Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
институт

Межинститутская базовая кафедра
«Прикладная физика и космические технологии»
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ В.Е. Косенко
подпись инициалы, фамилия
«_____» _____2023 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

«Разработка методики валидации пользователя по текстовому следу с помощью экспертной системы»
тема

09.04.01 «Информатика и вычислительная техника»
код и наименование направления

09.04.01.03 «Информационные системы космических аппаратов и центров управления полетами»
код и наименование магистерской программы

Руководитель	_____	доцент МБК ПФ и КТ, канд. техн. наук	В.А. Углев
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		А.О. Кириличев
	подпись, дата		инициалы, фамилия
Рецензент	_____	згд по качеству АО «РЕШЕТНЁВ», канд. техн. наук	Ю.В. Кочев
	подпись, дата	должность, ученая степень	инициалы, фамилия
Нормоконтролер	_____	профессор МБК ПФиКТ, д-р техн.наук	В.Е. Чеботарев
	подпись, дата	должность, ученая степень	инициалы, фамилия

Красноярск 2023

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
институт

Межинститутская базовая кафедра
«Прикладная физика и космические технологии»
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ В.Е. Косенко
подпись инициалы, фамилия
«_____» _____2023 г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ
в форме магистерской диссертации

Красноярск 2023

Студенту Кириличев Александр Олегович
фамилия, имя, отчество

Группа КИ21-01-3М Направление (специальность) 09.04.01
номер код

«Информатика и вычислительная техника»
полное наименование

Тема выпускной квалификационной работы «Разработка методики валидации пользователя по текстовому следу с помощью экспертной системы»

Утверждена приказом по университету от 20.03.2023 № 4434/С

Руководитель ВКР Виктор Александрович Углев, кандидат технических наук, доцент МБК «Прикладная физика и космические технологии», СФУ

Исходные данные для ВКР: в рамках ВКР разрабатывается методика валидации пользователя по текстовому следу с помощью экспертной системы

Перечень разделов ВКР введение; исследование предметной области; разработка методики валидации пользователя по текстовому следу с помощью экспертной системы; экспериментальная проверка; заключение.

Перечень графического материала презентация PowerPoint.

Руководитель ВКР _____ В.А. Углев
подпись инициалы и фамилия

Задание принял к исполнению _____ А.О. Кириличев
подпись инициалы и фамилия

«___» _____ 20__г.

РЕФЕРАТ

Выпускная квалификационная работа по теме «Разработка методики валидации пользователя по текстовому следу с помощью экспертной системы» содержит 77 страниц текстового документа, 36 использованных источников.

ТЕХНОЛОГИИ, ПРОДУКЦИОННЫЕ ПРАВИЛА, ФАЗИФИКАЦИЯ, ГИПОТЕЗЫ, ВАЛИДАЦИЯ, ИДЕНТИФИКАЦИЯ, ЭКСПЕРТНАЯ СИСТЕМА.

Цель работы: «Разработка методики валидации пользователя по текстовому следу с помощью экспертной системы».

Задачи исследования:

– анализ предметной области, анализ существующих методик валидации;

– разработка экспертной системы, которая позволит оценивать степень валидации пользователя;

– разработка новой методики валидации пользователя для автоматизированной информационной системы на базе экспертной системы;

– экспериментальный анализ качества методики.

В ходе научно-исследовательской работы описаны проблемы и цели исследования, обоснована актуальность данной темы, а также дано описание основных задач и методологий исследования. Рассмотрены существующие методы идентификации пользователя и их ограничения. Произведен сравнительный анализ различных подходов, а также выявлены преимущества и недостатки каждого метода. Разработана экспертная система, способная оценивать степень валидации пользователя на основе его текстового следа. Описана архитектура системы, принципы ее работы и используемые методы анализа текста. Представлена разработанная методика валидации пользователя, основанная на комбинациях различных параметров текстового следа. Описаны этапы методики, а также предложены алгоритмы обработки

данных и принятия решений. Описана экспериментальная проверка разработанной методики. Проведены эксперименты в ходе учебного процесса с участием студентов, проанализированы полученные данные, и произведена оценка эффективности методики. В заключении сделаны обобщения результатов исследования, подведены итоги выполненной работы и сформулированы основные выводы. Также указана научная новизна и практическая значимость данной работы.

В итоге, данная диссертационная работа представляет собой важный вклад в область валидации пользователя по текстовому следу и предлагает новый подход, который может быть применен в различных информационных системах для обеспечения безопасности и аутентификации пользователей.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В начале XXI века в сфере информационно-коммуникационных технологий обозначились новые проблемы. Темп внедрения компьютерных технологий достиг рекордных размеров. Наблюдается стремительный рост числа пользователей и информационных ресурсов глобальной сети Интернет. Сегодня с помощью Интернет люди покупают товары, заключают договора, совершают банковские и биржевые операции, получают образование, устраиваются на работу, отправляют и получают почту, узнают последние новости, знакомятся друг с другом и т.д. Ситуации, когда люди вынуждены иметь дело только с «виртуальными» образами своих партнеров, становятся привычной повседневностью. Нужны гарантии соответствия «виртуального партнера» реальному человеку, за которого он себя выдает.

Современный уровень развития информационных технологий, а также более высокие требования к обеспечению информационной безопасности привели к тому, что традиционные средства идентификации – логины, коды, ключи, карты доступа – перестают быть эффективными, что влечет за собой не только материальный ущерб из-за действий злоумышленников, но и не обеспечивает требуемую безопасность личности в информационном пространстве. Наблюдаются ситуации, когда один из пользователей сознательно передает свой пароль третьему лицу. Например, в дистанционном образовании при прохождении аттестационных заданий учащиеся готовы подменить себя более осведомленным лицом [9].

Таким образом, существуют актуальные задачи в необходимости использования более совершенных и надежных механизмов идентификации «виртуального партнера», с которым ведется общение с использованием сетей Интернет.

Решение проблемы возможно, если узнавать удаленного пользователя по уникальным и неотделимым от него признакам в режиме реального времени.

К таковым относятся физиологические (статические) и поведенческие (динамические) характеристики человека.

Целью научно-исследовательской работы является разработка методики валидации пользователя по тестовому следу с помощью экспертной системы для выявления подмены пользователя при дистанционном образовании, в ракетно-космической отрасли и других различных сферах.

Задачами являются:

– рассмотреть существующие методы валидации пользователя;

– разработать экспертную систему, которая позволит оценивать степень валидации пользователя;

– разработать новую методику валидации пользователя для автоматизированной информационной системы на базе экспертной системы;

– экспериментально подтвердить реализуемость предложенного решения.

Первая часть работы посвящена обзору существующих методов валидации пользователя и их проблемам. В ней рассмотрены различные подходы, включая биометрические методы. Особое внимание уделено их ограничениям и недостаткам, таким как сложность реализации, низкая точность или уязвимость к подмене.

Во второй части работы представлена разработанная методика валидации пользователя по текстовому следу с использованием экспертной системы. Описаны основные принципы и алгоритмы, лежащие в основе методики, а также рассмотрены технические аспекты ее реализации. Экспертная система использоваться для анализа текстовых следов и выявления характеристик, которые могут служить основой для валидации пользователя.

Третья часть работы посвящена экспериментальному подтверждению гипотезы, выдвинутой для разработанной методики. Описаны проведенные эксперименты, анализ полученных данных и оценка результатов. Рассмотрена

эффективность разработанной методики по сравнению с другими существующими подходами.

В заключительной части работы подводятся итоги проведенной работы, обобщаются результаты и делаются выводы о достигнутых результатах. Также рассмотрены возможности для дальнейших исследований и усовершенствования разработанной методики валидации пользователя по текстовому следу с помощью экспертной системы.

1 Существующие методы идентификации пользователя

Первые успехи в научных разработках средств идентификации человека были достигнуты в конце XIX в. на основе выводов антропологов о том, что геометрические размеры частей тела у разных людей никогда не совпадают полностью (метод А. Бертильона). На смену идентификации по сумме измерений в начале XX в. пришла дактилоскопия (Э. Генри), благодаря которой идентификация по отпечаткам пальцев занимала несколько минут.

Вторая половина XX в. с успехами в области средств связи, фото- и видеофиксации, появлением компьютеров и Интернета значительно продвинула идентификацию личности. Наступивший XXI в. продиктовал новые требования к системам идентификации человека, среди которых особую значимость приобретают оперативные автоматизированные методы распознавания личности с высокой точностью достигаемого результата [18].

1.1 Проблематика идентификации пользователей в информационных системах

Проблемы идентификации пользователей в информационных системах напрямую связаны с безопасностью и приватностью пользователей, а также с защитой информации, хранимой в системе. Самой распространенной проблемой при идентификации пользователей является недостаточная эффективность выбранной методики. Некоторые методы, такие как аутентификация по паролю, могут быть легко преодолены злоумышленниками при помощи методов фишинга, перехвата данных или использования слабых паролей.

Также существует проблема слишком жестких требований к проверке личности пользователя, что может приводить к дополнительным препятствиям для законных пользователей. Например, сложность

биометрических систем может вызывать трудности в работе для людей с физическими особенностями или структурными отклонениями.

Проблема недостаточной прозрачности системы заключается в том, что пользователи могут не знать, как именно система проверки идентичности работает и как их персональные данные обрабатываются. Это может привести к тому, что пользователи не будут доверять системе и откажутся от ее использования [34].

Наконец, следует учитывать проблему взлома системы в целом. Если злоумышленник получит доступ к системе, он может использовать этот доступ для изменения учетной записи или получения конфиденциальной информации.

В целом, проблематика валидации пользователей в информационных системах остается серьезным вызовом для разработчиков и администраторов информационных систем, и требует беспрерывного улучшения методик и технологий, чтобы гарантировать защиту данных и приватность пользователей.

1.2 Подходы к идентификации пользователя

Прежде чем рассматривать подходы поидентификации пользователя, разберемся что такое идентификация, аутентификация, авторизация, верификация и валидация и чем они отличаются друг от друга.

Идентификация, аутентификация, авторизация, верификация и валидация – это различные процессы, которые используются в контексте информационной безопасности и управления доступом к ресурсам. Несмотря на то, что эти термины часто используются взаимозаменяемо, они имеют существенные отличия.

Идентификация – это процесс определения личности пользователя на основе представленных им учетных данных, таких как имя пользователя, пароль, номер общей подписи и т.д. При этом не происходит проверка

правильности введенных данных. Как правило, идентификация выполняется в начале сеанса работы пользователя в системе.

Аутентификация – это процесс проверки подлинности пользователя на основе учетных данных, которые были указаны в процессе идентификации. Данная процедура выполняется перед началом работы пользователя в системе и позволяет установить, действительно ли введенные им учетные данные принадлежат ему.

Авторизация – это процесс предоставления пользователю доступа к ресурсам и возможностям системы, после успешной аутентификации. Авторизация может быть основана на ролях, разрешениях и других установленных правилах доступа.

Верификация – это процесс подтверждения подлинности документов, данных и информации. Она проводится путем сравнения предоставленных данных с исходными данными в источнике. Наиболее распространенная форма верификации – это сверка подписей или номеров документов.

Валидация – это процесс проверки подлинности пользователя на основе данных, полученных от него в процессе работы с системой. Валидация может использовать данные о поведении пользователя, его биометрические данные и другие параметры. Валидация обеспечивает более высокий уровень проверки, чем аутентификация.

Таким образом, идентификация и аутентификация позволяют определить личность пользователя и проверить его подлинность на основе учетных данных. Авторизация позволяет предоставить пользователю доступ к ресурсам системы, а верификация – подтвердить подлинность документов и данных. Валидация использует различные данные для проверки подлинности пользователя в процессе работы с системой.

На сегодняшний день существует несколько отличных друг от друга принципов идентификации пользователей. У каждого из них есть свои преимущества и недостатки, благодаря чему некоторые технологии подходят для использования в одних системах, остальные – в других. Однако во многих

случаях нет строго определенного решения. А поэтому как разработчикам программного обеспечения, так и пользователям приходится самостоятельно думать, какой способ идентификации реализовывать в выпускаемых или используемых продуктах [10].

Существующие способы идентификации пользователя условно можно разделить на идентификацию по паролю, с применением специализированных устройств (smart-card, touch-memory и т.д.), по биометрическим характеристикам личности (анализ отпечатков пальца, сетчатка глаза, почерка, голоса и т.д.), комплексные системы идентификации. Выбор средств определяется характеристиками системы идентификации [28].

1.2.1 Идентификация по паролю, с применением специализированных устройств

Еще не так давно парольная идентификация была чуть ли не единственным способом определения личности пользователя. И в этом нет абсолютно ничего удивительного. Дело в том, что парольная идентификация наиболее проста как в реализации, так и в использовании. Суть ее сводится к следующему. Каждый зарегистрированный пользователь какой-либо системы получает набор персональных реквизитов (обычно используются пары логин-пароль). Далее при каждой попытке входа человек должен указать свою информацию. Ну а поскольку она уникальна для каждого пользователя, то на основании ее система и делает вывод о личности.

Главное преимущество парольной идентификации – это простота реализации и использования. И действительно, она не требует специального обучения пользователей. Кроме того, введение парольной идентификации не требует совершенно никаких затрат: данный процесс реализован во всех продающихся сегодня программных продуктах. Таким образом, система защиты информация оказывается предельно простой и дешевой.

Теперь перейдем к недостаткам. К сожалению, их много. И самый главный – огромная зависимость надежности идентификации от самих пользователей, точнее, от выбранных ими паролей. Дело в том, что большинство людей используют ненадежные ключевые слова, которые легко подбираются. К ним относятся слишком короткие пароли, имеющие смысл слова и т.д. Поэтому некоторые специалисты в области информационной безопасности советуют использовать длинные пароли, состоящие из беспорядочного сочетания букв, цифр и различных символов. Вот только пользователи не хотят запоминать такие ключевые слова и начинают записывать их на бумажки, которые приклеивают прямо к монитору или прячут под клавиатуру. Нужно ли говорить, что подобные действия – серьезный удар по информационной безопасности. Хорошим решением описанной проблемы являются специальное программное обеспечение для работы с паролями. Особенно интересны два различных типа утилит: генераторы ключевых слов и менеджеры. Первые умеют самостоятельно создавать любые, сколь угодно сложные пароли, отвечающие всем требованиям информационной безопасности. Причем обычно пользователь может настраивать работу утилиты, включая и исключая различные наборы символов, устанавливая длину ключевых слов и т.д. Менеджеры являются специальными программами для безопасного хранения и удобного использования паролей. Использование этого программного обеспечения помогает свести к минимуму риски парольной идентификации.

Но, несмотря на свои недостатки, в некоторых областях парольная идентификация до сих пор остается своеобразным «монополистом». В частности, это относится к домашним компьютерам и персональным компьютерам тех компаний, которые не хотят или не могут тратить деньги на информационную безопасность, например, к бюджетным организациям. Кроме того, именно ключевые слова используются для доступа к различным сервисам в Интернете.

