

## Содержание

Введение.....	4
1 Методы биометрической идентификации.....	5
1.1. Сравнительный обзор методов биометрической идентификации.....	5
1.1.1. Идентификация личности по рисунку сосудов глазного дна.....	6
1.1.2. Идентификация личности по отпечатку пальца.....	7
1.1.3. Идентификация личности по 3D распознаванию лица.....	8
1.2. Перспективные методы биометрической идентификации.....	9
1.2.1. Идентификация по рисунку вен ладони.....	9
1.3. Сравнение современных методов биометрической идентификации.....	10
1.4. Формулировка цели работы.....	12
2 Обзор разработок в области идентификации по рисунку вен.....	13
2.1. Сканер Fujitsu Palmsecure.....	
2.2. Сканер Vera Palm Vein.....	
2.3. Российские разработки в области идентификации по рисунку вен.....	
3 Программно-аппаратная разработка модуля.....	
3.1. Обзор свойств венозной крови.....	
3.2. Выбор сканирующей матрицы.....	
3.3. Выбор датчика расстояния.....	
3.4. Выбор фильтра IR-диапазона.....	
3.5. Разработка программного обеспечения модуля.....	
3.6. Разработка программного обеспечения рабочей станции.....	
4 Тестирование устройства и анализа результатов.....	
Заключение.....	

## ВВЕДЕНИЕ

Конфиденциальность информации является одной из составляющих информационной безопасности, а обеспечение практической реализации мер по обеспечению конфиденциальности современных информационных систем – одной из основных задач информационной безопасности.

Одним из практических средств обеспечения конфиденциальности информации являются процедуры идентификации, аутентификации и авторизации. Существуют разные методы идентификации, среди которых выделяют отдельную группу биометрических методов идентификации, где в качестве идентификатора выступает биометрия.

Под биометрией понимается система идентификации человека по его одной или нескольким биологическим или поведенческим чертам. Технологии биометрической идентификации активно используются как в частной жизни, так и в бизнесе.

Наиболее распространёнными являются методы идентификации по отпечатку пальца и распознавания лица, которые внедряются в большой спектр устройств, в том числе и в смартфоны. Также существуют биометрические методы идентификации, которые обладают наиболее высокой точностью – идентификация по радужке и сетчатке глаза.

Однако данные методы идентификации обладают рядом существенных недостатков в определённых областях использования, например, при достаточно большом числе зарегистрированных пользователей системы идентификации. Данные недостатки зачастую не могут быть исправлены, так как биометрическая система идентификации должна отвечать ряду требований, которые часто несовместимы друг с другом. Основными требованиями являются достаточно низкий уровень ошибок ложного доступа, ложного отказа доступа при удовлетворении требований к безопасности, удобству и конфиденциальности.

## 1. МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

### 1.1. Сравнительный обзор методов биометрической идентификации

Методы биометрической идентификации различаются прежде всего по используемым биометрическим идентификаторам, где биометрический идентификатор – это биометрический уникальный признак объекта, по которому объект можно однозначно идентифицировать. Также существуют классические идентификационные методы, например, идентификация по паролю. В отличие от небиеметрических методов, биометрические используют понятие степени подобия. Использование аутентификации по паролю дает всегда точный результат на выходе: разрешение доступа при правильном пароле и отказ при неправильном. Такой подход исключает применение вероятности подобия. Но при применении биометрических методов необходимо руководствоваться терминами коэффициентов ошибок.

В основе оценки средств биометрической идентификации лежит понятие ложного допуска и ложного недопуска. Здесь вероятностью ложного допуска (ВЛД) является частота принятия того, что биометрические образцы принадлежат одной личности, хотя это не так. Вероятностью ложного недопуска (ВЛНД) является решение, что биометрические образцы принадлежат разным личностям, что также является ошибкой.

При сравнении методов биометрической идентификации далее будут использованы показатели ВЛНД при фиксированном значении ВЛД. Можно легко понять, что чем меньше значение ВЛНД системы при одинаковом уровне ВЛД, тем система является надёжней. Также будет рассмотрена характеристика окружающей среды, оценивающая влияние внешних свойств на работу системы. Ещё одним рассматриваемым параметром для биометрического сканера является устойчивость к подделке, то есть

возможность ложного доступа при снятии биометрического образца с объекта, имитирующего признаки зарегистрированного лица. Также важным этическим фактором является простота использования сканера. Физическими параметрами самой биометрической системы идентификации является скорость работы и её стоимость.

