

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ**

**«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ**

**Студенттер мен жас ғалымдардың  
«GYLYM JÁNE BILIM - 2023»  
XVIII Халықаралық ғылыми конференциясының  
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ  
XVIII Международной научной конференции  
студентов и молодых ученых  
«GYLYM JÁNE BILIM - 2023»**

**PROCEEDINGS  
of the XVIII International Scientific Conference  
for students and young scholars  
«GYLYM JÁNE BILIM - 2023»**

**2023  
Астана**

**УДК 001+37**  
**ББК 72+74**  
**G99**

**«GYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың  
XVIII Халықаралық ғылыми конференциясы = XVIII  
Международная научная конференция студентов и молодых  
ученых «GYLYM JÁNE BILIM – 2023» = The XVIII International  
Scientific Conference for students and young scholars «GYLYM JÁNE  
BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.**

**ISBN 978-601-337-871-8**

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

**УДК 001+37**  
**ББК 72+74**

**ISBN 978-601-337-871-8**

**©Л.Н. Гумилев атындағы Еуразия  
ұлттық университеті, 2023**

ерекшеліктерін қарастырады. Ол сондай– ақ сенсорлар, талдау және басқару жүйелері сияқты IDS архитектурасы мен құрамдас бөліктерін егжей– тегжейлі көрсетеді. Мақаланы қорытындылай келе, автор ақпараттық қауіпсіздікке қатерлерді анықтау және алдын алу үшін телекоммуникациялық желілерде IDS пайдаланудың маңыздылығын атап көрсетеді. Ол дұрыс конфигурацияланған және біріктірілген IDS телекоммуникация желісінің қауіпсіздігін айтарлықтай арттыра алатынын атап өтеді. Бұл телекоммуникациялық желілерді қорғауға және осы салада IDS қолдануына қызығушылық танытатын кез келген адам үшін пайдалы материал.

[4] – телекоммуникациялық желілердегі қол жеткізуді басқару жүйелеріне арналған мақала. Мақалада қол жеткізуді басқарудың әртүрлі әдістері мен тәсілдері қарастырылады, сондай– ақ оларды қолдану мысалдары қарастырылады.

[5] мақалада телекоммуникациялар мен ақпараттық технологиялардағы қауіпсіздік мәселелерінің беделді зерттеуі болып табылады. Авторы Карлос А.С. Дэвис ақпараттық қауіпсіздіктің заманауи әдістері, телекоммуникациялық жүйелердегі осалдықтарды талдау құралдары мен әдістері, сондай– ақ деректердің құпиялылығы мен тұтастығын қамтамасыз ету әдістері туралы маңызды білім береді.

Қорытынды. Зерттеу нәтижелерін қорытындылай келе, қарастырылған барлық мақалалар телекоммуникация желілеріндегі ақпараттық қауіпсіздік мәселелеріне арналған және кәсіпорынның телекоммуникациялық желісін кезең– кезеңмен қорғайтын қолданыстағы үлгілер мен қорғау жүйелеріне шолу жасайды ; талдау нәтижесінде ол әртүрлі жүйелер мен әдістерді қолдану деректердің қауіпсіздігі мен рұқсат етілмеген қол жеткізуден қорғаудың жоғары деңгейін арттыруға болатыны анық болды. Жүйелердің әрқайсысы белгілі бір функцияларды орындайды және телекоммуникациялық желінің нақты талаптары мен сипаттамаларына байланысты пайдаланылуы мүмкін.

