ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ НЕФТИ И ГАЗА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ) ИМЕНИ
И.М. ГУБКИНА»

На правах рукописи

Уймин Антон Григорьевич

СИСТЕМА НЕПРЕРЫВНО-ДИСКРЕТНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ АНАЛИЗА ПОТОКА ДАННЫХ КОМПЬЮТЕРНОЙ МЫШИ

Специальность 2.3.8 –
«Информатика и информационные процессы»
Специальность 2.3.6 –
«Методы и системы защиты информации, информационная безопасность»

Диссертация на соискание учёной степени
кандидата технических наук

Научный руководитель:
кандидат технических наук, доцент
Белоусов Александр Валерьевич

Москва – 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В условиях интенсивной цифровой трансформации и повсеместного внедрения распределенных вычислительных сред обеспечение информационной безопасности трансформируется из прикладной инженерно-технической задачи в фундаментальный критерий системной устойчивости сложноструктурированных комплексов. В классической теории информационных процессов предполагается, что идентификация источника информации либо предшествует взаимодействию, либо осуществляется однократно в момент установления соединения [86; 89; 90]. Соответственно, базовые механизмы защиты строятся на дискретной «шлюзовой» модели, где идентификация, заключающаяся в присвоении и сравнении идентификаторов, и аутентификация, направленная на проверку подлинности субъекта, реализуются как разовый акт при входе в систему [20; 126; 152].

Однако такой подход имеет жесткие границы применимости в условиях удаленного взаимодействия. В современных децентрализованных системах первоначальная сверка с базой учетных записей на центральном сервере решает лишь задачу начального разграничения доступа, но не обеспечивает динамическую устойчивость защищаемого контура. Возникает критическая временная уязвимость: после однократной проверки субъект получает долгосрочный мандат на выполнение операций. В этих условиях основной вектор угроз смещается на постаутентификационную фазу, где главной проблемой становится не отказ аппаратных узлов, а компрометация доверенного субъекта. Классическая серверная парадигма порождает специфические векторы атак, такие как подмена контекста с перехватом управления после авторизации легитимного пользователя, отложенная компрометация сеанса и деградация атрибутов безопасности, о которых система остается неосведомленной до следующего планового запроса [42; 163].

Для повышения эффективности защищенности систем требуется концептуальный переход от дискретного контроля к непрерывной

верификации. Механизм проверки подлинности трансформируется из сервисной функции в перманентный информационный процесс. В отличие от бинарного решения на этапе входа, непрерывная аутентификация характеризуется асинхронностью, высокой энтропией исходных данных и потоковой природой. Результатом такого процесса является динамически вычисляемая функция доверия, значения которой доступны подсистемам управления доступом в режиме реального времени. Реализация подобного подхода требует источников данных, анализ которых происходит прозрачно для пользователя, что позволяет преодолеть ограничения традиционных методов, основанных на паролях или токенах.

Одним из перспективных направлений в этой области выступает использование поведенческой биометрии, в частности – анализ информационного потока данных о движениях компьютерной мыши. В рамках разрабатываемой модели под надёжностью биометрической системы на основе паттернов движения мыши понимается её способность точно и перманентно распознавать субъекта на основании уникальных характеристик поведения при взаимодействии с устройством. Данная надежность и устойчивости к внешним шумам, повторяемости признаков, высокой скорости обработки, а также минимизации уровней ложных срабатываний (FAR и FRR). Кроме того, эффективная система должна обладать адаптивностью к изменению состояния пользователя и обеспечивать высокий уровень удобства использования. Только комплексное сочетание этих характеристик позволяет создать надежный механизм непрерывного контроля подлинности, отвечающий актуальным вызовам информационной безопасности.

Актуальность данной работы в контексте теории информационных процессов обусловлена необходимостью формализации и алгоритмизации непрерывных потоков контроля подлинности, протекающих параллельно с целевыми потоками данных. В отличие от традиционных задач кодирования, здесь требуется оперативный анализ косвенных поведенческих признаков для минимизации задержки принятия решения при обнаружении аномалий,

сохраняя при этом допустимую нагрузку на вычислительные узлы и каналы связи.

С точки зрения информационной безопасности актуальность темы определяется необходимостью устранить разрыв между тем доверием, которое сервер устанавливает в момент входа, и фактической подлинностью пользователя в каждый последующий момент времени. Главным механизмом, обеспечивающим динамическую устойчивость системы к атакам на легитимные сессии, выступает непрерывный контроль подлинности. Исследование располагается на стыке двух направлений. Первое – изучение слабоструктурированных фоновых информационных процессов. Второе – защита сессионного уровня в условиях, когда состояние клиентской среды не может считаться неизменным.

Проблематика исследования. Конфликт между уровнем безопасности и приватностью пользователя – основная проблема современных биометрических систем. Применение статических признаков (овал лица, отпечатки пальцев) предполагает специализированное оборудование, ощутимые серверные мощности и сопряжено с высокими рисками при утечке чувствительных данных. Возрастные изменения или травмы пользователя дополнительно снижают эффективность таких систем.

