є проведення компаративного аналізу відомих математичних моделей, методів та систем аутентифікації за клавіатурним почерком з метою виявлення основних їх недоліків та формування напряму подальшого дослідження в цій галузі. Власне така задача і розв'язується у цій науковій роботі.

Виклад основного матеріалу

Передусім зазначимо, що різні математичні моделі, методи та системи біометричної аутентифікації за клавіатурним почерком різняться застосуванням та призначенням. У роботі [6], у якій клавіатурний почерк розглядається як один із ключових елементів моніторингу психофізіологічного стану (ПФС) оператора на підприємствах нафтохімічної промисловості, запропоновано підхід до побудови підсистеми автоматизованого визначення психофізіологічного стану оператора автоматизованого робочого місця (АРМ) автоматизованої системи управління та прийняття рішень (АСУТП), який ґрунтується на типовій структурі локальної обчислювальної мережі, що об'єднує АРМ-операторів всієї автоматизованої системи управління та прийняття рішень з АРМ-диспетчером й оснований на математичній моделі біометричного опрацювання клавіатурного почерку, на математичній моделі визначення ПФС і алгоритмі прийняття рішення про оповіщення особи, що приймає рішення (диспетчера). Для вирішення цього завдання автор вибрав математичний апарат опрацювання біометричних даних нейронними мережами. У роботі [7] розроблено та реалізовано полігауссівський алгоритм аутентифікації користувачів за клавіатурним почерком з метою підвищення достовірності аутентифікації, що, своєю чергою, також дає можливість відстежувати психофізичний стан людини. У цій роботі систематизовано параметри клавіатурного почерку користувачів і для підвищення достовірності аутентифікації введено новий параметр – швидкість натискання клавіш. Також розроблено спосіб обчислення швидкості руху клавіш під час набору користувачем символів на клавіатурі, де швидкість руху клавіш представляють як процес зміни ємності контактної пари клавіші в часі. Проведено дослідження стандартних плівкових клавіатур і отримано значення ємностей контактних пар клавіш, а також вирішено проблему паразитних складових за рахунок інтегрованого способу вимірювання ємності. Застосовуючи усі ці методи та полігауссівський алгоритм, автору вдалося підвищити коефіцієнт достовірності аутентифікації до рівня 95 %. Перевагою такого напряму аутентифікації за

клавіатурним почерком є можливість визначення адекватного психофізіологічного стану людини. У роботі [6] не досягнуто високої точності аутентифікації, оскільки використовується лише відхилення від нормального значення часових характеристик клавіатурного почерку. У роботі [7] зазначено, що з розробленням нових матеріалів, які будуть використовуватись для виготовлення комп'ютерних клавіатур, часові характеристики комп'ютерного почерку змінюватимуться і, отже, змінюватиметься клас точності системи біометричної аутентифікації загалом, оскільки введений параметр (швидкість натискання клавіш) також буде змінюватись.

У роботі [8] автор запропонував метод формування та корекції баз біометричних еталонів користувачів розподілених інформаційних систем за поведінковими характеристиками, що дає змогу спростити реалізацію процедур поточного аналізу біометричних профілів і врахувати можливість зміни поведінкових характеристик користувачів; запропоновані методи ідентифікації користувачів за клавіатурним почерком та стилем роботи з використанням теорії нечітких множин, що дають змогу врахувати невизначеності, характерні для етапу формування поточних біометричних профілів користувачів. Здійснено експериментальне дослідження розроблених методів динамічної аутентифікації користувачів для різних типів розподілених інформаційних систем, а також розроблено рекомендації з використання цих методів у системі дистанційного навчання, автоматизованій інформаційній системі машинобудівного підприємства, інформаційно-аналітичній системі "Університет". Значення помилок аутентифікації за клавіатурним почерком і стилем роботи для різних класів користувачів містяться в діапазоні 0,05 – 0,17, що є допустимим для біометричних систем. Середній відсоток правильної аутентифікації для розглянутих тестових вибірок становить 83 %.

Найбільшу зацікавленість викликають роботи щодо розроблення методів та математичних моделей прихованого клавіатурного моніторингу з тривалим використанням клавіатури (набір вільного тексту). Так, у роботі [9] розроблено метод виділення найінформативніших параметрів особливостей динаміки роботи на клавіатурі на основі послідовно-часових фільтрів. Автор зазначає, що на етапі опрацювання вхідних даних необхідно позбутися параметрів, які є малоінформативними і погіршують відображення особливостей динаміки роботи на клавіатурі. Для виявлення та виключення параметрів, викликаних першими двома причинами, запропоновано використовувати такі послідовно-часові фільтри: частотний, часовий, клавіатурний.