Принцип идентификации с применением специализированных устройств основывается на определении личности пользователя по какому-то предмету, ключу, находящемуся в его эксклюзивном пользовании. Естественно, речь идет не об обычных, привычных для большинства людей ключах, а о специальных электронных. На данный момент наибольшее распространение получили два типа устройств. К первому относятся всевозможные карты. Их довольно много, и работают они по различным принципам. Так, например, весьма удобны в использовании бесконтактные карты, которые позволяют пользователям проходить идентификацию, как в компьютерных системах, так и в системах доступа в помещения. Наиболее надежными считаются смарт-карты – аналоги привычных многим людям банковских карт. Кроме того, есть и более дешевые, но менее устойчивые к взлому карты: магнитные, со штрих-кодом и т.д. Вторым типом ключей, которые могут использоваться для идентификации, являются так называемые токены. Эти устройства обладают собственной защищенной памятью и подключаются непосредственно к одному из портов компьютера.

Главным достоинством применения идентификации с использованием специализированных устройств является достаточно высокая надежность. И действительно, в памяти токенов могут храниться большие ключи, подобрать которые хакерам не удастся. Кроме того, в них реализовано немало различных защитных механизмов. Ну а встроенный микропроцессор позволяет электронному ключу не только участвовать в процессе идентификации пользователя, но и выполнять некоторые другие полезные функции. Самой, пожалуй, серьезной опасностью в случае использования такой идентификации является возможность кражи злоумышленниками токенов у зарегистрированных пользователей [1].

Идентификация с использованием специализированных устройств, конечно же, обладает рядом недостатков. Об одном из них мы уже упомянули – это возможность кражи электронных ключей. Второй минус рассматриваемой технологии – цена, хоть в последнее время стоимость, как

самих электронных ключей, так и программного обеспечения, которое может работать с ними, заметно снизилась. Тем не менее, для введения в эксплуатацию системы имущественной идентификации все равно потребуются некоторые вложения. Все-таки каждого зарегистрированного пользователя (или хотя бы привилегированных пользователей – администраторов, руководство предприятия и т.д.) нужно обеспечить персональными токенами. Кроме того, со временем некоторые типы ключей могут изнашиваться, кроме того, они могут быть утеряны и т.д. То есть данная идентификация требует некоторых эксплуатационных затрат.

Система контроля доступа, основанная на смарт-картах, может контролировать доступ кусочков пластика, «наделенных соответствующими полномочиями», но не тех, кто является владельцем смарт-карты.

Системы, использующие персональный идентификационный номер, требуют только того, чтобы человек знал определенный номер – тогда доступ ему гарантируется вне зависимости от того, кто конкретно вводит данный код.

Технологии преодоления таких способов защиты, разработанные в последнее десятилетие, хорошо известны. Поэтому актуальность задач повышения достоверности распознавания пользователей и обнаружения вторжений незарегистрированных лиц при взаимодействии с терминалами распределенных сетей продолжает расти.

1.2.2 По биометрическим характеристикам личности

Биометрические же устройства, удостоверяют личность конкретного человека вне зависимости от того, какой способ биометрической идентификации используется – геометрии руки, отпечатков пальцев, сетчатки глаза или голосовая идентификация.

Биометрия может также устранить необходимость использования карт. Существенное сокращение стоимости карт в последние годы снизило и расходы на администрирование подобных систем, однако, оптимальным

вариантом было бы вовсе исключить эту статью расходов. Утраченная карта должна быть заменена – следовательно, кому-то нужно заново выпускать ее. Вряд ли можно украсть, потерять или забыть где-то руки или глаза. К тому же они не изнашиваются и не нуждаются в замене [19].

Все биометрические системы характеризуются высоким уровнем безопасности, прежде всего потому, что используемые в них данные не могут быть утеряны пользователем, похищены или скопированы. В силу своего принципа действия многие биометрические системы пока еще отличаются сравнительно малым быстродействием и низкой пропускной способностью. Тем не менее, они представляют собой единственное решение проблемы контроля доступа на особо важных объектах с малочисленным персоналом. Например, биометрическая система может контролировать доступ к информации и хранилищам в банках, ее можно использовать на предприятиях, занятых обработкой ценной информации, для защиты ЭВМ, средств связи и т.д. По оценкам специалистов, более 85% установленных в США средств биометрического контроля доступа предназначались для защиты машинных залов ЭВМ, хранилищ ценной информации, исследовательских центров, военных установок и учреждений [6].

Современная биометрическая аутентификация основывается на двух методах:

Статический метод аутентификации – распознает физические параметры человека, которыми он обладает на протяжении всей жизни: от своего рождения и до самой смерти (отпечатки пальцев, отличительные характеристики радужной оболочки глаза, рисунок глазной сетчатки, термограмма, геометрия лица, геометрия кисти руки и даже фрагмент генетического кода);

Динамический метод – анализирует характерные черты, особенности поведения пользователя, которые демонстрируются в момент выполнения какого-либо обычного повседневного действия (подпись, клавиатурный почерк, голос).

Основным на всемирном рынке биометрической защиты, всегда являлся статический метод. Динамическая аутентификация и комбинированные системы защиты информации занимали всего лишь 20 % рынка. Однако, в последние годы, наблюдается активное развитие динамических методов защиты. Особенный интерес сетевых технологий представляют методы клавиатурного почерка и аутентификации по подписи [18].

В связи с довольно быстрым развитием современных биометрических технологий, появляется критически важная проблема – определение общих стандартов надежности биометрических систем защиты. Большим авторитетом среди специалистов пользуются средства, имеющие сертификаты качества, которые выдает Международная ассоциация по компьютерной безопасности ICSA (International Computer Security Association) [14].

1.2.2.1 Статические методы

Дактилоскопия – наиболее популярная технология биометрической аутентификации, основанная на сканировании и распознавании отпечатков пальцев. Данный метод активно поддерживается правоохранительными органами, с целью привлечения в свои архивы электронных образцов. Также, метод сканирования отпечатков пальцев легок в использовании и надежен универсальностью данных.

Главным устройством этого метода биометрической аутентификации – сканер, который сам по себе имеет не большие размеры и является относительно недорогим. Такая аутентификация осуществляется достаточно быстро за счет того, что система не требует распознавания каждой линии узора и сравнения её с исходными образцами, находящимися в базе. Системе достаточно определить совпадения в масштабных блоках и проанализировать раздвоения, разрывы и прочие искажения линий. Уникальность каждого отпечатка позволяет использовать данный метод биометрической аутентификации как в криминалистике, в процессах серьезных бизнес-

операций, так и в быту. В последнее время появилось множество ноутбуков со встроенным сканером отпечатков пальцев, клавиатур, компьютерных мышей, а также смартфонов для аутентификации пользователя. Есть и минусы в этой, казалось бы, неоспоримой и не поддельной, аутентификации. Из-за использования сложных алгоритмов распознавания мельчайших папиллярных линий, система аутентификации может демонстрировать сбои при недостаточном контакте пальца со сканером. Обмануть средство аутентификации и саму систему защиты можно и с помощью муляжа (очень качественно выполненного) или мертвого пальца. По принципу работы, используемые для аутентификации сканеры, делятся на три вида:

Оптические сканеры, функционирующие на технологии отражения, или по принципу просвета. Из всех видов, оптическое сканирование не способно распознать муляж, однако, благодаря своей стоимости и простоте, именно оптические сканеры наиболее популярны;

Полупроводниковые сканеры – подразделяются на радиочастотные, емкостные, термочувствительные и чувствительные к давлению сканеры. Тепловые (термосканеры) и радиочастотные сканеры лучше всех способны распознать настоящий отпечаток и не допустить аутентификацию по муляжу пальца. Полупроводниковые сканеры считаются более надежными, нежели оптические;

Ультразвуковые сканеры. Данный вид устройств является самым сложным и дорогим. С помощью ультразвуковых сканеров можно совершать аутентификацию не только по отпечаткам пальцев, но и по некоторым другим биометрическим параметрам, таким как частота пульса и прочим [13].

Аутентификацию по сетчатке глаза стали использовать еще в 50х годах прошлого столетия. В то время как раз, была изучена и определена уникальность рисунка кровеносных сосудов глазного дна.

Сканеры сетчатки глаза имеют довольно большие габариты и более высокую цену, нежели сканеры отпечатков пальцев. Однако, надежность такого вида аутентификации гораздо выше дактилоскопии, что и оправдывает

вложения. Особенности рисунка кровеносных сосудов глазного дна таковы, что он не повторяется даже у близнецов. Поэтому, такая аутентификация имеет максимальную защиту. Обмануть сканер сетчатки глаза, практически невозможно. Сбои при распознавании глазного рисунка незначительно малы – примерно, один на миллион случаев. Если, у пользователя нет серьезных глазных заболеваний (например, катаракта), он может уверенно использовать систему аутентификации по сетчатке глаза для защиты доступа к всевозможным хранилищам, приватным кабинетам и сверхсекретным объектам.

Сканирование сетчатки глаза предусматривает использование инфракрасного низкоинтенсивного излучения, которое направляется к кровеносным сосудам глазного дна через зрачок. Сигнал отображает несколько сотен характерных точек, которые записываются в шаблон. Самые современные сканеры вместо инфракрасного света направляют лазер мягкого действия.

Для прохождения данной аутентификации, человек должен максимально приблизить к сканеру лицо (глаз должен быть не далее 1,5 см от устройства), зафиксировать его в одном положении и направить взгляд на дисплей сканера, на специальную метку. Около сканера, в таком положении, приходится находиться приблизительно минуту. Именно столько времени требуется сканеру для осуществления операции сканирования, после чего, системе понадобится еще несколько секунд для сравнения полученного образца с установленным шаблоном. Длительное нахождение в одном положении и фиксация взгляда на вспышку света и являются самыми большими недостатками использования данного вида аутентификации. Плюс, из-за относительно долгого сканирования сетчатки и обработки результатов, данное устройство невозможно устанавливать для аутентификации большого количества людей (например, проходной).

Аутентификация по радужной оболочке глаза основан на распознавании уникальных особенностей радужной оболочки глаза.

Схожий на сеть, сложный рисунок подвижной диафрагмы между задней и передней камерами глаза – это и есть уникальная радужная оболочка. Данный рисунок человеку дается еще до его рождения и особо не изменяется в течении всей жизни. Надежности аутентификации методом сканирования радужной оболочки глаза способствует различие левого и правого глаз человека. Такая технология, практически, исключает ошибки и сбои при аутентификации [21].

Однако сложно назвать устройства, считывающие рисунок радужной оболочки – сканерами. Это, скорее всего, специализированная камера, которая делает 30 снимков в секунду. Затем оцифровывается одна из записей и преобразовывается в упрощенную форму, из которой отбираются около 200 характерных точек, и информация по ним записывается в шаблон. Это куда более надежно, чем сканирование отпечатков пальцев – для формирования таких шаблонов используются всего лишь 6070 характерных точек.

Данный вид аутентификации предполагает дополнительную защиту от поддельных глаз – в некоторых моделях устройств, для определения «жизни» глаза, изменяется поток света, направленный в него, и система отслеживает реакцию и определяет изменяется ли размер зрачка.

Данные сканеры уже широко используются, к примеру, в аэропортах многих стран для аутентификации сотрудников во время пересечения зон ограниченного доступа, а также, неплохо зарекомендовали себя в Англии, Германии, США и Японии во время экспериментального использования с банкоматами. Следует отметить, что при аутентификации по радужной оболочке глаза, в отличие от сканирования сетчатки, считывающая камера может находиться от 10 см до 1 метра от глаза и процесс сканирования и распознавания проходит намного быстрее. Данные сканеры стоят дороже, нежели вышеуказанные средства биометрической аутентификации, но, в последнее время и они становятся все более доступными [27].

Аутентификация по геометрии руки – данный метод биометрической аутентификации предполагает измерение определенных параметров

человеческой кисти(длина, толщина, изгибы пальцев, общая структура кисти, расстояние между суставами, ширина и толщина ладони). Руки человека не являются уникальными, поэтому для надежности данного вида аутентификации необходимо комбинировать распознавание сразу по нескольким параметрам. Вероятность ошибок при распознавании геометрии кисти составляет около 0,1%, а это значит, что при ушибе, артрите и прочих заболеваниях и повреждениях кисти, скорее всего, пройти аутентификацию не удастся. Так что, данный метод биометрической аутентификации не подходит для обеспечения безопасности объектов высокой степени секретности.

Однако, данный метод нашел широкое распространение благодаря тому, что он удобен для пользователей по целому ряду причин. Одной из немаловажных таких причин является то, что устройство для распознания параметров руки не принуждает пользователя к дискомфорту и не отнимает много времени (весь процесс аутентификации осуществляется за несколько секунд). Следующей причиной популярности аутентификации по геометрии руки можно назвать тот факт, что ни температура, ни загрязненность, ни влажность кисти не влияют на процедуру аутентификации. Также, удобен данный метод и тем, что для распознавания кисти можно использовать изображение низкого качества – размер шаблона, хранящегося в базе всего 9 байт. Процедура сравнения кисти пользователя с установленным шаблоном очень проста и легко может быть автоматизирована. Устройства данного вида биометрической аутентификации могут иметь разный внешний вид и функционал – одни сканируют лишь два пальца, другие делают снимок всей руки, а некоторые современные устройства при помощи инфракрасной камеры сканируют вены и по их изображению осуществляют аутентификацию [31].

Данный метод впервые был использован в начале 70х годов прошлого века. Сегодня подобные устройства можно встретить в аэропортах и различных предприятиях, где необходимо формировать достоверные сведения о присутствии того, или иного человека, учета рабочего времени и прочих процедур контроля.

Аутентификация по геометрии лица. Этот биометрический метод аутентификации является одним из «трёх больших биометрик» наряду с распознаванием по радужной оболочке и сканированию отпечатков пальцев.

Данный метод аутентификации подразделяется на двухмерное и трехмерное распознавание.

Двухмерное (2D) распознавание лица используется уже очень давно, в основном, в криминалистике. Но, с каждым годом данный метод усовершенствуется, повышая, этим самым, уровень своей надежности. Однако, до совершенства двухмерному методу распознавания лица еще далеко – вероятность ложных срабатываний при данной аутентификации варьируется от 0,1 до 1 %. Еще выше частота ошибок непризнания.

Куда больше надежд возлагают на новейший метод – трехмерное (3D) распознавание лиц.

Разработкой систем трехмерного распознавания лиц занимаются около десяти ведущих мировых ITкомпаний, в том числе и из России. Большинство таких разработчиков предоставляют на рынок сканеры вместе с программным обеспечением. И только некоторые работают над созданием и выпуском сканеров [2].