#### 1.1.1. Идентификация личности по рисунку сосудов глазного дна

Сканирование рисунка кровеносных сосудов глазного дна было одним из первых методов идентификации личности, обладающих достаточно высокой надёжностью. Оно берёт лучшие черты от идентификации по радужной оболочке и по венам руки. Для реализации метода достаточно внешней подсветки глазного дна, чтобы различить капилляры. Уникальность рисунка сосудов сетчатки была доказана ещё в 1935 году [4]. Рисунок этих капилляров неподвижен по своей структуре, не изменяется с возрастом. Изменения возможны только при некоторых болезнях, затрагивающих глазное дно, например, катаракте. При этом, полученные образцы будут различаться даже у близнецов (Рисунок 2)

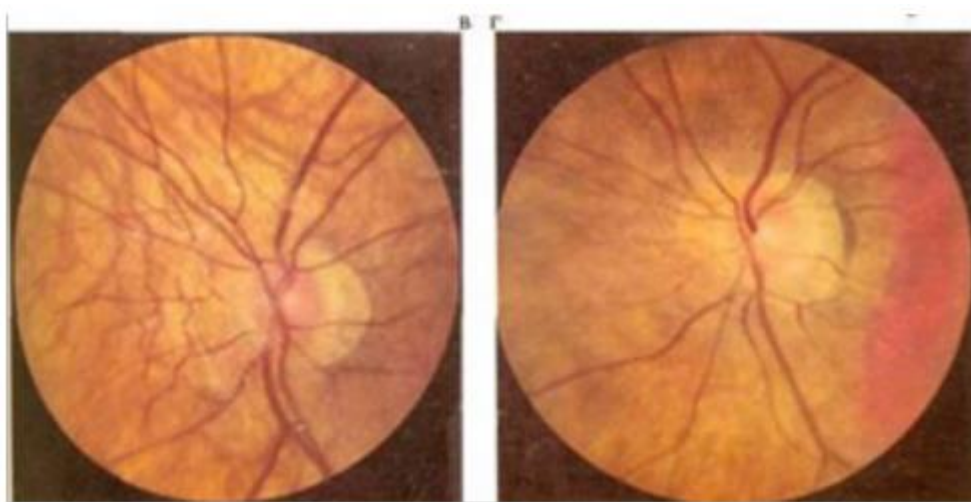


Рисунок 1 - Биометрические образцы сетчатки близнецов

Само сканирование заключается в инфракрасной подсветке окуляра, в который смотрит человек, и снятии изображения глазного дна, в котором выделяется рисунок кровеносных сосудов.

Одной из проблем данного метода биометрической идентификации является психологический фактор, поскольку процедура сканирования может вызвать дискомфорт у субъекта сканирования. Также нельзя упускать и техническую сложность устройства сканера, которым является дорогостоящая оптическая система. К тому же время работы данной системы достаточно велико, что опять же может вызвать дискомфорт у субъекта сканирования.

Ошибки сканировании происходят из-за отклонений головы субъекта сканирования и неверной фокусировкой им взгляда на удаленном источнике света. При этом, технически пока невозможно изготовить муляж, способный обмануть систему.

Сканирование сетчатки глаза пользуется особой популярностью в СКУД на секретных и государственных объектах, поскольку данные системы обладают одним из самых низких процентов отказа в доступе среди зарегистрированных субъектов и почти невозможным ошибочным разрешением доступа. По данным компании EyeDentify [5], для сканера ICAM2001 при ВЛД=0,0001% значение ВЛНД составляет 0,4%.

#### 1.1.2. Идентификация личности по отпечатку пальца

Использование отпечатков пальцев для идентификации личности началось в первой половине XX века в криминалистике. На сегодняшний день дактилоскопия является самым распространённым и доступным методом биометрической идентификации. Папиллярный узор каждого человека уникален, что позволяет принять этот фактор за основу для идентификации.

