

Финансовый университет при Правительстве Российской Федерации



На правах рукописи

Козлов Юрий Евгеньевич

**Разработка и исследование методов мультимодальной  
аутентификации пользователей мобильных приложений с  
использованием механизма жестовой манипуляции**

Специальность 05.13.19 —  
«Методы и системы защиты информации, информационная безопасность»

Диссертация на соискание учёной степени  
кандидата технических наук

Научный руководитель:  
канд. тех. наук., доцент  
Евсеев Владимир Леонович

Москва — 2019

## Оглавление

Стр.

<b>Введение . . . . .</b>	<b>5</b>
<b>Глава 1. Анализ предметной области и постановка задачи исследования . . . . .</b>	<b>10</b>
1.1 Сущность проблемы методов аутентификации в мобильных приложениях . . . . .	10
1.2 Анализ существующих механизмов аутентификации в мобильных приложениях . . . . .	11
1.2.1 Механизмы парольной аутентификации в мобильных приложениях . . . . .	12
1.2.2 Механизмы аутентификации с использованием сторонних устройств . . . . .	12
1.2.3 Методики аутентификации с использованием биометрических признаков . . . . .	13
1.2.4 Многофакторные и мультимодальные методики методики аутентификации . . . . .	17
1.3 Анализ проблем в области . . . . .	18
1.3.1 Проблема парольной защиты . . . . .	18
1.3.2 Проблемы аутентификации при помощи внешних устройств .	20
1.3.3 Проблемы биометрических способов аутентификации . . .	22
1.3.4 Системы аутентификации, использующие механизмы жестовой манипуляции . . . . .	28
1.4 Постановка задачи и обоснование выбора метода исследования . .	28
1.5 Выводы к главе . . . . .	30
<b>Глава 2. Исследование алгоритмов обработки биометрических признаков жестовой манипуляции . . . . .</b>	<b>32</b>
2.1 Пространство биометрических признаков жестовой манипуляции .	32
2.2 Формализация задачи определения соответствия биометрического признака при использовании механизма жестовой манипуляции .	33

2.3	Алгоритмы определения меры различия в системах аутентификации с использованием механизма жестовой манипуляции . . . . .	35
2.4	Функциональная схема аутентификации с использованием механизма жестовой манипуляции одним устройством . . . . .	38
2.5	Функциональная схема локальной аутентификации при помощи МТДП . . . . .	40
2.6	Формирование МТДП . . . . .	43
2.6.1	Выбор правил установки порога срабатывания . . . . .	43
2.6.2	Определение порога при помощи серии жестов . . . . .	44
2.6.3	Фиксированные пороги срабатывания . . . . .	46
2.6.4	Доверительный интервал определения ошибок первого и второго рода . . . . .	47
2.7	Система оценки МТДП . . . . .	49
2.8	Выводы к главе . . . . .	55

**Глава 3. Результаты экспериментов исследования методов мультимодальной аутентификации пользователей с использованием механизма жестовой манипуляции . . . . .**

3.1	Определение уровня шумов в показаниях акселерометра . . . . .	57
3.2	Формирование базы попыток аутентификации с использованием механизма жестовой манипуляции . . . . .	58
3.3	Определение доверительного интервала ошибок первого и второго рода . . . . .	60
3.4	Результаты эксперимента . . . . .	60
3.4.1	Тестирование методики МТДП с использованием макета . .	60
3.4.2	Визуализация равновероятного уровня ошибок . . . . .	64
3.4.3	Тестирование методики ранжирования надежности МТДП по сумме значений всех ускорений . . . . .	75
3.5	Реализация электромеханического замка интеллектуального замка на базе биометрической аутентификации с использованием механизма жестовой манипуляции . . . . .	76
3.6	Выводы к главе . . . . .	76

<b>Глава 4. Практическая реализация мобильного приложения с аутентификацией пользователя с использованием механизма жестовой манипуляции в системах разграничения доступа . . . . .</b>	<b>77</b>
4.1 Удаленная аутентификация пользователей с использованием механизма жестовой манипуляции в мобильных приложениях . . . . .	77
4.2 Особенности средств и методов разграничения доступа к физическим объектам с использованием информационных технологий . . . . .	78
4.3 АПК «Замок МТДП» . . . . .	80
4.4 Выводы к главе . . . . .	82
<b>Заключение . . . . .</b>	<b>84</b>
<b>Список сокращений и условных обозначений . . . . .</b>	<b>86</b>
<b>Словарь терминов . . . . .</b>	<b>87</b>
<b>Список литературы . . . . .</b>	<b>89</b>
<b>Список рисунков . . . . .</b>	<b>94</b>
<b>Список таблиц . . . . .</b>	<b>97</b>
<b>Приложение А. Диплом 2 степени за доклад на молодежной конференции «Информационная безопасность в банковско-финансовом секторе» в рамках IV международного форума Финансового Университета . . . . .</b>	<b>98</b>
<b>Приложение Б. Приказ о корректировке темы . . . . .</b>	<b>99</b>

## Введение

Информационная безопасность в современном обществе приобретает все большую актуальность, так как большое количество информации, появление современных гаджетов и развитие технологий привели к становлению постинформационного общества. Данное общество можно характеризовать как общество потребления большого количества информации, зависимости от информационных и компьютерных технологий, а также как общество с ведущим типом коммуникации – массовой коммуникацией [1]. Человек оказывается в непрерывном удаленном взаимодействии с людьми, юридическими лицами и различным цифровыми инструментами, при этом в течении дня он вынужден многократно проходить процедуры идентификации и аутентификации в различных мобильных приложениях для совершения различных действий, будь то отправка сообщений, чтение почты или совершение платежа. При выполнении этих процедур задействованы самые разнообразные мобильные устройства, а значит задача обеспечения надежной, быстрой и удобной аутентификации в мобильных приложениях является на сегодняшний день крайне актуальной.

Безусловно, среди технологий аутентификации наибольшую привлекательность имеют биометрические методики. Они имеют высокую степень достоверности за счет уникальности биометрических признаков и неотделимости их от дееспособной личности. Однако, использование традиционных биометрических методик для аутентификации порою оказывается не достаточно надежными, в связи с параллельными работами над методиками их взлома [2].

Одним из путей повышение надежности аутентификации является использование комбинированных (мультимодальных) методик, сочетающих в себе технологии идентификации одновременно по нескольким признакам или категориям. Например технологии попадающие одновременно во все три категории аутентификации: «что человек знает», «что человек имеет» и «что есть сам человек». Реализация таких методик может предполагать использование дополнительных устройств. Логичнее всего в качестве таких устройств использовать что-то достаточно распространенное. В настоящее время становятся популярными умные устройства, подразумевающие повседневное ношение на запястье и осуществляющие постоянное взаимодействие с человеком - это различные модификации фитнес-браслетов и умных часов. Эти устройства разработаны, в том

числе, для контроля биологических параметров и в соответствии с парадигмой интернета вещей представляют собой интерфейс «Человек-тело-вещь». Объем продаж эти устройств в мире составляет десятки миллионов единиц в год.

Использование данного класса устройств совместно с традиционными смартфонами в биометрической аутентификации позволяет повысить информационную безопасность пользователей без необходимости разработки нового оборудования. При этом повышение точности аутентификации будет достигнуто за счет следующих факторов:

1. Наручное устройство будет являться ключом (токеном) для аутентификации в мобильном устройстве, реализуя проверку, которую можно отнести к категории «что пользователь имеет». В случае кражи любого из устройств доступ злоумышленника к данным пользователя будет закрыт.
2. Наручное устройство, совместно с мобильным, будут задействованы в аутентификации, использующей жестовую манипуляцию, и, следовательно являющуюся биометрической, относящейся к категории «что есть сам человек». При этом регистрация биометрического признака (в данной работе в качестве него выбран жест) проводится датчиками двух устройств, одновременно контактирующими с разными частями тела человека - с кистью руки и запястьем, и следовательно, учитывающими большее количество информации о биометрическом признаке по сравнению с аналогичной методикой, использующей только одно устройство.
3. Аутентификация при помощи двух устройств использующая механизм жестовой манипуляции подразумевает, что пользователь должен знать и уметь выполнить определенный заранее придуманный жест. Следовательно такую аутентификацию можно отнести к категории «что человек знает».

**Целью** данной работы является повышение эффективности биометрической аутентификации при помощи жеста, совершаемого мобильным устройством.

Для достижения поставленной цели решались следующие **задачи**:

1. Анализ разработанных методик аутентификации пользователей в мобильных приложениях, выявление их достоинств и недостатков.
2. Выявление класса задач, повышение эффективности решения которых может быть достигнута с использованием аутентификации при помощи

жеста, совершаемого мобильным устройством (далее – механизма жестовой манипуляции).

3. Разработка и исследование методов повышения надежности аутентификации за счет одновременного использования дополнительного устройства.
4. Разработка комплекса программ аутентификации с помощью жеста.
5. Проведение экспериментов по применению методики аутентификации для подтверждения полученных результатов, а также получение базы попыток, достаточной для получения приемлемой достоверности результатов при обработке статистических данных и последующего моделирования.
6. Выбор наиболее эффективного с точки зрения надежности алгоритма реализации методики.
7. Реализация разработанной методики в виде аппаратно-программного комплекса и проведение его опытной эксплуатации.

**Объект исследования:** Биометрические системы, использующие для идентификации и аутентификации жесты, совершаемые мобильными устройствами.

**Предмет исследования:** Методы аутентификации пользователей мобильных приложений с использующих жесты, совершаемые мобильными устройствами.

#### **Научная новизна:**

1. Методика биометрической аутентификации с помощью жестовой манипуляции, регистрируемая акселерометрами двух взаимодействующими друг с другом устройствами.
2. Определение порога срабатывания как максимального расстояния от эталона, полученного выполнением серии жестовых манипуляций.
3. Ранжирование надежности примененного для аутентификации жеста в зависимости от суммы модулей значений ускорений.

#### **Практическая значимость:**

1. Было выполнено оригинальное исследование по классификации жестов пользователей, выбранных в качестве идентификаторов, на устойчивость к спуфингу.
2. Проведено исследование, определившее равновероятный уровень ошибок первого и второго рода для девяти алгоритмов, позволившее наглядно доказать эффективность выбранного алгоритма.

3. Разработаны мобильное приложение и аппаратно-программный комплекс, реализующий разработанную методику.

Результаты данной работы были результатами научно-исследовательской работы (НИР), проводимой ФГОБУ «Финансовый университет» за 2017 года и признано результатом интеллектуальной деятельности данной НИР. Результаты данной работы были применены в создании аппаратно-программного комплекса АПК «Замок МТДП», опытная эксплуатация которого успешно проводиться на предприятии АО «НИИЧаспром».

**Методология и методы исследования.** В ходе исследования применялись методы математической статистики, теории вероятности, теории информации, теории распознавания образов, компьютерного имитационного моделирования.

Для компьютерного моделирования применялись программы, написанные на языке Matlab. Для реализации комплекта программ применялись языки Java и C.

**Основные положения, выносимые на защиту:**

1. Использование двух взаимодействующих друг с другом источников регистрации жестовой манипуляции для увеличения надежности системы аутентификации.
2. Методика суммарной оценки соответствия воспроизведенного жеста эталону.
3. Методика ранжирования по сумме значений ускорений для классификации надежности жестовой манипуляции.

**Достоверность** полученных результатов подтверждена проведенными экспериментами.

**Апробация работы.** Основные результаты работы докладывались на трех Российских и одной международной конференциях.

**Личный вклад.** Автор принимал активное участие в научно-исследовательском процессе Финансового университета. Им был разработан макет для демонстрации возможностей методики, а также образец аппаратно-программного комплекса, реализующий управления запирающим устройством посредством мультимодальной аутентификации пользователя при помощи механизма жестовой манипуляции.

**Публикации.** Основные результаты по теме диссертации изложены в 6 печатных изданиях, 2 из которых изданы в журналах, рекомендованных ВАК, 2 — в периодических научных журналах, индексируемых Web of Science и Scopus.

**Объем и структура работы.** Диссертация состоит из введения, четырех глав, заключения и двух приложений. Полный объём диссертации составляет 100 страниц, включая 32 рисунка и 5 таблиц. Список литературы содержит 49 наименований.

## Глава 1. Анализ предметной области и постановка задачи исследования

### 1.1 Сущность проблемы методов аутентификации в мобильных приложениях

Сегодня цифровые инструменты объединяют миллиарды людей и предметов, при этом взаимодействие этих инструментов с людьми все чаще является удаленным, и осуществляется с использованием установленных в смартфоне мобильных приложений. При этом смартфон является персонализированным хранилищем разнообразной, в том числе конфиденциальной информации в том числе он настроен на предоставление автоматического доступа к сетевым сервисам и цифровым инструментам. Такими сервисами являются корпоративные инструменты, платежные инструменты, хранилища личного медиаконтента, инструменты управления умными вещами и социальные сети. Объем цифровых инструментов зачастую так велик, что разработчики очень часто называют их цифровой экосистемой [3].

Страясь сделать использование мобильных приложений наиболее комфорtnым, человек может выбрать стратегию максимальной доступности, предполагая, что в случае потери будет иметь возможность быстро заблокировать смартфон и доступ к своей персональной информации через сетевые интерфейсы. Такие механизмы очень часто предоставляют сами сервисы, включая автоматизацию аутентификации, когда она осуществляется со стороны системы, а не пользователя.

Такой подход таит в себе большие опасности, так как выполнение вышеописанных действий могут потребовать от пользователя несколько часов, а злоумышленнику для совершения противоправных действий, например для публикации экстремистской информации в социальной сети, понадобиться несколько минут.

Зная риски, возникающие при потере смартфона, компании, предоставляющие услуги, связанные с платежными инструментами, стараются использовать несколько методик аутентификации, но тем не менее этого порою оказывается недостаточно.

Рассматривая смартфон с точки зрения персонифицированного интерфейса в задачах информационной безопасности стоит отметить, что в настоящее время он выступает в двух ипостасях:

- как объект аутентификации (например, пользователь вводит пинкод для разблокирования телефона);
- как субъект аутентификации (например, пользователю приходит одноразовый пароль для совершения платежа).

Так как для задач, где смартфон выступает в качестве субъекта аутентификации, он является лишь вспомогательным средством. Наиболее важной, с точки зрения информационной безопасности, является надежность аутентификации пользователя в мобильном приложении - когда смартфон выступает в качестве объекта для аутентификации.

## **1.2 Анализ существующих механизмов аутентификации в мобильных приложениях**

Аутентификация — проверка подлинности объекта или субъекта на основе его существенных признаков, как обобщенное понятие включает в себя два класса задач: идентификация и верификация [4, с. 21].

Верификация — процесс подтверждения соответствия некоторому эталону. При верификации программа принимает одно из двух решений: объект (пользователь) является тем, за кого он себя выдаёт, или не является таковым.

Идентификация — процесс установления пользователя и сводится к выбору того, чье эталонное описание наиболее близко к описанию, полученному по входному сигналу.

Задачи аутентификация в мобильных приложениях в подавляющем большинстве представляют собой задачи верификации. Так как мобильный телефон и номера сотовых операторов, через которые осуществляется обращение к удаленным сервисам, жёстко привязаны к определённой личности. В этом случае задача сводится к определению - использует ли мобильное устройство законный хозяин или оно в чужих руках.

Современные методы аутентификации можно подразделить на три категории:

1. Использующий механизмы парольной защиты, «то что знает пользователь»;
2. Механизмы аутентификации, использующие сторонние устройства - «то, чем обладает пользователь»;
3. Биометрические методики аутентификации - «то, что «есть» сам пользователь».
4. Комбинированные (мультимодальные и многофакторные) методики аутентификации.

### **1.2.1 Механизмы парольной аутентификации в мобильных приложениях**

К механизмам парольной защиты следует отнести не только запомненный пользователем набор букв и цифр, но и все другие основанные на «факторе памяти» пароли - например использование графического ключа для разблокировки телефона. Аутентификация такого типа относительно проста для проникновения. Как показывают исследования, пользователь, как правило не стремиться использовать разнообразные сложные пароли, а использует один или несколько универсальных, зачастую слабых комбинаций.

Несмотря на значительное количество минусов парольная защита является очень популярной в силу своей легкой реализации. Кроме того надежностные характеристики механизмов парольной защиты позволяют использовать ее в качестве одного из этапов многофакторной аутентификации, или для совершения операций не имеющих критического значения (например разблокировки мобильного телефона).

### **1.2.2 Механизмы аутентификации с использованием сторонних устройств**

Механизмы аутентификации с использованием сторонних устройств подразумевают использование для аутентификации предмета, содержащего электронный ключ, который не может попасть злоумышленнику.

В настоящее время очень часто таким устройством является сам смартфон. Например технология проведения операций с использованием приходящих по СМС одноразовых паролей является использованием смартфона в качестве токена.

Для решения предшествующей задачи - аутентификации пользователя в самом смартфоне, современные производители электроники предлагают, помимо прочих механизмов, использовать устройства носимые на запястье и получившие популярности сравнительно недавно - это фитнес-браслеты и умные часы.

Эти устройства предназначены для выполнения различных функций - от контроля биологических параметров до трансляции сообщений из социальных сетей. Предполагается, что фитнес-браслет или умные часы постоянно связаны со смартфоном по интерфейсу bluetooth. Механизм аутентификации с использованием таких устройств (далее будем называть их запястными) подразумевает использование для аутентификации уникального кода.

Этот метод пока рекомендуется лишь как вспомогательный.

### **1.2.3 Методики аутентификации с использованием биометрических признаков**

Биометрическая аутентификация в мобильных телефонах начала развиваться с появлением самих мобильных телефонов. Многие из этих методик обеспечивают наиболее комфортное, с точки зрения эргономики решение задачи распознавания личности. К наиболее естественным и удобным следует отнести методику анализа отпечатков пальцев, речевую аутентификацию и аутентификацию с помощью анализа изображения, снятого камерой смартфона.

Так как в основном биометрические идентификаторы (например такие как отпечатки пальцев или рисунок радужной оболочки глаза) присущи только одному человеку и никому другому, кроме того, они неотторжимы от этого человека, ими труднее манипулировать. Поэтому биометрические признаки имеют постоянную и сильную связь между личностью и самим человеком. Однако, за счет влияния времени на организм человека многие признаки будут меняться. Кроме того резкое изменение может происходить во время болезней - больше всего этому подвержены речевые характеристики. Внешний облик человека то-

же сильно меняться с возрастом. Большое распространение получают работы по фальсификации биометрических признаков, это касается и подделок речевой аутентификации, отпечатков пальцев и даже формы лица. Биометрическая аутентификация в своей работе использует признаки недавно признанные Европейским положением о защите данных (GDPR) персональными и подлежащими защите. Это еще одна из причин, почему в развитых странах биометрическая аутентификация не принимается в широком масштабе. Необходимость соблюдения строгих правил по защите персональных данных требует иногда значительных усилий по формализации отношений пользователя и ресурса где он будет аутентифицироваться [5].

Само понятие «биометрия» появилось в конце 19 века и сформировалась как научная дисциплина, занимающаяся изучением характерных для человека признаков с использованием математических методов и подразумевающих количественные биологические эксперименты.

В настоящее время интерес к биометрии продолжает расти благодаря ее применению в технологиях безопасности, в том числе противостоянию угрозе терроризма, например при распознавании лиц [6].

Стоит отметить, что в России использование биометрических данных регулируются Статьей 11 Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 г.

Достоинства систем аутентификации основанных на применении биометрических признаков — постоянное наличие идентификаторов у пользователей.

В настоящее время в мобильных приложениях распространены четыре биометрических методики аутентификации:

- по отпечатку пальца;
- по лицу;
- по голосу;
- по радужной оболочке глаза.

Кроме указанных методик существуют методики, использующие другие биометрические данные человека, но не получившие распространения в силу ряда причин, например в силу своей новизны или специфики использования.

Одним из таких методик служат методики, использующие в качестве биометрического признака поведенческие характеристики, например деятельность человека в течении дня или манипуляции мобильными устройствами:

- аутентификация при помощи подписи, выполненной на смартфоне стилусом [7];
- аутентификация на основе анализа жеста рукой заснятого видеокамерой телефона [8],
- аутентификация на основе анализа движения кистью и пальцами регистрируемыми 3D датчиком движения [9].
- аутентификация на основе жеста, регистрируемого акселерометром смартфона.
- распознавание движений кисти и пальцев, регистрируемых акселерометром специального устройства [10];
- распознавание пользователя по жесту, регистрируемого акселерометром фитнес-браслета [11];
- распознавание автором текста путём анализа данных, полученный при письме от надетых на пишущую руку умных часов [12];
- Непрерывная аутентификация, использующая датчики носимых устройств, такие как акселерометр или гироскоп в течении длительного времени и строящих процесс аутентификации на основе анализа поведения [13].

Как можно заметить, последние два метода предполагают использование трех факторов для аутентификации - «чем человек обладает» (запястное устройство), «что человек знает» (жест или абзац рукописного текста) и «что есть сам человек» - уникальные данные, присущие только конкретному человеку при выполнении движений рукой (жестовой манипуляции).

На рисунке 1.1 представлена классификация биометрических методов, используемых для аутентификации в мобильных приложениях [14].

Биометрические методики аутентификации используют в своей работе сложные алгоритмы выработки и хранения шаблонов, для определения их надежности используют вероятностные характеристики. Самыми распространенными из них являются ошибка первого рода  $\alpha$  (FAR -False Acceptance Rate,  $\alpha$  errors) - вероятность ложного пропуска и ошибка второго рода  $\beta$  (FRR - False Rejection Rate,  $\beta$  errors) - вероятность ложного отказа.

Ошибки типа  $\alpha$  и  $\beta$  взяты из теории математической статистики и используются для принятия решения об аутентификации или отказе в аутентификации, которое является бинарным (да/нет) и принимается на основе некоего критерия, для которого существует вероятность ложного результата не равная нулю.

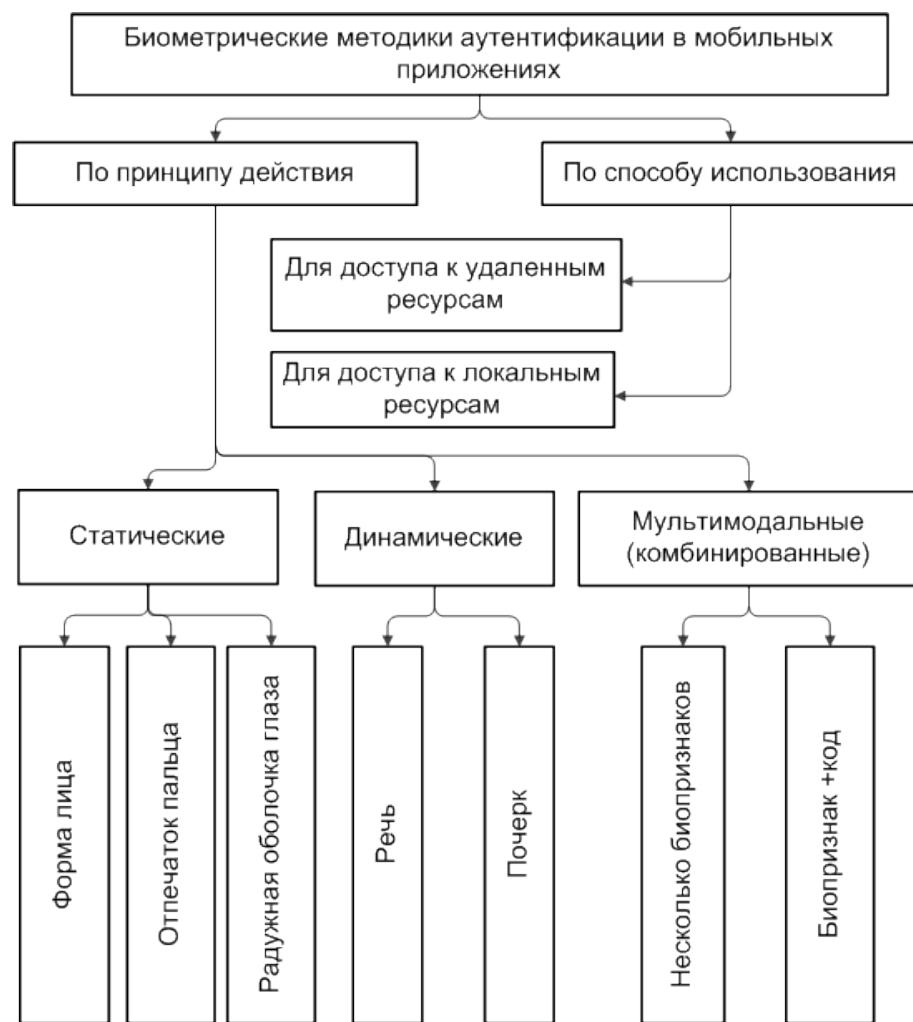


Рисунок 1.1 — Классификация биометрических методов, используемых для аутентификации в мобильных приложениях

В таблице 1 представлены средние значения  $\alpha$  и  $\beta$  для самых популярных на сегодняшний день методик биометрической аутентификации с использованием мобильного устройства [15].