#### **Қолданылған әдебиеттер**

1. А. Н. Макаров, А. В. Барсуков, И. С. Герасимов, И. А. Запольский. "Информационная безопасность в телекоммуникационных сетях: модели и методы защиты". М.: Издательский дом "Техносфера", 2013. 415 с. ISBN 978– 5– 94836– 212– 4.
2. Яковлев А.В., Кузнецов А.В. "Моделирование информационной безопасности в телекоммуникационных системах". М.: Издательский дом "СОЛОН– Пресс", 2012. 256 с. ISBN 978– 5– 90564– 168– 2.
3. А. В. Шестаков. "Системы обнаружения вторжений в телекоммуникационных сетях". М.: Издательский дом "Форум", 2007. 272 с. ISBN 978– 5– 91180– 431– 6.
4. Д. А. Гаврилов, А. В. Комиссаров. "Защита информации в телекоммуникационных сетях на основе систем управления доступом". М.: Издательство Московского университета, 2005. 240 с. ISBN 5– 211– 04916– 3.
5. Davis, C.A.S. "Security in Telecommunications and Information Technology" (7th Edition). John Wiley & Sons, Inc. 2016. 392 с. ISBN 978– 1– 118– 87152– 5

УДК 654.94

#### **АНАЛИЗ СУЩЕСТВУЮЩИХ БИОМЕТРИЧЕСКИХ МЕТОДОВ**

Мадиев А.М<sup>1</sup>., Шурен Ж.Б<sup>2</sup>

<sup>1</sup>Магистрант кафедры «Радиотехника, электроника и телекоммуникации» ЕНУ им. Л.Н.Гумилева, Астана, Казахстан.

<sup>2</sup>Преподаватель кафедры «Радиотехника, электроника и телекоммуникации» ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – к.ф. – м.н. К.М. Маханов  
makanov@inbox.ru

Аннотация. В настоящее время существует необходимость повышения уровня безопасности в различных сферах деятельности человека, начиная от финансовых транзакций до доступа к личной информации и секретам государства. И это приводит к возрастанию потребности в использовании биометрических методов и технологий, которые являются наиболее эффективными и надежными в идентификации и аутентификации личности.

В статье рассматривается анализ существующих биометрических методов и технологий, их преимущества и недостатки, а также оценка эффективности их применения в различных сферах. Также, необходимо учитывать, что биометрические методы имеют свои ограничения и риски. Например, возможны ошибки распознавания, технические проблемы и возможность злоупотребления данными. Поэтому, важно проводить анализ и оценку качества биометрических методов, чтобы выбрать наиболее эффективные и надежные решения для конкретных сфер применения. Однако, существуют проблемы в использовании биометрических методов, такие как технические ограничения, ошибки распознавания и возможность злоупотребления данными, что требует более детального анализа и оценки качества биометрических методов.[1]

Биометрические методы могут быть классифицированы на основе используемых физических и поведенческих характеристик. Ниже приведена классификация основных типов биометрических методов:

- Физиологические методы:*– Сканирование отпечатков пальцев;
- Сканирование сетчатки глаза;
  - Распознавание лица;
  - Сканирование структуры кожи ладони.
  - Сканирование геометрических параметров ушной раковины;
  - Измерение голосовых характеристик;
- Поведенческие методы:*– Распознавание подписи;
- Распознавание голоса;
  - Распознавание по почерку.
  - Распознавание по образцу набора текста;
  - Распознавание по походке;
- Гибридные методы:*
- Комбинация нескольких физиологических или поведенческих методов.[1]

Каждый тип биометрического метода имеет свои преимущества и ограничения в зависимости от ситуации применения. Например, сканирование отпечатков пальцев является одним из наиболее распространенных биометрических методов и обладает высокой степенью точности, но может быть неэффективным в условиях, когда у человека повреждена кожа пальцев. Распознавание по походке может быть полезным для идентификации людей на больших расстояниях, но может оказаться неэффективным в условиях, когда человек ходит неестественно. Поэтому, выбор конкретного биометрического метода должен быть основан на тщательном анализе требований к безопасности и условий применения.[3]

Идентификация по отпечатку пальцев. В каждом отпечатке пальца можно определить признаки двух типов, используемые при их идентификации: глобальные и локальные. К первому типу относятся признаки, которые можно разглядеть и/или различить на отпечатках пальцев невооруженным взглядом: папиллярные узоры; область образа; ядро; пункты «дельта»; тип папиллярных линий их число.