Идентификация по отпечатку пальца начала переходить на автоматизацию в конце 1960-х годов вместе с появлением компьютерных технологий.

Отпечаток пальца обычно выглядит как серия темных линий, которые представляют собой высокую, выступающий гребень, в то время как впадина между этими гребнями выглядит как белое пространство и представляет собой низкую неглубокую часть.

Для получения цифрового изображения поверхности отпечатка пальца используются различные типы датчиков - оптические, емкостные, ультразвуковые и тепловые. Оптические датчики снимают изображение отпечатка пальца и сегодня являются наиболее доступными и распространенными датчиками.

Также стоит отметить, что время, затрачиваемое на идентификацию, в современных системах не превышает 1 с, в зависимости от числа зарегистрированных пользователей.

Статистические данные ВЛД и ВЛНД были предоставлены VeriFinger SDK [6], полученные при помощи сканера отпечатков пальцев DP U.are.U. При ВЛД=0,001% значение ВЛНД составляет 0,6%.

### 1.1.3. Идентификация личности по 3D распознаванию лица

Распознавание лиц в 3D стало тенденцией исследований как в промышленности, так и в академических кругах. Он наследует преимущества традиционного 2D-распознавания лиц, такие как естественный процесс распознавания и широкий спектр приложений. Более того, системы трехмерного распознавания лиц могут точно распознавать человеческие лица даже при тусклом свете и с различными положениями лица и выражениями, в таких условиях системы распознавания двумерных лиц будут иметь огромные трудности в эксплуатации.

Для получения трехмерных образцов лица требуется специальное оборудование, которое можно разделить на активные системы сбора данных и пассивные системы сбора данных в зависимости от используемых технологий. Активные системы сбора данных активно излучают невидимый свет,

например, инфракрасные лазерные лучи, чтобы осветить целевое человеческое лицо. Затем системы измеряют отражение, чтобы определить особенности формы лица цели.

В iPhone X используется Face ID - технология, которая позволяет разблокировать телефон с помощью сканирования в инфракрасном и видимом свете, чтобы однозначно идентифицировать лицо субъекта. Он работает в различных условиях и полностью безопасен.

Полные данные о ВЛНД и ВЛД для алгоритмов этого класса на сайтах производителей открыто не приведены. Но для моделей фирмы Bioscript (3D EnrolCam, 3D FastPass) [7] при ВЛД = 0,0005% ВЛНД составляет 0,1%.

Считается, что статистическая надежность метода сравнима с надежностью метода идентификации по отпечаткам пальцев.

## 1.2. Перспективные методы биометрической идентификации

На сегодняшний день имеется множество разработок в области перспективных методов биометрической идентификации. Среди них выделяют такие методы, как ДНК-идентификация, идентификация по запаху тела, идентификация по тону сердца, идентификация по эмоциональному состоянию и мимике, идентификация по рисунку вен ладони. Однако данные методы, за исключением последнего, ещё недостаточно изучены, чтобы сравниться по характеристикам с распространёнными методами идентификации. Идентификация по рисунку вен ладони является перспективным методом, который способен сравниться по характеристикам с распространёнными методами биометрической идентификации.

### 1.2.1. Идентификация по рисунку вен ладони

Идентификация путем сканирования вен ладони прочно зарекомендовала себя как метод обеспечивающий достаточно высокий

уровень безопасности. В отличие от упоминавшихся ранее методов, таких как технология идентификации по сканированию отпечатка пальца, геометрии рук и лица, васкулярное сканирование обладает явным преимуществом, поскольку рисунок вен у совершеннолетнего человека не меняется с возрастом, рисунок вен практически невозможно подделать, а также на сканирование не влияют внешние дефекты кожи. Можно заметить, что данный метод имеет некоторое сходство с методом сканирования сетчатки глаза, поскольку за объект сравнения также берётся рисунок кровеносных сосудов. К тому же сканирование сетчатки глаза на сегодняшний день является одним из самых надёжных биометрических методов. Однако васкулярное сканирование лишено основного недостатка систем сканирования сетчатки – негативного психологического фактора. К тому же глаза более подвержены болезням, влияющим на рисунок сосудов, например, катаракте.