Таблица 1 — Значения ошибок  $\alpha$  и  $\beta$  для наиболее распространенных биометрических методик

Методика	Тест	$\alpha$ , %	$\beta$ , %
Отпечаток пальца	FpVTE 2012	0,1	1,9
Распознавание лица	FIVE 2017	0,01	0,7 - 0,998
Речевая аутентификация	NIST 2012	1	3
Распознавание глаза	FRVT 2006 и ICE 2006	0,1	1,1

Стоит отметить, что вероятности ошибок первого рода не учитывает возможностей подделки биометрических признаков.

## 1.2.4 Многофакторные и мультимодальные методики методики аутентификации

В современном подходе к аутентификации многие компании выбирают смартфон как один из факторов в многофакторной аутентификации, например в том случае когда смартфон принимает СМС с одноразовым паролем.

Поскольку смартфон приобретает все большую значимость в жизни человека и содержит личную, а иногда и корпоративную конфиденциальную информацию, растет запрос на применение более надежных методов аутентификации пользователей в операционной системе самого смартфона.

Одним из логичных способов повышения надежности является применение двух и более методик аутентификации последовательно (многофакторная аутентификация) или одновременно (мультимодальная аутентификация).

В случае если аутентификация использует полностью независимые методики (например по форме лица и речевым характеристикам) ее надежности можно определить используя сумму вероятностей ошибок первого и второго рода. При этом принимается следующая стратегия - если аутентификация не прошла хотя бы по одной из методик, то она считается не пройденной в целом.

Пример изменения ошибок первого и второго уровня в зависимости от используемых методик лучше всего показать на примере:

Предположим имеется три независимые (не коррелирующие) между собой методики  $A$ ,  $B$  и  $C$  с уровнями ошибок  $\alpha = \beta = 0,1$  при совместном использовании уровни ошибок будут следующими 1.1:

$$\begin{aligned} \alpha(A \cdot B \cdot C) &= \alpha(A) \cdot \alpha(B) \cdot \alpha(C) = 0,001 \\ \beta(A + B + C) &= \beta(A) + \beta(B) + \beta(C) - \beta(A \cdot B) - \\ &\quad - \beta(A \cdot C) - \beta(B \cdot C) + \beta(A \cdot B \cdot C) = 0,271 \end{aligned} \tag{1.1}$$

При этом видно, что вероятность ошибки не допуска своего  $\beta$  будет незначительно расти, зато вероятность ошибок допуск чужого -  $\alpha$  будет значительно уменьшаться. Это связано с тем, что для возникновения ошибки недопуска своего необходимо возникновении ошибки в любой из методик (сумма вероятностей совместных событий). А для возникновения ошибки допуска чужого все методики должны допустить ошибку (произведение вероятностей совместных событий). Биометрическая аутентификация позволяет изменять ошибки первого рода за счет

роста ошибок второго рода и наоборот следовательно мультимодальные и многофакторные методики в целом имеют лучшие характеристики по сравнению с остальными.

Однако, стоит заметить, что основная задача комбинированных (мультимодальных и многофакторных) методик – противостоять взлому – если один из использующихся факторов оказался скомпрометирован, то в целом аутентификация все еще останется достаточно надежной.

### **1.3 Анализ проблем в области**

#### **1.3.1 Проблема парольной защиты**

Методы и приемы, применяемые злоумышленниками с целью обойти парольную защиту в мобильных приложениях, постоянно совершенствуются, однако существует ряд методов, которые используются сейчас достаточно широко. Например в следствии того, что клавиатура мобильно телефона гораздо менее удобна по сравнению с клавиатурой настольного персонального компьютера разработчики приложений стараются не устанавливать правила обязательного использования длинных сложных паролей. Более того, многие программы используют автоматическую аутентификацию, предполагая, что пользователь уже прошел аутентификацию при разблокировании смартфона. В следствии этого, мобильные приложения получают стандартные проблемы, свойственные программам со слабым паролем, однако есть некоторые особенности и приемы обхода парольной защиты в мобильных приложениях отличается от методов обхода аналогичной защиты на персональном компьютере:

1. Полный перебор — это самая простая с технической точки зрения атака.

Однако злоумышленник не всегда имеет доступ к программному, например в тех случаях когда аутентификация проводится на сервере. В этих случаях полный сервер заблокирует пользователя после нескольких неудачных попыток.

Еще одним механизмом препятствующим проведению полного перебора являются задержки, вводимые после ряда неудачных попыток. Это зна-

чительно затрудняет перебор, но теме не менее для коротких пролей он все еще может быть проведен.

В том случае, когда доступ к ПО имеется и не стоит ни каких ограничений полный перебор короткого пароля выполняется практически мгновенно.

2. При краже паролей злоумышленники используют не только его подбор, но и различные технологии подсматривания, например с помощью устройств видеонаблюдения. Кража паролей в общедоступных местах представляет большую угрозу для мобильных приложений, так как смартфон очень часто используется для аутентификации именно там. При этом одним из распространенных методов является кража при помощи видеонаблюдения. Очень часто аутентификация при помощи смартфона выполняется в общественном месте где установка видеокамеры не представляет труда.
3. Все больше набирает популярность кража паролей с помощью социальной инженерии [16].

Очень часто всего пользователи, чтобы не забыть или не ошибиться с паролем, записывают его на вещественные или электронные носители, что делает его уязвимым для кражи [17].

Социальная инженерия – один из новых методов манипулирования людьми. Данный метод опирается на механизмы воздействия на психику человека и использует достижения не столько в области техники, сколько на знаниях психологии. Основной целью воздействия является убеждение пользователя самому скомпрометировать данные для входа в СКУД. Тактики социальной инженерии весьма разнообразны и непрерывно совершенствуются. Они могут включать в себя телефонные звонки от имени подставных лиц. Создание клонов известных сайтов с целью кражи логинов и паролей и т.д.

Несмотря на правила, направленные на предотвращения компрометации данных, ежегодно жертвами социальной инженерии становится огромное количество людей, а компании несут многомиллионные убытки [18].

4. Одним из видов социальной инженерии можно назвать фишинг – этот вид кражи опирается на невнимательность или некомпетентность пользователей.

Процедура фишинга обычно заключается в копировании известных сайтов «подставных» сайтов, которые опираясь на невнимательность пользователя вынуждают ввести свой логин и пароль.

Еще один способ фишинга основан на том факте, что пользователь может использовать одинаковый пароль для различных сайтов, в таком случае проведя успешную атаку на один из них, злоумышленники получают доступ ко всем остальным.

Как правило переход пользователя по подставным сайтам достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов. При этом рассылка будет содержать ссылку на подставной сайт.

5. Кража паролей при помощи вирусов или троянского коня. Так как смартфон представляет собой вычислитель с установленной операционной системой использование вирусов и троянских коней достаточно распространено и для мобильны приложений. Как правило это случается если пользователь устанавливает приложения из непроверенных источников.
6. Кража паролей с использованием перехвата трафика (снифинга). Использование данного вида краж возможно при проведении аутентификации с использованием непроверенной сети wifi, владелец которой может оказаться мошенником.

### **1.3.2 Проблемы аутентификации при помощи внешних устройств**

Единственными внешними устройствами, применение которых в качестве токенов для аутентификации в операционной системе мобильного телефона можно рассматривать наручные фитнес-браслеты и умные часы.

Эти устройства только недавно получили свое распространение и их применение в системах обеспечения информационной безопасности практически отсутствует. Это вызвано рядом особенностей функционирования устройств.

Прежде всего стоит разделить эти устройства два класса:

1. Фитнес-браслеты - устройства, чаще всего не имеющие экрана, имеют самую простую конструкцию и не очень большую функциональность. Основное предназначение - сбор данных об активности человека. Основ-

ным преимуществом этих устройств служит большой срок автономности - до месяца. Это позволяет пользователю меньше думать о необходимости зарядки устройства. Функция использования фитнес-браслетов для разблокировки смартфона предусмотрена многими производителями. Для взаимодействия фитнес-браслета и смартфона используется интерфейс bluetooth. Для разблокировки смартфона подразумевает присутствие фитнес-браслета на небольшом расстоянии. В ином случае смартфон запросит пароль.

2. Умные часы - устройства имеющие операционную систему. Их функционал гораздо шире чем у фитнес-браслетов. Они могут позволять:

- принимать сообщения, звонки и электронную почту, и отправлять короткие ответы;
- воспринимать голосовые команды с помощью систем Google Now, Siri или других ассистентов;
- уведомлять об активности в социальных сетях;
- измерять пульс, калории и шаги;
- управлять некоторыми функциями в смартфоне;
- использоваться как навигатор;
- указывать на местоположение смартфона;
- некоторые умные часы позволяют осуществлять звонки независимо от смартфона;

Основным минусом умных часов является маленькая автономность - не более нескольких суток без подзарядки. Для связи со смартфоном часы могут использовать не только bluetooth, но и wifi. Кроме автономности есть еще ряд проблем. Например являясь полноценным вычислителем, умные часы могут хранить в себе множество медицинских параметров, которые признаются конфиденциальными и требуют защиты, поэтому например аутентификация требуется не только для смартфона, но и для умных часов. Попытки создать взаимную надежную аутентификацию ведутся, однако предложенные реализации подразумевают использование удаленного сервера для своего функционирования [19].

### 1.3.3 Проблемы биометрических способов аутентификации

Серьезная проблема биометрических методик состоит в том, что биометрические данные можно похитить особенно это касается статических признаков, таких как форма лица, отпечаток пальца или радужная оболочка глаза.

Надежность биометрических систем идентификации обеспечивается проверкой, во-первых, что биометрические данные получены от конкретного лица именно во время проверки, а во-вторых, что эти данные совпадают с образцом.

Проблему проверки подлинности пользователя необходимо начинать с построения адекватной математической модели. При этом под математической моделью стоит понимать приближенное описание существенных признаков объекта с помощью математической символики. Признаками объекта в модели могут служить биометрические данные индивидуума, пароли, специальный код и т.д. От надёжности методов аутентификации напрямую зависит сохранность информации и, как следствие, надежность всей системы.

Несмотря на все очевидные преимущества распространённых методик биометрической аутентификации, они обладают рядом недостатков, не позволяющих говорить о них как об абсолютно надёжных [20]:

1. Биометрия не секретна: основанные на знаниях методы аутентификации полностью зависят от секретности. Например, пароли и криптографические ключи известны только пользователю, и, следовательно, секретность может поддерживаться. Основные биометрические данные, такие как голос, лицо, подпись и даже отпечатки пальцев, напротив, могут быть легко записаны и потенциально без согласия пользователя. Биометрия лица и голоса уязвима для захвата без явных знаний об этом пользователе.
2. Биометрия не может быть заменена или отменена: Например, биометрические системы аутентификации должны выявлять поддельные биометрические данные, а также препятствовать распространению атак на биометрические системы. Если хакер получает доступ к образцам биометрии и может представить их системе, имитируя присутствие другого человека, то такой системе не будет доверия. В этом случае можно сказать, что биометрия была скомпрометирована навсегда. Пароли, крипто-ключи и PIN-коды могут быть изменены, если они скомпрометированы.

рованы. Предметы, такие как кредитные карты и значки, украдены, их можно заменить. Биометрия постоянно связана с пользователем и не может быть отменена или заменена, если она скомпрометирована.

3. Кросс-аутентификация: В традиционных системах аутентификации настоятельно рекомендуется использовать разные пароли и токены. Однако методы аутентификации на основе биометрии основаны на одной и той же биометрии. Если биометрический шаблон скомпрометирован один раз, он скомпрометирован навсегда. Если биометрический шаблон скомпрометирован в одном приложении, то тот же самый метод может быть использован для компрометации всех приложений, в которых используется биометрический метод. Кроме того, поскольку та же биометрия используется во всех приложениях, использующих привязку к местности при аутентификации, пользователь может потенциально отслеживаться. Если одна или несколько организаций объединяются и совместно используют свои биометрические базы данных, то они будут скомпрометированы обе и при использовании кросс-аутентификации.
4. Устойчивость: Хотя относительная надёжность с течением времени является благом для биометрии, она также может быть большой проблемой с точки зрения конфиденциальности, когда ее необходимо изменить. Единственность, содержащаяся в них, остаётся прежней.
5. Информация по построению биометрической аутентификации, принципам формирования и обработки шаблонов, а также алгоритмы функционирования и тестирования общедоступны. Это позволяет злоумышленникам проводить разработку систем преодоления защиты при помощи биометрии параллельно с разработкой самих систем аутентификации.

Эти недостатки выливаются в развитие технологий организации атак на биометрические системы. Особенно много сообщений связанных именно с биометрией внедряемой в мобильных приложениях [21] [22] [23].

При этом, развитие технологий применения распространенных биометрических признаков не всегда успевает парировать опасность, вызванную данными атаками.

Разработчики СКУД для мобильных приложений с одной стороны экспериментируют с установкой новых датчиков в мобильный телефон, например сканер сетчатки глаза, так и с использованием уже имеющихся, таких как акселерометр.

Кроме того идет работа по использованию носимых мобильных устройств, недавно получивших свое распространение [24].

Например, проводятся исследования по использованию специального жеста для аутентификации. Жест, производимый человеком, регистрируется устройством, находящимся в этот момент в руке при помощи акселерометра этого устройства [12].

Для определения эффективности аутентификации СКУД на основе биометрической идентификации используют следующие показатели:

- $\alpha$  - вероятность ложного пропуска;
- FMR - вероятность, что система неверно сравнивает входной образец с несоответствующим шаблоном в базе данных;
- $\beta$  - вероятность ложного отказа;
- FNMR - вероятность того, что система ошибается в определении совпадений между входным образцом и соответствующим шаблоном из базы данных;
- график ROC - визуализация компромисса между характеристиками  $\alpha$  и  $\beta$ ;
- коэффициент отказа в регистрации (FTE или FER) – коэффициент безуспешных попыток создать шаблон из входных данных (при низком качестве последних);
- коэффициент ошибочного удержания (FTC) - вероятность того, что автоматизированная система не способна определить биометрические входные данные, когда они представлены корректно;
- емкость шаблона - максимальное количество наборов данных, которые могут храниться в системе.

Основными при этом являются два параметра ошибки типа  $\alpha$  – вероятность возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе и  $\beta$  – вероятность отказа в доступе настоящему пользователю системы.

Обе характеристики получают расчетным путем на основе методов математической статистики. Чем ниже эти показатели, тем точнее распознавание объекта.

Стоит отметить, что методики аутентификации в мобильных приложениях могут быть использованы двумя способами:

- как клиент-серверные (вычисления осуществляют удаленный сервер);

- как локальные (вычисления осуществляют само мобильное устройство, например для разблокирования мобильного телефона).

Современные СКУД, как правило, рекомендуют использовать оба способа аутентификации и при этом использовать разные методики (например – отпечаток пальца для разблокирования телефона и речевая команда для подтверждения транзакции).

Современный уровень электроники позволяет использовать все указанные в таблице 1 методики аутентификации используя при этом вычислительные мощности только мобильного устройства, однако с точки зрения обеспечения безопасности и сохранности биометрических идентификаторов хранение их на сервере предпочтительней.

Для построения эффективной системы контроля доступа низких вероятностей  $\alpha$  и  $\beta$  недостаточно, требуется еще хорошая эргономика методики. Например, пока сложно придумать СКУД в мобильном приложении на основе анализа ДНК, несмотря на то, что  $\alpha$  и  $\beta$  этой методики стремятся к нулю. Психологический комфорт пользователей – также достаточно актуальный показатель при выборе системы безопасности. Если в случае с двухмерным распознаванием лиц или радужной оболочкой – оно происходит незаметно, то сканирование сетчатки глаза – довольно неприятный процесс.

Таким образом, для качественного анализа биометрической системы контроля доступа необходимо использовать и другие данные, многие из которых возможно только опытным путем.

В первую очередь, к таким данным нужно отнести возможность подделки биометрических данных для идентификации в системе и способы повышения уровня безопасности. Во вторых, стабильность биометрических факторов – их неизменность со временем и независимость от условий окружающей среды.

В таблице 2 приведено сравнение методов аутентификации при воздействии разных внешних факторов.

Очень часто места с высоким уровнем шума очень часто являются и местами с плохим освещением. Тем не менее, аутентификация в мобильном приложении может требоваться и для них.

В таблице 3 приведен перечень таких мест. Тем не менее, аутентификация в мобильном приложении может требоваться и для них.

Из таблицы видно многие из методик имеют сильную зависимость от условий использования. Кроме того, из всех представленных методик только методики

Таблица 2 — Методики аутентификации при воздействии разных внешних факторов

Методика	Плохая освещенность	Шумное место	Низкая температура	Высокая температура
Отпечаток пальца	нет	нет	среднее	среднее
Распознавание лица	высокое	нет	низкое	низкое
Речевая аутентификация	нет	высокое	нет	нет
Распознавание глаза	высокое	нет	нет	нет
Механизмы жестовой аутентификации, использующие акселерометр устройств	нет	нет	нет	нет

Таблица 3 — Влияние внешних факторов в городских условиях

Методика	Метро	Шумная улица	Наземный транспорт
Отпечаток пальца	нет	нет	нет
Распознавание лица	среднее	среднее	среднее
Речевая аутентификация	высокое	среднее	среднее
Распознавание глаза	высокое	нет	нет
Механизмы жестовой аутентификации, использующие акселерометр устройств	низкое	нет	низкое

речевой аутентификации и методики использующие механизмы жестовой аутентификации, являются динамическими, а следовательно позволяют многократную смену биометрического признака, например в случае компрометации.

Возможность замены биометрического признака — это важный параметр. Так, например, в случае утечки оцифрованных отпечатков пальцев, заменить их новыми будет уже невозможно. Замена идентификатор речевой аутентификации тоже ограничены, так как при большой базе речевых сообщений у злоумышленника возникает возможность генерации любых речевых команд.

Методики использующие механизмы жестовой аутентификации, обладают самой большой из представленных выше методик возможностью многократной замены, однако, ценой за это преимущество будет являться необходимость формирования функционально-динамического комплекса навыков и переобучение системы.

Еще одной эргономической характеристикой СКУД в мобильных приложениях является возможность использование ее людьми с ограниченными возможностями. Методики использующие механизмы жестовой аутентификации могут стать удобным средством для людей с нарушениями речи или зрения, когда использование других средств аутентификации затруднено.

Далее под методиками, использующими механизмы жестовой аутентификации будем подразумевать те из них, что использует в качестве данных показания акселерометра — датчика ускорений, присутствующего в любом мобильном устройстве.

Стоит заметить, что использование данного датчика в задачах распознавания личности ведутся в разных направлениях, например, авторы статьи [25] предлагают метод распознавания речи, и в том числе, идентификацию автора по голосу с помощью акселерометра мобильного телефона. Данный метод распознавания работает при очень ограниченных условиях. В идеальных условиях вероятность идентификации личности составила 23% - 26% в зависимости от тембра голоса.

Потенциально для аутентификации в мобильном телефоне может использоваться и рукописная подпись [7], но ее надежность будет существенно ниже, чем при использовании специальных устройств, так как регистрация силы нажатия, а также точность позиционирования на экране мобильного телефона значительно хуже.

Несмотря на очень хорошие показатели надежности и неотторжимость биометрических признаков они могут быть похищены.

В качестве примера можно привести сообщения СМИ о краже отпечатка пальцев министра обороны Германии и рисунка радужной оболочки глаза канцлера Германии. Фактом кражи автор сообщений подчеркивает уязвимость современных датчиков.

### **1.3.4 Системы аутентификации, использующие механизмы жестовой манипуляции**

Безусловно мультимодальные методики аутентификации будут иметь все большее и большее распространение. Их основные недостатки — большое число данных, хранимых в качестве эталонов, а также объем вычислений при их обработке.

Распространение нового вида мобильных устройств — умных часов и фитнес-браслетов, содержащих акселерометр, сделало возможным использование их для биометрической аутентификации. И как следствие увеличение надежности методики при использовании механизма жестовой манипуляции. Такая аутентификации, за счет использования двух устройств одновременно, будет иметь больше схожести с рукописной подписью по своим динамическим свойствам (биометрические особенности воспроизведения по скорости и амплитуде) и может быть названа мультимодальная трехмерная динамическая подпись (далее — МТДП) [26].

На рисунке 1.2 представлен пример МТДП, которая может служить для аутентификации. Точкой на нем обозначено начало траектории, а стрелкой указывается ее направление.

В качестве жеста может быть использован жест, который пользователь сможет запомнить и впоследствии воспроизводить.

## **1.4 Постановка задачи и обоснование выбора метода исследования**

Актуальность диссертационной работы обусловлена необходимостью разработки методики биометрической аутентификации, позволяющей проводить



Рисунок 1.2 — Пример мультимодальной трехмерной динамической подписи процедуры скрытно или со значительным затруднением возможности копирования биометрического признака. Кроме указанных свойств методика должна позволять быструю смену биометрического признака при подозрении на его компрометацию.

С помощью методов мультимодальной аутентификации, использующих механизмы жестовой манипуляции можно решить следующие задачи:

Первая — проводить аутентификацию, имеющую повышенную надежность за счет использования одновременно трех категорий аутентификации: «что пользователь знает», «что пользователь имеет» и «что есть сам пользователь».

Вторая — проведения скрытой аутентификации в людных местах за счет использования жестов, не привлекающих внимание.

Третья — использовать мультимодальную биометрическую аутентификацию, устойчивую к спуфинг атакам.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ систем биометрической аутентификации пользователей, использующие механизмы жестовой манипуляции и выявить их достоинства и недостатки;
2. Разработать методы повышения надежности за счет одновременного использования смартфона и дополнительного устройства. Рассчитать доверительный интервал определения вероятностей ошибок первого вто-

- рого рода, а так же прохождения спуфинг атаки для разработанных методов;
3. Разработать комплекс программ аутентификации с помощью механизма жестовой манипуляции;
  4. Провести эксперимент для подтверждения полученных результатов и сравнения с аналогами

Основными методами исследования будут являть методы математической статистики, теории вероятности, теории информации и теории распознавания образов.

## 1.5 Выводы к главе

Как уже было отмечено ранее используемые методики аутентификации в мобильных приложения имеют проблемы скрытия паролей и биометрических признаков, и не позволяют решать задачи скрытой аутентификации в людном месте, например в городских условиях. Одновременно эти же методики имеют уязвимости в части обеспечения устойчивости к проведению спуфинг атак.