При трёхмерном распознавании лиц используется множество сложных алгоритмов, эффективность которых зависит от условий их применения. Процедура сканирования составляет около 20-30 секунд. В этот момент лицо может быть повернуто относительно камеры, что принуждает систему компенсировать движения и формировать проекции лица с четким выделением черт лица, таких как контуры бровей, глаз, носа, губ и др. Затем система определяет расстояние между ними. В основном, шаблон составляется из таких неизменных характеристик, как глубина глазных впадин, форма черепа, надбровных дуг, высота и ширина скул и прочих ярко выраженных особенностей, благодаря которым впоследствии система сможет распознать лицо даже при наличии бороды, очков, шрамов, головного убора и

прочего. Всего для построения шаблона используется от 12 до 40 особенностей лица и головы пользователя.

Международный подкомитет по стандартизации в области биометрии (IS0/IEC JTC1/SC37 Biometrics) в последнее время занимается разработкой единого формата сведений для распознавания человеческих лиц на основе двух и трехмерных изображений. Скорее всего, два данных метода объединят в один биометрический метод аутентификации.

Термография лица. Данный биометрический метод аутентификации выражается в установлении человека по его кровеносным сосудам.

Лицо пользователя сканируется при помощи инфракрасного света и формируется термограмма – температурная карта лица, являющаяся достаточно уникальной. Данный метод по своей надежности сравним с методом аутентификации по отпечаткам пальцев [21].

Сканирование лица при данной аутентификации можно производить с десятиметрового расстояния. Этот метод способен распознать близнецов (в отличии от распознавания по геометрии лица), людей, перенесших пластические операции, использующих маски, а также он эффективен не смотря на температуру тела и старение организма.

Однако, данный метод не распространен широко, возможно, из-за невысокого качества получаемых термограмм лиц.

1.2.2.2 Динамические методы

Метод распознавания голоса. Биометрический метод аутентификации пользователя по голосу является наиболее доступным для реализации. Данный метод позволяет произвести идентификацию и аутентификацию личности при помощи лишь одного микрофона, который подключен к записывающему устройству.

Использование данного метода бывает полезным в судебных случаях, когда единственной уликой против подозреваемого служит запись

телефонного разговора. Метод распознавания голоса является очень удобным – пользователю достаточно лишь произнести слово, без совершения каких либо дополнительных действий. Огромным преимуществом данного метода является право осуществления скрытой аутентификации. Пользователь не всегда может быть осведомлен о включении дополнительной проверки, а значит, злоумышленникам будет еще сложнее получить доступ [4].

Формирование персонального шаблона производится по многим характеристикам голоса.

Это может быть тональность голоса, интонация, модуляция, отличительные особенности произношения некоторых звуков речи и другое. Если система аутентификации должным образом проанализировала все голосовые характеристики, то вероятность аутентификации постороннего лица ничтожно мала. Однако, в 13 % случаев, система может дать отказ и настоящему обладателю ранее определенного голоса. Дело в том, что голос человека может меняться во время болезни (например, простуды), в зависимости от психического состояния, возраста и т.п. Поэтому, биометрический метод голосовой аутентификации нежелательно использовать на объектах повышенной безопасности. Он может быть использован для доступа в компьютерные классы, бизнес-центры, лаборатории и подобного уровня безопасности объекты. Также, технология распознавание голоса может применяться не только в качестве аутентификации и идентификации, но и как незаменимый помощник при голосовом вводе данных [33].

Метод распознавания клавиатурного почерка – является одним из перспективных методов биометрической аутентификации сегодняшнего дня. Клавиатурный почерк представляет собой биометрическую характеристику поведения каждого пользователя, а именно – скорость ввода, время удержания клавиш, интервалы между нажатиями на них, частота образования ошибок при вводе, число перекрытий между клавишами, использование функциональных клавиш и комбинаций, уровень аритмичности при наборе и др.

Данная технология является универсальной, однако, лучше всего, распознавание клавиатурного почерка подходит для аутентификации удаленных пользователей. Разработкой алгоритмов распознавания клавиатурного почерка активно занимаются как зарубежные, так и российские IT компании.

Аутентификация по клавиатурному почерку пользователя имеет два способа: ввод известной фразы (пароля); ввод неизвестной фразы (генерируется случайным образом).

Оба способа аутентификации предполагают два режима: режим обучения и режим самой аутентификации. Режим обучения заключается в многократном вводе пользователем кодового слова (фразы, пароля). В процессе повторного набора, система определяет характерные особенности ввода текста и формирует шаблон показателей пользователя [25].

Надежность такого вида аутентификации зависит от длины вводимой пользователем фразы.

Среди преимуществ данного метода аутентификации следует отметить удобство пользования, возможность осуществления процедуры аутентификации без специального оборудования, а также возможность скрытой аутентификации. Минусом данного метода, как и в случае с распознаванием голоса, можно назвать зависимость отказа системы от возрастных факторов и состояния здоровья пользователя. Ведь, моторика, куда сильнее, нежели голос, зависит от состояния человека. Даже простая человеческая усталость может повлиять на прохождение аутентификации. Смена клавиатуры, также может быть причиной отказа системы – пользователь способен не сразу адаптироваться к новому устройству ввода и поэтому, при вводе проверочной фразы, клавиатурный почерк может не соответствовать шаблону. В частности, это влияет на темп ввода. Хотя, исследователи предлагают повысить эффективность данного метода за счет использования ритма.

Искусственное добавление ритма (например, ввод пользователем слова под какую-то знакомую мелодию) обеспечивает устойчивость клавиатурного почерка и более надежную защиту от злоумышленников.

Верификация подписи. В связи с популярностью и массовому использованию различных устройств с сенсорным экраном, биометрический метод аутентификации по подписи становится очень востребованным.

Максимально точную верификацию подписи обеспечивает использование специальных световых перьев. Во многих странах электронные документы, подписанные биометрической подписью, имеют такую же юридическую силу, что и бумажные носители. Это позволяет осуществлять документооборот значительно быстрее и беспрепятственно. В России, к сожалению, доверие оказывает лишь бумажный подписанный документ, или электронный документ, на который наложена официально зарегистрированная электронная цифровая подпись (ЭЦП). Но, ЭЦП легко передать другому лицу, что не сделаешь с биометрической подписью. Поэтому, верификация по биометрической подписи является более надежной.

Биометрический метод аутентификации по подписи имеет два способа:

На основе анализа визуальных характеристик подписи. Данным способом предполагается сравнение двух изображений подписи на соответствие идентичности – это может осуществляться как системой, так и человеком;

Способ компьютерного анализа динамических характеристик написания подписи.

Аутентификация таким способом происходит после тщательного исследования сведений о самой подписи, а также о статистических и периодических характеристиках ее написания.

Формирование шаблона подписи осуществляется в зависимости от требуемого уровня защиты. Всего, одна подпись анализируется по 100-200 характерным точкам. Если же, подпись ставится с использованием светового пера, то помимо координат пера, учитывается и угол его наклона, нажатие

пера. Угол наклона пера исчисляется относительно планшета и по часовой стрелке.

Данный метод биометрической аутентификации, как и распознавание клавиатурного почерка, имеют общую проблему – зависимость от психофизического состояния человека.

1.2.3 Валидация по динамической модели пользователя (по текстовому следу)

Методика валидации пользователя по текстовому следу основывается на анализе его письменной речи, например, текстов из социальных сетей, форумов, электронной почты и т.д. В процессе анализа используются различные алгоритмы и технологии машинного обучения для определения вероятности того, что данный текст был написан именно этим пользователем.

Основным преимуществом такой методики является возможность точно определить, является ли пользователь тем, за кого он себя выдаёт. Это важно для многих сервисов, которые опираются на личную идентификацию пользователей, например, банки, онлайн-платформы и другие сервисы, где требуется защита персональных данных. Кроме того, методика может использоваться для обнаружения мошенничества и других незаконных действий [17].

Также методика валидации пользователя по текстовому следу позволяет повысить уровень безопасности систем проверки личности, т.к. она предоставляет надежные данные для проверки подлинности пользователя. Кроме того, этот подход обеспечивает быструю и легкую систему проверки, которая может быть интегрирована в любой онлайн-сервис.

Среди основных недостатков методики можно отметить возможность ложных срабатываний, связанных с использованием разных устройств или изменением стиля написания текстов. Также методика может быть

недостаточно эффективной для проверки анонимных пользователей, которые не оставляют достаточного количества информации о себе в интернете.

1.3 Цель работы

Объектом исследования данной диссертационной работы являются различные подходы, методы и технологии, используемые для идентификации пользователей в информационных системах.

Предметом исследования является текстовый след, который представляет собой набор данных, полученных от пользователя при его взаимодействии с информационной системой. Текстовый след может включать в себя письменные работы, ответы на вопросы, комментарии, сообщения и другие текстовые элементы, которые оставляют след после взаимодействия пользователя с системой.

Гипотеза исследования заключается в том, что разработанная новая методика валидации пользователя по текстовому следу позволит динамично производить идентификацию в дистанционном формате. Это означает, что на основе анализа текстового следа, собранного от пользователя, можно будет определить его уникальные характеристики и использовать их для идентификации и валидации в различных автоматизированных информационных системах. Гипотеза предполагает, что новая методика будет более эффективной и точной по сравнению с существующими методами идентификации.

Целью исследования является разработка и экспериментальная проверка методики валидации пользователя по текстовому следу с использованием экспертной системы. Результаты исследования могут способствовать улучшению систем идентификации и валидации пользователей в информационных системах, а также повышению безопасности и достоверности взаимодействия в дистанционном формате.

Цель создания методики валидации пользователя по текстовому следу с помощью экспертной системы заключается в разработке эффективного и надежного инструмента, который позволит идентифицировать пользователя на основе его текстовой активности. Основной целью является установление подлинности пользователя и обеспечение безопасности в информационном пространстве. Методика должна предоставить систему, способную анализировать текстовый след пользователя и выявлять его уникальные характеристики, такие как стиль письма, частота орфографических ошибок, использование специальных символов и другие параметры. Это позволит создать базу знаний и продукционные правила, на основе которых экспертная система сможет производить валидацию и определение подлинности пользователя. В результате успешной разработки методики, она может быть применена в различных областях, таких как кибербезопасность, дистанционное образование, электронная коммерция и другие, где необходима достоверная идентификация пользователей на основе их текстовой активности.

1.4 Постановка задачи

При разработке методики валидации пользователя по текстовому следу с помощью экспертной системы будем придерживаться следующих задач:

– требуется проанализировать и собрать данные из различных источников, таких как on-line ввод текста в поля с открытой формой, форумы, электронная почта, ранее набранные тексты чтобы выявить стиль написания и лексикон пользователя;

– требуется создать и использовать инструменты анализа текста, которые позволят автоматически распознавать и анализировать текст в режиме реального времени. Создание этих инструментов также включает выбор методов анализа текста, которые позволят определить, насколько точно характеристики текста могут быть связаны с конкретным пользователем;

– требуется разработать и вычислить конкретные показатели, используемые для оценки подлинности пользователя. Это включает в себя анализ стиля написания слов, языковых структур и других важных аспектов письменной речи пользователя;

– требуется разработать набор экспертных правил, основанных на данных анализа текста, который позволит определить стиль письменной речи пользователей и сопоставить его с пользователями, которые скрывают свою личность или пытаются войти в аккаунт другого пользователя.

Осуществление этих задач поможет создать эффективную методику валидации пользователя по текстовому следу с использованием экспертной системы, которая будет способна точно и надежно определять валидность пользователя на основе его текстового поведения.

1.5 Допущения

При создании методики валидации пользователя по текстовому следу с помощью экспертной системы могут быть следующие допущения:

– основное допущение состоит в том, что текстовый след пользователя содержит информацию, которая является уникальной и связанной с его идентичностью. Основываясь на этом предположении, методика строит модель, которая анализирует текстовый след и делает выводы о подлинности пользователя;

– для эффективной работы экспертной системы необходимо иметь надежные данные обучения. Допущение заключается в том, что данные, на основе которых происходит обучение системы, являются представительными и достоверными для широкого спектра пользователей и контекстов использования;

– методика требует разработки правил и эвристик, которые определяют критерии валидации и принимают решения на основе анализа текстового

следа. Эти правила и эвристики могут быть субъективными и основываться на предварительных предположениях или экспертных знаниях;

– методика может быть разработана с учетом определенных аспектов текстового следа, таких как грамматика, стиль, использование специальных символов и т. д. Однако она может не учитывать некоторые другие аспекты, такие как семантика, интонация или контекстуальные факторы. В результате, методика может ограничиться только определенными аспектами текстового следа пользователя;

– даже при использовании экспертной системы, возможны случаи ложноположительных (ошибочно признаваемых пользователей недействительными) или ложноотрицательных (ошибочно признаваемых пользователей действительными) результатов. Это связано с ограничениями в точности и достоверности алгоритмов и моделей, используемых в методике.

– время от времени может потребоваться обновление и адаптация методики для учета изменяющихся условий, новых видов текстового следа или эволюции пользовательского поведения. Это требует постоянного сопровождения и поддержки со стороны разработчиков методики;

– эффективность методики может зависеть от внешних условий, таких как качество ввода текста (например, ошибки клавиатуры), скорость набора текста или наличие шума в данных. Такие факторы могут повлиять на точность и надежность системы.

Важно учитывать эти допущения при разработке и применении методики валидации пользователя по текстовому следу с помощью экспертной системы, чтобы достичь оптимальных результатов и учесть возможные ограничения системы.

1.6 Ограничения

При создании методики валидации пользователя по текстовому следу с помощью экспертной системы могут возникнуть следующие ограничения:

– ограниченный объем данных о текстовых следах пользователей может ограничить эффективность методики. Если недостаточно данных для обучения или анализа, точность системы может быть низкой;

– методика валидации пользователя по текстовому следу может быть чувствительна к выбору конкретных характеристик текста. Если определенные характеристики не являются информативными или не включены в анализ, это может повлиять на точность и надежность методики;

– текстовый след пользователя может быть вариативным и изменяться в зависимости от различных факторов, таких как настроение, контекст или временные условия. Это может усложнить задачу анализа и привести к неоднозначным результатам [17];

– методика может ограничиться анализом только текстового следа и не учитывать контекстуальные факторы, такие как контекст использования, цель коммуникации или предыдущие взаимодействия пользователя. Это может привести к недостаточной точности и надежности при валидации;

– методика валидации пользователя по текстовому следу может быть ограничена в своей применимости к определенным контекстам или типам текстового ввода. Например, она может быть более эффективна в случае коротких текстов или специфического стиля коммуникации, но менее эффективна в случае сложных или длинных текстов.

Все эти ограничения необходимо учитывать при разработке и применении методики валидации пользователя по текстовому следу с помощью экспертной системы, чтобы достичь оптимальных результатов и учесть возможные ограничения системы.