Глобальные признаки интерпретируются следующим образом:

- Узоры папиллярные, образованные валиками и бороздками верхнего слоя кожи;
- Область образа – некоторый выделенный фрагмент отпечатка, в котором локализованы все признаки;
- Ядро – пункт, локализованный в середине отпечатка или в какой– либо выделенной области;
- Пункт «дельта» – начальная точка, то место, в котором происходит разделение бороздки папиллярной линии или очень короткая (доходящая до точки) бороздка;

– Тип линии – две наибольшие линии, которые начинаются как параллельные, а затем расходятся и огибают всю область образа;

– Счетчик линии – число линий (бороздок) на области образа или между ядром и пунктом дельта.

Ко второму типу относятся локальные признаки, называемые минуциями: это уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий, ориентацию папиллярных линий и координаты X и Y в этих пунктах.[4]



1–4 – узоры типа «петля»; 5 и 6 – узоры типа «дельта»; 7–8 – узоры типа «спираль».

Рисунок 1 – Некоторые типы папиллярных узоров на пальцах.

Для получения сведений об отпечатках пальцев применяются три типа сканеров: емкостные, прокатные и оптические. Емкостные сканеры наиболее дешевы, но не практичны и выходят из строя при наличии статического электричества. Прокатные сканеры требуют от пользователя единообразной скорости и манеры сканирования, что сложно. Оптические сканеры являются наиболее совершенными технологиями идентификации по отпечаткам пальцев, обладают высоким качеством изображения и экономичны. Они безопасны в антибактериальном отношении.



Рисунок 2 – Оптический сканер отпечатка пальцев Futronic FS80H USB 2.0

Идентификация по лицу. Лицо вполне естественно использовать в качестве биометрического идентификатора, поскольку в повседневной жизни люди узнают друг друга, в первую очередь, по лицу. По этой причине распознавание человека по лицу более приемлемым для общества, чем большинство методов биометрической идентификации.

Независимо от метода получения изображений лиц, для идентификации личности необходимы так же системы распознавания лица, которые находят изображения лица в пространстве, оценивают его относительно принятого шаблона, нормализуют, масштабируют и вращают в плоскости.

После того как лицо локализовано, применяется один из трех наиболее распространенных методов анализа:

- внешний вид лица («eigenfaces»);
- геометрия лица;
- автоматическая обработка изображения лица.

Внешний вид лица. Идея этого подхода заключается в том, чтобы уменьшить разрешение изображения лица с нескольких тысяч пикселей до небольшого числа, чтобы оставить наиболее яркие черты, нечувствительные к шуму, появляющемуся, например, из-за

изменений освещенности. Эта технология использует двумерные изображения в градациях серого, которые представляют отличительные характеристики изображения лица.

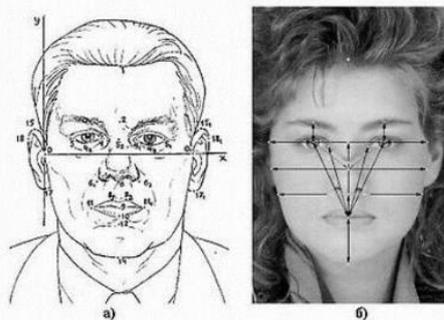


Рисунок 3 – Некоторые «eigenfaces»

Геометрия лица. Основная идея этого подхода является моделирование человеческого лица в единицах определенных черт, таких, как глаза, рот, брови и т. д., а также изучение геометрии этих черт. Технология «отличительных черт» подобна «eigenfaces», но в большей степени адаптирована к изменению внешности или мимики лица человека. Техники распознавания, основанные на внешних чертах, могут быть как глобальными, т. е. принимать лицо в целом, так и локальными, в которых создаются репрезентации отдельных областей лица. [7]

Автоматическая обработка изображения лица – наиболее простая технология, использующая расстояния и отношение расстояний между легко определяемыми точками лица, такими как глаза, кончик носа, уголки рта (рис.4). Хотя данный метод не столь мощный как другие, он достаточно эффективен в условиях слабой освещенности.