Кроме того, наиболее надежные мультимодальные биометрические системы аутентификации работают по клиент-серверной технологии и не могут быть использованы без доступа к беспроводным информационным сетям.

Перспективным направлением повышения защищенности средств обеспечения информационной безопасности мобильных приложений, и вероятности надежной работы систем разграничения доступа, является расширенное применение в них биометрических систем аутентификации.

Аутентификация личности при помощи МТДП обладает широкими перспективами применения в мобильных приложениях, и имеет следующие преимущества:

- высокая доступность биометрического признака;
- высокая устойчивость внешним факторам;
- возможность скрытой аутентификации за счет использования жестов не привлекающих внимание;
- устойчивость к проведению спуфинг атак за счет сложности копирования биометрического признака;

- высокая надежность систем аутентификации за счет использования многих факторов одновременно;
- возможность применения методики для работы в условиях отсутствия доступа к информационным сетям.

Следует учесть, что как и любая другая подпись (речевая или рукописная), МТДП будет сильно зависеть от психоэмоционального состояния человека [27]. Это приводит к выводу, что возможны ситуации, когда пользователь принципиально не сможет аутентифицироваться, следовательно при проектировании СКУД необходимо предусматривать резервные методики аутентификации.

## Глава 2. Исследование алгоритмов обработки биометрических признаков жестовой манипуляции

### 2.1 Пространство биометрических признаков жестовой манипуляции

Данный раздел посвящен исследованию биометрической части аутентификации при помощи механизма жестовой манипуляции. В представленных ниже схемах и алгоритмах для упрощения изложения намеренно отсутствуют необходимые при практической реализации стандартные средства защиты информации, такие как шифрование данных, хранимых устройствами, защита канала связи, проверка ID устройств и т.д. Все необходимы небиометрические механизмы защиты описаны в главе 4.

В случае использовании двух устройств, когда одно из них (смартфон) захватывается кистью, а второе находится на запястье (умные часы), регистрируемые параметры жеста будут зависеть от анатомических особенностей строения руки человека.

Рука человека представляет собой три шарнирно соединенных звена: плечо, предплечье, кисть и имеет девять степеней свободы (подвижности) [26].

Предполагается, что при выполнении аутентифицирующего жеста человек держит мобильное устройство достаточно жестко, зажав его между большим пальцем и кистью, как показано на рисунке 1.2. В этом случае считается, что мобильное устройство относительно кисти (но не запястья) неподвижно.

МТДП, как и в случае рукописной подписи, потребует выработки специфического ФДКН (функционально-динамический комплекс навыков). ФДКН - явление психофизиологической природы, сущность которого составляет система навыков, предназначенных для целевой реализации определенных действий. Следовательно, кроме задачи распознавания жестовой манипуляции — как уникального идентификатора, МТДП должна иметь средства анализа надежность жеста, ведь если в качестве эталона будет выбран простой круг, то вероятность удачного спуфинга значительно увеличивается, при этом пользователь может быть уверен в надежность системы.

Показания акселерометра, получаемые с устройств, будут содержать характеристики, которые можно отнести к уникальным биометрическим особенностям человека:

- строение предплечья имеет большое различие у различных индивидов и сильно влияет на положение умных часов относительно смартфона. Это расстояние будет определять соотношение фигур, описываемых мобильным и запястным устройством;
- привычное положение локтя человека сильно зависит от фигуры, от развития мышечных тканей, а также от особенностей позвоночника. Это положение будет уникальным для каждого из людей и будет определять жестикуляцию предплечья относительно плечевого сустава;
- выработанный ФДК для жеста, содержащий уникальные характеристики свойственные только конкретному человеку.

## **2.2 Формализация задачи определения соответствия биометрического признака при использовании механизма жестовой манипуляции**

Основной задачей биометрических методик верификации пользователя является задача проверки предъявляемого биометрического признака на соответствие заранее определенным параметрам для определения степени сходства предъявленного образца с шаблоном, где степень сходства может вычисляться на основе оценки вероятности или на основе определенной метрики.

В задачах, использующих в качестве признака механизм жестовой манипуляции с использованием мобильных устройств, такими данными будут являться показания акселерометра, являющиеся временными рядами. Прежде чем определять наиболее подходящий алгоритм, определяющий соответствие, следует описать поставленную перед ним задачу.

При аутентификации с помощью механизма жестовой манипуляции, используемой в МТДП, в качестве идентификатора будет выступать жест человека, регистрируемый акселерометрами двух устройств.

Пусть эталон МТДП состоит из двух трехмерных векторов — эталона для мобильного устройства  $\vec{M}$  и эталона для запястного устройства  $\vec{W}$ . Тогда эталонный жест МТДП можно представить в виде шести временных рядов ( $\vec{M}, \vec{W}$ ):

$$\vec{M} = \begin{cases} m_{x1} & m_{x2} & \dots & m_{xd} \\ m_{y1} & m_{y2} & \dots & m_{yd} \\ m_{z1} & m_{z2} & \dots & m_{zd} \end{cases} \quad \vec{W} = \begin{cases} w_{x1} & w_{x2} & \dots & w_{xn} \\ w_{y1} & w_{y2} & \dots & w_{yn} \\ w_{z1} & w_{z2} & \dots & w_{zn}, \end{cases} \quad (2.1)$$

где  $m_x, m_y, m_z, w_x, w_y, w_z$  – временные ряды, содержащие значения ускорений по осям  $x, y, z$ .

Воспроизведенный жест — идентификатор предъявляемый субъектом при аутентификации ( $\vec{E}, \vec{F}$ ):

$$\vec{E} = \begin{cases} e_{x1} & e_{x2} & \dots & e_{xi} \\ e_{y1} & e_{y2} & \dots & e_{yi} \\ e_{z1} & e_{z2} & \dots & e_{zi} \end{cases} \quad \vec{F} = \begin{cases} f_{x1} & f_{x2} & \dots & f_{xj} \\ f_{y1} & f_{y2} & \dots & f_{yj} \\ f_{z1} & f_{z2} & \dots & f_{zj}, \end{cases} \quad (2.2)$$

где  $m_x, m_y, m_z, w_x, w_y, w_z$  – временные ряды, содержащие значения ускорений по осям  $x, y, z$ . Стоит отметить, что эти ряды будут обладать монотонностью и непрерывностью.

Очевидно, что размерность временных рядов -  $d, n, i, j$  в общем случае не равны друг другу, так как скорости работы акселерометров мобильного и запястного устройств обычно отличаются, устройства могут иметь разное время начала приема информации, а так же время воспроизведения жеста и эталона будет отличаться.

При этом стоит ввести ограничение и считать, что скорость работы акселерометра каждого из устройств всегда одинакова и определена характеристиками оборудования.

Стоит отметить тот факт, что если во время жеста умные часы надеты на той же руке в которой находится смартфон их данные будут коррелировать.

Для определения меры различия между векторами  $\vec{M}$  и  $\vec{E}$ , а также  $\vec{W}$  и  $\vec{F}$ . Можно выделить два критерия, на основе которого можно строить меру различия:

- близость значений (совпадение их с некоторой погрешностью);
- монотонность (совпадение направления движения).

Вероятность абсолютного соответствия между эталоном МТДП и воспроизведенным жестом 2.3 крайне мала:

$$\begin{cases} \vec{M} = \vec{E} \\ \vec{W} = \vec{F} \end{cases} \quad (2.3)$$

Возникновении такой ситуации должно вызывать подозрение на попытку взлома.

При формировании МТДП кроме фиксации эталонного жеста система должна определить максимальную меру различия  $P_{max}$  (далее – порог отсечки) допускаемую при верификации. Если  $P = < P_{max}$  аутентификация считается пройденной.

### 2.3 Алгоритмы определения меры различия в системах аутентификации с использованием механизма жестовой манипуляции

**Расстояние Махalanобиса** Вычисление степени различия этого признака можно рассматривать как задачу распознавание образов путем определения меры различия, которую можно определить, как поиск оптимального пути на графе.

Поскольку временные ряды 2.1 и 2.2 будут иметь свойства непрерывности и монотонности можно выразить (меру различия)  $P$  как расстояния Махalanобиса между воспроизведенным жестом и эталоном для мобильного  $P_M$  и запястного устройства  $P_W$ :

$$P = \begin{cases} P_M(\vec{M}, \vec{E}) = \sqrt{(\vec{M} - \vec{E})^T S^{-1} (\vec{M} - \vec{E})} \\ P_W(\vec{W}, \vec{F}) = \sqrt{(\vec{W} - \vec{F})^T S^{-1} (\vec{W} - \vec{F})}, \end{cases} \quad (2.4)$$

где  $S^{-1}$  - матрица ковариации.

Очевидно, что чем значительней жест отличается от эталона тем больше значение  $P$ .

**Расстояние Евклида** Очевидно, что для решения задачи сравнения матрицу ковариации можно принять равной нулю. В этом случае расстояние Махalanобиса сводится к расстоянию Евклида.

Метрика Евклида основана на использовании в нахождении расстояния теоремы Пифагора. Для использования метрики необходимо нормализовать временные ряды, например, дополнив меньший из них нулями или последним значение. Вычисление расстояния Евклида проводится по формуле 2.5:

$$D(S, T) = \sqrt{\sum_{n=1}^k s_k^2 + t_k^2} \quad (2.5)$$

**Расстояние городских кварталов** Существует еще более простой алгоритм нахождения меры различия для временных рядов, который также как и расстояние Евклида относится к метрике Минковского — это расстояние городских кварталов 2.6:

$$D(S, T) = \sum_{n=1}^k |s_k + t_k| \quad (2.6)$$

Преимущество использования метрики Минковского в минимальности вычислительных операций. Однако есть и ряд недостатков. Первый из них — это необходимость нормализации векторов для их обработки. Второй недостаток, отсутствие учета временного сдвига — это ведет к неоправданному росту меры различия при нечеткой фиксации начала и конца жеста, а так как эти моменты определяются непосредственно человеком, реакция которого значительно ниже скорости потока данных, производимого акселерометрами, то этот недостаток может являться критическим.

Алгоритмы не адаптирующиеся под данные, к которым относятся и алгоритмы метрики Минковского часто применяются для сравнения временных рядов [28].

Вместо нормализации для них может быть применена аппроксимация, однако ее применение может вызвать и негативные последствия.

Например применение аппроксимации, дающей равномерное растяжение или сжатие входного сигнала для алгоритмов не адаптирующихся под входные данные может привести к ухудшению стойкости биометрического признака к спуфингу. Для МТДП продолжительность жеста имеет значение аналогичное силе нажатия на перо в рукописной подписи.

Для формул мер схожести, требующих нормализацию.

**Квадратичное расстояние Евклида** Квадратичное расстояние Евклида не является частью метрики Минковского, так как не удовлетворяет

Это расстояние применяется если надо придать большую значимость наиболее удаленным элементам. Вычисление квадратичного расстояния Евклида проводится по формуле 2.7:

$$D(S, T) = \sum_{n=0}^k (s_k^2 + t_k^2) \quad (2.7)$$

**Расстояние Чебышева** Вычисление расстояния Чебышева проводится по формуле [29, с. 35] 2.8:

$$D(S, T) = \max_{n=1 \dots k} |s_n + t_n| \quad (2.8)$$

**Косинусное расстояние** Вычисление косинусного расстояния проводится по формуле 2.9:

$$D(S, T) = \frac{S \cdot T}{\|S\| \cdot \|T\|} = \frac{\sum_{i=1}^k s_i \cdot t_i}{\sqrt{\sum_{i=1}^k (s_i)^2} \cdot \sqrt{\sum_{i=1}^k (t_i)^2}} \quad (2.9)$$

Как и в случае с метрикой Минковского, алгоритмы получения косинусной меры не относятся к адаптирующимся под данные. Следовательно, требуется нормализация данных. В поэтому для векторов  $S$  и  $T$  она указана как  $k$ .

Диапазон значение меры сходства буде лежать в интервале от 0 до 1.

**Корреляционное расстояние** Корреляционное расстояние 2.10:

$$D(S, T) = 1 - \frac{\sum (S - \bar{S}) \cdot (T - \bar{T})}{\sqrt{\sum (S - \bar{S})^2} \cdot \sqrt{\sum (T - \bar{T})^2}}, \quad (2.10)$$

где  $\bar{S} = \frac{1}{k} \sum_{n=1}^k s_n$  и  $\bar{T} = \frac{1}{k} \sum_{n=1}^k t_n$  - среднее значение временного ряда.

**DTW алгоритмы** Один из способов получения меры схожести для временных рядов (какими будут являться выпиленные в пространстве жесты) — это решения задачи нахождение кратчайшего расстояния. Одним из самых распространенных алгоритмов, применяемых в том числе для распознавания речи и рукописных подписей является алгоритм динамической трансформации шкалы времени (DTW).

Алгоритмы DTW, несмотря на большее количество вычислений по сравнению с предыдущими, очень часто используется для получения меры схожести временных рядов. Кроме того, существуют модификации позволяющие повысить его быстродействие, что особенно важно смартфонов, имеющих не очень высокие вычислительные мощности [30]. Особенность алгоритмов DTW в том, что для проведения вычислений не требуется нормализации входных данных.

Первым этапом алгоритма DTW является построение матрицы расстояний  $D_{i,j} = d(i,j)$ , где  $d(i,j)$  может находиться различными математическими методами. Для классического DTW алгоритма это расстояние Евклида, однако подойдут

и все остальные приведенные выше алгоритмы. Матрица  $D_{i,j}$  при размерностях векторов  $S = n$  и  $T = m$  будет иметь порядок  $n \times m$ .

Следующий этап DTW построение матрицы транспозиций  $K$  порядка  $n \times m$ :

$$K_{i,j} = \begin{cases} d_{i,j} + \min(d_{i-1,j}, d_{i-1,j-1}, d_{i,j-1}) & , \text{если } i > 1 \text{ и } j > 1 \\ d_{i,j} & , \text{если } i = 1 \text{ и } j = 1 \end{cases} \quad (2.11)$$

Следующим этапом идет построение пути трансформации  $P = (p_1, p_2, \dots, p_k)$ , где  $p_l = d(S_i, T_j)$ , а длина пути  $\max(n, n) \leq k < n + m$ .

Путь трансформации - это последовательность элементов матрицы  $K$ , которая минимизирует расстояние между траекториями.

При этом путь трансформации будет удовлетворять следующим ограничивающим условиям:

**Границные условия:** Поскольку  $p_1 = d(S_1, T_1)$ , а его конец  $p_k = d(S_n, T_m)$  конец пути.

Это ограничение обеспечивает наличие в пути трансформации содержание всех элементов обоих временных рядов.

**Непрерывность (условие на длину шага):** любые два смежных элемента пути  $P$ ,  $p_l = (p_i, p_j)$  и  $p_{l+1} = (p_{i+1}, p_{j+1})$ , удовлетворяют следующим неравенствам:  $p_i - p_{i+1} \leq 1$ ,  $p_j - p_{j+1} \leq 1$ . Это ограничение гарантирует, что путь трансформации передвигается на один шаг за один раз. То есть оба индекса  $i$  и  $j$  могут увеличиваться только на 1 на каждом шаге пути.

**Монотонность:** любые два смежных элемента пути  $P$ ,  $p_l = (p_i, p_j)$  и  $p_{l-1} = (p_{i-1}, p_{j-1})$ , удовлетворяют следующим неравенствам:  $p_i - p_{i-1} \geq 0$  и  $p_j - p_{j-1} \geq 0$ . Это ограничение гарантирует, что путь трансформации не будет возвращаться назад к пройденной точке. То есть оба индекса  $i$  и  $j$  либо остаются неизменными, либо увеличиваются (но никогда не уменьшаются).

## 2.4 Функциональная схема аутентификации с использованием механизма жестовой манипуляции одним устройством

Алгоритм жестовой манипуляции может использоваться для большого спектра устройств, имеющих датчики регистрации движения.

Примером может служить алгоритм «uWave», реализованный для аутентификации на игровом сервере и использующий для идентификации джойстик приставки, обладающим акселерометром [31].

При реализации системы аутентификации игровая приставка, через которую осуществлялась аутентификация, рассматривалась как многопользовательское устройство. Следовательно, система должна была хранить множество эталонов, по одному для каждого пользователя.

Кроме того, за счет ограниченных ресурсов памяти, в алгоритм было добавлено квантование, в пределах которого данные акселерометра одновременно подвергаются фильтрации. Это позволило, резко уменьшить количество обрабатываемых данных, и производить вычисления в условиях ограниченных ресурсов. При этом применена нелинейная схема распределения уровней и используются 32 уровня квантования. Для значений в диапазоне от 0 до  $g$  выделено 10 уровняй, для диапазона от  $g$  до  $2g$  выделено 5 уровняй, значения большие  $2g$  находятся на одном уровне. Такое распределение объясняется высокой частотой возникновения значений акселерометра в диапазоне от 0 до  $g$  и очень низкой частотой появления значений в районе  $2g$  и больших.

Поскольку аутентификация при помощи игровой приставки должна быть достаточно удобной, разработчиками было принято решение обновлять эталоны жестов для каждого пользователя при успешной аутентификации. Последовательность действий при работе системы аутентификации «uWave» представлена на рисунке 2.1.

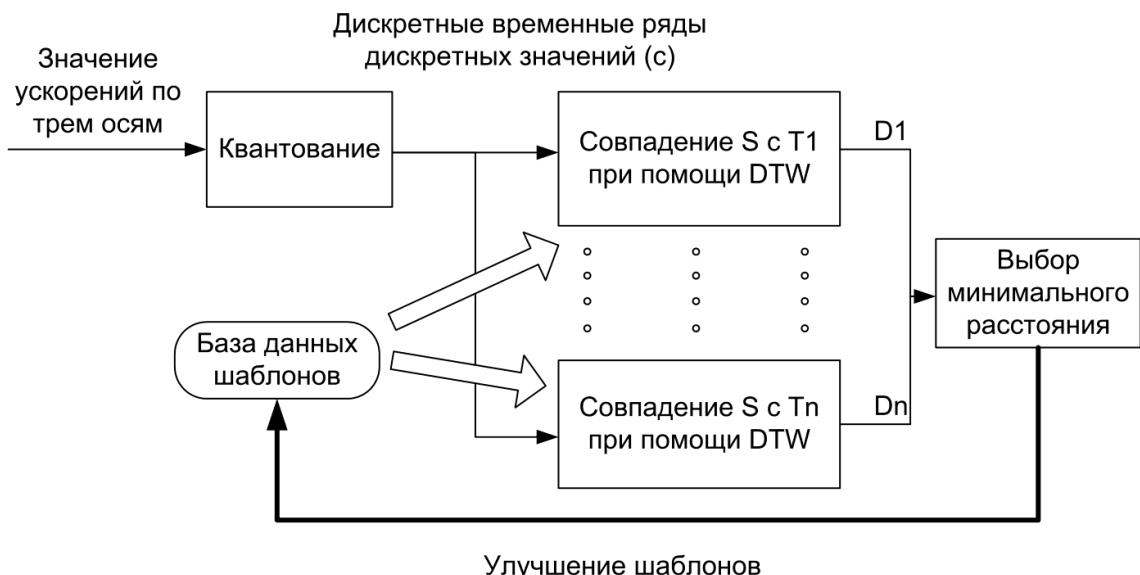


Рисунок 2.1 — Алгоритм «uWave»

Алгоритм работы , состоит из трех этапов:

- квантование данных акселерометра;
- поиск соответствующего шаблона движения;
- адаптация шаблонов.

С использованием данного алгоритма была создана и опубликована база жестов, которая позволила убедиться в эффективности распознавания [32].

## 2.5 Функциональная схема локальной аутентификации при помощи МТДП

Подходы к нахождению меры близости шаблона и жеста при идентификации человека, когда задействовано лишь одно устройство описаны достаточно подробно. Для двух устройств, участвующих в МТДП подходы будут похожи, но буду и свои нюансы.

Схема, реализующая аутентификацию взаимосвязанных устройств представлена на рисунке 2.2.

Связь обоих устройств в данной схеме реализуется через интерфейс bluetooth. Критическим для реализации такой схемы мог бы стать разброс задержки старта и остановки между умными часами (далее - часами) и смартфоном. Для протокола bluetooth задержки строго регламентированы, так например для версии 4 она составляет не более 5 мс. При этом важно отметить, что для стабильности работы важна не сама задержка, а тот факт, что при создании МТДП и при воспроизведении жеста, ее величина одинакова (с минимальным разбросом), что реализуется естественным образом, поэтому данным разбросом можно пренебречь

При этом некоторые операции показанные на схеме 2.12 можно исключить. На рисунке 2.3 представлен алгоритм функционирования МТДП в котором отсутствует проверка корреляции запястного и наручного устройства.

Использование такой схемы может снизить качество проверки биометрического признака, однако добавляет возможность при аутентификации задействовать обе руки когда смартфон находится в одной руке, а умные часы надеты на другой.



Рисунок 2.2 – Схема функционирования аутентификации на базе МТДП

Количество данных мультимодальной трехмерной динамической подписи, составляет не более 1 Мб. Следовательно, несмотря на объем вычислений, методика тоже может использоваться как локальная.

В данной модели эталонная модель 1 – модель данных с запястного устройства, а эталонная модель 2 – модель данных с мобильного устройства. Фильтрация данных необходима для того, чтобы убрать гравитационную составляющую, а так же вибрации вызванные дрожанием руки. Для устранения гравитационной составляющей следует использовать следующий высокочастотный фильтр рекомендованный разработчиком ОС Андроид [33] 2.12:

$$\begin{cases} g_i = a + (1 + a) \cdot v_i, \\ acc_i = v_i - g_i \end{cases} \quad (2.12)$$

где  $g_i$  – изолированная сила гравитации,  $v_i$  - данные полученные от акселерометра,  $0 \leq a \leq 1$  константа;  $acc_i$  - данные акселерометра с убранной гравитационной составляющей.