1.7 Выводы по главе

Несмотря на то, что аутентификация пользователя по биометрическим данным считается одним из наиболее надежных методов идентификации, у нее также имеются ряд недостатков.

К примеру, системы аутентификации по биометрии требуют дорогостоящего оборудования и программного обеспечения, что может повысить стоимость внедрения и эксплуатации системы. Кроме того, у некоторых людей могут быть проблемы с распознаванием биометрических данных (например, проблемы с распознаванием голоса, отпечатков пальцев и т.д.). Так же из-за использования специального оборудования такие системы лишены возможности скрытой аутентификации и аутентификации удаленных пользователей что является критическим недостатком для обеспечения безопасности информационной системы.

Методы аутентификация пользователя, которые основаны на учетных данных, таких как пароль, PIN-код и т.д., так же имеют ряд недостатков. Первый недостаток таких методов – это «слабые» пароли, которые легко поддаются взлому. Второй недостаток заключается в том, что учетные данные могут быть украдены или подсмотрены, что может привести к компрометации системы и утечке конфиденциальных данных, а также возможны случаи, когда один из пользователей сознательно передает свой пароль более осведомленному лицу с целью успешного прохождения аттестационных заданий [9].

Несмотря на множество методов усиления статической и динамической аутентификации, данные подходы не смогли полностью решить проблему обеспечения безопасности информационной системы, а сам метод аутентификации в полной мере не пригоден для информационных систем, где осуществляется проверка пользователя на подлинность, так как аутентификация пользователя имеет множество недостатков и не может обеспечить высокий уровень безопасности. Валидация пользователя является более эффективным методом проверки, который обеспечивает высокий уровень безопасности и затрудняет его компрометацию.

В этой связи, методика валидации пользователя по текстовому следу с помощью экспертной системы становится более привлекательной альтернативой. Она позволяет проверять подлинность пользователя на основе

анализа его текстового следа, который содержит уникальные черты и не может быть скомпрометирован таким образом, как это бывает с учетными данными. Такой метод обеспечивает более высокий уровень защиты, чем статическая и динамическая аутентификация, и может использоваться как независимый метод проверки, так и в качестве дополнительного усиления над другими методами.

Методика валидации пользователя по текстовому следу с помощью экспертной системы позволяет проверять подлинность пользователя на основе его текстовых данных, которые не требуют специального оборудования и программного обеспечения. Это позволяет упростить внедрение системы проверки, снизить ее стоимость и повысить ее эффективность.

Таким образом, хотя аутентификация по биометрии считается надежной, методика валидации пользователя по текстовому следу оказывается более привлекательным вариантом, поскольку она позволяет решить многие проблемы, связанные с аутентификацией по биометрии, и обеспечивает более высокий уровень проверки подлинности пользователя.

2 Разработка методики динамической валидации пользователя по текстовому следу

Динамическая валидация пользователя по текстовому следу использует алгоритмы машинного обучения и нейронные сети, чтобы обучать систему и сравнивать данные, полученные в режиме реального времени, с данными, сохраненными в базе данных. Этот метод позволяет улучшить качество валидации пользователя и увеличить точность сопоставления.

Динамическая валидация пользователя по текстовому следу имеет несколько преимуществ. Она основывается на актуальных данных и позволяет непрерывно отслеживать и анализировать пользовательскую активность. Это обеспечивает высокую точность аутентификации пользователя и позволяет системе оперативно реагировать на изменения в стиле написания пользователя.

Однако используя такой метод, могут возникнуть проблемы при использовании данных пользователей, которые работают с разными устройствами и сетями, например, в чувствах, связанных со стрессом, депрессией, усталостью, а также использование других языков и жаргонов. Также наблюдается проблема совместимости данного метода с GDPR (Общим регламентом о защите персональных данных), поскольку динамическая валидация пользователя по текстовому следу предполагает непрерывный сбор и обработку текстовых данных [5].

2.1 Параметрическая модель динамической валидации пользователя

Параметрическая модель динамической валидации пользователя – метод валидации, который основывается на анализе пользовательской активности в режиме реального времени, для определения возможных угроз безопасности и принятия соответствующих мер.

Основной принцип работы параметрической модели динамической валидации пользователя заключается в том, что каждый пользователь имеет свой индивидуальный цифровой отпечаток на основе своих параметров активности. Этот цифровой отпечаток может быть использован для верификации пользователя в будущем [8].

Этот метод подразумевает использование набора модулей, которые и производят анализ параметров пользовательской активности, таких как фиксация эмпирических закономерностей распределения частотности слов и букв, фиксация орфографических и пунктуационных ошибок в тексте, фиксация используемых специальных символов употребляемых пользователем в тексте, фиксация скорости набора текста с клавиатуры, фиксация используемых специальных клавиш при наборе текста на клавиатуре и другие факторы. Эти параметры сравниваются с историческими значениями, предварительно сохраненными в базе данных, для определения соответствия пользовательской активности легитимному пользователю или злоумышленнику.

2.1.1 Модуль по фиксации эмпирических закономерностей распределения частотности слов и букв в тексте

Это программный модуль, направленный на анализ текстовых данных на предмет распределения частотности слов и выявление эмпирических закономерностей в этом распределении.

Алгоритм строится на предположении, что у каждого человека имеется свой уникальный словарь, включающий различные слова, которые он обычно использует в своих текстах, а также частоты употребления определенных слов или фраз в тексте. Например, для идентификации пользователя можно анализировать как часто пользователь использует определенную группу слов.

Основным принципом данного метода является анализ частоты употребления слов в тексте и выявление наиболее часто используемых слов.

Для этого текст разбивается на отдельные слова (токены), которые затем сортируются по частоте их встречаемости в тексте.

Существует несколько шагов, которые необходимо выполнить, чтобы создать компьютерную модель частотного анализа слов в тексте:

– текст разбивается на отдельные слова или символы (токены), которые потом подвергаются анализу;

– выполняется составление словаря слов, который включает все уникальные слова, найденные в тексте;

– вычисляется частота встречаемости каждого слова в тексте, и определяется важность этих слов в тексте;

– выбираются наиболее важные слова, основываясь на их частоте встречаемости в тексте и степени их важности;

– модель фиксирует важные слова и заносит их в формируемый текстовый след. Для удобства интерпретации результатов производится визуализация данных с помощью графиков или других подходящих методов.

Таким образом, данный модуль позволяет анализировать и выявлять основные слова, используемые в тексте, и создавать текстовый след для дальнейшей интерпретации и использования в задачах валидации пользователей.

В процессе функционирования данного модуля, экспертная система будет принимать входной параметр, содержащий результат вычисления Евклидова расстояния между частотами появления букв при наборе текста. Это расстояние вычисляется путем сравнения двух векторов, полученных при анализе исторического текстового следа пользователя и вновь поступающего текста.

Евклидово расстояние между двумя векторами A и B в n-мерном пространстве можно вычислить с использованием следующей формулы:

$$d(A,B) = \text{sqrt}((a1 - b1)^2 + (a2 - b2)^2 + \ldots + (an - bn)^2) \quad (1)$$

где – d(A, B) – Евклидово расстояние между векторами A и B;

– a1, a2, ..., an – элементы вектора A;

– b1, b2, ..., bn – элементы вектора B.

В данной формуле осуществляется вычисление квадратов разностей соответствующих элементов двух векторов, затем суммируются полученные значения и берется квадратный корень из суммы. Это дает меру расстояния между двумя векторами в пространстве.

2.1.2 Модуль по тезаурусному анализу слов в тексте

Его основная цель заключается в анализе семантической близости и взаимосвязи между словами, используемыми в тексте, с целью более точной оценки и анализа текстового следа пользователя.

Тезаурус – это семантический словарь, который содержит связи между словами, их синонимы, антонимы, ассоциации и другие лексические отношения. Модуль по тезаурусному анализу использует такую информацию для определения семантической близости слов и их значимости в контексте текста [8].

Основные функции модуля по тезаурусному анализу слов включают:

– семантический анализ – модуль производит анализ смысловых связей между словами в тексте на основе информации из тезауруса. Это позволяет определить, насколько точно и последовательно пользователь использует слова, а также обнаружить возможные отклонения от ожидаемого семантического контекста;

– определение стилистической согласованности – модуль также оценивает стилистическую согласованность слов, используемых в тексте. Он может обнаружить несоответствия в выборе терминов, использование неподходящих синонимов или ассоциаций, что может указывать на неадекватность или неправильное понимание текста.

Модуль по тезаурусному анализу слов в тексте значительно повышает точность и эффективность валидации пользователя по текстовому следу. Он помогает выявить особенности и недочеты в использовании слов, связанных с их семантикой, стилистикой и контекстом. Это позволяет более глубоко анализировать и понимать текстовые активности пользователя и достичь более надежных результатов валидации.

2.1.3 Модуль по фиксации орфографических ошибок в тексте

Это программный модуль, который позволяет автоматически обнаруживать и фиксировать орфографические ошибки в тексте на основе правил и алгоритмов правильной орфографии. Основным принципом действия модуля для анализа орфографических ошибок является анализ каждого слова в тексте на правильность орфографии. Слово сравнивается со словарем правильно написанных слов, и, если оно не найдено в словаре, модуль считает его неправильным и фиксирует его.

Существует несколько шагов, которые необходимо выполнить, чтобы создать модуль по анализу орфографических ошибок в тексте:

– создание словаря правильных слов. Этот шаг включает в себя составление словаря правильно написанных слов (например, на основе орфографического словаря);

– анализ текста на наличие орфографических ошибок. Текст проходит через модель, которая ищет слова, отсутствующие в словаре правильных слов;

– фиксация орфографических ошибок. Модель фиксирует слова с орфографическими ошибками и заносит их в формируемый текстовый след. Для удобства интерпретации результатов производится визуализация данных с помощью графиков или других подходящих методов.

Таким образом, модуль по анализу орфографических ошибок в тексте играет важную роль в формировании текстового следа пользователя и

обеспечивает более точную валидацию на основе орфографической правильности текста.

В процессе функционирования данного модуля, экспертная система будет принимать входной параметр, представляющий собой коллекцию из слов, содержащих орфографические ошибки. С помощью алгоритма сравнения, система будет анализировать эту коллекцию и сопоставлять ее с уже существующими коллекциями исторического следа. Основная цель такого сравнения заключается в выявлении возможных совпадений и повторений слов, в которых пользователь часто допускает ошибки или опечатки.

2.1.4 Модуль по фиксации частоты орфографических ошибок в тексте

Модуль по фиксации частоты орфографических ошибок в тексте является важной составляющей в процессе валидации пользователя по его текстовому следу. Он предназначен для автоматического обнаружения и подсчета ошибок в орфографии, сделанных пользователем в тексте, и последующего использования этой информации для оценки качества его письменных навыков.

Данный модуль основывается на анализе текста и сравнении его со словарем или набором правильно написанных слов. При обнаружении слов, не соответствующих правильной орфографии, модуль регистрирует их как орфографические ошибки и увеличивает счетчик ошибок для данного пользователя. Частота ошибок определяется путем подсчета общего числа ошибок и деления его на общее количество слов или символов в тексте [29].

Для эффективной работы модуля необходимо иметь достаточно большой словарь или базу правильно написанных слов, которые будут использоваться в процессе сравнения. Также могут применяться дополнительные алгоритмы и методы, например, использование правил и исключений в орфографии, для более точного определения ошибок.

Частота орфографических ошибок в тексте может служить одним из критериев для оценки качества письменных навыков пользователя. Более высокая частота ошибок может указывать на недостаточное владение правилами орфографии и потенциальные проблемы с качеством письменных работ. Валидационная система может использовать эту информацию в сочетании с другими параметрами текстового следа для определения общей степени валидации пользователя.

Таким образом, модуль по фиксации частоты орфографических ошибок в тексте играет важную роль в процессе валидации пользователя по его текстовому следу, позволяя автоматически определить и учесть орфографические ошибки, что способствует более точной оценке письменных навыков и качества работы пользователя.

В процессе работы этого модуля, экспертная система будет принимать входной параметр, который представляет результат вычисления частоты орфографических ошибок в тексте, определенный по формуле:

Частота орфографических ошибок = (Количество орфографических ошибок / Общее количество слов) * 100 (2)

где – количество орфографических ошибок – количество слов, содержащих орфографические ошибки в тексте;

– общее количество слов – общее количество слов в тексте.

Таким образом, формула позволяет вычислить процентное соотношение орфографических ошибок от общего числа слов в тексте, что представляет собой меру частоты возникновения таких ошибок.

2.1.5 Модуль по фиксации пунктуационных ошибок в тексте

Это программные средства, которые используются для автоматической проверки правильности использования знаков препинания в тексте.

Ошибки в использовании знаков препинания могут произойти по разным причинам, например, это может быть незнание правил использования знаков препинания, опечатки при наборе и т.д. Например, он проверяет, расставлены ли точки, запятые, двоеточия, точки с запятой и другие знаки препинания в правильном порядке и месте. Если в тексте есть ошибки, модуль фиксирует их.

Основным принципом действия модуля по анализу пунктуационных ошибок является анализ каждого слова в тексте на правильность расстановки знаков препинания. Текст проходит через модуль, который проверяет правильность использования знаков препинания и выделяет места, где были обнаружены ошибки.

Также модуль может проверять наличие ошибок смешивания разных типов знаков препинания, например, обнаруживать ошибки в использовании кавычек, скобок, тире и других знаков препинания.

Существует несколько шагов, которые необходимо выполнить, чтобы создать модуль по анализу пунктуационных ошибок в тексте:

– создание списка правильных знаков препинания. Этот шаг включает в себя составление списка правильно использованных знаков препинания на основании правил языка;

– анализ текста на наличие пунктуационных ошибок. Текст проходит через модуль, который ищет места, где правила использования знаков препинания не были соблюдены;

– фиксация пунктуационных ошибок. После того, как модуль зафиксировал пунктуационную ошибку, он заносит ее в формируемый текстовый след. Для удобства интерпретации результатов производится визуализация данных с помощью графиков или других подходящих методов.

Использование модуля по анализу пунктуационных ошибок позволяет улучшить качество текстового следа, формируемого о каждом пользователе, и использовать этот след для идентификации и валидации пользователей.

2.1.6 Модуль по фиксации используемых специальных символов в тексте

Модуль используется для автоматического определения, фиксации и анализа специальных символов в любом текстовом файле или документе.

Он работает путем сканирования текста, который нужно проанализировать, и выделения всех символов, которые не являются частью обычного алфавита. Эти символы могут включать в себя такие вещи, как математические операции, специальные символы и прочее.

Далее эти символы сортируются и выводятся в удобном для анализа виде. Модуль может предоставлять информацию о количестве каждого символа в тексте.

Кроме этого, модель может предоставлять и дополнительную информацию, такую как частоту использования каждого символа в тексте, наиболее часто используемые комбинации символов и т. д.