Автор розробив метод багатозв'язного подання особливостей динаміки роботи на клавіатурі, оснований на стійких послідовностях подій клавіатури. Запропонований метод ґрунтується на припущенні, що інформативнішими є не значення часів утримань і пауз між утриманнями клавіш, а стійкі послідовності поєднань значень цих часів. Одним із недоліків цього методу є необхідність мати доволі велику репрезентативну вибірку для створення образу клавіатурного почерку особи у системі, що збільшуватиме час аутентифікації користувача. Відсоток успішності аутентифікації автор цієї роботи не наводить.

Однією з останніх розробок у галузі біометричної аутентифікації за клавіатурним почерком є робота [10]. У роботі обґрунтовано необхідність використання апарату теорії ймовірностей і математичної статистики, зокрема оцінювання математичного сподівання часу утримання клавіш (ЧУК) як характеристики клавіатурного почерку оператора. Запропоновано метод розпізнавання клавіатурного почерку за вільним текстом на основі механізму аналізу клавіатурного введення даних. Цей метод реалізовано в алгоритмі розпізнавання клавіатурного почерку за часом утримання клавіш і часу введення часто вживаних у мові послідовностей букв (N-грам). Розроблена система аутентифікації оператора системи інформаційної інфраструктури має точність 98 %, якщо кількість операторів, зареєстрованих у системі, дорівнює 100. Також доведено, що у зв'язку з використанням методу визначення клавіатурного почерку на основі врахування часу утримання клавіш уможливлюється визначення клавіатурного почерку за вільним текстом. Однак автор не врахував час між натисканнями клавіш, який іноді збільшує ЧУК, у зв'язку з перекриттям сусідніх клавіш. У таблиці наведено порівняльну характеристику результатів розглянутих робіт щодо задач аутентифікації осіб за клавіатурним почерком.

Порівняльна характеристика математичних моделей, методів та засобів біометричної аутентифікації за клавіатурним почерком

Автор / Характеристика	**В. Г. Абашин**	**Р. Р. Шарипов**	**Л. Є. Чала**	**Н. М. Казарин**	**А. Н. Савинов**
Математичні моделі, засоби та методи	Методи системного аналізу, методи теорії множин, теорія нейронних мереж, теорія прийняття рішень, теорія подання знань людино-машинних систем, методи об'єктно-орієнтованого програмування, програмні та мовні засоби сучасних інформаційних технологій	Методи теорії ймовірностей, розпізнавання образів, математичного аналізу, проектування радіоелектронних засобів, експериментальні дослідження, виконані з використанням середовища програмування Borland Delphi 7 і розробленого програмно-апаратного комплексу обчислення швидкості натискання клавіш	Теорія нечітких множин, фреймові моделі програмного агента, нейронні мережі із самоорганізацією, метод нечіткої багатофакторної кластеризації	Ітеративний пошуковий алгоритм, методи послідовно-часових фільтрів, а зокрема часовий та клавіатурний фільтри, метод багатозв'язного подання особливостей динаміки роботи на клавіатурі, оснований на стійких послідовностях подій клавіатури	Методи теорії ймовірностей і математичної статистики, системного аналізу, теорії множин, метрологічних методів, методів об'єктно-орієнтованого програмування, теорії захисту інформації
Рівень достовірності аутентифікації	Не вказано	95 %	83 %	Не вказано	98 %
Категорія застосування	Визначення психофізіологічного стану людини	Визначення психофізіологічного стану людини	Розподілені інформаційні системи	Системи прихованого моніторингу	Системи прихованого моніторингу
Прихований клавіатурний моніторинг	–	–	–	+	+

Результати досліджень

У результаті проведеного аналізу відомих математичних моделей, методів та засобів біометричної аутентифікації за клавіатурним почерком виявлено, що в деяких системах клавіатурний почерк розпізнається засобами нейронних мереж. З використанням нейронних мереж складно визначити набір вхідних параметрів і архітектуру нейронної мережі, які забезпечували б необхідний результат. Інші математичні моделі також мають недоліки, зокрема, деякі враховують лише певне відхилення від нормального значення часових характеристик клавіатурного почерку, інші мають високе значення помилок II роду, що є доволі критичним для систем захисту інформації, велика репрезентативна вибірка подовжує час аутентифікації.