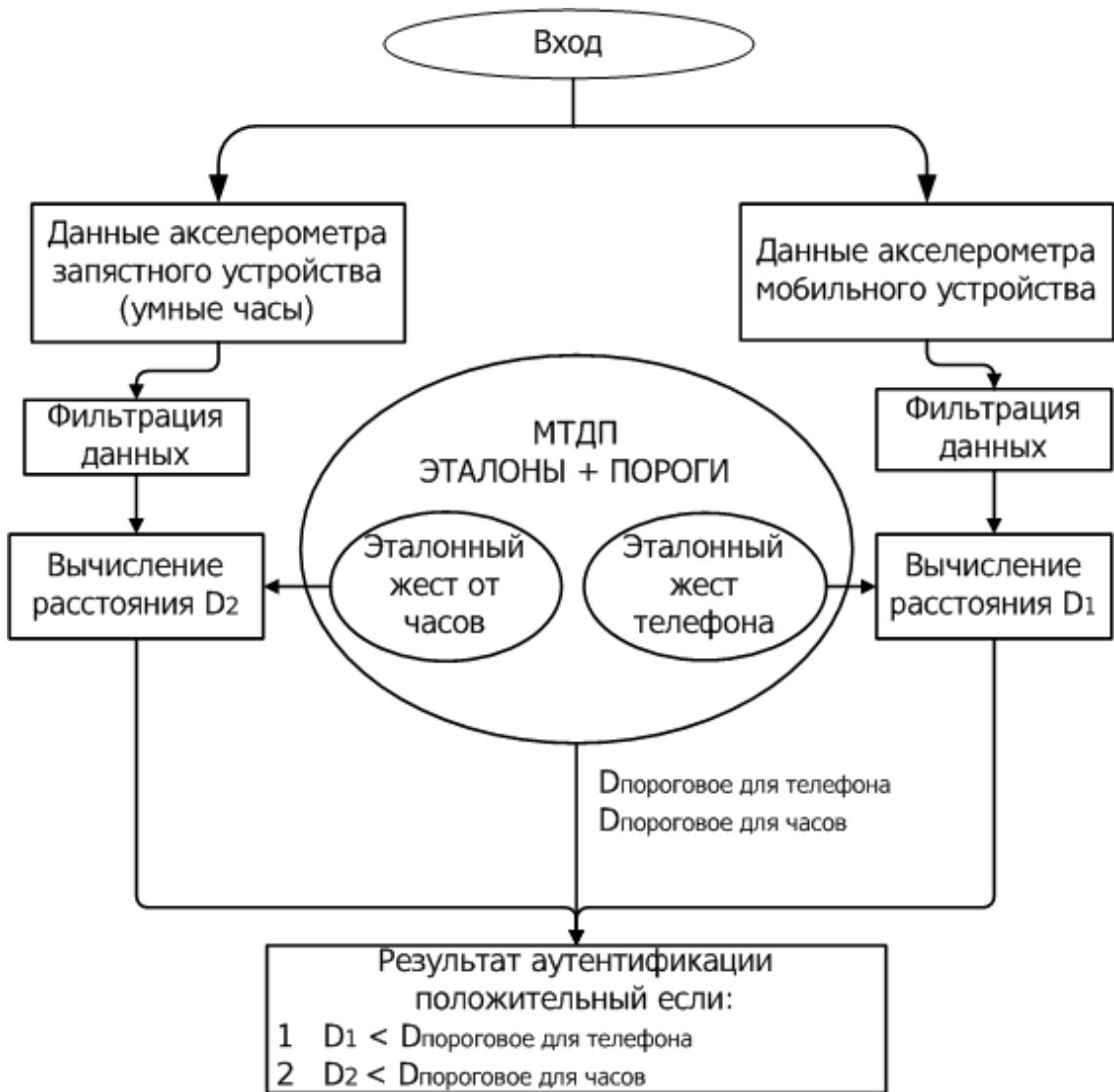


Рисунок 2.3 — Схема функционирования аутентификации на базе МТДП (без проверки корреляции траекторий устройств)

Кроме фильтра убирающего гравитационную составляющую необходимо убрать шумы, возникающие в силу разных причин [34]. Сглаживание высокочастотных помех может производится методом простого скользящего среднего, это метод хорошо себя зарекомендовал при работе с показаниями акселерометра 2.13:

$$A_t = \frac{1}{n} \sum_{i=0}^{n-1} p_{t-i}, \quad (2.13)$$

где  $t$  – значение взвешенного скользящего среднего в точке  $t$ ,  $n$  – количество значений исходной функции для расчета скользящего среднего,  $p_t$  –  $i$  – значение исходной функции в момент времени, отдаленный от текущего на  $i$  интервалов.

Траектория движения в трехмерном пространстве описывается тремя координатами. Сравнение с эталонным сигналом - это три сравнения с расстояниями

по каждой координате  $d(x_1, x_2)$ ,  $d(y_1, y_2)$ ,  $d(z_1, z_2)$ , где  $x_1, y_1, z_1$  значения хранящегося эталона, а  $x_2, y_2, z_2$  произведенный жест. Сумма расстояний для мобильного и запястного устройства  $D_2 + D_3$  должна сравниваться с пороговым значением  $D$  для принятия решения об аутентификации. При идеально воспроизведенном жесте  $D$  будет стремиться к нулю.

Вычисление расстояния  $D_1$  будет иметь некоторые особенности. Рука человека устроена таким образом, что телефон, удерживаемый, как показано на рисунке 1.2, будет развернут к надетым на руке часам приблизительно на  $90^\circ$ , следовательно, вычисление  $D_1$  лучше всего производить по формуле  $D_1 = d(x_1, z_2) + d(y_1, y_2) + d(z_1, x_2)$

## 2.6 Формирование МТДП

### 2.6.1 Выбор правил установки порога срабатывания

Вычисление меры схожести может производиться алгоритмами, описанными выше, но для принятия решения об аутентификации необходимо сравнивать эту меру схожести с некоторым пороговым значением

Задача выбора правил установления порога для принятия решения о схожести может сводится к достижению необходимых ошибок первого и второго рода. При этом порог должен быть установлен непосредственно при обучении системы и формировании эталонных сигналов. Если методика предполагает изменение эталонов, то должны обновляться и пороги.

В процессе верификации решение принимается по установлению порога, соответствующему заданной вероятности ошибок первого или второго рода. Уровень ошибок должен определяться разработчиками СКУД и в случае невозможности их выдержать необходимо принимать меры по усилению надежности аутентификации другими способами.

В тех случаях, когда необходимо максимально воспрепятствовать ложной аутентификации постороннего лица, следует уменьшить ошибку второго рода за счет увеличения ошибки первого рода. Это приводит к усложнению допуска «своего», и может потребовать увеличения числа повторных попыток аутен-

тификации. В случаях когда необходимо достичь максимального комфорта в использовании и «свой» должен быть допущен с первого жеста, следует уменьшить ошибку 1-го рода за счет увеличения ошибки 2-го рода, увеличивая при этом шансы проникновения «чужого».

Как правило, в мобильных приложениях стараются выбрать порог таким образом, чтобы ошибки первого и второго рода были равновероятны.

Для повышения надежности системы на основе использования механизмов жестовой манипуляции необходимо обеспечить пользователей инструментом, оценивающим надежность создаваемых биометрических признаков - МТДП. И с учетом полученных порогов и выдающих рекомендации о возможности применения. Без данной системы невозможно контролировать уровни ошибок первого и второго.

Задача создания системы оценки является задачей классификации и может быть решена многими способами.

При этом установка порогов срабатывания должна идти непосредственно с процессом фиксации шаблонов, это позволит проверить правильность аутентификации, а также провести тренировку пользователя, зафиксировав таким образом ФДК по воспроизведению жеста.

### **2.6.2 Определение порога при помощи серии жестов**

Для определения порога срабатывания может быть использован алгоритм подразумевающий анализ серии жестов пользователя. Пользователю предлагается воспроизвести выбранный жест несколько раз, максимальный разброс в показаниях по каждой оси между этими жестами будет принят за порог отсечки.

Укрупненный алгоритм формирования МТДП и определение порогов по серии из пяти жестов представлен рисунке 2.4 [34].

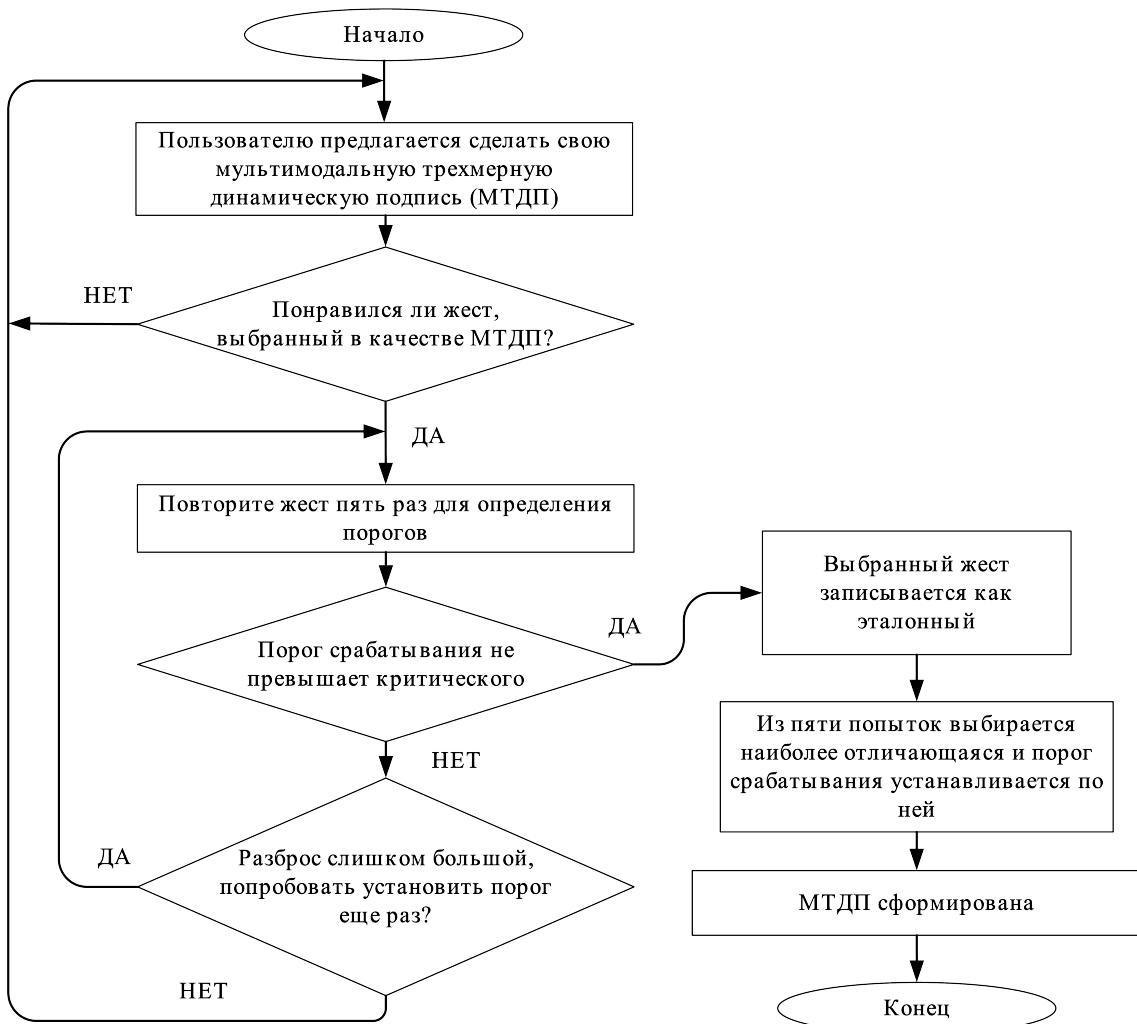


Рисунок 2.4 — Укрупненный алгоритм формирования МТДП

Данный алгоритм обладает несомненным плюсом в том, что для использования МТДП на новых устройствах нет необходимости их дополнительного исследования, так как чувствительность и скорость работы датчиков автоматически будут учтены логикой алгоритма.

Данный алгоритм, хоть и предполагает сравнение порогов с критическим (при котором ошибка первого рода будет неоправданно высокой) полностью установку порогов не контролирует. Поэтому существует вероятность, что пороги могут быть установлены слишком жестко и ошибка второго рода будет велика. Логика применения алгоритма предполагает вероятность следующих негативных сценариев формирования МТДП:

- жесты слишком различаются или выбран слишком простой жест. Порог будет установлен слишком мягко и это повысит вероятность ошибки  $\beta$  – допуск чужого и подделка МТДП (ошибка третьего рода);

- жесты выполнены очень точно и пороги установлены достаточно жестко. В реальных условиях это может вызвать рост ошибок  $\alpha$  – недопуск своего.

Оба сценария будут ставить под угрозу информационную безопасность мобильного приложения в случае выбора МТДП в качестве средства аутентификации.

### 2.6.3 Фиксированные пороги срабатывания

Алгоритм установки фиксированного порога предполагает исследование надежности жестов в зависимости от установленных порогов. И на основе накопленного опыта устанавливать порог автоматически. При этом установка порогов должна учитывать характеристики жеста.

Такой подход позволит более четко определять вероятности ошибок первого и второго рода, а также, путем увеличения или уменьшения жесткости установки порогов, уменьшать вероятность одной ошибки за счет роста другой.

Укрупненный алгоритм формирования МТДП с фиксированными порогами срабатывания представлен рисунке 2.5.

Определение подходящих порогов должно происходить на основе классификации жестов в зависимости от их сложности. Например в зависимости от суммы модулей показаний акселерометра показаний, которые имеют прямую зависимость от сложности и продолжительности жеста. Например порог отсечки мобильного и запястного устройств  $P_m$  и  $P_w$  можно определять как сумму порогов по каждой из осей  $P = p_x + p_y + p_z$ , где  $p_x, p_y, p_z$  вычисляются по формулам 2.14:

$$\begin{aligned} p_x &= R \cdot \sum |x_i| \\ p_y &= R \cdot \sum |y_i| \\ p_z &= R \cdot \sum |z_i|, \end{aligned} \tag{2.14}$$

где  $R$  - коэффициент, который может быть найден экспериментальным путем. Учитывая линейный рост значений показания акселерометра от сложности жеста, значение  $R$  будет являться скаляром.



Рисунок 2.5 — Укрупненный алгоритм формирования МТДП

#### 2.6.4 Доверительный интервал определения ошибок первого и второго рода

Надежность системы аутентификации определяют ошибки первого, второго и третьего рода.

Единственным способом определения этих ошибок является эксперимент, подразумевающий некоторое количество попыток аутентификации. Для правильной оценке полученных статистических данных следует использовать доверительный интервал в качестве интервальной оценки.

Сама процедура аутентификации предполагает использование трех попыток. Если хотя бы одна из трех попыток соответствует шаблону с точностью, не превышающей порога, то аутентификация считается пройденной.

Доверительный интервал  $p$  для оценки точности ошибок первого и второго рода можно определить по формуле 2.15 [35, с. 46].

$$p = \frac{n}{g^2 + n} \left( \omega + \frac{g^2}{2 \cdot n} \pm g \cdot \sqrt{\frac{\omega \cdot (1 - \omega)}{n} + \frac{g^2}{4 \cdot n^2}} \right), \quad (2.15)$$

где параметр  $g$  определяется уровнем доверительной вероятности на основе функции Лапласа. При уровне равном 0.95 параметр  $g = 1.96$ ,  $n$  - предполагаемое количество попыток,  $\omega$  - эмпирическая частота возникновения ошибки, которая может быть определена по аналогу.

Ближайшим аналогом МТДП, для которого были получены оценки ошибок первого и второго рода является алгоритм uWave, для которого  $\omega_1 = \omega_2 = 0.025$ . При  $n = 1000$  для определения ошибок первого рода и  $n = 4000$  для определения ошибок второго рода доверительные интервалы будут равны  $p_1 \in [0,016; 0,036]$ ,  $p_2 \in [0,02; 0,03]$  [36]. Экспериментальная оценка ошибок первого и второго рода показана в Главе 3.

### Определение оптимального количества попыток аутентификации

Формула 2.15 содержит переменную  $n$  как количество попыток аутентификации в целом. Однако для данного вида аутентификации есть необходимо давать пользователю несколько попыток. В таком случае  $n$  это от одной до нескольких попыток. Их количество будет иметь очень важное значение с точки зрения надежности.

Совершенно очевидно, что с ростом числа попыток будет уменьшаться вероятность ошибок второго рода  $\beta$ , рост ошибок первого рода  $\alpha$  и рост вероятности удачного спуфинга.

В главе 3 приведен результат моделирования для базы попыток аутентификации. Моделирование предполагало от 1 до 3 попыток. В случае если за три раза не предъявлялся жест определяемый системой как приемлемый аутентификация отклонялась. При этом уровень эквивалентной ошибки EER = 0,36 %. Этот показатель является приемлемым для эксплуатации.

Количество попыток равное трем выбран из общей практики применения подобного рода аутентификации (например по аналогии с разблокированием телефона по паролю).

## 2.7 Система оценки МТДП

Использование систем аутентификации на основе механизма жестовой манипуляции возможно в приложениях с разным уровнем значимости обрабатываемых данных. Формально данные мобильных приложений можно разделить на три группы:

- незначительная важность (например – программы, хранящие общедоступные документы);
- значимые (например – личный медиаконтент);
- имеющие критическую значимость (например – банк-клиенты, корпоративные приложения, хранящие коммерческую тайну).

Представленная классификация очень груба и может не отвечать личным представлениям пользователя, следовательно, оценка должна носить рекомендательный характер кроме критических ситуаций.

Естественно разработчик мобильных приложений чаще будут считать аутентификацию для банковского критически важным компонентом, в тоже время такие функции как разблокирование смартфона или доступ к общедоступному медиаконтенту требуют максимального удобства в своей работе, а это значит, что разработчики будут готовы снизить уровень информационной безопасности для достижения этой цели.

Поскольку механизм жестовой манипуляции дает большую свободу в выборе используемого для аутентификации жеста, необходимо дать пользователям и разработчикам возможность определять их надежность. Для этой цели совместно с самой системой аутентификации должна быть использована система оценки МТДП.

Система оценки МТДП должна выполнять несколько задач, и первой из них будет определение максимального порога, исходя из характеристик жеста — чем сложнее выбранных жест, тем ниже должен быть установлен порог и наоборот. Это позволит выдерживать ошибки первого, второго, и возможно третьего рода

для всех видов жестов в допустимых пределах. Один из способов этой оценки представлен в предыдущем разделе.

Разработчики мобильных приложений могут возложить на систему оценки МТДП еще одну задачу — снабжать пользователей рекомендациями по надежности жеста. И, например, для входа в критически важные приложения, такие как банк-клиенты, более сложные жесты. Одновременно этаже система оповестит, что для разблокирования смартфона рекомендуется взять не очень сложный и неприметный жест.

К критическим ситуациям, где, система оценки должна вмешаться, являются слишком простые жесты. Например, когда пользователь вместо жеста будет держать телефон неподвижно. Такой "жест" может быть без труда подделан, так как не содержит биометрических признаков.

Рекомендации будут опираться на предъявленный жест и должны следовать следующей логике:

- для адекватных (с точки зрения надежности) жестов (идентификаторов) рекомендации могут не выдаваться;
- в случае слишком слабых или слишком сложных жестов пользователь получает рекомендации и принимает решения о замене жеста ли о его использовании;
- слишком слабые жесты блокируются для дальнейшего использования о чем система оценки сообщает пользователю.

Ранжирование жестов определяется разработчиком мобильного в зависимости от определенными им требованиями предъявляемыми к надежности.

Еще одной особенностью реализации системы оценки будет являться возможность работы только с показаниями смартфона.

Такое упрощение стоит сделать исходя из того предположения, что, находясь на одной руке смартфон и умные часы физически жестко связаны и следовательно нет смысла исследовать избыточные данные.

Реализация системы оценки МТДП следует начинать с определения диапазона работы системы. Численной характеристикой, позволяющей охарактеризовать жест является сумма модулей всех элементов временных рядов которую условно можно назвать «масса временного ряда»  $M_t$ , в таком случае сумма "масс" временных рядов по осям  $X$ ,  $Y$  и  $Z$ , можно условно назвать «масса МТДП»  $M_{mtds}$ .

В таблице 4 представлены результаты суммирования всех элементов временных рядов (какими являются показания акселерометра по трем осям), выполненные по формуле 2.16 для различных жестов [36]:

$$M = \sum_{1}^{i} |x_i| + |y_i| + |z_i|, \quad (2.16)$$

где  $M$  – масса временного ряда,  $i$  – количество элементов во временном ряду,  $x_i, y_i, z_i$  – элементы ряда (показания акселерометра для осей  $x, y$  и  $z$ ).

Таблица 4 – Сумма значений ускорений для разных жестов

Жест	Сумма значений М
Круг	250 - 350
Квадрат	300 - 450
Крест	1300 - 1700
Тряска телефона	3000 - 5000

Представленные в таблице 4 жесты выполнялись в течении времени около 1 с, кроме того, для уменьшения влияния разницы в количестве элементов, из показаний акселерометра убирались значения гравитации.

Предельная же сумма элементов для 1 с, с учетом максимального значения ускорения равного 39 м/с<sup>2</sup> и частоте работы акселерометра 1600 Гц равна 187200.

Совершенно очевидно, что масса ряда значительно зависит от времени, особенно если показания гравитации будут в ней присутствовать.

Так как система оценки МТДП должна быть доступна широкому кругу пользователей, то представляется целесообразным, свести задачу системы к отнесению выбранного жеста к одному из четырех классов:

- высокая надежность;
- средняя надежность;
- низкая надежность;
- недопустимая МТДП.

## Анализ возможных алгоритмов системы оценки и классификации МТДП

Для решения задачи классификации данных, представленных в виде временного ряда, в современных мобильных приложениях используется широкий спектр алгоритмов. Стоит рассмотреть наиболее распространенные из них в порядке сложности их реализации:

1. использование нейронной сети;
2. использование метода k-ближайших соседей (k-NN);
3. ранжирование надежности в зависимости от M (суммы модулей ускорений).

Задача классификации МТДП в общем виде может быть формализована следующим образом. Пусть  $X$  - множество описаний объектов произвольной природы,  $Y$  - конечное множество меток классов.

Предполагается существование целевой функции - отображения, значения которого известны только на объектах обучающей выборки

Требуется построить алгоритм:  $X \rightarrow Y$  — отображение, приближающее целевую функцию  $Y$  на множестве  $X$ . При  $|Y| > 2$  задачу классификации следует называть многоклассовой.

Одним из подходов к реализации задачи является сравнение базы известных по надежности жестов (множество  $X$ ) с предъявленным жестом.

**Методика использования нейронной сети** Использование нейронной сети для классификации данных, представленных в виде временного ряда может применяться, по аналогии с рукописной подписью [37]. Реализация такого алгоритма возможна лишь с использованием как центр обработки МТДП, имеющий достаточную вычислительную мощность. Это связано с высокой ресурсоемкостью алгоритма. На настоящий момент реализация такого алгоритма на смартфоне сопряжено с рядом ограничений и, даже несмотря на эти ограничения, работа его требует значительных ресурсов смартфона [38].

Тем не менее системы классификации для нейронной сети хорошо зарекомендовали себя в области распознавания рукописных подписей.

Наиболее распространенные классификаторы:

- персептроны, ГОСТ Р 52633.5-2011, и их модификации;
- нечеткий экстрактор;

– сети квадратичных форм.

Нейронная сеть, в применении к МТДП, будет, опираясь на знания о примитивных элементах траектории, определять сложность предъявленного ей временного ряда, будет иметь несколько входов и несколько выходов.

Обычно при прогнозировании временных рядов используются многослойные, чаще всего трехслойные, нейронные сети прямого распространения. Общий вид такой нейронной сети представлен на рисунке 2.6.

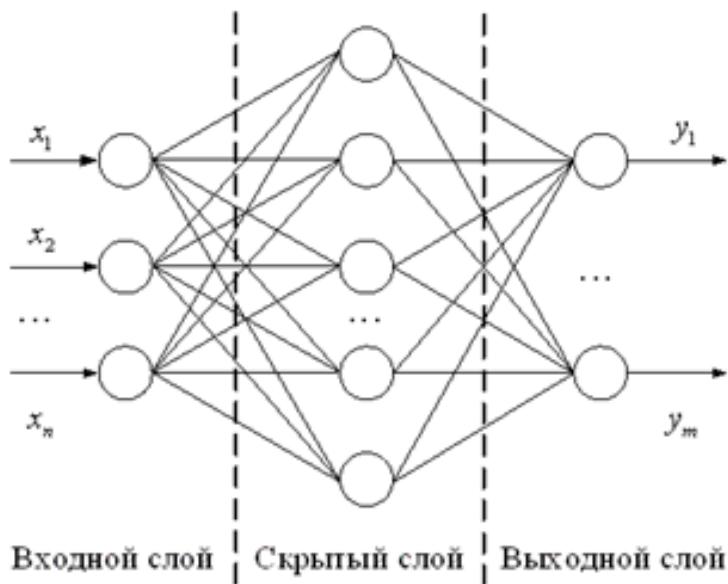


Рисунок 2.6 — Трехслойная нейронная сеть

Нужно понимать, что входов и выходов сети может быть различное количество. Как правило, на вход сети подаются фактические значения временного ряда, а также значения внешних факторов, на выходе получается одно или несколько прогнозных значений процесса.