В процессе работы данного модуля экспертной системы, входной параметр будет представлять собой коллекцию из набора специальных символов, которые пользователь использует при вводе текста. С использованием соответствующего алгоритма сравнения, система будет анализировать этот набор символов и сопоставлять его с предыдущими наборами символов, составляющими исторический след. Главная цель такого сравнения заключается в обнаружении возможных совпадений в использовании специальных символов, которые характерны для конкретного пользователя.

2.1.7 Модуль по фиксации даты создания текстового следа

Модуль по фиксации даты создания текстового следа является важной частью системы валидации пользователя по текстовому следу. Его основная задача заключается в регистрации точной даты и времени, когда текстовый след был создан или получен от пользователя. Эта информация имеет большое значение для процесса валидации и идентификации пользователя.

Определение даты создания текстового следа имеет несколько ключевых применений:

– зная дату создания текстового следа, можно определить, насколько свежим и актуальным он является. Это полезно для оценки активности пользователя и его участия в определенных процессах или заданиях;

– фиксация даты создания текстового следа позволяет отслеживать прогресс пользователя с течением времени;

– модуль по фиксации даты создания текстового следа также может быть использован для подтверждения подлинности работ;

– агрегирование и анализ дат создания текстовых следов может помочь выявить тренды и паттерны в активности пользователей. Это может быть полезным для аналитики и прогнозирования поведения пользователей в будущем.

Модуль по фиксации даты создания текстового следа обеспечивает точность и достоверность информации, необходимой для валидации пользователя по текстовому следу. Он предоставляет важные временные метки, которые помогают системе более эффективно анализировать и оценивать активность и поведение пользователей.

В процессе работы данного модуля экспертной системы используется входной параметр, представляющий собой разницу между датами создания текстового следа. Этот параметр позволяет определить степень устаревания исторического текстового следа и сравнить его с новым текстовым следом, который поступает от пользователя. Если наблюдаются значительные

различия между ними по определенным параметрам, система будет предупреждена о возможной необходимости дополнительной проверки пользователя.

2.1.8 Модуль по фиксации скорости набора текста с клавиатуры при наборе текста

Модуль является методом аутентификации личности на основе стиля печати. Он использует алгоритмы, которые сравнивают скорость и паттерны набора текста, которые связаны с конкретным пользователем, для автоматической проверки его личности.

Модуль работает, прежде всего, собирая данные о скорости ввода и стиле печати конкретного пользователя. Анализируя эти данные, он создает профиль печати пользователя.

При аутентификации модуль сравнивает набор текущего пользователя с профилем печати, ранее сохраненным в системе. Если результаты сравнения соответствуют этому профилю, то пользователь считается аутентичным.

Таким образом, это метод аутентификации, который не требует от пользователя ввода пароля или иной аутентификационной информации.

Чтобы убедиться в точности и надежности модуля, обычно используется метод обучения с учителем, который состоит в том, что модуль обучается на примерах известных пользователей.

Здесь главное – накопить максимальное количество информации о стиле печати каждого пользователя, чтобы можно было сравнить это с тем, как он вводит свой логин пароль или другой нужный ввод с клавиатуры, и определить, является ли он или нет тем, за кого себя выдает [11].

В рамках работы данного модуля экспертной системы осуществляется использование входного параметра, который представляет собой измеренную скорость ввода текста с клавиатуры пользователем. С использованием соответствующего алгоритма сравнения, система производит анализ этой

скорости набора и сравнивает ее с предыдущими значениями, составляющими исторический след. Основная цель данного сравнения заключается в выявлении различий в скоростях и определении степени отклонения от эталонного значения, характерного для проверяемого пользователя.

2.1.9 Модуль по фиксации средней длительности нажатия клавиши на клавиатуре при наборе текста

Модуль по фиксации средней длительности нажатия клавиши на клавиатуре при наборе текста является важной составной частью методики валидации пользователя по текстовому следу. Его основная задача заключается в измерении и записи времени, затраченного на нажатие каждой клавиши в процессе письменного ввода.

Для сбора данных о средней длительности нажатия клавиши модуль использует специальные алгоритмы и механизмы, которые позволяют точно измерять время между моментом нажатия и отпускания каждой клавиши на клавиатуре. При этом учитывается и обрабатывается время задержки между нажатиями разных клавиш.

Собранные данные о средней длительности нажатия клавиши могут предоставить информацию о письменных навыках и стиле печати каждого пользователя. Некоторые люди могут иметь более равномерное и стабильное время нажатия клавиши, в то время как другие могут иметь более переменные и неустойчивые значения. Такие различия в длительности нажатия клавиши могут служить важным критерием для валидации пользователя [12].

Модуль по фиксации средней длительности нажатия клавиши может быть интегрирован в платформу или систему, где пользователи выполняют письменные задания или вводят текстовую информацию. Полученные данные могут быть использованы вместе с другими параметрами текстового следа для создания уникального профиля каждого пользователя и проведения его валидации.

Однако, следует отметить, что модуль по фиксации средней длительности нажатия клавиши имеет свои ограничения. Например, он не учитывает индивидуальные физиологические особенности каждого пользователя, такие как размеры пальцев или скорость печати. Также, возможны факторы, которые могут искажать данные, такие как технические проблемы с клавиатурой или некорректное измерение времени нажатия.

В целом, модуль по фиксации средней длительности нажатия клавиши представляет собой важный инструмент для валидации пользователя по текстовому следу, позволяющий учесть и анализировать его письменные навыки и стиль печати. В сочетании с другими модулями и параметрами текстового следа, этот модуль способствует созданию более точной и надежной методики валидации пользователей.

В рамках данного модуля экспертной системы применяется входной параметр, который представляет собой среднюю продолжительность нажатия клавиши на клавиатуре во время набора текста. Этот модуль имеет сходство с основными целями и алгоритмами модуля по фиксации скорости набора текста с клавиатуры.

2.1.10 Модуль по фиксации средней паузы между нажатиями клавиши на клавиатуре при наборе текста

Он предназначен для измерения времени, которое пользователь проводит между нажатиями клавиш в процессе набора текста. Эта информация может быть использована для оценки специфических характеристик и стилей набора каждого пользователя [38].

Основная цель модуля – собрать данные о средней паузе между нажатиями клавиш и использовать их в процессе валидации пользователя по текстовому следу. Паузы между нажатиями клавиш могут предоставить ценную информацию о темпе и ритме набора текста. Некоторые пользователи могут иметь более стабильный и регулярный ритм набора, в то время как

другие могут иметь более переменный и неравномерный ритм. Эти особенности могут быть использованы для создания уникального профиля текстового следа для каждого пользователя.

Собранные данные о средней паузе между нажатиями клавиш могут быть анализированы и сравниваться с эталонными значениями или паттернами, определенными в базе знаний системы валидации. Если обнаружены существенные отклонения от ожидаемых паттернов, это может свидетельствовать о наличии ошибок или несоответствий в работе пользователя.

Модуль по фиксации средней паузы между нажатиями клавиш имеет ряд особенностей. Он должен быть способен точно измерять время между нажатиями клавиш и сохранять полученные данные для последующего анализа. Также необходимо учитывать факторы, которые могут влиять на паузы, такие как физические особенности клавиатуры и индивидуальные особенности пользователя, например, уровень навыков и скорость набора текста [39].

Модуль по фиксации средней паузы между нажатиями клавиш является важным компонентом системы валидации пользователя по текстовому следу. Он предоставляет дополнительную информацию о стиле и характеристиках набора текста, которая может быть использована для более точной и надежной идентификации и валидации пользователя.

В рамках данного модуля экспертной системы применяется входной параметр, который представляет собой среднюю длительность нажатия клавиши на клавиатуре при наборе текста. Этот модуль имеет сходство с основными целями и алгоритмами модуля по фиксации скорости набора текста с клавиатуры.

2.1.11 Модуль по фиксации используемых специальных клавиш на клавиатуре при наборе текста

Модуль является методом аутентификации, который используется для проверки уникального профиля пользователя.

Этот модуль отслеживает профиль использования специальных клавиш на клавиатуре при наборе текста конкретным пользователем.

Модуль фиксирует такие дополнительные клавиши, как Shift, CapsLock, Tab и другие специальные клавиши, которые используются как часть обычного процесса ввода текста на клавиатуре.

Во время аутентификации клавиатурный профиль нового пользователя сравнивается с профилем, сохраненным для конкретного стиля использования специальных клавиш каждого зарегистрированного пользователя в системе.

Модуль аутентификации использует алгоритмы, которые изучают различные характеристики использования специальных клавиш на клавиатуре.

Каждый пользователь имеет свой уникальный клавиатурный профиль, который фиксируется в текстовом следе, а результаты идентификации пользователей могут быть переданы для дальнейшей обработки [37].

В рамках данного модуля экспертной системы применяется входной параметр, который представляет собой коллекцию из набора специальных клавиш, которые пользователь использует при вводе текста с клавиатуры. Этот модуль имеет сходство с основными целями и алгоритмами модуля по фиксации используемых специальных символов в тексте.

2.2 Модель мониторинга и принятия решений

Модель мониторинга и принятия решений представляет собой алгоритмический подход к обработке данных и принятию решений на основе анализа текстовых следов пользователя (рисунок 1). Она состоит из нескольких ключевых компонентов и этапов, описанных ниже:

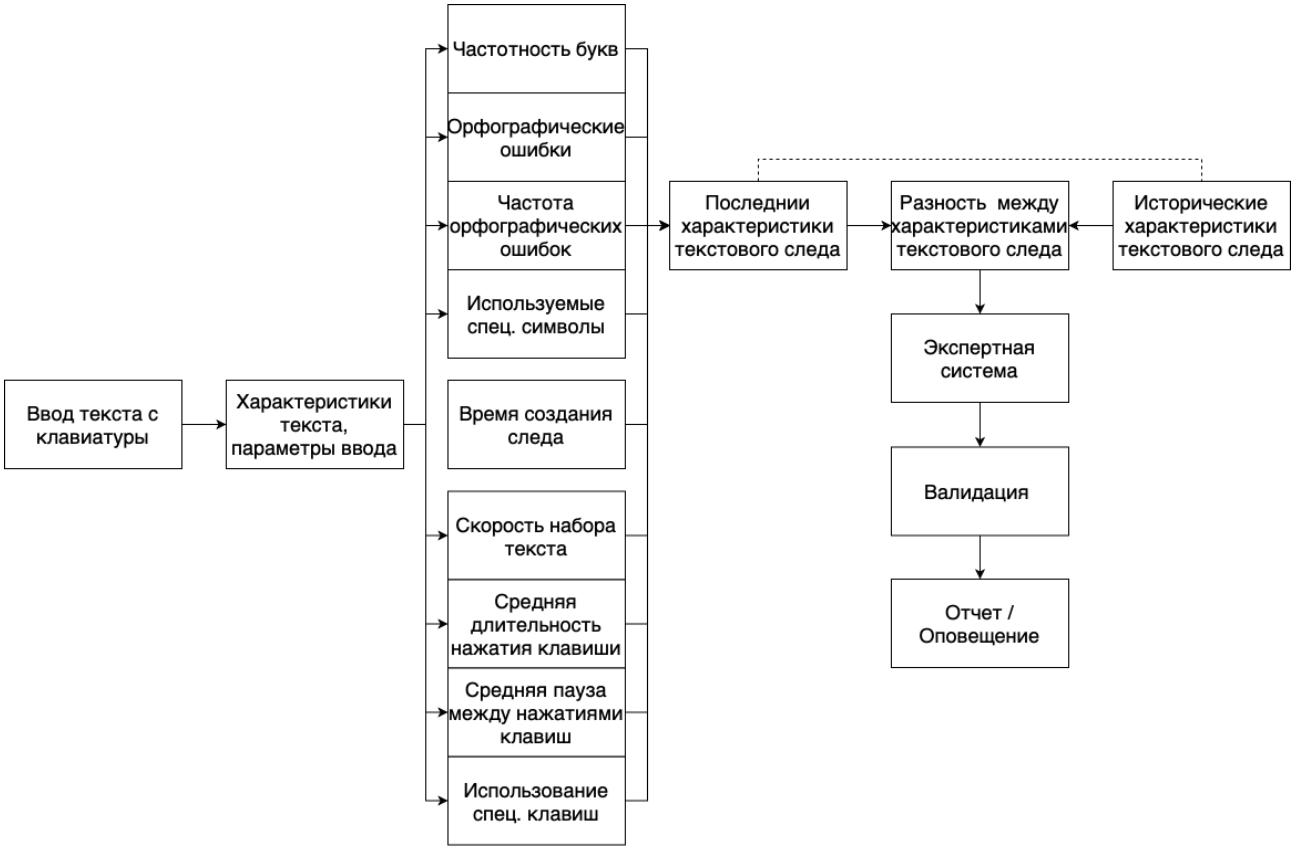

Рисунок 1 – Модель мониторинга и принятия решений

– сбор данных – на этом этапе происходит сбор текстовых следов пользователя, которые могут включать написанные тексты, ответы на вопросы, комментарии и другие письменные активности. Эти данные могут быть получены из различных источников, таких как онлайн-платформы, социальные сети или электронные дневники;

– собранные данные проходят предварительную обработку, которая может включать удаление шума, стандартизацию формата текста, токенизацию для дальнейшей обработки и анализа;

– извлечение признаков – на этом этапе из текстовых следов извлекаются различные признаки, которые могут быть полезны для валидации пользователя;

– с использованием извлеченных признаков проводится моделирование и анализ текстовых следов пользователя. Это может включать применение

методов машинного обучения, статистического анализа или экспертных систем для определения степени валидации и выявления аномалий или необычных паттернов;

– на основе результатов анализа и моделирования принимаются решения относительно валидности пользователя. Это может быть представлено в виде числовой оценки, категоризации или других форм результата. При этом могут применяться заданные пороговые значения или продукционные правила для определения степени валидации;

– модель мониторинга и принятия решений может работать в режиме непрерывного мониторинга, обновляя данные и принимая решения по мере получения новых текстовых следов. Это позволяет адаптировать методику и улучшать ее с течением времени на основе накопленного опыта.

Модель мониторинга и принятия решений валидации пользователя по текстовому следу позволяет автоматизировать процесс оценки письменных навыков и активностей пользователей, обеспечивая более объективную и систематическую оценку. Она имеет потенциал для применения в различных сферах, включая образование, анализ текстовых данных и многие другие.

2.2.1 База знаний и характеристики текстового следа

Для разработки базы знаний, которая будет использоваться в экспертной системе для валидации пользователей на основе текстового следа, необходимо определить, какие характеристики текстового следа мы хотим фиксировать и какие выходы должны быть у экспертной системы [7]. Для этого воспользуемся программой FLM_Builder. Также требуется разработать внутреннюю логику вывода, фазифицировать входные параметры и создать базу продукционных правил [3].