Технология распознавания позволяет сканировать человеческие лица в режиме реального времени. Видеокамера подключается к терминалу, и система распознавания определяет, соответствует ли лицо в кадре фотографий из базы данных. В результате каждое лицо описывается уникальным набором параметров, причем с некоторым избытком. Для идентификации с высокой степенью точности требуется не более 40 характеристик, тогда как система обычно выдает около 2 тыс. оценочных параметров. Это обеспечивает высокую надежность опознания независимо от поворота головы, наличия очков, косметики.



*а – используется при криминалистической фото– экспертизе;  
б – при построении автоматизированных систем идентификации*  
Рисунок 4 – Идентификационные точки расстояния.

В целом же распознавание лиц имеет множество проблем, которые можно разбить на 4 категории:

– Физическое правление, которые заключаются в быстрых изменениях выражения лица, например мигание, речевая, эмоциональная и коммуникативная мимика. Важны также изменения, которые происходит во внешности медленно, например с возрастом.

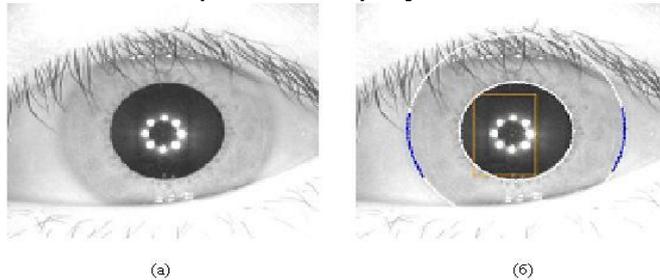
– Геометрия съятия образцов. В большинстве случаев лицо на фотографии имеет неизвестное расположение, неизвестный угол поворота и неизвестный размер. Бывает, что человек смотрит прямо в камеру. Поворот головы, например в профиль или в фас, определенным образом меняет внешность человека на разных изображениях

– Условия съятия параметра. Свет, падающий на лицо человека, может сильно изменить его внешность. Характеристика и параметры камеры также могут сильно влиять на внешность человека на фотографии, даже независимо от света. К таким характеристикам можно отнести автоматическую балансировку белого цвета, регулицию усиления и снижения шума.

– Артефакты сжатия. При сжатии и декомпрессии изображения происходит довольно сильное ухудшение его качества. Общепринятые стандарты сжатия, такие как JPEG и MPEG, базируются на компрессии блоков изображения и не гарантируют, что оно останется неизменным. Артефакты сжатия могут оказать значительное влияние на точность работы алгоритмов распознавания лиц при использовании архивных баз фотоизображений и видеоматериалов.[7]

Идентификация по радужной оболочке глаз. Доктор Джон Даугман в 1994 г. запатентовал в США метод распознавания радужной оболочки глаза. Его алгоритмы используются до сих пор для преобразования видеоизображений глаза в уникальный Iris-код, полученный в результате определения позиции радужки и выполнения математических операций для описания текстуры радужки в виде последовательности фаз.

На рисунке 5 изображено идентификация по радужной оболочке глаза.



(а) – исходное изображение; (б) – изображение с выделенной радужной оболочкой.

Рисунок 5 – Идентификация по радужной оболочке глаза

Многие эксперты подчеркивают «незрелость» технологии, хотя потенциальные возможности метода достаточно высоки, так как характеристики рисунка радужной оболочки человеческого глаза достаточно стабильны и не изменяются практически в течение всей жизни человека, невосприимчивы, к загрязнению и ранам. Отметим также, что радужки правого и левого глаза по рисунку существенно различаются. Этот метод идентификации отличается от других большей сложностью в использовании, более высокой стоимостью аппаратуры и жесткими условиями регистрации.[5]

Идентификация голоса – удобный биометрический подход, но с низкой точностью идентификации, которая может быть ослаблена заболеваниями. Распознавание речи охватывает широкий круг вопросов, от построения датчиков до баз данных и интерактивного обучения.

