Департамент образования города Москвы

Государственное бюджетное общеобразовательное учреждение

города Москвы

«Гимназия № 1505 «Московская городская педагогическая гимназия-лаборатория»»

**ДИПЛОМНОЕ ИССЛЕДОВАНИЕ**

на тему:

**Система биометрической идентификации**

Выполнил (а):

Акинина Софья Андреевна 10 «Б» класс

Руководитель

Наумов Алексей Леонидович

подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензент:

ФИО (указать должность, при наличии – указать ученую степень, ученое звание)

подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Москва

 20\_\_\_/20\_\_\_уч.г.

Оглавление

Введение 3

Первая глава 4

1.1 Идентификация пользователя 4

1.2 Механизм идентификации пользователя 5

1.3 Идентификация по биометрическим признаками (физическим) 5

1.3.1 Отпечатки пальцев 5

1.3.2 Радужная оболочка глаза 6

1.3.3 Распознавание лица 7

1.3.4 Распознание по венам рук 8

1.4 Идентификация по клавиатурному почерку 9

# Введение

Каждый человек имеет свои особенности, которые являются его биометрическими характеристиками. Биометрические характеристики индивидуальны у каждого человека, поэтому растет интерес к идентификации с использованием этих характеристик. В качестве критерия биометрической идентификации я предлагаю использовать особенности, связанные с клавиатурным вводом. Данный способ идентификации является программным и не требует специальных устройств, таких как сканер отпечатков пальцев. Поэтому он может применяться скрытно, незаметно для пользователя, что дает возможность также его использовать для обнаружения несанкционированного доступа.

Традиционные методы идентификации по паролю или коду доступа недостаточно достоверны и надежны. Пароль можно украсть, подсмотреть или просто подобрать. А биометрические характеристики сопутствуют человеку всю его жизнь.

В моем исследовании я собираюсь написать программу, собирающую статистические данные, а так же программу для их обработки. После чего я хочу проанализировать результаты и выявить лучший способ для биометрической идентификации.

# Первая глава

## 1.1 Идентификация пользователя

Идентификация – это присвоение субъектам или объектам личного идентификатора и сравнение его с заданным. Идентификация пользователя позволяет выяснить, является ли пользователь тем, за кого он себя выдает.

Существует много вариантов идентификаторов пользователей. В целом их можно разделить на две группы:

* Набор символов ( пароль, секретный ключ, персональный идентификатор и т.д), который пользователь запоминает и вводит при необходимости идентификации
* Биометрические характеристики: физические параметры человека или характеристики, связанные с поведением

Наиболее привычным в наши дни является использование пароля. Парольные методы можно разделить по степени изменяемости паролей на:

* Методы, использующие постоянные пароли
* Методы, используемые одноразовые пароли

Использование одноразовых паролей является более надежным.

Но в наше время, все больше и больше популярности и актуальности набирают методы идентификации, связанные с биометрическими параметрами:

* Проверка физических параметров ( отпечатки пальцев, рисунок радужной оболочки глаза)
* Проверка поведенческих характеристик ( особенности клавиатурного почерка и т.д)

## 1.2 Механизм идентификации пользователя

Пользователь предоставляет системе свой личный идентификатор (например, вводит пароль или предоставляет палец для сканирования отпечатка). Далее система сравнивает полученный идентификатор со всеми хранящимися в ее базе идентификаторами,хранящимися в ее базе. Если результат сравнения успешный, то пользователь получает доступ к системе в рамках установленных полномочий. В случае отрицательного результата система сообщает об ошибке и предлагает повторно ввести идентификатор. В тех случаях, когда пользователь превышает лимит возможных повторов ввода информации (ограничение на количество повторов является обязательным условием для защищенных систем) система временно блокируется и выдается сообщение о несанкционированных действиях (причем, может быть, и незаметно для пользователя).

В целом, алгоритм работы систем идентификации заключается в получении от субъекта или объекта информацию, удостоверяющую личность и, проверив ее подлинность, разрешении доступа или нет.

## 1.3 Идентификация по биометрическим признаками (физическим)

### 1.3.1 Отпечатки пальцев

Дактилоскопия (распознание отпечатков пальцев) является одним из самых разработанных и популярных биометрических методов распознавания личности.

Каждый человек имеет свой собственный папиллярный рисунок, что позволяет возможна почти достоверная идентификация. Система использует характерные точки на отпечатках пальцев: окончание линий узора, разветвления и одинокие точки. После сканирования отпечаток преобразовывается в уникальный код. И именно коды отпечатков пальцев хранятся в базе данных.