Входными параметрами для экспертной системы будут:

– частотность букв набранного текста с параметрами фазификации «уменьшилась», «в допуске», «увеличилась»;

– частотность орфографических ошибок в набранном тексте с параметрами фазификации «уменьшилась», «в допуске», «увеличилась»;

– слова с ошибками в набранном тексте с параметрами «нет совпадений», «есть совпадения»;

– используемые специальные символы встречающиеся в набранном текста с параметрами «нет совпадений», «есть совпадения»;

– время создания текстового следа с параметрами фазификации «недавний», «устаревший»;

– скорость набора текста на клавиатуре с параметрами фазификации «уменьшилась», «в допуске», «увеличилась»;

– средняя длительность нажатия клавиши на клавиатуре при наборе текста с параметрами фазификации «уменьшилась», «в допуске», «увеличилась»;

– средняя пауза между нажатиями клавиш на клавиатуре при наборе текста с параметрами фазификации «уменьшилась», «в допуске», «увеличилась»;

– используемые специальные клавиши на клавиатуре при наборе текста с параметрами «нет совпадений», «есть совпадения» [22].

2.2.2 Фазификация исходных данных

Многие из перечисленных входов необходимо предварительно перевести из количественного представления в качественный, произведя процесс фазификации. Фазификация используется для того, чтобы учесть неопределенность или нечеткость данных, которые могут быть связаны с измеряемыми характеристиками пользовательского текстового следа. Например, скорость набора текста на клавиатуре, может быть фазифицирована на основе следующих категорий: медленная, средняя и быстрая [22].

Процесс фазификации обычно включает определение нечетких множеств и функций принадлежности для каждой категории. Функция

принадлежности определяет, насколько данное значение принадлежит определенной категории, пример приведен на рисунке 1.

Рисунок 1 – Вид характеристических функций для параметра «Частотность орфографических ошибок»

2.2.3 Этапы конструирования экспертной системы

После обработки входных параметров необходимо произвести проверку следующих гипотез:

– динамика оценки по частотности с параметрами «уменьшилась», «в допуске», «увеличилась»;

– динамика личностных параметров текста с параметрами «уменьшилась», «в допуске», «увеличилась»;

– динамика личностных параметров текста с параметрами «уменьшилась», «в допуске», «увеличилась»;

– общая оценка стиля с параметрами «не соответствует», «соответствует»;

– общая оценка динамики с параметрами «не соответствует», «соответствует».

Их последовательность проверки приведена на рисунке 2. На выходе экспертная система на основании продукционных правил принимает решение по валидации пользователя [23].

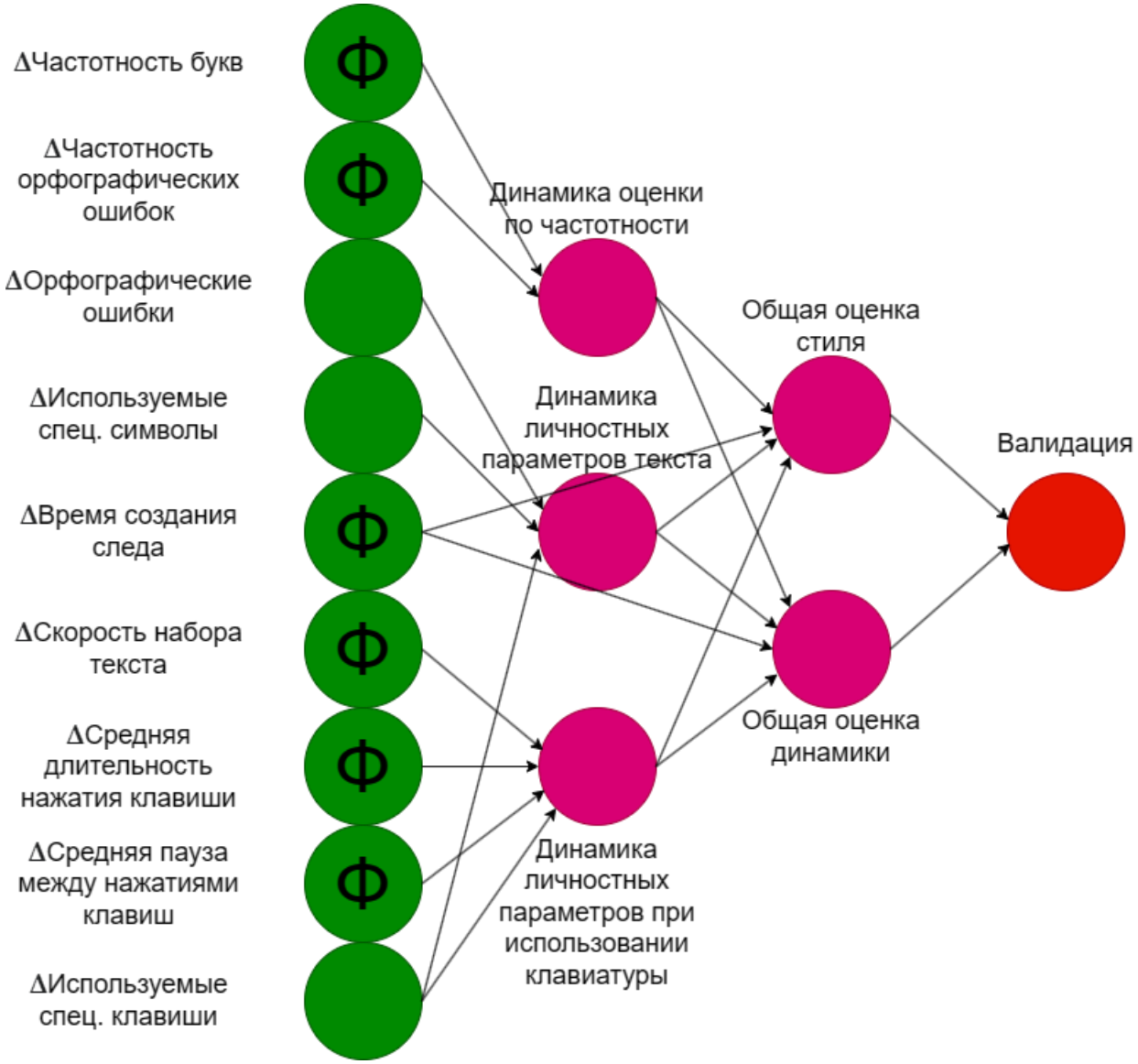

Рисунок 2 – Структура модели с нечеткой логикой

После формирования структуры базы знаний необходимо задать коллекции продукционных правил пример которых отображен на рисунке 3, которые будут переводить предпосылки в следствия для проверки гипотезы «Динамика оценки по частотности». Это тоже можно сделать в программе FLM_Builder, получив на выходе базу знаний для использования в языке Python. В результате конструирования мы получили процесс вывода, проверяющего 5 гипотез, который опирается на коллекцию из 107 правил.

№	ΔЧастотность орфографических ошибок	ΔЧастотность букв (Евклидово расстояние)	Динамика оценки по частотности
1	Уменьшилась	Уменьшилась	Уменьшилась 1
2	Уменьшилась	В допуске	В допуске 0,8
3	Уменьшилась	Увеличилась	Уменьшилась 0,5
4	В допуске	Уменьшилась	В допуске 0,8
5	В допуске	В допуске	В допуске 1
6	В допуске	Увеличилась	В допуске 0,8
7	Увеличились	Уменьшилась	Увеличилась 0,5
8	Увеличились	В допуске	В допуске 0,8
9	Увеличились	Увеличилась	Увеличилась 1

Рисунок 3 – Фрагмент коллекции правил в базе знаний

2.3 Методика динамической валидации пользователя по текстовому следу

Технология валидации пользователя по текстовому следу с использованием дерева решений может быть разделена на следующие этапы, включающие использование указанных модулей:

– модуль по фиксации эмпирических закономерностей распределения частотности букв в тексте:

1) собираются данные о распределении частотности каждой буквы в текстовых следах пользователей;

2) анализируются полученные данные для определения эмпирических закономерностей и формирования статистического профиля.

– модуль по фиксации орфографических ошибок в тексте:

1) идентифицируются орфографические ошибки в текстовых следах на основе словаря;

2) ошибки фиксируются и записываются для дальнейшей обработки.

– модуль по фиксации частоты орфографических ошибок в тексте:

1) рассчитывается частота орфографических ошибок в текстовых следах каждого пользователя;

2) информация о частоте ошибок записывается и используется для формирования статистического профиля.

– модуль по фиксации используемых специальных символов в тексте:

1) идентифицируются специальные символы, такие как знаки препинания, математические символы и другие особые символы;

2) записывается информация о частоте использования каждого специального символа для анализа текстового следа.

– модуль по фиксации даты создания текстового следа:

1) регистрируется дата и время создания каждого текстового следа для последующего анализа и сравнения.

– модуль по фиксации скорости набора текста с клавиатуры:

1) измеряется скорость набора текста пользователем на клавиатуре;

2) записывается информация о скорости набора для формирования статистического профиля пользователя.

– модуль по фиксации средней длительности нажатия клавиши на клавиатуре:

1) измеряется средняя длительность нажатия каждой клавиши при наборе текста;

2) записывается информация о длительности нажатия для формирования статистического профиля пользователя.

– модуль по фиксации средней паузы между нажатиями клавиш:

1) регистрируется средняя пауза между последовательными нажатиями клавиш;

2) информация о паузах используется для анализа пользовательской скорости и ритма печати.

– модуль по фиксации используемых специальных клавиш на клавиатуре:

1) идентифицируются специальные клавиши, такие как Shift, Ctrl, Alt и другие;

2) записывается информация о частоте использования каждой специальной клавиши для анализа пользовательского поведения [22].

Каждый модуль собирает и обрабатывает соответствующую информацию, формируя текстовый след для каждого пользователя. После этого, с использованием дерева решений, происходит сравнение текстовых следов и определение степени валидации пользователя на основе установленных правил и пороговых значений.

2.4 Выводы по главе

В данной главе была разработана методика динамической валидации пользователя по текстовому следу с использованием экспертной системы.

Были определены ключевые модули, необходимые для создания методики валидации по текстовому следу. Эти модули включают фиксацию эмпирических закономерностей распределения частотности букв, фиксацию орфографических ошибок, фиксацию частоты орфографических ошибок, фиксацию специальных символов, фиксацию времени создания текстового следа, фиксацию скорости набора текста на клавиатуре, фиксацию средней длительности нажатия клавиши, фиксацию средней паузы между нажатиями клавиш и фиксацию использования специальных клавиш на клавиатуре [15].

Так же следует отметить некоторые ограничения методики. Например, она может быть ограничена определенными языковыми особенностями или спецификой использования текстовых данных. Также, для эффективной работы методики требуется достаточное количество данных для обучения и настройки экспертной системы.

В целом, разработанная методика динамической валидации пользователя по текстовому следу с использованием экспертной системы является

перспективным подходом к идентификации пользователей на основе их письменных активностей.

3 Проверка работы методики на примере учебного процесса

Учебный процесс является ключевым компонентом образовательной среды и имеет высокую значимость в образовательных учреждениях. Он предоставляет возможность студентам проявить свои знания, навыки и компетенции через письменное общение, выполнение заданий и активное участие в дискуссиях.

В учебном процессе студенты генерируют значительное количество текстовых следов, таких как эссе, ответы на вопросы, комментарии и т.д. Эти следы могут содержать информацию о знаниях, умениях и личных особенностях студента.

Учебные платформы и системы часто сохраняют и хранят текстовые следы студентов, что облегчает доступ к данным для анализа и валидации.

В учебном процессе студенты проявляются в различных жанрах письменного выражения, от формальных академических текстов до неформальных комментариев и обсуждений. Это позволяет оценить эффективность методики валидации в различных контекстах.

Таким образом, выбор учебного процесса для проверки методики валидации по текстовому следу обоснован его значимостью, наличием доступных данных, разнообразием текстовых стилей и жанров, а также возможностью провести объективную оценку результатов.

3.1 Информационные источники для текстовой модели для систем автоматизированного обучения

Онлайн-учебная платформа обычно предоставляет студентам доступ к заданиям, которые они должны выполнить в рамках учебного процесса. Эти задания могут быть представлены в различных форматах, включая письменные работы, проекты, онлайн-тесты и другие активности. Студенты

могут загружать свои работы на платформу, где они будут оценены и получат обратную связь от преподавателей.

Одним из ключевых преимуществ онлайн-учебного процесса является возможность взаимодействия студентов с преподавателями и другими студентами через виртуальную среду. Это может осуществляться с помощью форумов обсуждений, чатов, электронной почты или онлайн-конференций. Студенты могут задавать вопросы, участвовать в обсуждениях, делиться своими мыслями и идеями, а также получать поддержку и советы от преподавателей и коллег.

Для внедрения методики валидации пользователя по текстовому следу в учебную платформу необходимо интегрировать разработанную методику в существующую структуру платформы. Это может быть достигнуто путем добавления новых полей с открытой формой, где пользователи будут выполнять письменные работы, отвечать на вопросы, публиковать свои проекты и другие активности, в результате чего будет формироваться их текстовый след.

При взаимодействии пользователей с платформой, система валидации будет обрабатывать данные, полученные от них, согласно заранее определенным алгоритмам. Эти алгоритмы основываются на базе знаний, которая содержит правила и эмпирические закономерности текстового следа, такие как частотность букв, орфографические ошибки, использование специальных символов и другие параметры.

Система будет создавать текстовый след для каждого пользователя, основываясь на его взаимодействии с платформой. Текстовый след будет представлять собой уникальную комбинацию характеристик и паттернов, которые определяют стиль и особенности письменной активности каждого пользователя. Этот текстовый след будет использоваться для идентификации и валидации пользователя.

Экспертная система, основываясь на продукционных правилах, будет проводить валидацию пользователя по его текстовому следу. Система будет

сравнивать характеристики и паттерны текстового следа с заранее установленными критериями и правилами, чтобы определить подлинность и качество работы пользователя. Результаты валидации сведут к минимизации проблем, связанных с подтверждением подлинности и качества работы студентов, а также могут быть использованы для дальнейшего анализа и оценки учебных достижений пользователя.

Интеграция методики валидации по текстовому следу в онлайн-учебную платформу позволит автоматизировать процесс проверки работ пользователей, обеспечивая более объективные и надежные результаты.

3.2 Условия проведения и фиксации результатов эксперимента

Эксперимент был проведен в условиях учебного процесса. В нем приняли участие представители трех групп магистрантов в рамках дисциплины «Методология научной деятельности».

Данная группа магистрантов выполняла ряд практических заданий, которые нужно было фиксировать на персональном компьютере в специально разработанной для эксперимента программной среде с открытой формой для ввода ответов.