Недостаток нейронных сетей состоит в том, что нам, разработчикам, недоступно то, что происходит внутри сети. Если сформированы входы, после этого рассчитываются выходы и просто сопоставляется одно с другим. Нет возможности детально и пошагово проследить то, как полученные на выходе значения были рассчитаны. Этот режим выполнения вычислений в «черном ящике» чрезвычайно усложняет процесс интерпретации результатов и модификации сети - неясно, что в ней нужно изменить, чтобы стало точнее.

**Методика k-ближайших соседей** Методика k-ближайших соседей широко используется для решения широкого класса задач, как в анализе видео сигнала,

например в анализе активности человека [39], так и для классификации рукописных подписей [40]. Работа алгоритма предполагает создание базы МТДП для которых проведено определение надежности. При этом МТДП в базе разложены по классам и при формировании новой МТДП происходит отнесение ее какому либо классу. В качестве меры схожести для такой классификации может быть использован алгоритм DTW 2.17:

$$Q_i = \sum_{i=1}^n \frac{1}{DTW(x, a_i)}, \quad (2.17)$$

где  $Q_j$  – классы МТДП,  $x$  – воспроизведенный жест,  $a_i$  - объекты класса.

Система оценки МТДП, основанная на методике k-ближайших соседей, может быть построена на использовании вычислительных мощностей мобильных устройств. Она менее ресурсоемка чем нейронная сеть (применяется, например для анализа деятельности человека при помощи акселерометра [41] или распознания жестов на видео [42]).

**Классификация надежности МТДП на основе ее массы** Методика классификации надежности в зависимости от массы МТДП -  $M$ , может иметь следующую логику работы. Как мы определили ранее  $M$  сильно зависит как от времени исполнения жеста, так и от активности жестикуляции, следовательно порог (максимальное значение меры схожести) должно расти со сложностью МТДП.

Тогда можно определить максимально возможный разброс  $P_{max}$ , как линейную зависимость от  $M$  2.18:

$$P_{max} = M / (M + \Delta), \quad (2.18)$$

где  $\Delta$  - экспериментально полученный коэффициент который будет ограничивать  $P_{max}$ . Жесты, имеющие слишком маленькое значение  $M$ , либо слишком большой разброс  $P > P_{max}$ , стоит признать недопустимыми. Для остальных жестов эмпирически могут быть определены  $P$ , при превышении которых жест будет классифицироваться как имеющий высокую, среднюю или низкую надежности. Таким образом при классификации можно определить пять классов  $P$ :

- $P_{extremallow}$  - недопустимо низкий уровень разброса (возможно для создания МТДП применяется автоматизированное средство);
- $P_{low}$  - низкий разброс;
- $P_{normal}$  - нормальный разброс;

- $P_{high}$  - высокий разброс;
- $P_{extremalhigh}$  - слишком высокий разброс (отказ в применении).

Описанная классификация предполагает, что порог отсечки определяется как максимальная мера схожести (наиболее удаленный вариант) между жестом выбранным как эталон и пятью последующими попытками (проверочными жестами). Результат реализации такого подхода описан в разделе 3.4.3.

## 2.8 Выводы к главе

Аутентификация на основе жестовой манипуляции, например МТДП, должна использовать алгоритмы для работы с биометрическими признаками, реализующие следующие задачи:

- нахождение меры сходства между предъявлением биометрическим признаком и эталоном, хранимым системой в качестве подлинного;
- определение порога срабатывания (меры схожести), при котором будет принято решение - принять аутентификацию пользователя или отвергнуть ее;
- определения надежности жеста, выбранного пользователем в качестве своего биометрического признака.

Подбор алгоритмов для решения данных задач требует проведения ряда экспериментов, включающих в себя как эксперименты по аутентификации, так и эксперименты по спуфингу.

Поскольку потенциально системы биометрической аутентификации должны быть широкому кругу людей к экспериментам следует привлечь добровольцев, которые должны не только оценить надежность системы, но и определить ее эргономичность. Проведенные эксперименты должны позволить создать базу МТДП, хранящую большое количество попыток аутентификации и позволяющую проводить компьютерное имитационное моделирование с целью подбора алгоритмов, решающих все необходимы задачи.

Моделирование должно включать в себя определение лучшего алгоритма нахождения меры схожести между предъявлением биометрическим признаком и эталоном, хранимым системой в качестве подлинного. При этом должны быть рассмотрены следующие алгоритмы:

- расстояние Махalanобиса;
- расстояние Евклида;
- расстояние городских кварталов;
- расстояние Хаусдорфа;
- DTW алгоритм.

Критериям качества, по которым следует проводить выбор алгоритма, будут являться ошибки первого и второго рода, а также устойчивость к спуфингу.

Проведение эксперимента подразумевает создание аппаратно-программного комплекса имитирующего поведение процедуры аутентификации. Данный комплекс будет представлять собой смартфон в связке с умными часами, а комплекта программ будет реализован с использованием языков Java и C.

В качестве инструмента компьютерного имитационного моделирования выбран язык Matlab.

## Глава 3. Результаты экспериментов исследования методов мультимодальной аутентификации пользователей с использованием механизма жестовой манипуляции

### 3.1 Определение уровня шумов в показаниях акселерометра

Поскольку жест, предъявляемый как биометрический признак, регистрируется акселерометрами мобильных устройств, важно определить, какую ошибку могут внести посторонние шумы, такие как собственные шумы датчика, акустические шумы или естественные дрожания руки человека.

Для определения уровня этих шумов было взято несколько мобильных устройств разной массы и проведены эксперименты, показывающие влияние различных факторов на показания акселерометра [34]. При этом были определены следующие показатели:

- определение среднего уровня шумов покоя (уровень собственных шумов);
- средний уровень показаний акселерометра при воздействии акустического сигнала, содержащего речевую информацию;
- уровень показаний акселерометра, удерживаемого неподвижно в руке;

Как показали эксперименты, естественные вибрации тела человека могут давать амплитуду сигнала, регистрируемого акселерометром до  $0.2 \text{ м/с}^2$ . При этом шумы будут лежать в верхней части спектра сигнала, регистрируемого акселерометром. На рисунке 3.1 представлен сигнал акселерометра мобильного устройства, удерживаемого неподвижно в руке.

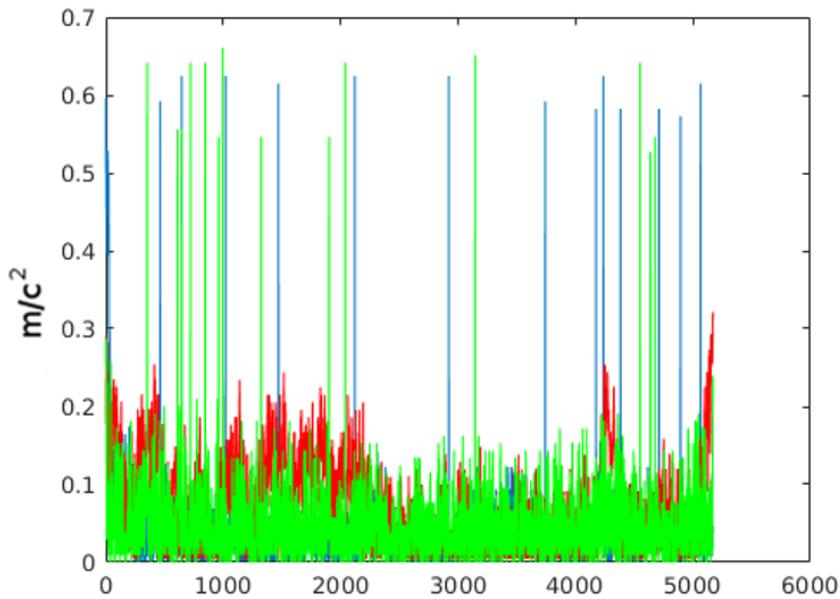


Рисунок 3.1 — Сигнал акселерометра мобильного устройства, удерживаемого неподвижно в руке

Результаты эксперименты выявили необходимость использования сглаживающего фильтра при обработке сигнала акселерометра в системах аутентификации на основе механизма жестовой манипуляции.

### **3.2 Формирование базы попыток аутентификации с использованием механизма жестовой манипуляции**

Поскольку натурное исследование большого числа алгоритмов на группе людей процесс неоправданно долгий и дорогостоящий, большинство экспериментов по подбору наиболее подходящих математических методов и определение наилучших параметров их работы было проведено с использованием компьютерного имитационного моделирования.

Для получения базы жестов, которые могут использоваться для моделирования была создан макет позволяющий имитировать аутентификацию и регистрировать жесты.

Макет представляет собой смартфон и умные часы с установленным на них программным обеспечением. Смартфон поддерживал связь с умными часами по интерфейсу bluetooth.

Логика работы была следующая, после нажатия на экране смартфона, данные акселерометров начинали регистрироваться. Спустя 1 секунду смартфон ждет снижения среднего уровня амплитуды данных акселерометра до состояния близкого к покою. Как только нужный уровень достигнут регистрация данных прекращается.

Макет МТДП предполагает выработку двух порогов для смартфона и часов по формулам 3.1. Под порогом срабатывания подразумевается значение, при превышении которого, аутентификация считается не пройденной:

$$\begin{aligned} P_M &= DTW(X_s, X_{se}) + DTW(Y_s, Y_{se}) + DTW(Z_s, Z_{se}) \\ P_W &= DTW(X_w, X_{we}) + DTW(Y_w, Y_{we}) + DTW(Z_w, Z_{we}) \end{aligned} \quad (3.1)$$

где  $P_M$  и  $P_W$  – соответственно расстояния Махalanобиса между жестом и эталоном смартфона и жестом и эталоном умных часов;  $X_s, Y_s, Z_s$  – значения ускорений по трем осям, полученные от смартфона;  $X_w, Y_w, Z_w$  - значения ускорений по трем осям, полученные от умных часов;  $X_{se}, Y_{se}, Z_{se}, X_{we}, Y_{we}, Z_{we}$  - значения ускорений, хранящиеся в качестве эталона, для трех осей смартфона и трех осей умных часов.

Решение об успешной аутентификации  $A = 1$  принимается в случае, если расстояние Махalanобиса между воспроизведенным жестом и эталонами смартфона и умных часов не превышают установленных порогов 3.2:

$$A = (P_s \leq P_{se}) \cap (P_w \leq P_{we}), \quad (3.2)$$

где  $P_{se}$  - порог для смартфона,  $P_{we}$ - порог для умных часов.

Пороги макета формируются следующим образом:

- пользователь придумывает жест и принимает решение о том, что он будет эталоном;
- выбранных жест пользователь воспроизводит пять раз. Для каждого раза вычисляются меры схожести по формуле 3.1;
- наибольшие меры схожести из пяти попыток выбираются в качестве порогов.

### 3.3 Определение доверительного интервала ошибок первого и второго рода

Предварительная оценка частоты ошибок первого и второго рода может быть найдена исходя из анализа ошибок аналогов, учетом увеличения точности на 30 %, и будет составлять для ошибок первого рода  $w_1 = 0.025$  и второго рода  $w_2 = 0.025$  [43], [26].

Для получения достоверных данных о надежности системы было проведено не менее 4000 экспериментов определения вероятности ошибок первого рода и не менее 1000 экспериментов для определения вероятности ошибок второго рода.

Подставляя эти данные в формулу 2.15, получаем предварительные границы доверительных интервалов для ошибок первого и второго рода:  $p_1[0.02; 0.03]$  и  $p_2[0.016; 0.036]$ . Данный расчет является прикидочным, и показывает порядок оценки точности вероятностей, которые должны быть подтверждены экспериментально.

Кроме задачи распознавания второй по значимости является задача классификации жеста. Так как, в отличии от рукописной подписи, жест невозможно сравнить визуально, то такую функцию должна взять на себя система обучения. Ее задача определить надежность понравившегося жеста и определить пороги, при которых аутентификацию можно считать надежной. При этом очевидно, что чем проще жест тем жестче должны быть пороги.

## 3.4 Результаты эксперимента

### 3.4.1 Тестирование методики МТДП с использованием макета

Одним из распространенных способов определения характеристик таких методик является определение ошибок первого и второго рода, а также получение комплексного показателя качества, которое можно определить при визуализации компромисса между ошибками первого рода  $\alpha$  и ошибками второго рода  $\beta$ .

Совместное построение графиков зависимости  $\beta$  и  $\alpha$  от значения порога возможно лишь с использованием компьютерного моделирования и инструмен-

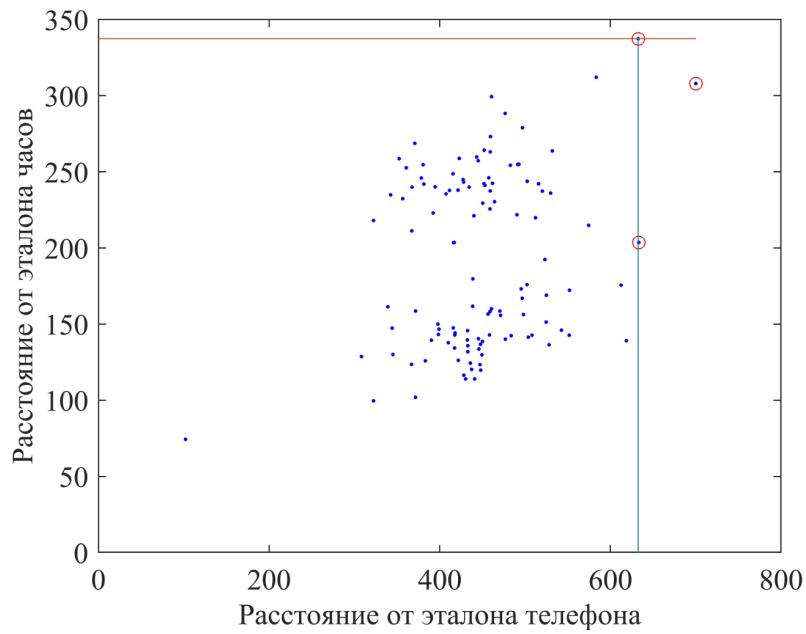


Рисунок 3.2 — Распределение попыток аутентификации для спокойного жеста

тов визуальной аналитики, позволяющих наглядно убедиться в правильности сделанных выводов. Традиционно для биометрических систем аутентификации, имеющих вероятностные показатели надежности, параметром, характеризующим комплексный показатель качества, является равный уровень ошибок (EER), располагающийся на пересечении кривых  $\beta$  и  $\alpha$ .

Макет позволил опробовать методику на группе людей и набрать данные для последующего анализа. В основе работы макета был заложен алгоритм динамической трансформации шкалы времени DTW, определяющий меру схожести между эталоном и воспроизведенным жестом. Уровень порогов определялся как максимальное расстояние, полученное из пяти попыток воспроизведения жеста.

Эксперимент показал, что уровень порогов сильно разнится в зависимости от интенсивности (активности) и длительности жеста. Если отобразить по оси ординат расстояния между эталоном и сделанным жестом для умных часов, а по оси абсцисс расстояния для смартфона, мы получим распределения попыток аутентификации на плоскости.

Необходимо отметить, что для корректности моделирования аутентификация предполагает до трех попыток. Если за три попытки системе не предъявлялся жест удовлетворяющий порогам, аутентификация считалась не принятой.

Визуализация попыток аутентификации для спокойного и интенсивного жестов представлены на рисунках 3.2, 3.3.

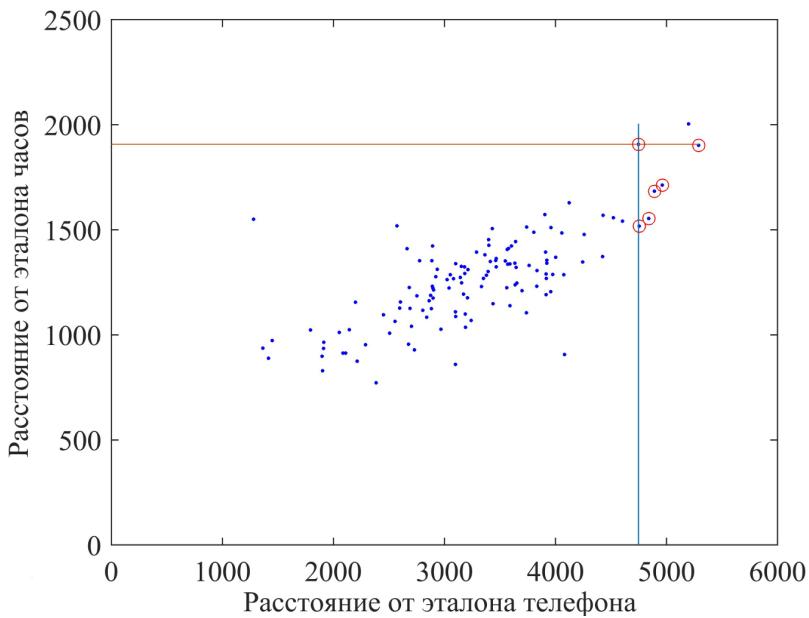


Рисунок 3.3 — Распределение попыток аутентификации для интенсивного жеста

Вертикальная черта на рисунках - порог отсечки для телефона. Горизонтальная черта – порог отсечки для умных часов. Кружком обведены попытки, отсеченные порогом только одного устройства.

Из рисунков видно, что значение порогов отличаются почти в 10 раз, и чем интенсивнее жест, тем больше численное значение порога МТДП. Однако вывод, что один из жестов менее надежен, чем другой, сложно, рисунки лишь иллюстрируют удачные и неудачные аутентификации для самого пользователя.

Ошибка первого рода -  $\beta$  для обоих жестов была равна нулю. При этом для первого жеста сделано 154 попытки, а для второго 389 попыток (как было сказано выше, аутентификация дает пользователю до трех попыток).

Для получения лучшего представления о надежности было проведено моделирование для визуализации ошибки второго рода  $\alpha$ . Для этого попытки для иных МТДП, представленных в базе, были использованы в качестве попыток аутентификации.

На рисунках 3.4 и 3.5 представлена визуализация попыток аутентификации при помощи других жестов.

По результатам моделирования спокойный жест пропустил одну неверную аутентификацию из 1077 попыток, интенсивный жест не пропустил ни одной из 840 попыток, что позволяет говорить о приемлемой надежности обоих вариантов МТДП, однако рисунки 1 и 2 не дают достаточно информации о правильности выбранного алгоритма и надежности методики в целом.

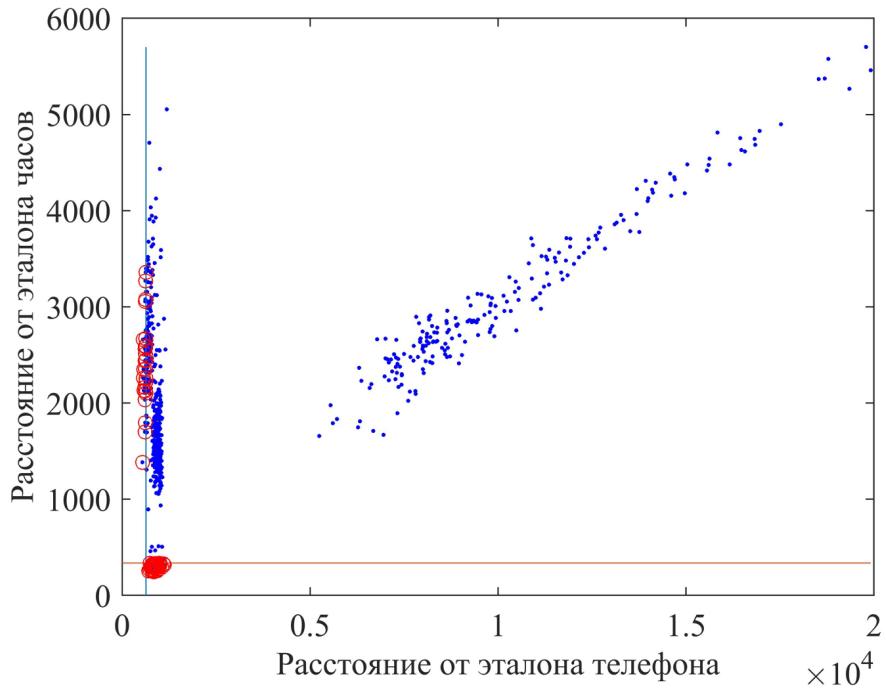


Рисунок 3.4 — Распределение попыток аутентификации для спокойного жеста

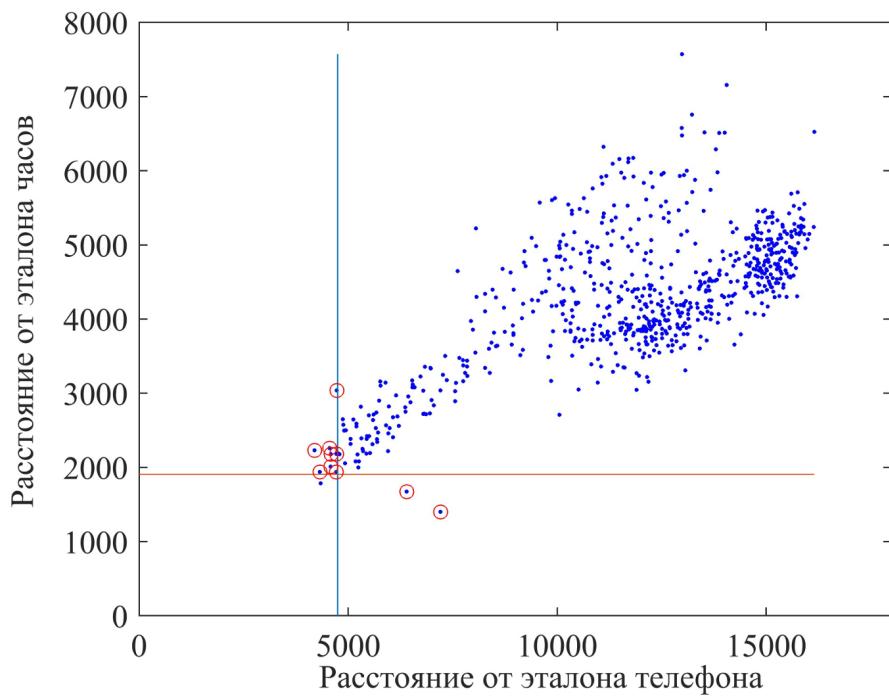


Рисунок 3.5 — Распределение попыток аутентификации для интенсивного жеста

### 3.4.2 Визуализация равновероятного уровня ошибок

Выработка порогов указанным выше способом не допускает их корректировки и изменения соотношений ошибок первого и второго рода. Кроме того, для полноценного исследования следует сравнить эффективность известных алгоритмов, позволяющих осуществлять сравнение временных рядов.

В качестве алгоритмов получения расстояния были выбраны алгоритмы описанные во второй части.

Сравнения качества работы нескольких алгоритмов с точки зрения надежности можно провести, определив ошибки  $\alpha$  и  $\beta$ , а также получив комплексный показатель качества - EER (equal error rate - равный уровень ошибок).

Отличительной особенностью методики аутентификации с помощью механизма жестовой манипуляции является необходимость индивидуальной установки порогов в зависимости от сложности жеста, следовательно, надежность, а также ошибки  $\alpha$  и  $\beta$ , также будут зависеть от сложности жеста. При этом в МТДП сложность жеста для смартфона и умных часов будет различной - в жесте участвуют движения запястьем, предплечьем, кистью руки и пальцев.

Для определения значения EER мультимодальной, использующей два устройства, можно воспользоваться следующим приемом.