Встановлено, що важливу роль у завданнях біометричної аутентифікації за клавіатурним почерком відіграє прихований моніторинг клавіатурного почерку під час набору вільного тексту. Власне його використання та розроблення ефективних математичних моделей, методів та засобів

біометричної аутентифікації за даними прихованого моніторингу клавіатурного почерку є перспективним напрямом подальшого дослідження в галузі інформаційної безпеки, оскільки уможливлює підвищення достовірності аутентифікації особи.

Висновки

У роботі проведено огляд та аналіз відомих математичних моделей, методів та засобів біометричної аутентифікації за клавіатурним почерком особи. Особливу увагу приділено найвисокоінформативнішим системам. Проведений огляд дав можливість виявити недоліки, притаманні різним системам, а саме високе значення виникнення помилок першого (“впустити чужого”) та другого (“не впустити свого”) роду, велика репрезентативна вибірка, яка збільшує час аутентифікації, чи занадто велике коло задач (обмеження доступу до певних інформаційних ресурсів для деяких класів користувачів; моніторинг звертання користувачів до різних типів ресурсів РІС; верифікація результатів тестування у комп'ютерних системах дистанційного навчання; оцінка кваліфікації користувачів РІС і динаміки її підвищення), яке зменшує відсоток правильної аутентифікації.

Різні автори по-різному інтерпретують характеристики якості роботи біометричних систем загалом: помилки І і ІІ роду, коефіцієнт достовірності, помилки ідентифікації, відсоток правильної ідентифікації. У подальших наукових дослідженнях оперуватимемо показниками помилок І і ІІ роду, які є інформативнішими для систем такого виду. Необхідно також розробити нову математичну модель, методи та засоби статистичного опрацювання даних прихованого моніторингу клавіатурного почерку особи для підвищення ефективності систем біометричної аутентифікації.

1. R. Gaines, W. Lisowski, S. Press, and N. Shapiro. Authentication by Keystroke Timing: Some Preliminary Results,” Rand Report R-256-NSF, Rand Corporation, Santa Monica, C A, 1980. 2. J. Leggett and Williams Verifying identity via keystroke characteristics // International Journal of Man-Machine Studies, 28:67-76, 1988. 3. Rick Joyce and Gopal Gupta. Identity authentication based on keystroke latencies. Communications of the ACM, 33(2): 168 – 176, February 1990. 4. Расторгуев С. П. Цель как криптограмма: криптоанализ синтетических целей (монография и два варианта пролегоменов к теории) / С. П. Расторгуев, В. Н. Чибисов – М.: Изд-во Агентства “Яхтсмен” – 1996. 5. Лупенко С. А. Розвиток теорії моделювання та обробки циклічних сигналів в інформаційних системах: дис. … д-ра техн. наук 01.05.02 / Лупенко Сергій Анатолійович. – Львів, 2010. – 515 с. 6. Абашин В. Г. Автоматизация процесса определения психофизического состояния оператора автоматизированного рабочего места в АСУТП: автореф. дис. на соискание науч. степени канд. техн. наук: спец. 05.13.06 “Автоматизация и управление технологическими процессами и производствами (промышленность)” / В. Г. Абашин. – Орел, 2008. – 18 с. 7. Шарипов Р. Р. Разработка полигауссового алгоритма аутентификации пользователей в телекоммуникационных системах и сетях по клавиатурному почерку: автореф. дис. на соискание науч. степени канд. техн. наук: спец. 05.12.13 “Системы, сети и устройства телекоммуникаций” / Р. Р. Шарипов. – Казань, 2006. – 20 с. 8. Чала Л. Е. Методи динамічної ідентифікації користувачів розподілених інформаційних систем: автореф. дис. на здобуття наук. ступеня канд. техн. наук: спец. 05.13.06 “Автоматизовані системи управління та прогресивні інформаційні технології” / Л. Е. Чала. – Харків, 2006. – 20 с. 9. Казарин Н. М. Разработка и исследование методов скрытого клавиатурного мониторинга: автореф. дис. на соискание науч. степени канд. техн. наук: спец. 05.13.19 “Методы и системы защиты информации, информационная безопасность” / Н. М. Казарин. – Таганрог, 2006. – 20 с. 9. 10. Савинов А. Н. Методы, модели и алгоритмы распознавания клавиатурного почерка в ключевых системах: автореф. дис. на соискание науч. степени канд. техн. наук: спец. 05.13.19 “Методы и системы защиты информации, информационная безопасность” / А. Н. Савинов. – Санкт-Петербург, 2013. – 19 с.