Программная среда была выполнена в виде оконного приложения, которое предоставляет следующий функционал:

– функционал выбора пользователя – этот функционал позволяет исследователю выбрать пользователя из списка существующих учетных записей или создать новую учетную запись. Выбор пользователя является важным шагом, поскольку каждый пользователь будет иметь свой собственный текстовый след, который будет анализироваться и проверяться системой валидации;

– функционал добавления пользователя – на этом этапе исследователь создает учетную запись для каждого пользователя. Каждая учетная запись будет служить контейнером для сбора и формирования текстового следа

пользователя. Создание учетной записи обеспечивает индивидуализацию и отслеживание деятельности каждого пользователя в рамках эксперимента;

– после создания учетной записи и выбора пользователя, активируется поле с открытой формой, в котором пользователь может вводить текст определенной тематики, внешний вид данного приложения показан на рисунке 4. В этом поле пользователь может выполнять различные письменные задания, отвечать на вопросы, представлять свои проекты и другие активности. Важно отметить, что введенный текст захватываться приложением, которое фиксирует различные характеристики текста, используя предварительно разработанные модули. Эти модули обрабатывают текст и формируют текстовый след пользователя, который затем будет использоваться для его валидации.

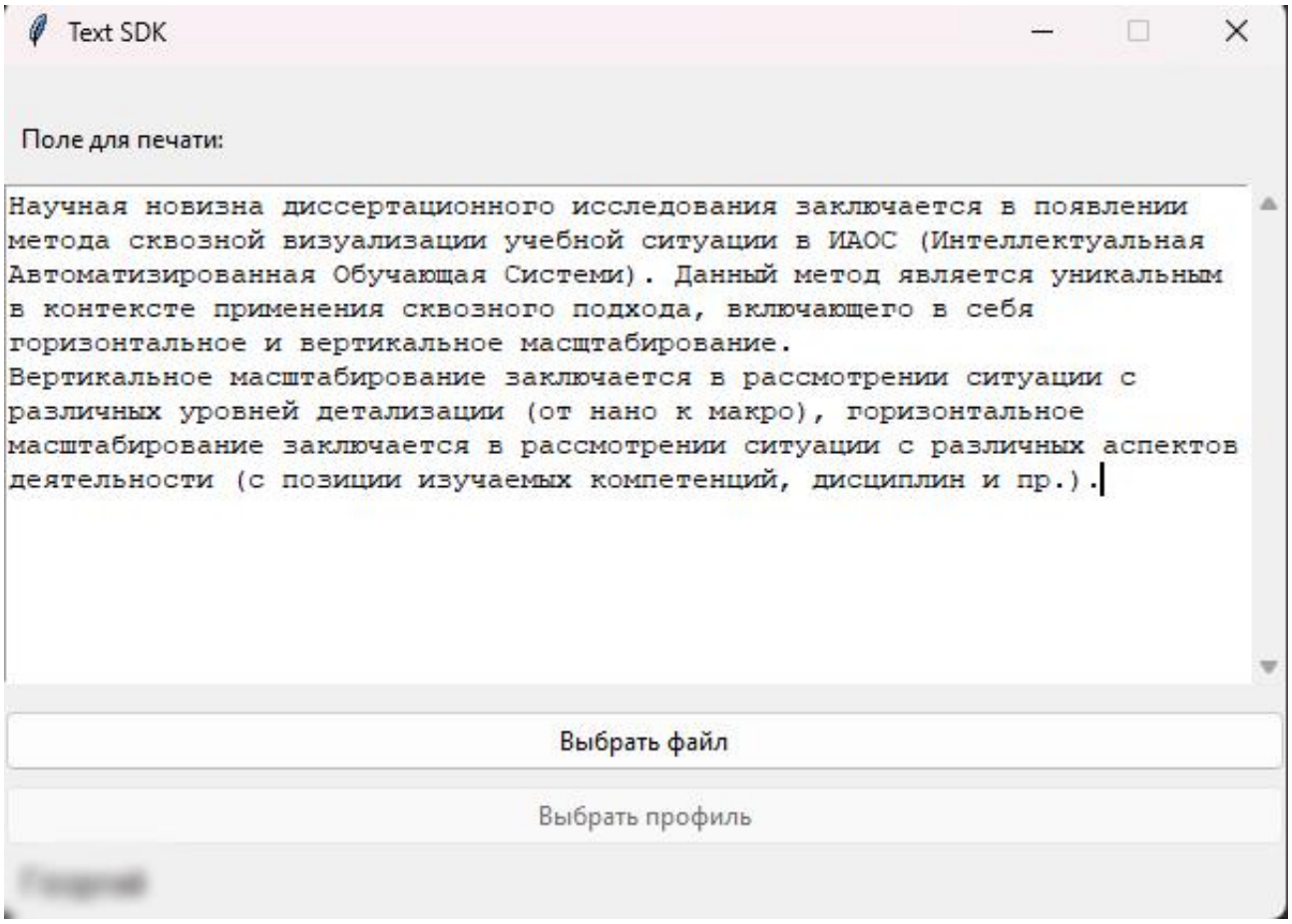

Рисунок 4 – Ввод текста пользователем

Это оконное приложение обеспечивает сбор и анализ данных текстового следа для каждого пользователя в рамках эксперимента. Оно позволяет исследователю контролировать ввод и сбор текстовых данных, а также автоматически обрабатывать и формировать текстовый след на основе предварительно разработанных модулей. Это важный инструмент для проверки работоспособности методики валидации пользователя по текстовому следу и оценки ее эффективности в контексте учебного процесса.

После завершения набора текста испытуемым необходимо закрыть приложение. Только после этого будет сформирован первый текстовый след испытуемого. На рисунке 5 представлена визуализация этого процесса. Закрытие приложения позволяет собрать и зафиксировать все необходимые данные, которые составляют текстовый след, включая информацию о частотности букв, наличии орфографических ошибок, использовании специальных символов и других параметрах.

Рисунок 5 – Визуализация создания текстового следа

Для возможности проведения валидации пользователя необходимо выполнить несколько итераций ввода текста. В каждой итерации пользователь будет вводить текст, после чего его текстовый след будет сравниваться с предыдущими текстовыми следами, накопленными в коллекции. Это позволит установить сходство или различия между текстовыми следами и определить подлинность идентифицируемого пользователя. На рисунке 6 представлена визуализация этого процесса, где каждый текстовый след сравнивается с предыдущими следами для проверки идентичности или изменений.

Рисунок 6 – Визуализация процесса сравнивания текстовых следов

Таким образом, проведение нескольких итераций ввода текста позволяет накопить коллекцию текстовых следов, которые могут быть использованы для последующей валидации и идентификации испытуемых. Сравнение нового текстового следа с предыдущими позволяет оценить степень сходства и установить, является ли испытуемый подлинным пользователем. Этот процесс повышает надежность и точность валидации пользователя по текстовому следу, основанной на экспертных знаниях и правилах.

После сбора текстовых следов от испытуемого и формирования набора данных, эти следы подвергаются сравнению. Сравнение осуществляется путем

анализа различий между текстовыми следами испытуемого. Для этого используются различные методы и алгоритмы, которые позволяют выявить уникальные характеристики в каждом следе.

Результаты сравнения текстовых следов подаются на вход экспертной системе. Экспертная система использует продукционные правила, которые определяют критерии и параметры для валидации пользователя. Эти правила основаны на экспертных знаниях и опыте, связанных с текстовым следом и его характеристиками.

При помощи продукционных правил, экспертная система анализирует разность между текстовыми следами и оценивает степень валидации каждого испытуемого. Оценка может основываться на различных факторах, таких как точность орфографии, использование специальных символов, стиль и структура текста, частотность определенных слов и другие характеристики текстового следа.

Итоговая оценка степени валидации может быть представлена в виде числовой или категориальной шкалы, отражающей уровень достоверности и качества текстового следа каждого пользователя. На рисунке 7 представлен процесс этой валидации.

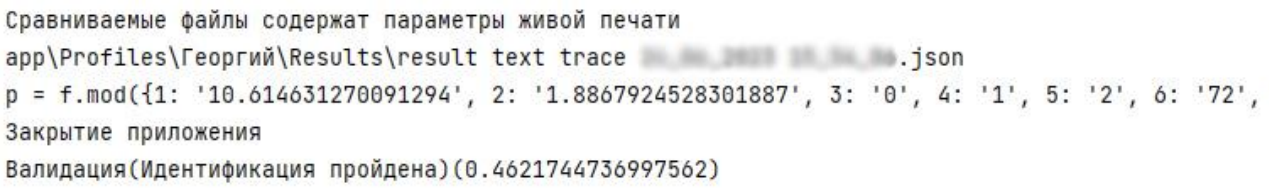

Рисунок 7 – Визуализация процесса принятия решения ЭС

Таким образом, сравнение текстовых следов и использование продукционных правил в экспертной системе позволяет определить степень валидации пользователя по его текстовому следу. Это важный шаг в разработке методики валидации, так как позволяет объективно и автоматизировано

оценить качество и подлинность работы пользователя на основе его письменных активностей.

3.3 Анализ результатов эксперимента

В ходе проведения эксперимента были получены данные о текстовом следе каждого участника эксперимента, которые сведены в таблицы и представлены в приложении.

На основе анализа данных были построены гистограммы, изображенные на рисунке 8 и 9, по которым четко видно разделение пользователей по следующим классам сравнения:

– сравнение двух текстовых следов одного и того же пользователя;

– сравнение текстовых следов разных пользователей.

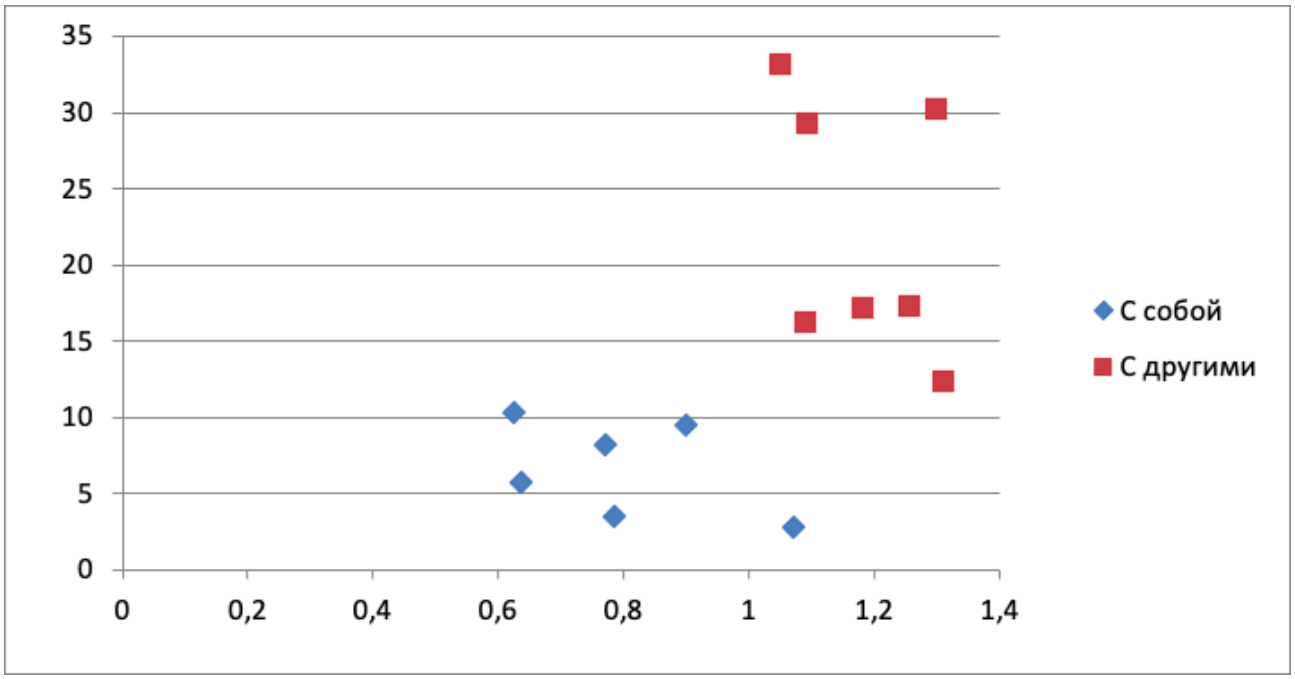

Рисунок 8 – Сравнительный анализ текстовых следов

По гистограмме, представленной на рисунке 8 видно, что текстовые следы одного и того же пользователя сконцентрированы в облаке точек, а текстовые следы разных пользователей хаотично разбросаны.

По гистограмме, представленной на рисунке 9 так же сохраняется эта закономерность.

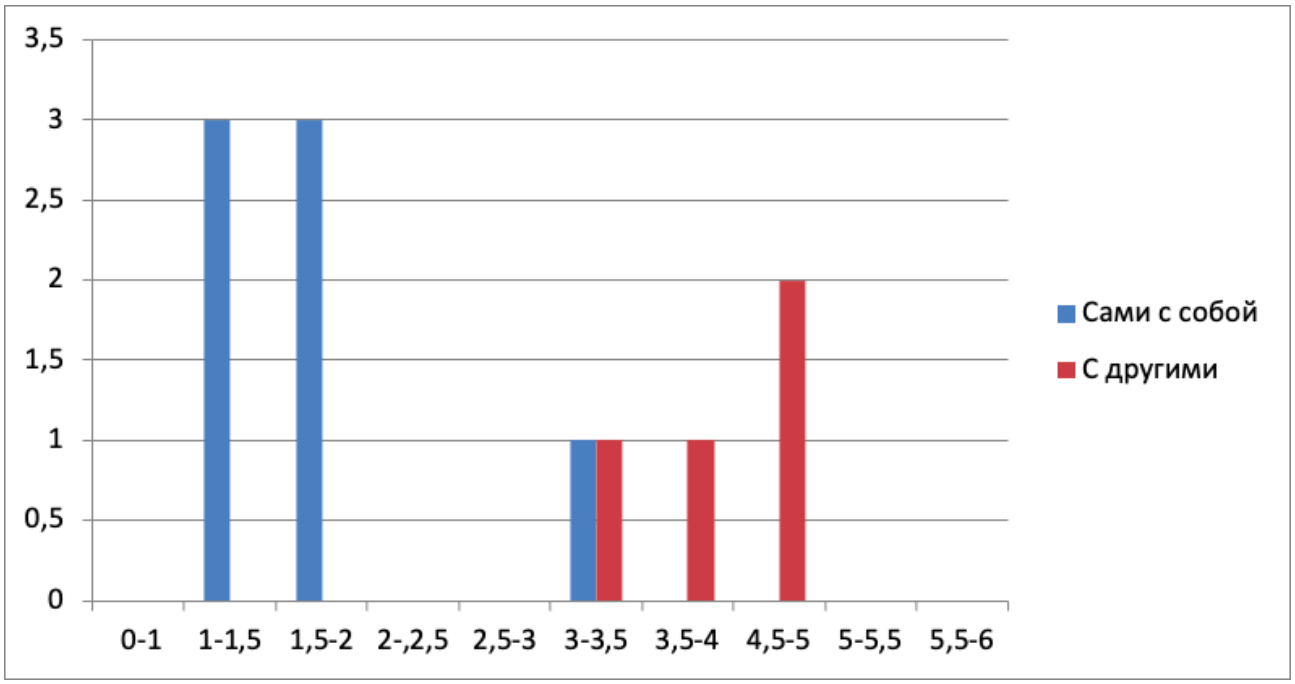

Рисунок 9 – Сравнительный анализ текстовых следов

Следовательно, можно сделать вывод что основываясь на характеристических значениях текстового следа можно различать пользователей друг от друга, а следовательно выявлять подмену.