Преимуществами голосовой идентификации являются удобство и дешевизна ввода, а также возможность исследования БХЧ субъектов независимо от их желания. Распознавание речи осуществляется путем анализа параметров сигнала и сравнения их с параметрами биометрического эталона, хранящегося в базе данных. Главной проблемой является не стационарность речевого сигнала. Биометрические технологии могут использоваться для создания систем контроля и управления доступом.[6]

В таблице 1 представлен сравнительный анализ биометрических методов рассмотренных в статье.[2]

Таблица 1 – Сравнительный анализ биометрических методов

Метод идентификации	Биометрические характеристики	Преимущества	Недостатки
 Отпечаток пальца	<ul style="list-style-type: none"> <li>– Текстурный рисунок определяется чередующимися гребнями и впадинами на кончике пальца.</li> <li>– Уникальные для каждого отпечатка признаки, определяющие пункты изменения структуры папиллярных линий</li> </ul>	<ul style="list-style-type: none"> <li>– Наиболее распространено</li> <li>– Зрелая технология</li> <li>– Относительно высокая точность согласования</li> <li>– Высокая скорость согласования</li> <li>– Низкая стоимость</li> <li>– Можно использовать несколько пальцев</li> <li>– Различает близнецов</li> </ul>	<ul style="list-style-type: none"> <li>– Специальный датчик, который требует прикосновения и обслуживания.</li> <li>– Датчики могут быть сбиты с толку обманутыми отпечатками пальцев.</li> <li>– Небольшой, но значительный процент отказов в зачислении.</li> </ul>
 Лицо	<ul style="list-style-type: none"> <li>– Расположение и форма атрибутов лица.</li> <li>– Правильная поверхность (взвешенная комбинация нескольких канонических граней)</li> </ul>	<ul style="list-style-type: none"> <li>– Может работать на простом 2D-изображении или 3D в статических или видеоизображениях.</li> <li>– высокая приемлемость для пользователя</li> <li>– Разумная точность</li> <li>– Бесконтактность</li> </ul>	<ul style="list-style-type: none"> <li>– Точность зависит от контролируемого сбора данных (фон, освещение, ...)</li> </ul>
 Радужная оболочка глаза	<ul style="list-style-type: none"> <li>– Текстурный рисунок радужной оболочки (цветная часть глаза: Код радужной оболочки глаза, более 200 баллов)</li> </ul>	<ul style="list-style-type: none"> <li>– Высокая точность.</li> <li>– Трудно поддаться обману (даже при использовании объектива или мертвой радужной оболочки).</li> <li>– Низкая чувствительность к внешним воздействиям</li> </ul>	<ul style="list-style-type: none"> <li>– Низкая приемлемость для пользователя (физический дискомфорт)</li> <li>– Стоимость, как правило, высока.</li> </ul>
 Голос	<ul style="list-style-type: none"> <li>– отличительные особенности голоса</li> <li>– может сочетаться с другими физическими аспектами (например, голосовые пути, рот, носовые полости и губы)</li> </ul>	<ul style="list-style-type: none"> <li>– Простота использования.</li> <li>– Низкая стоимость.</li> <li>– простой интерфейс с фразами и словами</li> </ul>	<ul style="list-style-type: none"> <li>– Низкая точность</li> <li>– Возможная повторная атака</li> <li>– Возможность обхода со стороны лиц, обладающих навыками имитации</li> <li>– Может зависеть от условий записи (шум, технология записи ...)</li> <li>– Чувствителен к изменениям голоса</li> </ul>

Современные биометрические методы широко применяются в различных сферах деятельности, таких как безопасность, медицина, финансы и т.д. В статье произведен анализ биометрических методов и рассмотрены их достоинства и недостатки.