Обозначим значение уровня равной ошибки для умных часов и смартфона  $EER_w$  и  $EER_p$  соответственно. В таком случае  $EER_s$  методики использующей оба устройства будет не выше минимального из них 3.3:

$$EER_s \leq \min\{EER_w, EER_p\} \quad (3.3)$$

Основываясь на данном выводе можно провести моделирование, с целью поиска EER разных алгоритмов, используя простой линейный сдвиг порога для каждого устройства отдельно.

Одновременно графики позволяют оценить надежность аутентификации только одним устройством.

Всего в моделировании участвовало 1229 реальных попыток аутентификации для восьми МТДП, выполненных разными людьми и имеющие максимальное количество попыток. На основе этих попыток для каждого алгоритма смоделировано  $6,1 \times 10^7$  попыток для визуализации кривой  $\beta$  и  $4,3 \times 10^8$  попыток для визуализации кривой  $\alpha$ .

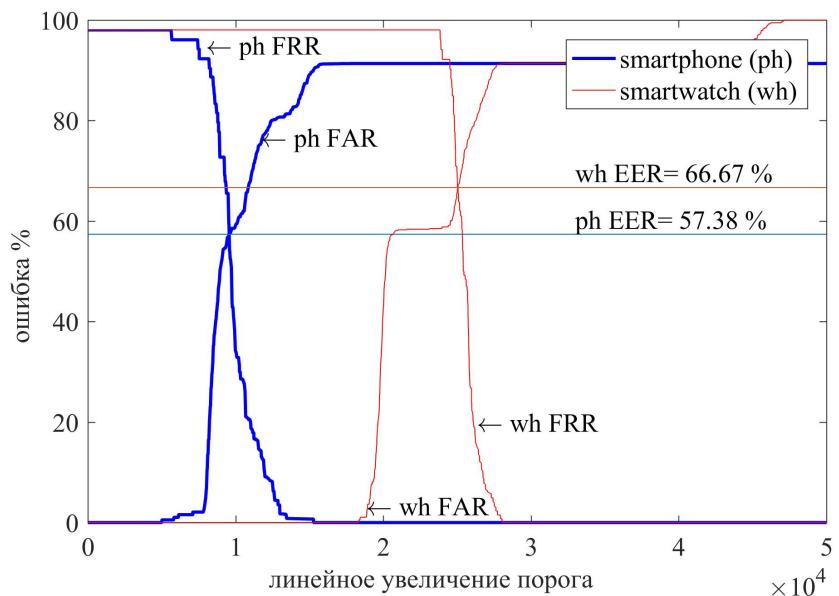


Рисунок 3.6 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Евклида

Моделирование предполагало линейное увеличение порога таким образом, чтобы наиболее наглядно отобразить на графике пересечение  $\beta$  и  $\alpha$ .

Графики  $\alpha$  и  $\beta$ , аналогичные показанным ниже, были получены для всех восьми МТДП. Ниже представлены два типичных случая – жест с высокой надежностью (интенсивный жест - сумма модулей ускорений по всем осям около 15000 у.е. При этом из показаний не убиралась гравитационная составляющая) и слабой надежностью (спокойный жест - сумма модулей ускорений по всем осям около 1500 у.е.). Подробно о нахождении суммы модулей ускорений изложено в статье "Подходы к определению надежности мультимодальной трехмерной динамической подписи".

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием расстояния Евклида для определения меры схожести между временными рядами (формула 2.5) для спокойного жеста представлена на рисунке 3.6, для интенсивного жеста представлена на рисунке 3.7.

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием квадратичного расстояния Евклида для поиска расстояния между временными рядами (формула 2.7) для спокойного жеста представлена на рисунке 3.8, для интенсивного жеста представлена на рисунке 3.9.

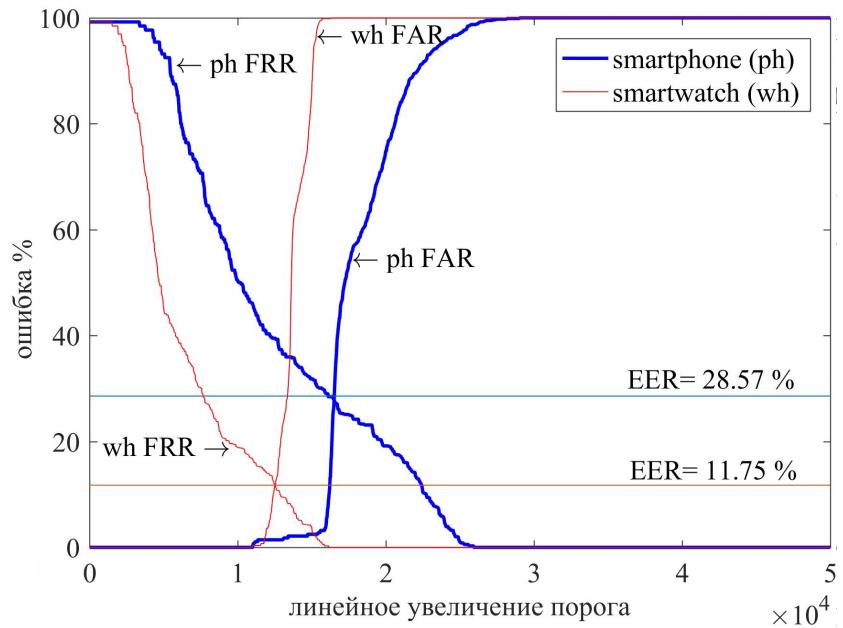


Рисунок 3.7 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Евклида

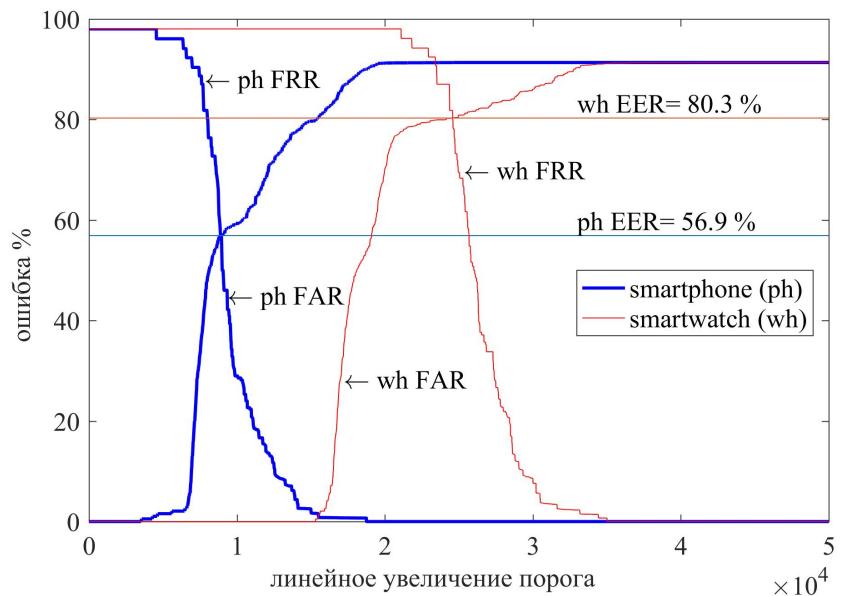


Рисунок 3.8 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании квадратичного расстояния Евклида

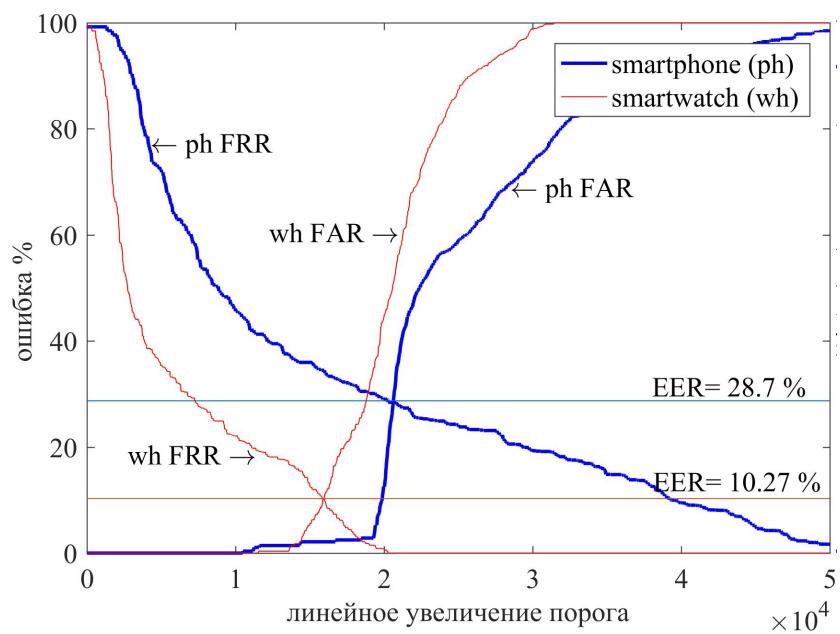


Рисунок 3.9 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании квадратичного расстояния Евклида

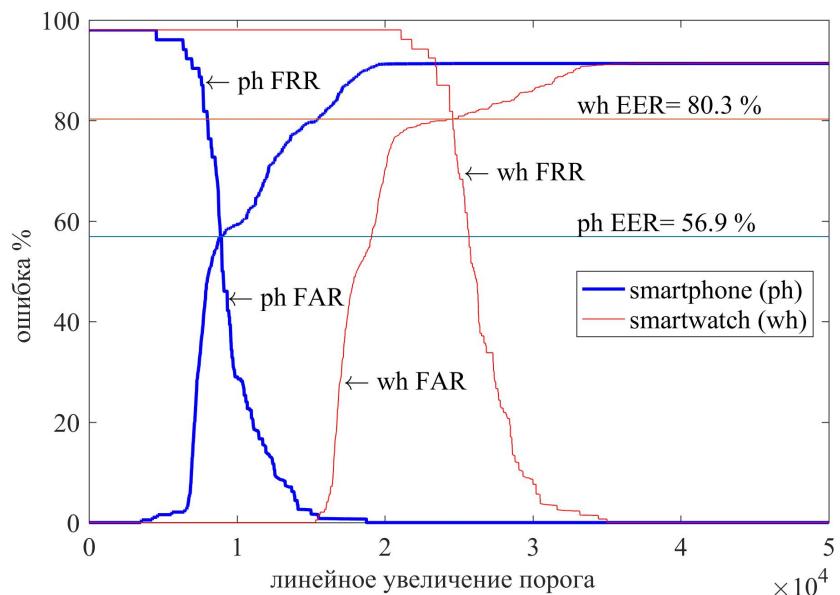


Рисунок 3.10 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании расстояния городских кварталов

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием расстояния городских кварталов для поиска расстояния между временными рядами (формула 2.6) для спокойного жеста представлена на рисунке 3.10, для интенсивного жеста представлена на рисунке 3.11.

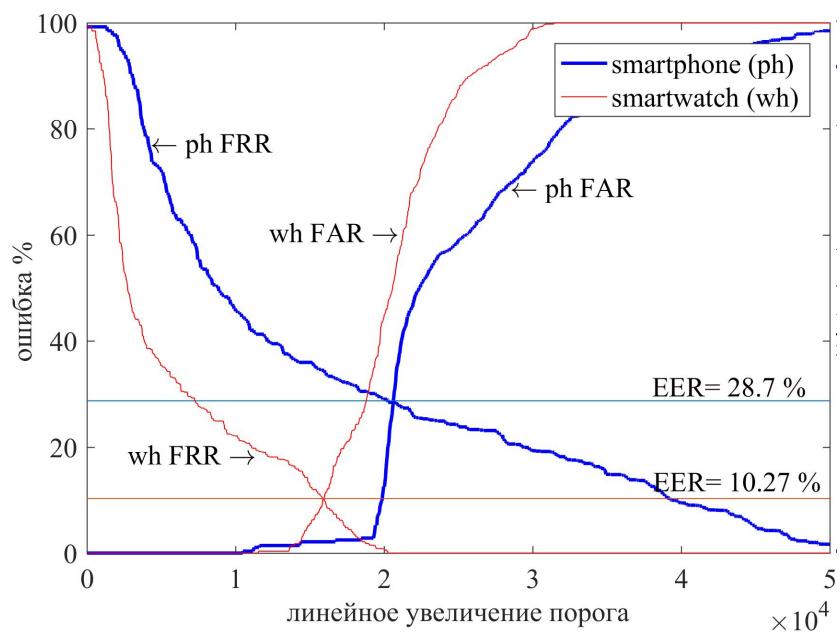


Рисунок 3.11 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании расстояния городских кварталов

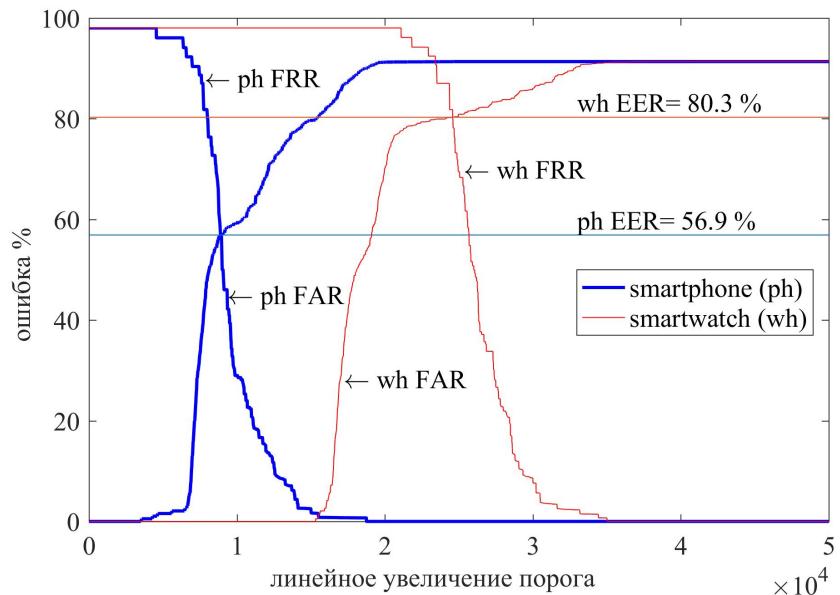


Рисунок 3.12 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Чебышева

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием алгоритма Чебышева для поиска расстояния между временными рядами (формула 2.8) для спокойного жеста представлена на рисунке 3.12, для интенсивного жеста представлена на рисунке 3.13.

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием косинусной меры для по-

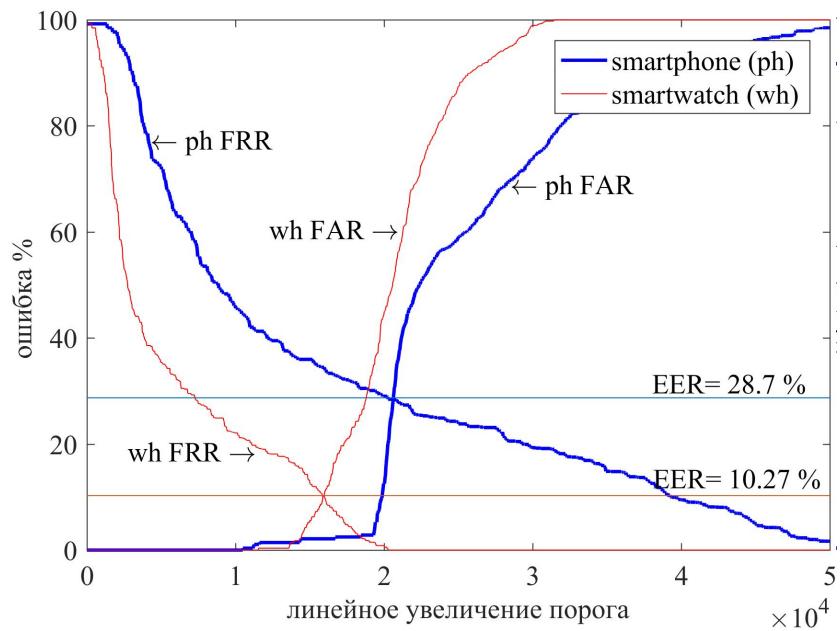


Рисунок 3.13 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Чебышева

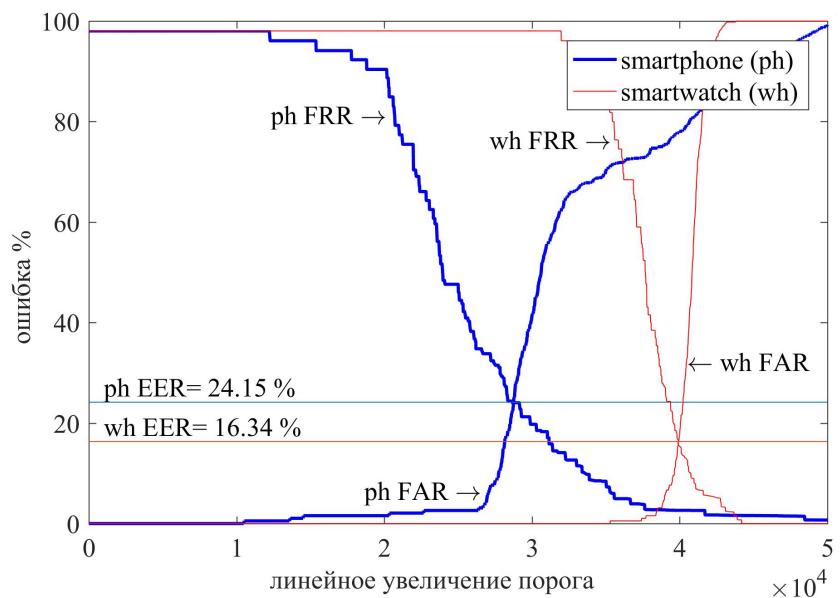


Рисунок 3.14 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании косинусной меры

иска расстояния между временными рядами (формула 2.9) для спокойного жеста представлена на рисунке 3.14, для интенсивного жеста представлена на рисунке 3.15.

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием корреляционного расстояния для поиска меры схожести между временными рядами (формула 2.11) для

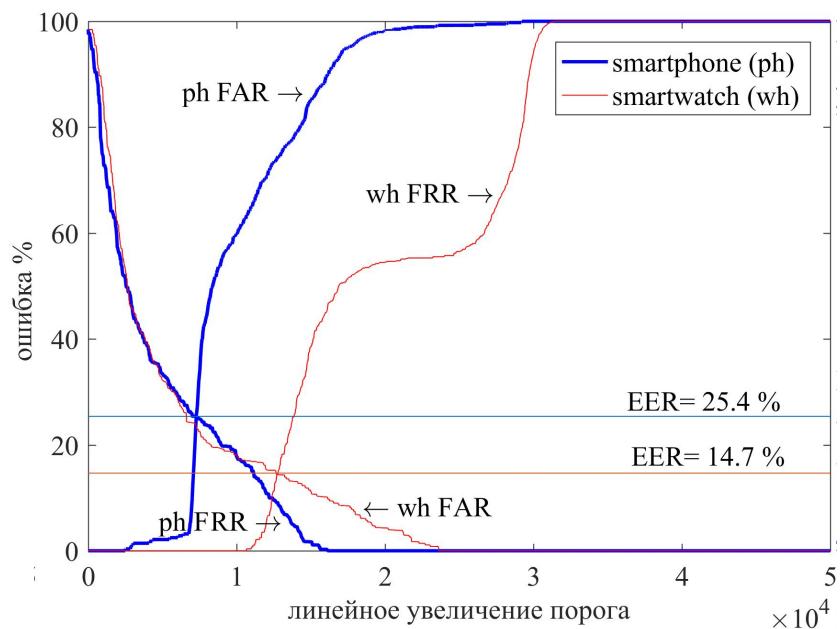


Рисунок 3.15 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании косинусной меры

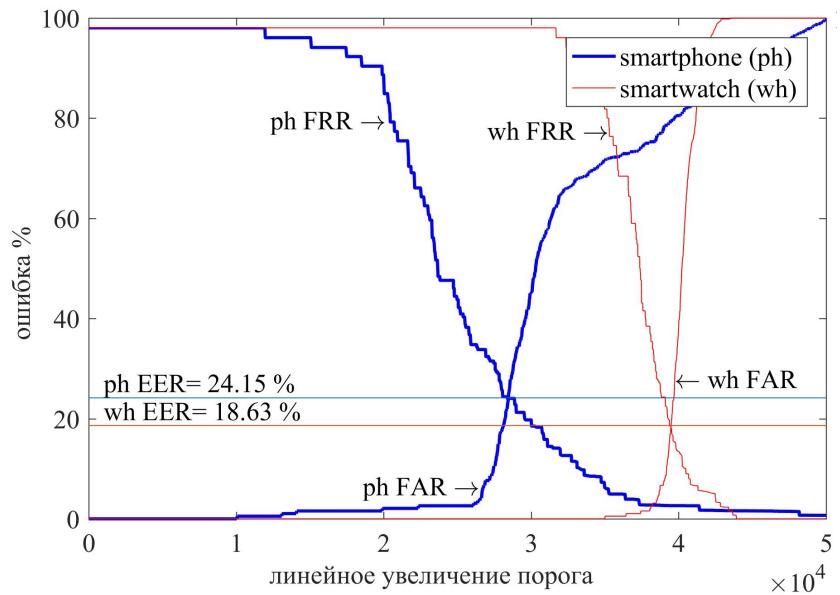


Рисунок 3.16 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании корреляционного расстояния

спокойного жеста представлена на рисунке 3.16, для интенсивного жеста представлена на рисунке 3.17.

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием алгоритма DTW, использующего для построения матрицы расстояний расстояние Евклида, для поиска меры схожести между временными рядами (формула 2.10) для спокойного жеста

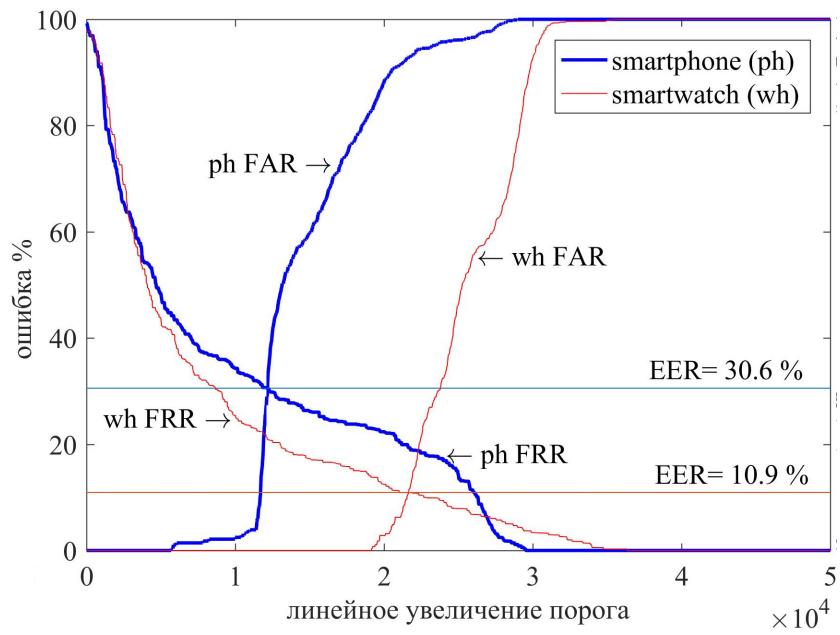


Рисунок 3.17 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) при использовании корреляционного расстояния

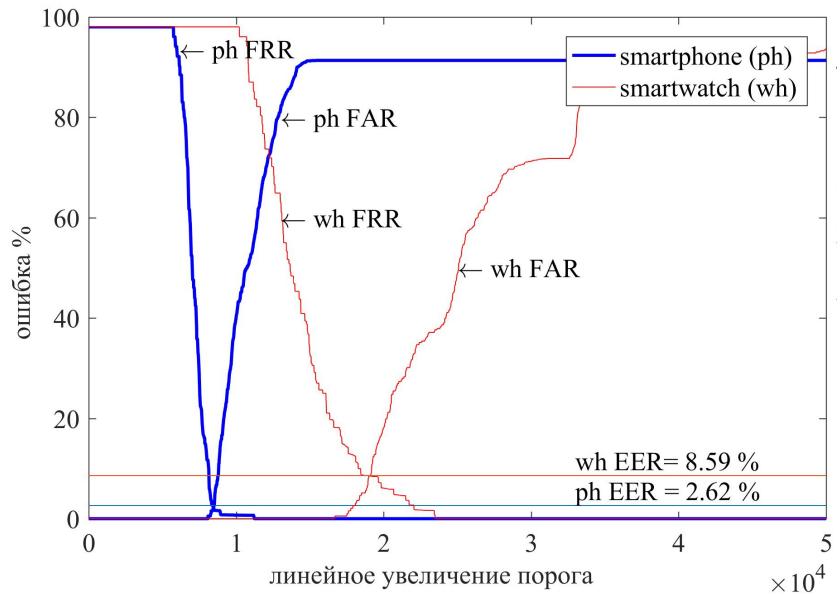


Рисунок 3.18 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) с использованием алгоритма DTW, использующего для построения матрицы расстояний расстояние Евклида

представлена на рисунке 3.18, для интенсивного жеста представлена на рисунке 3.19.