Преимущества метода:

* Достоверность, по сравнению с идентификацией по голосу или лицу
* Низкая стоимость устройств, сканирующих отпечатки пальцев
* Простая процедура сканирования

Недостатки метода:

* Папиллярный рисунок очень легко повреждается мелкими царапинами или порезами
* Присутствует недостаточная защищенность, связанная с широким распространением метода

### 1.3.2 Радужная оболочка глаза

Радужная оболочка глаза является уникальной характеристикой человека. Она стабилизируется в возрасте около двух лет и не практически не меняется на протяжении всей жизни. Следовательно этот метод является одним из наиболее точных среди биометрических методов.

Система идентификации личности по радужной оболочке логически делится на две части: устройство захвата изображения, его первичной обработки и передачи вычислителю и вычислитель, производящий сравнение изображения с изображениями в базе данных, передающий команду о допуске исполнительному устройству.

Преимущества метода:

* Статистическая надежность алгоритма.
* Захват изображения радужной оболочки можно производить на расстоянии от нескольких сантиметров до нескольких метров.
* Радужная оболочка не изменяется на протяжении жизни, за исключением травм или патологий

Недостатки метода:

* Цена системы
* Низкая доступность готовых решений

### 1.3.3 Распознавание лица

2-D распознавание является статистически неэффективным методом. Появился он достаточно давно и применялся, в основном в криминалистике. Затем появились компьютерные интерпретации метода, в результате он стал более надежным, но все же уступал другим методам.

Преимущества:

* Не требуется дорогостоящее оборудование
* Возможно распознание на значительных расстояниях

Недостатки:

* Низкая статистическая достоверность
* Необходимо правильное освещение, например невозможно распознать лицо человека, входящего в помещение с улицы в солнечный день
* Для некоторых систем помехи, вроде очков или бороды, могут быть неприемлемыми
* Некоторые системы не учитывают изменение мимики

### 1.3.4 Распознание по венам рук

Это достаточно новая технология в сфере биометрической идентификации, появилась всего 5-10 лет назад. Инфракрасная камера делает снимки внешней или внутренней стороны руки. Рисунок вен формируется благодаря тому, что гемоглобин крови поглощает ИК излучение. В результате, степень отражения уменьшается, и вены видны на камере в виде черных линий. Специальная программа на основе полученных данных создает цифровую свертку. Не требуется контакта человека со сканирующим устройством.

Преимущества:

* Отсутствие необходимости контактировать со сканирующим устройством
* Высокая достоверность
* Скрытость характеристики, затруднительно получить ее от человека просто так

Недостатки:

* Недопустима засветка сканера солнечными лучами или лучами галогеновых ламп
* Некоторые возрастные заболевания, например артрит, сильно ухудшают достоверность

## 1.4 Идентификация по клавиатурному почерку

Набирая тексты на клавиатуре ежедневно, человек формирует собственный клавиатурный почерк

Клавиатурный почерк - поведенческая биометрическая характеристика, которую описывают следующие параметры:

* Скорость ввода - количество введенных символов разделенное на время печатания
* Динамика ввода - характеризуется временем между нажатиями клавиш и временем их удержания
* Частота возникновение ошибок при вводе
* Использование клавиш - например, какие функциональные клавиши нажимаются для ввода заглавных букв

Человека можно отличить по ряду особенностей:

* зависимость почерка от сочетаний букв в слове
* глубокие связи между набором разных символов
* задержки — при вводе символов

Эти уникальные характеристики выявляются с помощью:

* по набору собственного текста
* по набору ключевой фразы

Механизм идентификации по клавиатурному вводу:

Идентификация по клавиатурному вводу основывается на статистических данных. То есть необходимо сформировать закономерности, например, какие буквы он нажимает быстрее всего, между какими клавишами он меньше всего задумывается и т.д. После этого следует обучение программы, которая будет не только по кодовой фразе идентифицировать человека, но и по его биометрическим особенностям.

Преимущества:

* Простота реализации и внедрения. Реализация исключительно программная, ввод осуществляется со стандартного устройства ввода (клавиатуры), а значит использование не требуется приобретение никакого дополнительного оборудования. Это самый дешевый способ аутентификации по биометрическим характеристикам субъекта доступа.
* Не требует от пользователя никаких дополнительных действий, кроме привычных. Пользователь так или иначе, наверняка, использует пароль, который можно назначить парольной фразой, по которой будет проводиться аутентификация.
* Возможность скрытой идентификации

Недостатки:

* Требуется обучение программы
* Сильная зависимость от эргономичности клавиатуры (в случае смены, придется обучать программу заново)
* Сильная зависимость от психофизического состояния оператора.

# Список источников

1. Дубровин Д.А «Клавиатурный почерк как способ аутентификации и  идентификации пользователя пользователя»: научная работа
2. Дубровин Д.А. «Использование клавиатурного почерка для идентификации пользователя»
3. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: ПГУ, 2000.