Для проведения исследования были выбраны четыре основных метода биометрической идентификации: сканер отпечатков пальцев, распознавание лица и сканер радужки глаза и идентификация по голосу. Были проанализированы их характеристики, преимущества и недостатки рассмотренные в Таблице– 1.

В заключение, надо отметить, что биометрические методы представляют собой один из наиболее перспективных и инновационных подходов к идентификации и аутентификации личности. Однако, чтобы реализовать полный потенциал этих методов, необходимо продолжать исследования и разработки, а также решать проблемы, связанные с приватностью, доступностью и точностью.

### Список литературы

1. Путьто М. М, Макарян А. С., Чич Ш. М., Маркова В. К., ИССЛЕДОВАНИЕ СИСТЕМЫ ИДЕНТИФИКАЦИИ И ПОДТВЕРЖДЕНИЯ ЛЕГИТИМНОСТИ ДОСТУПА НА ОСНОВЕ ДИНАМИЧЕСКИХ МЕТОДОВ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ // Прикаспийский журнал: управление и высокие технологии. 2020. №3 (51). – С.85 URL: <https://cyberleninka.ru/article/n/issledovanie– sistemy– identifikatsii– i– podtverzhdeniya– legitimnosti– dostupa– na– osnove– dinamicheskikh– metodov– biometricheskoj> (дата обращения: 19.03.2023).
2. Кузьминых Е. С., Маслова М. А., АНАЛИЗ И СРАВНЕНИЕ БИОМЕТРИЧЕСКИХ СПОСОБОВ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ ЧЕЛОВЕКА // Научный результат. Информационные технологии. 2021. №4. – С.14– 15 URL: <https://cyberleninka.ru/article/n/analiz– i– sravnenie– biometricheskikh– sposobov– identifikatsii– lichnosti– cheloveka> (дата обращения: 19.03.2023).
3. Ворона В.А., БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ // Горячая Линия – Телеком. 2021. – С.228
4. Идентификация по отпечаткам пальцев [Электронный ресурс] Режим доступа: <https://www.biolink.ru/technology/fingerprint.php>, свободный. Яз. рус. (Дата обращения: 21.03.2023)
5. Барсуков С. С., КРИМИНАЛИСТИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ПО РАДУЖНОЙ ОБОЛОЧКЕ И СЕТЧАТКЕ ГЛАЗА: СОВРЕМЕННЫЕ ВОЗМОЖНОСТИ И ПРОБЛЕМЫ ПРИМЕНЕНИЯ // ЮП. 2021. №1 (96). – С.14– 15 URL: <https://cyberleninka.ru/article/n/kriminalisticheskaya– identifikatsiya– po– raduzhnoy– obolochke– i– setchatke– glaza– sovremennye– vozmozhnosti– i– problemy– primeneniya> (дата обращения: 21.03.2023).

УДК 004.3'122

### СИСТЕМНЫЙ ПОДХОД ПО ВНУТРИСХЕМНОЙ ДИАГНОСТИКЕ И ПРОЕКТИРОВАНИЮ ПОЛОСОВОГО ФИЛЬТРА L– ДИАПАЗОНА

Назиркулов Нодирбек Халилжанович

[nodirbek.nazirkulov@mail.ru](mailto:nodirbek.nazirkulov@mail.ru)

Магистрант Кафедры «Радиотехника, электроника и телекоммуникации»

ЕНУ Л.Н.Гумилева, Астана, Казахстан

Научный руководитель – Н.А.Бурамбаева

Магистрант по направлению Конструирование и технология электронных средств  
профиля Комплексное проектирование микросистем средствами Mentor Graphics

НИУ «МИЭТ», Москва, Россия

Научный руководитель – В.В.Калугин

Аннотация: Данная тема посвящена системному подходу к внутрисхемной диагностике и проектированию полосового фильтра. Системный подход позволяет