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием алгоритма DTW, использующего для построения матрицы расстояний квадрат расстояния Евклида, для поиска меры схожести между временными рядами (формула 2.10) для спокой-

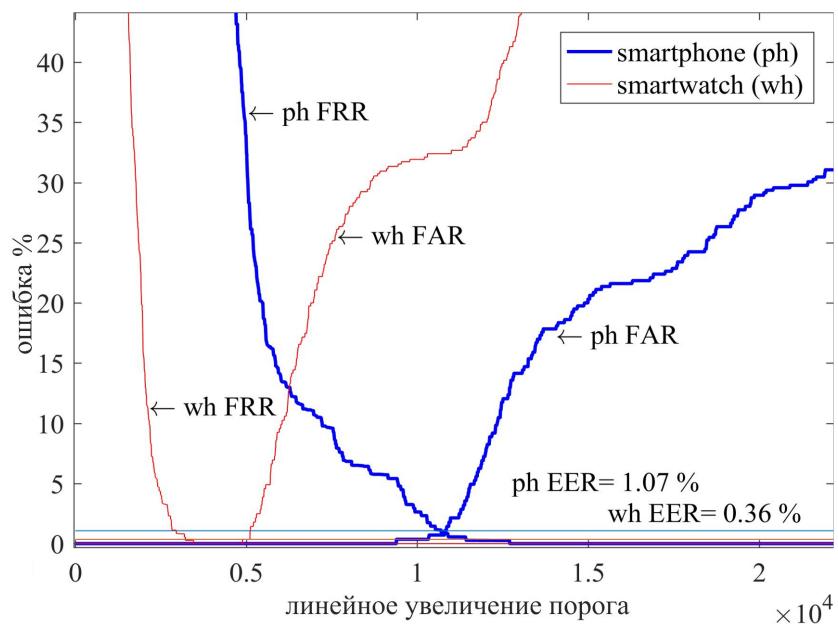


Рисунок 3.19 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) с использованием алгоритма DTW, использующего для построения матрицы расстояний расстояние Евклида

ногого жеста представлена на рисунке ??, для интенсивного жеста представлена на рисунке 3.20.

Зависимости  $\alpha$  и  $\beta$  от значения порога при аутентификации при помощи смартфона и при помощи умных часов с использованием алгоритма DTW, использующего для построения матрицы расстояний расстояние городских кварталов, для поиска меры схожести между временными рядами (формула 2.6) для спокойного жеста представлена на рисунке 3.21, для интенсивного жеста представлена на рисунке 3.22.

В таблице 5 представлены обобщенные результаты проведенного моделирования для двух МТДП.

Для алгоритмов 1-6 применение аппроксимации, дающей равномерное растяжение или сжатие входного сигнала, вероятно, дало бы лучшие результаты, но такой прием может привести к ухудшению стойкости биометрического признака к спуфингу. Для МТДП продолжительность жеста имеет значение аналогичное силе нажатия на перо в рукописной подписи.

Уровень EER был получен для всех восьми МТДП, выполненных различными людьми. База попыток МТДП, и программа визуализации EER доступна для свободного скачивания.

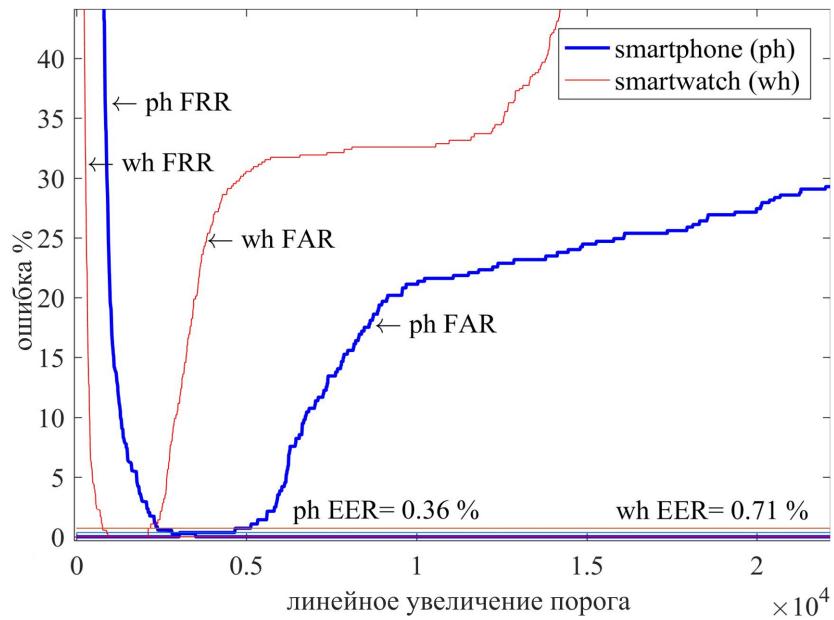


Рисунок 3.20 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) с использованием алгоритма DTW, использующего для построения матрицы расстояний квадрат расстояния Евклида

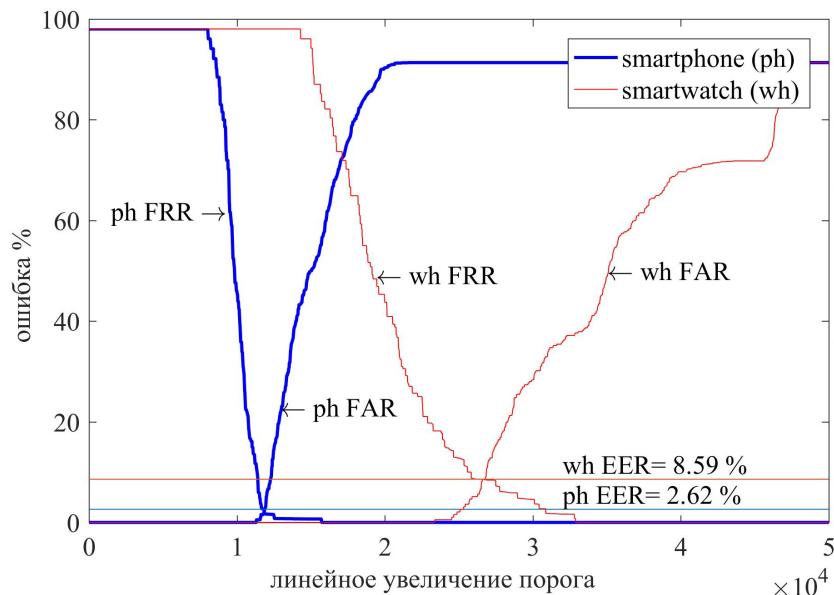


Рисунок 3.21 — Спокойный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) использующего для построения матрицы расстояний расстояние городских кварталов

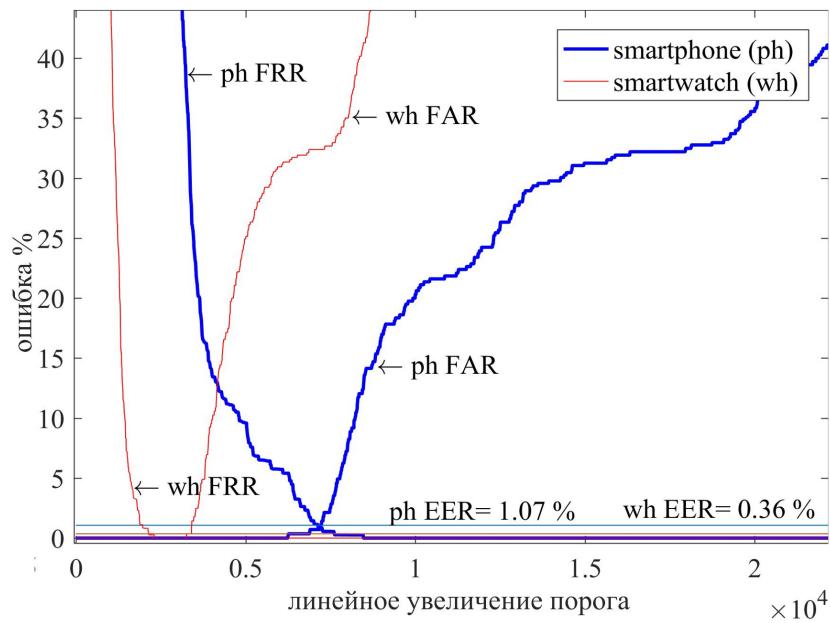


Рисунок 3.22 — Интенсивный жест.  $\beta$ ,  $\alpha$  и EER умных часов (красные графики) и смартфона (синие графики) использующего для построения матрицы расстояний расстояние городских кварталов

Таблица 5 — Результаты моделирования для двух МТДП

№	Алгоритм	Спокойный жест		Интенсивный жест	
		смартфон, %	часы, %	смартфон, %	часы, %
1	Расстояние Евклида	57,4	66,7	28,6	11,7
2	Квадратичное расстояние Евклида	80,3	56,9	28,7	10,3
3	Расстояние городских кварталов	70,7	58,4	36,7	7,9
4	Расстояние Чебышева	82,7	60,4	28	7,6
5	Косинусное расстояние	24,2	16,3	25,4	14,7
6	Корреляционное расстояние	25,4	14,7	30,6	11
7	DTW с использованием алгоритма Евклида	8,6	2,6	1,1	0,36
8	DTW с использованием квадрата алгоритма Евклида	7,6	2,1	0,36	0,71
9	DTW с использованием алгоритма городских кварталов	8,6	2,6	1,1	0,36

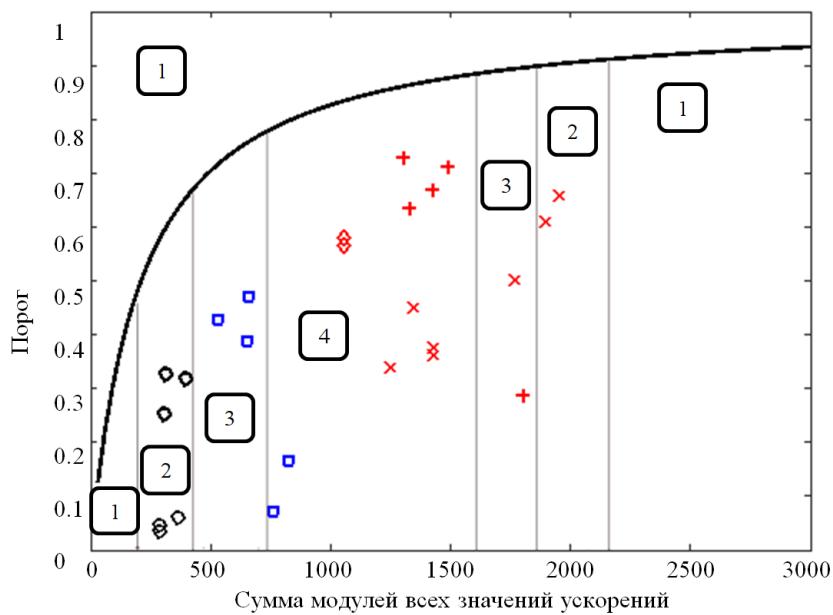


Рисунок 3.23 — Результаты опробования первого макета

### 3.4.3 Тестирование методики ранжирования надежности МТДП по сумме значений всех ускорений

На рисунке 3.23 представлены результаты тестирования работы методики классификации надежности МТДП, использующей ранжирование по сумме значений всех ускорений, при этом из показаний была убрана гравитационная составляющая.

На рисунке 3.23, кроме ограничения, заданного по формуле 2.18 показаны зоны, ранжированные по величине  $M$ :

1. Зона недопустимых жестов;
2. Зона жестов с низкой надежностью;
3. Зона жестов с низкой надежностью;
4. Зона жестов с высокой надежностью.

Для каждого представленного на рисунке МТДП были проведены проверки воспроизводимости, около десяти для каждого жеста и не менее пяти попыток взлома. Проверку методики ранжирования можно провести на некритичных приложениях при использовании в эксплуатации различных марок смартфонов.

### 3.5 Реализация электромеханического замка интеллектуального замка на базе биометрической аутентификации с использованием механизма жестовой манипуляции

#### 3.6 Выводы к главе

Разработанный макет системы аутентификации с помощью механизмов жестовой манипуляции (мультимодальной трехмерной динамической подписи) позволил доказать повышенную надежность примененных решений с помощью эксперимента. В результате проведенных опытов в которых участвовало около 15 человек удалось собрать базу данных попыток аутентификации, которая позволила определить уровень ошибок первого и второго рода, а так же устойчивость МТДП к спуфингу.

Достигнутые результаты позволяют утверждать, что применение МТДП позволит повысить надежность систем аутентификации в мобильных приложениях за счет следующих факторов:

1. Наручное устройство будет являться ключом (токеном) для аутентификации в мобильном устройстве, реализуя проверку по технологии «что пользователь имеет». В случае кражи любого из устройств доступ злоумышленника к данным пользователя будет закрыт.
2. Наручное устройство, совместно с мобильным, будут задействованы в аутентификации, использующей жестовую манипуляцию, и, следовательно являющуюся биометрической, относящейся к классу «что есть сам человек». При этом регистрация биометрического признака (в данной работе в качестве него выбран жест) проводится датчиками двух устройств, одновременно контактирующими с разными частями тела человека - с кистью руки и запястьем, и следовательно, учитывающими большее количество информации о биометрическом признаком по сравнению с аналогичной методикой, использующей только одно устройство.
3. Аутентификация при помощи двух устройств использует механизм жестовой манипуляции, и подразумевает, что пользователь должен знать и уметь выполнить определенный заранее придуманный жест. Такую аутентификацию можно отнести к классу «что человек знает»

## Глава 4. Практическая реализация мобильного приложения с аутентификацией пользователя с использованием механизма жестовой манипуляции в системах разграничения доступа

### **4.1 Удаленная аутентификация пользователей с использованием механизма жестовой манипуляции в мобильных приложениях**

Особенностью систем аутентификации в мобильных приложениях является высокая частота прохождения такой процедуры. Это связано с их портативностью, использованию в общественных сетях и высоким риском потери или кражи, а так же возможности мгновенного их использования злоумышленником сразу после попадания к нему в руки.

В связи с этой особенностью в том числе прорабатываются методики непрерывной аутентификации, в том числе биометрические [44].

Небиометрические методики представлены в настоящее время только как разблокировка мобильного устройства носимым устройством.

Однако существует класс задач, где для мобильных приложений не требуется частая аутентификация. К таким задачам можно отнести:

- доступ к приложению, хранящие не часто используемые данные (это может быть облачный сервис с архивом документов);
- доступ через мобильные приложения к устройствами умного дома (контроль таких устройств редко требует непрерывного наблюдения, при этом злоумышленник может принести значительный ущерб в случае доступа к оборудованию);
- аутентификация выполняющаяся с невысокой периодичностью (например социальные сети, где повторную аутентификацию можно проводить только в случае длительной паузы в использовании).
- доступ в мобильные приложения при работе внутри защищенных помещений (в случае переключения от работы сети оператора к работе в корпоративной сети внутри здания).
- при работе с мобильными приложениями, являющимися частью систем аутентификации при разграничении доступа к физическим объектам. Подробнее этот случай рассмотрен в разделе 4.2.

Алгоритмы работы систем аутентификации в сетях могут строиться с различными подходами к криптографической защиты [45].

Однако, если не учитывать деталей, защита требуется везде, где происходит хранение данных:

1. Применительно к клиент серверной архитектуре:

- показания акселерометра, полученные при воспроизведении жеста должны шифроваться перед отправкой на сервер;
- МТДП не должна храниться в на мобильных устройствах. Сравнение должно идти на сервере;
- МТДП, хранящаяся на сервере, должна быть защищена в соответствии с требованиями для хранения персональных данных.

2. Применительно к локальному использованию (когда мобильное приложение не имеет серверной части и осуществляет действия только в смартфоне):

- МТДП должна быть зашифровано;
- при шифровании должно быть учтено время аутентификации для устранения возможность подстановки;
- смартфон не должен хранить данных выполненных жестов.

Кроме указанных моментов должна быть предусмотрена возможность резервной аутентификации, для восстановления доступа в случае утери мобильных устройств.

## **4.2 Особенности средств и методов разграничения доступа к физическим объектам с использованием информационных технологий**

Отличительной чертой современного развития индустрии эксплуатации зданий является высокий уровень автоматизации с широким использованием информационных технологий, где человек является активным участником процесса [46].

Особенно актуально это в связи с наличием тенденции к изменению стратегий проектирования инфраструктуры в целом. Например, после теракта 11 сентября в США был принят свод документов, например таких как UFC 4-010-01, который включает в себя подробные рекомендации по разграничению и контролю

доступа для жилых и промышленных зданий города, а критически важные объекты рассматриваются как состоящие из «человеческого капитала, физических и кибернетических систем, совместно работающих в процессах, отличающихся высокой степенью взаимозависимости» [47].

Разнообразные запирающие устройства являются неотъемлемой частью систем разграничения доступа и охраны помещений. Как правило до настоящего времени подавляющим устройством отпирания являлся физический ключ, который мог представлять собой не только металлический предмет, но и смарт-карту или какой либо иной вид токена.

Использование информационный технологий позволяет по новому подойти к вопросам обеспечения безопасности ресурсов или документов, представленных физическими объектами и требующими учета и недопущения до них злоумышленников. Например, администраторы безопасности широко используют системы регистрации событий в том числе проникновения в помещения. К сожалению иногда такие системы могут зафиксировать лишь использование ключа, но ни как не личность, которая его использовала.

Преодолеть данную проблему можно используя для доступа биометрические данные в качестве ключей, например вход по отпечатку пальца. Разрабатываются и более сложные системы, анализирующие параметры лиц пользователей [48].

Использование информационных технологий и биометрических системам аутентификации дает неоспоримое преимущества перед остальными системами, а именно:

- возможность использования оповещения о состоянии, например с использованием мобильного приложения;
- возможность автоматической непрерывной передачи состояния и, как следствие, использование его как часть системы контроля объекта в целом (например, для контроля безопасности на предприятии или в проектах типа «Умный дом» или «Безопасный город»);
- возможность использования неотъемлемых (биометрических) идентификаторов без опасений в возможности их утери;
- существенное сокращение возможностей классического взлома, такого как подбор ключа или использование отмычек.

К сожалению некоторые биометрические системы имеют ограничения в применении. Что касается отпечатков пальцев, то их уязвимость уже была от-

мечена в Разделе 1, в тоже время сложные интеллектуальные системы требуют подключения к мощным вычислительным устройствам, требующих значительного пространства и затрат на электроэнергию.

Существует класс систем хранения материальных ценностей имеющих особое значение - это многочисленные виды железных шкафов и сейфов. Они безусловно требуют внимательного надзора и могут хранить особо значимые ценности, в том числе информацию, составляющую государственную тайну.

В продаже сегодня существуют модификации, где в качестве идентификатора может служить пароль или отпечаток пальца.

Итак, в качестве особенностей появившихся в системах разграничения доступа на физическом уровне, использующих информационные технологии, можно отметить следующие:

- использование систем аутентификации, позволяющих идентифицировать личность, вместо систем предоставляющих доступ по паролю или при помощи ключа;
- агрегация информации в информационных системах;
- использование мобильных приложений для контроля состояния объектов.

Грубо системы контроля на физическом уровне можно разделить на две части - информационная система и запирающие устройства.

Задачи запирающих устройств в системах разграничения доступа можно разделить на следующие крупные группы:

- контроль доступа на контролируемую территорию;
- контроль доступа в здания (в том числе в подъезды жилых домов);
- контроль доступа в помещения (в том числе в квартиры);
- контроль доступа к ценностям хранящимся в железных шкафах и сейфах.

Для всех случаев, приведенных выше могут быть применены биометрические методы аутентификации для получения доступа.

### 4.3 АПК «Замок МТДП»

Для хранения документации и иных материальных ценностей в было разработано запирающее устройство, для сейфов и несгораемых шкафов, используя-

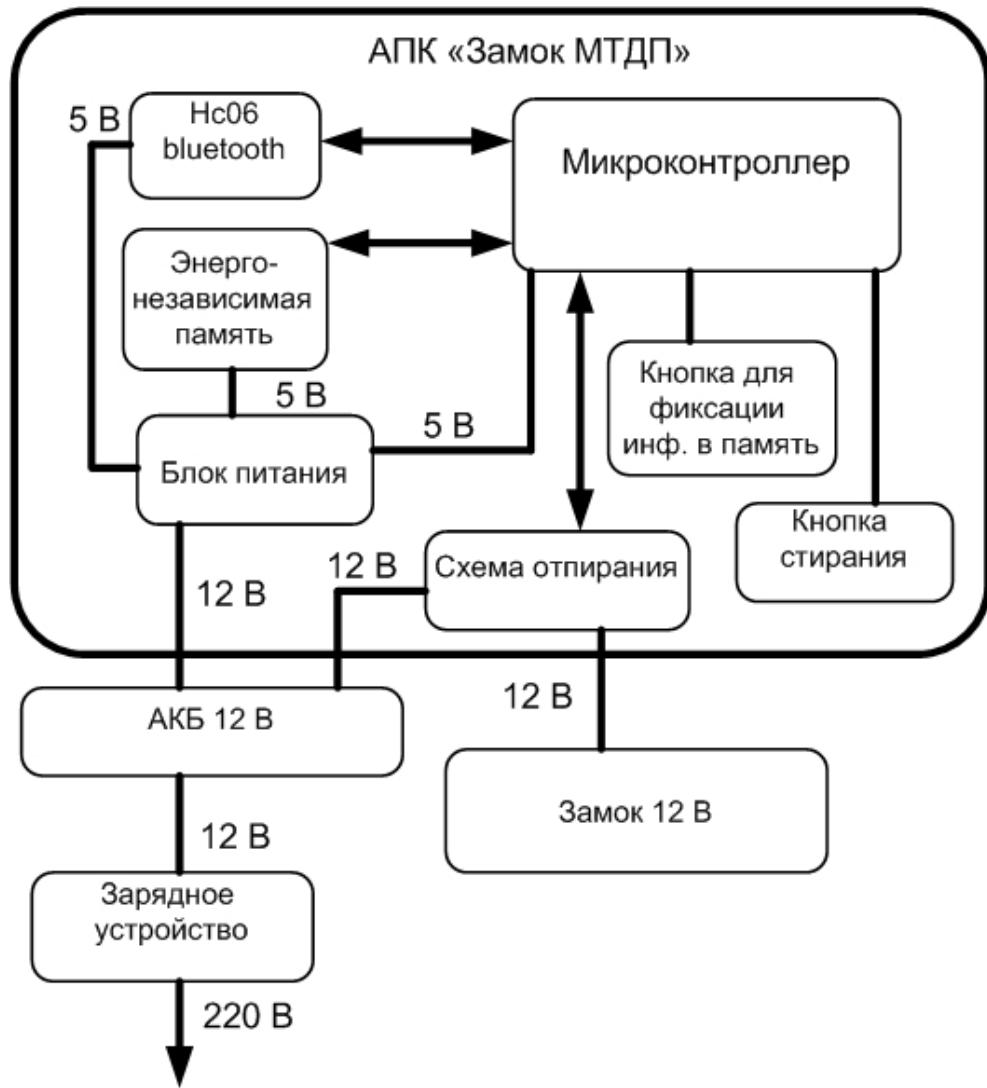


Рисунок 4.1 – Функциональная схема АПК «Замок-МТДП»

ющее мульимодальную аутентификацию с использованием механизма жестовой манипуляции.