3.4 Выводы по главе

В ходе эксперимента была подтверждена гипотеза разработанной методики валидации пользователя по текстовому следу с использованием экспертной системы. Эта методика была применена на примере учебного

процесса, что позволило проверить ее работоспособность и эффективность в реальной среде.

Проверка методики на примере учебного процесса позволила получить ценные результаты. Были собраны данные о текстовом следе студентов, включая информацию о частотности букв, орфографических ошибках, использовании специальных символов и других параметрах. Эти данные были обработаны с помощью экспертной системы, и на основе полученного текстового следа была осуществлена валидация студентов.

Результаты проверки методики показали ее эффективность в определении и идентификации пользователей на основе текстового следа. Методика позволила достичь точности и надежности при валидации студентов. Она смогла различить подмену одних студентов другими по их индивидуальным особенностям текстового следа, таким как орфография, стиль написания и другим характеристикам.

Применение методики валидации пользователя по текстовому следу в процессе дистанционного обучения имеет значительный потенциал. Она может быть использована для существенного снижения вероятности перехвата удаленного управления информационной системой и подмены пользователя более осведомленным лицом при прохождении аттестационных заданий.

Дальнейшее развитие исследования может включать расширение методики валидации пользователя по текстовому следу для других областей применения, а также улучшение ее алгоритмов и адаптацию под различные типы текстовых данных. В целом, проверка работы методики на примере учебного процесса подтвердила ее эффективность и потенциал для использования в различных сферах, связанных с идентификацией и оценкой пользователей на основе их текстового следа.

ЗАКЛЮЧЕНИЕ

Исследование, посвященное разработке методики валидации пользователя по текстовому следу с помощью экспертной системы, завершено. В ходе работы были достигнуты поставленные цели и решены задачи, связанные с рассмотрением существующих методов идентификации пользователя, разработкой экспертной системы для оценки степени валидации пользователя, разработкой новой методики валидации для автоматизированной информационной системы и экспериментальным подтверждением реализуемости предложенного решения.

Результаты исследования позволяют сделать следующие выводы. Первоначальный анализ существующих методов идентификации пользователя позволил выявить их преимущества и недостатки. Разработанная экспертная система демонстрирует эффективность в оценке степени валидации пользователя на основе текстового следа. Новая методика валидации, основанная на комбинации различных параметров текстового следа, позволяет достичь более точной и надежной оценки пользователя.

Гипотеза исследования, о том, что разработанная методика валидации пользователя по текстовому следу с использованием экспертной системы будет эффективной и применимой в автоматизированных информационных системах, подтверждена. Научная новизна и практическая значимость работы заключаются в разработке новой методики валидации, которая может быть применена при выявлении подмены пользователя при дистанционном образовании, в ракетно-космической отрасли при работе с электронным документооборотом и других различных сферах требующие проверки идентичности пользователя.

В ходе выполнения данной НИР было опубликовано две статьи:

– база знаний для системы валидации пользователей по текстовому следу [22];

– конструирование и реализация экспертной системы валидации пользователей по текстовому следу [23].

Дальнейшие исследования в этом направлении имеют перспективы. Можно провести дополнительные эксперименты, расширить функциональность экспертной системы, улучшить алгоритмы обработки данных текстового следа и провести сравнительный анализ с другими методами идентификации пользователя. Также стоит рассмотреть возможности применения разработанной методики в других областях и провести дополнительные исследования по ее применимости и эффективности.

В целом, данная работа имеет важное научное и практическое значение, расширяет представления о возможностях валидации пользователя по текстовому следу и предлагает новый подход, который может быть применен в различных информационных системах для обеспечения безопасности и аутентификации пользователей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Беленков, В. Д. Электронные системы идентификации подписей / В. Д. Беленков ; Защита информации. – Санкт-Петербург : Конфидент, 1997. – №6. – С. 39-42.

2 Белоцерковский О. М. Компьютерное распознавание человеческих лиц / О. М. Белоцерковский, А. С. Глазунов, В. В. Щенников ; Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. – Москва : [б.и.], 1997. – №8. – С. 3-14.

3 Болсуновский, Н. А. Конструктор продукционных экспертных систем с элементами нечёткой логики FLM_Builder и интеграция его моделей в пользовательские проекты / Н. А. Болсуновский, А. Д. Пронин, В. А. Углев ; Нейроинформатика, ее приложения и анализ данных: XXX Всероссийский семинар. – Красноярск : ИВМ СО РАН, 2022. – С. 24-33.

4 Бочкарев, С. Л. Новые возможности биометрических голосовых технологий / С. Л. Бочкарев, Л. Н. Сапегин ; Защита информации. – Санкт-Петербург : Конфидент, 2003. – №5. – С. 34-39.

5 Брюхомицкий, Ю. А. Система скрытного клавиатурного мониторинга / Ю. А. Брюхомицкий, М. Н. Казарин ; Известия ТРТУ. Таганрог : ТРТУ, 2006. – № 9. – С. 153-154.

6 Васильев, В. И. Распознавание психофизиологических состояний пользователей на основе скрытого мониторинга действий в компьютерных системах / В. И. Васильев, А. Е. Сулавко, Р. В. Борисов ; Искусственный интеллект и принятие решений. Москва : ФИЦ ИУ РАН, 2017. – № 3. – С.21-37.

7 Гаврилова, Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский ; Санкт-Петербург.: Питер, 2001. – 384 с.

8 Гальперин, И. Р. Текст как объект лингвистического исследования / И. Р. Гальперин ; – 4-е изд., стереотип. – Москва.: КомКнига, 2006. – 144 с.

9 Горелик, В. Ю. Идентификация и аутентификация пользователей веб – ориентированной информационной системы / В. Ю. Горелик, Г. А.

Пискунов ; Перспективные системы и технологии как парадигма технического прорыва: сборник статей по итогам Международной научно-практической конференции. – Тюмень: Агентство международных исследований, 2020. – С. 14-21.

10 Гузик, В. Ф. Биометрический метод аутентификации пользователя / В. Ф. Гузик, М. Н. Десятерик ; Известия ТРТУ. Технические науки. – Таганрог : ТРТУ, 2000. – № 2. – С. 129-133.

11 Довгаль, В.А. Захват параметров клавиатурного почерка и его особенности /А. В. Довгаль ; Материалы всероссийской научно-практической конференции «Информационные системы и технологии в моделировании и управлении». Симферополь : Ариал, 2017. – С.230-236.

12 Довгаль, В. А. Обзор характеристик производительности наборов данных, используемых для обеспечения информационной безопасности на основе клавиатурного почерка / В. А. Довгаль ; Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. Майкоп : АГУ, 2016. – №191. – С. 157-163.

13 Дэвид Уиллис Шесть биометрических устройств идентификации отпечатков пальцев / Дэвид Уиллис, Майк Ли. ; Сети и системы связи. Москва : «Ритм-Пресс», 1998. – С. 146-155.

14 Епифанцев, Б. Н. Альтернативные сценарии авторизации при идентификации пользователей по динамике подсознательных движений / Б. Н. Епифанцев, П. С. Ложников, А. Е. Сулавко ; Вопросы защиты информации ФГУП «ВИМИ». Москва : Компас, 2013. – № 2. – С. 28-35.

15 Еременко, А. В. Двухфакторная аутентификация пользователей компьютерных систем на удаленном сервере по клавиатурному почерку / А. В. Еременко, А. Е. Сулавко ; Прикладная информатика. Москва : Синергия, 2015. – Т. 6. – №60. – С. 48-59.

16 Еременко, Ю. И. Идентификация пользователя по его клавиатурному почерку / Ю. И. Еременко, Ю.С. Олюнина ; Сборник материалов Двенадцатой Всероссийской научно-практической конференции с международным участием

«Современные проблемы горно-металлургического комплекса. Наука и производство». Старый Оскол : СТИ НИТУ МИСиС, 2015. – С. 147-151.

17 Заде, Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. А. Заде ; Москва.: Мир, 1976. – 165 с.

18 Задорожный, В. Обзор биометрических технологий / В. Задорожный ; Защита информации. Санкт-Петербург : Конфидент, 2003. – № 5. – С. 26-29.

19 Иванов, А. И. Нейросетевые алгоритмы биометрической идентификации личности / А. И. Иванов ; Москва.: Радиотехника. 2004. – 143 с.

20 Калужин, А. С. Подтверждение личности пользователя по его клавиатурному подчерку / А. С. Калужин, Д. Д. Рудер ; Известия Алтайского государственного университета. Барнаул : Алтайского гос. ун-та, 2015. – Т. 1. – №85. – С. 158-162.

21 Филлипс, К. Ваше лицо – гарант безопасности / К. Филлипс ; PCWEEK RUSSIAN EDITION. Москва : Термика, 1997. – С. 35-38.

22 Кириличев, А. О. База знаний для системы валидации пользователей по текстовому следу / А. О. Кириличев, В. А. Углев ; АКТУАЛЬНЫЕ НАУЧНЫЕ ИССЛЕДОВАНИЯ: сборник статей XII Международной научно-практической конференции. В 4 ч. Ч. 2. – Пенза : МЦНС «Наука и Просвещение», 2023. – С. 73-76.

23 Кириличев А.О., Болсуновский Н.А. Конструирование и реализация экспертной системы по валидации пользователя на основе текстового следа / А.О. Кириличев, Н.А. Болсуновский ; Нейроинформатика, ее приложения и анализ данных: XXXI Всероссийский семинар. Красноярск : ИВМ СО РАН, 2023. (в печати)

24 Коляда, Н. А. Адаптивная технология идентификации пользователя по клавиатурному почерку / Н. А. Коляда, Ю.А. Чернявский ; Информатика. Москва : Мир, 2007. № 1. – С. 106-113.

25 Коротаев, Г. А. Анализ и синтез речевого сигнала методом линейного предсказания / Г. А. Коротаев ; Зарубежная радиоэлектроника. Москва : [б. и.], 1990. – №3. – С. 31-50.

26 Мазниченко, Н. И. Анализ возможностей систем автоматической идентификации клавиатурного подчерка / Н. И. Мазниченко, М. В. Гвозденко ; Вестник Национального технического университета Харьковский политехнический институт. Серия: Информатика и моделирование. Харьков : НТУ «ХПИ», 2008. – №24. – С. 77-81.

27 Мартынова, Л. Е. Исследование и сравнительный анализ методов аутентификации / Л. Е. Мартынова, М. Ю. Умницын, К. Е. Назарова ; Молодой ученый. Казань : Молодой ученый, 2016. –№ 19 (123). – С. 90-93.

28 Минаев, В. А. Оценка рисков идентификации и аутентификации субъектов электронного взаимодействия / И.Д. Королев, А.Г. Сабанов ; Вестник УрФО. Безопасность в информационной сфере. Челябинск : УрФО, 2018. – № 4(30). – С. 43-49.

29 Рыбченко, Д. Е. Критерии устойчивости и индивидуальности клавиатурного почерка при вводе ключевых фраз / Д. Е. Рыбченко ; Специальная техника средств связи. Серия Системы, сети и технические средства конфиденциальной связи. Пенза : ПНИЭИ, 1997. Выпуск №2. – С.104-107.

30 Рыбченко, Д. Е. Анализ клавиатурного почерка аппаратом нечетких множеств для целей ограничения доступа и аудита. / Д. Е. Рыбченко, А.И. Иванов ; Специальная техника средств связи. Серия Системы, сети и технические средства конфиденциальной связи. Пенза : ПНИЭИ, 1996. Выпуск 1. – С.116-119.

31 Сарбуков, А. Е. Аутентификация в компьютерных системах / А. Е. Сарбуков, А. А. Грушко ; Системы безопасности. Москва : Гротек, 2003. – № 5(53). – С. 118-122.

32 Скуратов, С. В. Использование клавиатурного почерка для аутентификации в компьютерных информационных системах / С. В. Скуратов ; Безопасность информационных технологий. Москва : МЦНМО, 2010. – № 2. – С. 35-38.

33 Сулавко, А. Е. Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей / А. Е. Сулавко ; Компьютерная оптика. Самара : ИСОИ РАН, 2020. – № 1. – С. 82-91.

34 Фунтиков, В. А. Автоматическое прогнозирование уровня безопасности / В. А. Фунтиков, О. В. Ефремов, А. И. Иванов ; Защита информации. Конфидент. Санкт-Петербург : Конфидент, 2003. – №5. – С.30-33.

35 Хоменко, А. Ю. Автоматическая обработка текста и лингвистическое моделирование как способы решения проблем атрибуционной лингвистики / А. Ю. Хоменко, Е. Р. Бенькович, Д. И. Гайнутдинова ; Политическая лингвистика. Екатеринбург : УрГПУ, 2020. – № 3 (81). – С. 215-224.

36 Ходашинский, И. А. Технология усиленной аутентификации пользователей информационных процессов / И. А. Ходашинский, М. В. Савчук, И.В. Горбунов ; Доклады Томского государственного университета систем управления и радиоэлектроники. Томск : ТУСУР, 2011. – № 2–3 (24). – С. 236-248.

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий
институт

Межинститутская базовая кафедра
«Прикладная физика и космические технологии»
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ В.Е. Косенко
подпись инициалы, фамилия
«28» 06 2023 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

«Разработка методики валидации пользователя по текстовому следу с помощью экспертной системы»
тема

09.04.01 «Информатика и вычислительная техника»
код и наименование направления

09.04.01.03 «Информационные системы космических аппаратов и центров управления полетами»
код и наименование магистерской программы

Руководитель	_____	доцент МБК ПФ и КТ, канд. техн. наук	В.А. Углев
	подпись, дата	должность, ученая степень	инициалы, фамилия
Выпускник	_____		А.О. Кириличев
	подпись, дата		инициалы, фамилия
Рецензент	_____	згд по качеству АО «РЕШЕТНЁВ», канд. техн. наук	Ю.В. Кочев
	подпись, дата	должность, ученая степень	инициалы, фамилия
Нормоконтролер	_____	профессор МБК ПФиКТ, д-р техн.наук	В.Е. Чеботарев
	подпись, дата	должность, ученая степень	инициалы, фамилия

Красноярск 2023

Scanned with AnyScanner