Значение ВЛНД и ВЛД приведено для сканера Palm Vein. Согласно данным разработчика, при ВЛД = 0,0008%, ВЛНД составляет 0,01%.

### 1.3. Сравнение современных методов биометрической идентификации

Для самых популярных на сегодняшний день методов биометрической идентификации средние значения FAR и FRR выглядят следующим образом:

Таблица 1 – Сравнительный анализ характеристик FAR и FRR

Метод идентификации	ВЛД	ВЛНД
Отпечаток пальца	0,001%	0,6%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Следует также учитывать возможность фальсификации объекта сканирования. Данный фактор по каждому методу указан в Таблице 2.

Таблица 2 – Сравнительный анализ возможности фальсификации



<b>Метод идентификации</b>	<b>Устойчивость к подделке</b>
Отпечаток пальца	Низкая
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Средняя
Сетчатка глаза	Высокая
Рисунок вен	Высокая

При сканировании большую роль играют внешние факторы. Влияние этих факторов на результат указана в Таблице 3.

Таблица 3 – Чувствительность методов идентификации к внешним факторам

<b>Метод идентификации</b>	<b>Чувствительность к влиянию внешних факторов</b>
Отпечаток пальца	Высокая
Распознавание лица 2D	Высокая
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Средняя
Сетчатка глаза	Высокая
Рисунок вен	Средняя

Также рассматриваются такие факторы как скорость работы и возможность бесконтактной аутентификации в Таблице 4 и Таблице 5

Таблица 4 – Сравнительный анализ скорости аутентификации

<b>Биометрическая СКУД использует:</b>	<b>Скорость идентификации</b>
Отпечаток пальца	Высокая
Распознавание лица 2D	Средняя
Распознавание лица 3D	Низкая
Радужная оболочка глаза	Высокая
Сетчатка глаза	Низкая
Рисунок вен	Высокая

Таблица 5 – Возможность бесконтактной идентификации

<b>Биометрическая СКУД использует:</b>	<b>Возможность бесконтактной идентификации</b>
Отпечаток пальца	Отсутствует
Распознавание лица 2D	На большом расстоянии
Распознавание лица 3D	На небольшом расстоянии
Радужная оболочка глаза	На большом расстоянии

Сетчатка глаза	Отсутствует
Рисунок вен	На небольшом расстоянии

Делая общий вывод к приведённым таблицам, можно сказать, что наиболее выигрышным в сфере безопасности и удобства использования на сегодняшний день являются методы сканирования сетчатки глаза и васкулярное сканирование. Однако первый метод обладает достаточно большой стоимостью реализации. Стоит сказать, что стоимость сканеров сетчатки глаза может в десятки раз превышать стоимость сканеров вен. Обусловлено это технической сложностью исполнения сканирования сетчатки глаза.

#### 1.4. Формулировка цели работы

Как уже было сказано ранее, метод идентификации по рисунку вен обладает преимуществами по сравнению с остальными. Однако, стоит отметить, что данный метод всё равно является куда затратнее, чем распространённые методы идентификации: 3D-сканирования лица и идентификация по отпечатку пальца. Стоит отметить, что идентификация методом сканирования вен ладони может быть реализована в том же ценовом сегменте, что и выше перечисленные методы, при этом приблизившись по показателям ВЛД и ВЛНД к данным методам.

Целью работы является программно-аппаратная разработка модуля идентификации по рисунку вен ладони, соответствующего требованиям стоимости и характеристик ВЛД и ВЛНД для метода идентификации по отпечатку пальца.

## 2. ОБЗОР РАЗРАБОТОК В ОБЛАСТИ ИДЕНТИФИКАЦИИ ПО РИСУНКУ ВЕН

### 2.1.

#### Список использованных источников

- 1 Future of Biometrics & Human Identification Industry [Электронный ресурс] – URL: <https://www.bccresearch.com/whitepapers/future-of-biometrics-and-human-identification.html>
- 2 Smartphone ownership on the rise in emerging economies [Электронный ресурс] – URL: <https://www.pewresearch.org/global/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economies/>

- 3 Болл Р. М., Панканти Ш., Ратха Н. К., Коннел Дж. Х., Сеньор Э.  
У. «Guide to Biometrics» 2007 г. ISBN - 978-5-94836-109-3