Устройство состоит из двух частей - мобильного приложения, осуществляющего аутентификацию и отправляющее сигнал об отпирании или запирании устройства, и запирающего устройства, представляющего собой нормально закрытый электромеханический замок и микроконтроллер с модулем bluetooth, управляющий замком.

Функциональная схема микроконтроллера и замка представлена на рисунке 4.1.

Отличительной особенностью конструкции является отсутствие внешних признаков установки. Злоумышленник может не подозревать о установке замка. Таким образом замок более защищен от традиционных методов взлома по сравне-

нию с классическими замками использующими различные модификации ключей такими [49]:

- взлом при помощи подбора ключа или изготовление дубликата;
- вы сверливание цилиндра;
- использование свертыша;
- бампинг;
- использование отмычек;
- переламывание цилиндрового механизма пополам
- химический взлом.

Использование радиоуправляемых замков широко распространено как для обеспечения безопасности квартир, так и для применения в составе несгораемых шкафов и сейфов. Все имеющиеся устройства можно разделить на два типа, первый предполагает наличие отдельного пульта или цифрового ключа, второй предполагает использование мобильного приложения.

Подобные устройства имеют те же подходы к аутентификации пользователя. Как правило, считается, что в случае потери ключа или телефона у пользователя будет достаточно времени для удаления потерянных «ключей» из базы замка.

Аппаратно-программный комплекс «Замок-МТДП» был установлен в группе главного конструктора АО «НИИЧаспром» для хранения материально-технических ценностей. За время временной эксплуатации для устройства силами коллектива был проведен эксперимент по спуфингу системы, показавший высокую надежность примененной в АПК системы аутентификации.

#### 4.4 Выводы к главе

Глава описывает примеры реализации методики, представленной в диссертационном исследовании, в том числе применение одного из образцов в реальных условиях.

Применение АПК «Замок-МТДП» кроме повышения безопасности хранения дало возможность решить еще несколько задач:

- регистрацию состояний (кто отпирал замок, когда он был закрыт);
- подключение к системе оповещения об открытии замка;

- легкую смену сопряженных устройств (в качестве ключей используются личные смартфоны и умные часы сотрудников).

## Заключение

Основные результаты работы заключаются в следующем:

1. На основе анализа механизмов жестовой манипуляции была разработана концепция методики мультимодальной биометрической аутентификации с использованием двух независимых мобильных устройств - смартфона и умных часов.
2. Создан макет для умных часов и смартфона, реализующий аутентификацию, а также сохраняющей данные аутентификации в виде массива временных рядов.
3. Макет был опробован и доработан в рамках научно-исследовательских работ «Финансового Университета» и поставлен на баланс как результат интеллектуальной деятельности Университета.
4. При участии группы людей, с использованием макета, была создана база данных попыток аутентификации, составляющая более тысячи попыток.
5. С использованием базы данных попыток аутентификации было проведено моделирование, определившее уровни равновероятного соотношения ошибок первого и второго уровня (комплексные показатели качества) для различных алгоритмов и определен наиболее удовлетворяющий с точки зрения надежности - алгоритм динамической трансформации шкалы времени с использование алгоритма Евклида для формирования матрицы расстояния.
6. С применением выбранного алгоритма реализован аппаратно-программный комплекс «Замок-МТДП» - осуществляющий аутентификацию и открытие замка при помощи механизма жестовой манипуляции применяемого для помещений или сейфовых хранилищ предприятия.
7. Аппаратно-программный комплекс применен для хранения материальных ценностей на предприятии АО «НИИЧаспром» и прошел успешную опытную эксплуатацию. Применение АПК «Замок-МТДП» позволило повысить надежность хранения ценностей.

Полученные результаты позволяют говорить об отработанности методики, и готовности внедрение ее в те сферы обеспечения информационной безопасности, где необходимо проводить скрытую и надежную аутентификацию - например

аутентификацию в мобильных приложениях, предполагающих работу в людных местах.

Вторым направлением применения методики могут стать биометрические замки для различных сфер применения со сниженным уровнем энергопотребления.

В заключение автор выражает благодарность и большую признательность сотрудникам кафедры «Информационная безопасность» - научному руководителю Евсееву Владимиру Леоновичу за поддержку, помощь, обсуждение результатов и научное руководство, также Дворянкину Сергею Владимировичу за методические рекомендации и помошь в системотехническом подходе к исследованию.

**Список сокращений и условных обозначений**

<b>МТДП, МТДС</b>	мультимодальная трехмерная динамическая подпись, multimodal three-dimensional dynamic signature
<b>DTW</b>	Dynamic Time Warping – алгоритм динамической трансформации шкалы времени
<b>ФДКН</b>	функционально-динамический комплекс навыков
<b>СМС</b>	служба коротких сообщений
<b>АПК</b>	аппаратно-программный комплекс
<b>k-NN</b>	k-nearest neighbors algorithm – метрический алгоритм для автоматической классификации объектов или регрессии
$\alpha$	вероятность ошибки первого рода, FAR -False Acceptance Rate, $\alpha$ errors - вероятность ложного допуска
$\beta$	вероятность ошибки второго рода, FRR - False Rejection Rate, $\beta$ errors - вероятность ложного отказа

## Словарь терминов

**Биометрия** : Система распознавания людей по одной или более физическим или поведенческим чертам

**Механизм жестовой манипуляции** : Специальный жест в воздухе, выполняемый одним или несколькими мобильными устройствами одновременно, используемый для аутентификации

**Сниффинг** : Перехват и анализ сетевого трафика (своего и/или чужого)

**Спупинг** (англ. spoofing — подмена) : Вид хакерской атаки, заключающийся в использовании чужих данных с целью обмана системы безопасности, например — это может быть попытка воспроизвести аутентифицирующий жест субъекта подсмотрев его каким либо образом

**Социальная инженерия** : Способ манипулирования людьми опирающийся в основном на знания психологии

**Фишинг** (англ. phishing, от fishing) : Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Достигается путём проведения массовых рассылок электронных писем от имени популярных брендов и личных сообщений внутри различных сервисов

**Троянский конь** : Разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения

**Компьютерный вирус** : Вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи

**Идентификатор** : Уникальный признак объекта, позволяющий отличать его от других объектов

**Токен** : Компактное устройство, предназначенное для обеспечения информационной безопасности пользователя, также используется для идентификации его владельца, безопасного удалённого доступа к информационным ресурсам и т. д. Как правило, это физическое устройство, используемое для упрощения аутентификации

**Интернет вещей (англ. Internet of Things, IoT)** : Концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой

**Смартфон:** (англ. smartphone — умный телефон) - мобильный телефон, дополненный функциональностью карманного персонального компьютера

**Контент :** Содержимое - любое информационное наполнение вся информация, которую пользователь сможет загрузить на своё медиаустройство, например смартфон

**Медиаконтент:** Контент, содержащий звуковую и визуальную информацию

**Пин-код:** (англ. Personal Identification Number — персональный идентификационный номер) — аналог пароля

**Масса МТДП:** Условное обозначение суммы модулей всех элементов временных рядов по осям  $X$ ,  $Y$ ,  $Z$  для МТДП

**Масса временного ряда:** Условное обозначение суммы модулей всех элементов временного ряда

**Порог отсечки:** Максимальное значение меры различия выше которой будет происходить отказ в принятии биометрического признака (отказ в аутентификации)

## Список литературы

1. Самойлова, Е. О. Трансформации бытия современного человека в условиях развития информационных технологий и интернета вещей / Е. О. Самойлова, Ю. М. Шаев // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. — 2016. — № 12/3. — С. 158—161.
2. Богданов, Е. А. Обзор уязвимостей биометрических систем аутентификации / Е. А. Богданов, А. Р. Айдинян // Роль инноваций в трансформации современной науки. — 2017. — С. 25—27.
3. Авдеенко, Т. Цифровизация экономики на основе совершенствования экспериментальных систем управления знаниями / Т. Авдеенко, А. А. Алетдинова // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. — 2017. — Т. 10, № 1.
4. Руководство по биометрии / Р. М. Болл [и др.]. — Москва : Техносфера, 2007. — 370 с.
5. Regulation, G. D. P. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / G. D. P. Regulation // Official Journal of the European Union (OJ). — 2016. — Vol. 59. — P. 1—88.
6. Gao, Y. Semi-supervised sparse representation based classification for face recognition with insufficient labeled samples / Y. Gao, J. Ma, A. L. Yuille // IEEE Transactions on Image Processing. — 2017. — Vol. 26, no. 5. — P. 2545—2560.
7. Темлянцев, А. С. Разработка информационной системы для распознавания подписей / А. С. Темлянцев // Вестник научного общества студентов, аспирантов и молодых ученых. — 2015. — № 3. — С. 209—212.
8. Shrestha, B. Wave-to-Access: Protecting Sensitive Mobile Device Services via a Hand Waving Gesture / B. Shrestha, N. Saxena, J. Harrison // Cryptology and Network Security. — 2013. — Nov. 20. — P. 199—217. — (Lecture Notes in Computer Science). — (Visited on 02/25/2018).

9. *Imura, S.* A hand gesture-based method for biometric authentication / S. Imura, H. Hosobe. — 2018.
10. *Xu, C.* Finger-writing with smartwatch: A case for finger and hand gesture recognition using smartwatch / C. Xu, P. H. Pathak, P. Mohapatra // Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications. — ACM. 2015. — P. 9—14.
11. *Liang, G.* User-Authentication on Wearable Devices Based on Punch Gesture Biometrics / G. Liang, X. Xu, J. Yu // ITM Web of Conferences. Vol. 11. — EDP Sciences. 2017. — P. 1—9.
12. *Griswold-Steiner, I.* Handwriting watcher: A mechanism for smartwatch-driven handwriting authentication / I. Griswold-Steiner, R. Matovu, A. Serwadda. — 2017.
13. Authentication of smartphone users based on activity recognition and mobile sensing / M. Ehatisham-ul-Haq [et al.] // Sensors. — 2017. — Vol. 17, no. 9. — P. 2043.
14. *Козлов, Ю. Е.* Современные методы речевой аутентификации в приложениях мобильных устройств / Ю. Е. Козлов, В. Л. Евсеев // Безопасность информационных технологий. — 2016. — Т. 23, № 1. — С. 32—36.
15. Fingerprint vendor technology evaluation / C. I. Watson [et al.] // NIST Interagency/Internal Report (NISTIR)-8034. — 2015.
16. *Тулупьева, Т. В.* Психологические аспекты оценки безопасности информации в контексте социоинженерных атак / Т. В. Тулупьева, А. Л. Тулупьев, А. А. Азаров // Медико-биологические и социально-психологические проблемы безопасности в чрезвычайных ситуациях. — 2016. — № 1. — С. 77—83.
17. *Шакер, И. Е.* Использование биометрической аутентификации и перспективы ее применения в банковской системе России / И. Е. Шакер // Экономика. Налоги. Право. — 2016. — № 5. — С. 85—86.
18. *Albladi, S. M.* User characteristics that influence judgment of social engineering attacks in social networks / S. M. Albladi, G. R. Weir // Human-centric Computing and Information Sciences. — 2018. — Vol. 8, no. 1. — P. 5.
19. Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment / A. K. Das [et al.]. — 2017. — Sept. 18.

20. *Patel, V. M.* Cancelable biometrics: A review / V. M. Patel, N. K. Ratha, R. Chellappa // IEEE Signal Processing Magazine. — 2015. — Vol. 32, no. 5. — P. 54—65.
21. *Czajka, A.* Presentation attack detection for iris recognition: an assessment of the state of the art / A. Czajka, K. W. Bowyer // arXiv preprint arXiv:1804.00194. — 2018.
22. Attack potential evaluation in desktop and smartphone fingerprint sensors: can they be attacked by anyone? / I. Goicoechea-Telleria [et al.] // Wireless communications and mobile computing. — 2018. — Vol. 2018.
23. A spoofing benchmark for the 2018 voice conversion challenge: Leveraging from spoofing countermeasures for speech artifact assessment / T. Kinnunen [et al.] // arXiv preprint arXiv:1804.08438. — 2018.
24. A survey of wearable biometric recognition systems / J. Blasco [et al.] // ACM Computing Surveys (CSUR). — 2016. — Vol. 49, no. 3. — P. 43.
25. *Michalevsky, Y.* Gyrophone: Recognizing Speech from Gyroscope Signals. / Y. Michalevsky, D. Boneh, G. Nakibly // USENIX Security Symposium. — 2014. — P. 1053—1067.
26. *Козлов, Ю. Е.* Метаматематическая модель мультимодальной жестовой аутентификации при помощи двух независимых мобильных устройств / Ю. Е. Козлов, В. Л. Евсеев // Безопасность информационных технологий. — 2017. — Т. 24, № 1. — С. 49—55.
27. *Алюшин, А. М.* Оценка психоэмоционального состояния человека по его подписи / А. М. Алюшин // Вопросы психологии. — 2018. — № 2. — С. 133—140.
28. Querying and mining of time series data: experimental comparison of representations and distance measures / H. Ding [et al.] // Proceedings of the VLDB Endowment. — 2008. — Vol. 1, no. 2. — P. 1542—1552.
29. *Деза, Е. И.* Энциклопедический словарь расстояний / Е. И. Деза, М. М. Деза. — Москва : Наука, 2008. — 448 с.
30. Speeding up dynamic time warping distance for sparse time series data / A. Mueen [et al.] // Knowledge and Information Systems. — 2018. — Vol. 54, no. 1. — P. 237—263.

31. uWave: Accelerometer-based personalized gesture recognition and its applications / J. Liu [et al.] // Pervasive and Mobile Computing. — 2009. — Vol. 5, no. 6. — P. 657—675.
32. Akl, A. Accelerometer-based gesture recognition via dynamic-time warping, affinity propagation, & compressive sensing / A. Akl, S. Valaee // 2010 IEEE International Conference on Acoustics, Speech and Signal Processing. — IEEE. 2010. — C. 2270—2273.
33. Google, i. Motion Sensors - Android Developers / i. Google. — 2018. — URL: [https://developer.android.com/guide/topics/sensors/sensors\\_motion.html](https://developer.android.com/guide/topics/sensors/sensors_motion.html) (visited on 03/06/2018).
34. Козлов, Ю. Е. Экспериментальное определение уровня речевого сигнала в показаниях акселерометра мобильных устройств / Ю. Е. Козлов, В. Л. Евсеев // Вопросы кибербезопасности. — 2016. — № 5. — С. 37—42.
35. Б.Л., В.-д.-В. Математическая статистика / В.-д.-В. Б.Л. — Москва : Изд-во иностранной литературы, 1960. — 435 с.
36. Козлов, Ю. Е. Мультимодальная трехмерная динамическая подпись / Ю. Е. Козлов, В. Л. Евсеев // Безопасность информационных технологий. — 2017. — Т. 24, № 4. — С. 44—51.
37. Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персепtronами / П. С. Ложников [и др.] // Информационно-управляющие системы. — 2016. — № 5. — С. 73—85.
38. Compression of deep convolutional neural networks for fast and low power mobile applications / Y.-D. Kim [et al.] // arXiv preprint arXiv:1511.06530. — 2015.
39. Recognizing human activity in mobile crowdsensing environment using optimized k-NN algorithm / A. Tharwat [et al.] // Expert Systems With Applications. — 2018. — Vol. 107. — P. 32—44.
40. Kaur, J. A comparison of artificial neural network and k-nearest neighbor classifiers in the off-line signature verification / J. Kaur, S. Dr. Reecha // International Journal of Advanced Research in Computer Science. — 2017. — Vol. 8, no. 7. — P. 380—383.
41. Human Activity Recognition using Embedded Smartphone Sensors / R. Deshmukh [et al.]. — 2018.

42. *Maro, J.-M.* Event-based Gesture Recognition with Dynamic Background Suppression using Smartphone Computational Capabilities / J.-M. Maro, R. Benosman // arXiv preprint arXiv:1811.07802. — 2018.
43. Application of LCS algorithm to authenticate users within their mobile phone through in-air signatures / J. Guerra-Casanova [et al.] // Advanced Biometric Technologies. — InTech, 2011.
44. Gesture-based continuous authentication for wearable devices: the google glass case / J. Chauhan [et al.] // arXiv preprint arXiv:1412.2855. — 2014. — Р. 1—28.
45. *Фомичев, В.* Криптографические методы защиты информации (в 2-х частях): Учебник / В. Фомичев, Д. Мельников. — 2016.
46. *Силюянов, А. В.* Анализ эргономичности интерфейсов управления интеллектуальными зданиями / А. В. Силюянов, И. Н. Пономаренко // Электротехнические и информационные комплексы и системы. — 2012. — Т. 8, № 3.
47. Умные города, инфраструктуры и их антитеррористическая устойчивость. Опыт интеграции антитеррористических стандартов США и создания программного обеспечения для цифровой безопасности / И. А. Соколов [и др.] // International Journal of Open Information Technologies. — 2017. — Т. 5, № 7.
48. *Юркин, В. А.* Разработка системы контроля и управления доступом «Умный замок», способной идентифицировать пользователей по объемным моделям лиц, построенных с помощью стереокамеры, а также анализируя мимические движения мышц лица / В. А. Юркин, С. А. Басов // Современные проблемы науки и образования. — 2016. — С. 324—327.
49. *Рясов, А. А.* Способы взлома запирающих устройств и их криминалистическое значение / А. А. Рясов, Г. Г. Жигалова // Мир науки, культуры, образования. — 2015. — № 4. — С. 229—231.

## Список рисунков

1.1 Классификация биометрических методов, используемых для аутентификации в мобильных приложениях . . . . .	<b>16</b>
1.2 Пример мультимодальной трехмерной динамической подписи . . . . .	<b>29</b>
2.1 Алгоритм «uWave» . . . . .	<b>39</b>
2.2 Схема функционирования аутентификации на базе МТДП . . . . .	<b>41</b>
2.3 Схема функционирования аутентификации на базе МТДП (без проверки корреляции траекторий устройств) . . . . .	<b>42</b>
2.4 Укрупненный алгоритм формирования МТДП . . . . .	<b>45</b>
2.5 Укрупненный алгоритм формирования МТДП . . . . .	<b>47</b>
2.6 Трехслойная нейронная сеть . . . . .	<b>53</b>
3.1 Сигнал акселерометра мобильного устройства, удерживаемого неподвижно в руке . . . . .	<b>58</b>
3.2 Распределение попыток аутентификации для спокойного жеста . . . . .	<b>61</b>
3.3 Распределение попыток аутентификации для интенсивного жеста . . . . .	<b>62</b>
3.4 Распределение попыток аутентификации для спокойного жеста . . . . .	<b>63</b>
3.5 Распределение попыток аутентификации для интенсивного жеста . . . . .	<b>63</b>
3.6 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Евклида . . . . .	<b>65</b>
3.7 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Евклида . . . . .	<b>66</b>
3.8 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании квадратичного расстояния Евклида . . . . .	<b>66</b>
3.9 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании квадратичного расстояния Евклида . . . . .	<b>67</b>
3.10 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании расстояния городских кварталов . . . . .	<b>67</b>

3.11 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании расстояния городских кварталов . . . . .	68
3.12 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Чебышева . . . . .	68
3.13 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании алгоритма Чебышева . . . . .	69
3.14 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании косинусной меры . . . . .	69
3.15 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании косинусной меры . . . . .	70
3.16 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании корреляционного расстояния . . . . .	70
3.17 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) при использовании корреляционного расстояния . . . . .	71
3.18 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) с использованием алгоритма DTW, использующего для построения матрицы расстояний расстояние Евклида . . . . .	71
3.19 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) с использованием алгоритма DTW, использующего для построения матрицы расстояний расстояние Евклида . . . . .	72
3.20 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) с использованием алгоритма DTW, использующего для построения матрицы расстояний квадрат расстояния Евклида . . . . .	73
3.21 Спокойный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) использующего для построения матрицы расстояний расстояние городских кварталов . . . . .	73
3.22 Интенсивный жест. $\beta$ , $\alpha$ и EER умных часов (красные графики) и смартфона (синие графики) использующего для построения матрицы расстояний расстояние городских кварталов . . . . .	74

3.23 Результаты опробования первого макета . . . . .	75
4.1 Функциональная схема АПК «Замок-МТДП» . . . . .	81

**Список таблиц**

1	Значения ошибок $\alpha$ и $\beta$ для наиболее распространенных биометрических методик . . . . .	16
2	Методики аутентификации при воздействии разных внешних факторов . . . . .	26
3	Влияние внешних факторов в городских условиях . . . . .	26
4	Сумма значений ускорений для разных жестов . . . . .	51
5	Результаты моделирования для двух МТДП . . . . .	74

**Приложение А**

**Диплом 2 степени за доклад на молодежной конференции «Информационная безопасность в банковско-финансовом секторе» в рамках IV международного форума Финансового Университета**



## Приложение Б

### Приказ о корректировке темы



Федеральное государственное образовательное бюджетное  
учреждение высшего образования  
**«Финансовый университет при Правительстве Российской Федерации»**  
**(Финансовый университет)**

#### ПРИКАЗ

«23» апреля 2018 г.

№ 0950/0

Москва

#### **Об утверждении тем научно-квалификационных работ (диссертаций) аспирантам**

В соответствии с пунктом 2.4 Порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам подготовки научно-педагогических кадров в аспирантуре, утвержденного приказом Финуниверситета от 23.01.2017 № 0056/о, приказываю:

утвердить в новой редакции темы научно-квалификационных работ (диссертаций) на соискание ученой степени кандидата наук по научной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» аспирантам 3 курса кафедры «Информационная безопасность», обучающимся по направлению подготовки 10.06.01 Информационная безопасность (направленность программы «Методы и системы защиты информации, информационная безопасность»), согласно приложению.

Основание: выписка из протокола заседания Ученого совета Факультета прикладной математики и информационных технологий от 17.04.2018 № 04.

Ректор

М.А. Эскиндаров

63095

Приложение  
к приказу Финуниверситета  
от 23.04. 2018 г. № 0950/0

**СПИСОК**  
тем научно-квалификационных работ (диссертаций)

№	Ф.И.О. аспиранта	Тема научно-квалификационной работы (диссертации)
1.	Козлов Ю.Е.	Разработка и исследование методов мультимодальной аутентификации пользователей мобильных приложений с использованием механизма жестовой манипуляции
2.	Кузнецов А.В.	Разработка математического аппарата комплексной обработки потоков информации о событиях безопасности в автоматизированных системах специального назначения
3.	Ненашев С.М.	Метод оптимизации противодействия угрозам информационной безопасности банков со стороны социальных сетей
4.	Устинов Р.А.	Разработка и исследование методов бинаризации изображений сонограмм в решении задач защиты речевой информации

Начальник  
Управления аспирантуры

М.М. Пухова