Указанные риски нивелирует поведенческая биометрия – в первую очередь анализ динамики взаимодействия пользователя с компьютерной мышью. Данный подход извлекает уникальные признаки из стандартных потоков информационного обмена (движения курсора, клики) без необходимости дооснащать рабочее место аппаратными средствами. С математической точки зрения движение мыши представляет собой высокоэнтропийный поток данных, которого достаточно для поддержания непрерывной функции доверия. За пределами конкретной системы подобный поток не позволяет однозначно деанонимизировать личность, что снимает вопрос конфиденциальности.

Методологическую базу исследования составляют положения теории вероятностей, математической статистики и теории системного анализа. При решении прикладных задач идентификации и моделирования функции доверия использовались методы машинного обучения (в частности, глубоких сверточных нейронных сетей), математического моделирования временно изменяющихся процессов [33; 34; 35; 37; 38; 40; 43; 46; 47; 48; 50], а также методы сравнительного и структурно-функционального анализа сложноструктурированных систем. Теоретический фундамент работы опирается на три ключевых направления:

Теоретической основой работы являются труды в области

– исследования биометрических данных и систем биометрической аутентификации: Anil K. Jain, Lin Hong, Sharath Pankanti, Ajay Kumar, а также работы Ю.П. Гаврильченко, М.Ю. Ларионова и И.Н. Карцана;

– методы цифровой обработки сигналов и моделирования: исследования Потапова А.А., Коробовой Л.А., Самарского А.А., Михайлова А.П., а также прикладные разработки Е.К. Брагина и Т.И. Лапиной;

– информационная безопасность систем аутентификации: работы Шелупанова А.А., Miloslav Hub, Dimitrios Hatzinakos, J. Wayman и A.C. Weaver.

Рабочей гипотезой в данном случае выступает предположение о том, что интеграция методов потоковой обработки сигналов динамики компьютерной мыши в архитектуру сессионного уровня позволяет создать эффективный механизм непрерывной биометрической аутентификации, устойчивый к атакам подмены контекста.

Целью диссертационной работы является разработка методов повышения эффективности информационных процессов аутентификации пользователей информационных систем с применением нейросетевых технологий на основе создания программной системы, обеспечивающей непрерывно-дискретную биометрическую аутентификацию.

Для достижения указанной цели в рамках исследования были поставлены и решены следующие задачи:

– *Проведен* анализ существующих подходов к идентификации и аутентификации пользователей для выявления ограничений, влияющих на стоимость и качество решения.

– *Исследованы* возможности использования в информационных процессах аутентификации стандартных средств ввода-вывода персональных компьютеров.

– *Разработан новый* метод аутентификации пользователя на основе индивидуальных признаков, выделяемых в потоке данных, получаемых от компьютерной мыши.

– *Сформулированы* требования к программной системе, обеспечивающей постоянную (непрерывно-дискретную) биометрическую аутентификацию пользователей, на основе результатов анализа.

– *Создана* программная реализация системы непрерывно-дискретной биометрической аутентификации пользователей.

– *Предложены рекомендации* по применению разработанной системы в различных контекстах.

Объектом исследования являются информационные процессы в децентрализованных автоматизированных информационных системах с разграничением доступа, применяемые для аутентификации пользователей.

Предметом исследования выступают методы, модели, алгоритмические и программные средства обработки информации для аутентификации пользователей, реализуемые на основе анализа поведенческих (биометрических) паттернов.

Теоретическая значимость работы состоит в развитии подходов к моделированию информационных процессов удалённого взаимодействия пользователей с информационными ресурсами, формализации цифрового поведения субъекта, находящегося вне контролируемой зоны, и применению методов поведенческой биометрии в задачах аутентификации. Предложенные

модели и методы могут использоваться для анализа непрерывно-дискретных информационных потоков, формирования паттернов цифрового поведения и их распознавания в условиях нестабильных коммуникационных сред.

Научная новизна исследования:

– Предложен новый метод аутентификации пользователей на основе динамики движения компьютерной мыши, отличающийся устойчивостью к поведенческой изменчивости пользователей и наличием механизмов адаптации к разнородным условиям взаимодействия, что позволяет усовершенствовать информационные процессы аутентификации в части повышения точности цифровой интерпретации поведения в условиях удалённого доступа (пункт 3 паспорта специальности 2.3.8, пункт 2 паспорта специальности 2.3.6).

– Разработана многоуровневая модель информационного процесса удалённого управления, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков, что обеспечивает возможность формализации и автоматической интерпретации действий пользователя как информационного субъекта, находящегося вне контролируемой зоны, для проведения его аутентификации (пункт 1 паспорта специальности 2.3.8, пункт 12 паспорта специальности 2.3.6).

– Разработана архитектура системы биометрической аутентификации на основе сверточных нейронных сетей, учитывающая особенности непрерывно-дискретного поведенческого потока при удаленной работе с режимом адаптивного обучения, что обеспечивает устойчивую классификацию цифрового поведения в реальном времени с высокой точностью при низкой вычислительной нагрузке (пункт 9 паспорта специальности 2.3.8, пункт 15 паспорта специальности 2.3.6).

Результаты диссертационного исследования докладывались и получили положительную оценку на международных, всероссийских и региональных научных конференциях.

Практическая значимость работы заключается в повышении эффективности цифрового контроля административных действий путем внедрения программной системы, реализующей предложенные методы анализа поведенческих признаков без использования дополнительного оборудования. Полученные результаты применены при построении систем доверенного удалённого доступа, в том числе в инфраструктурах образовательных, корпоративных и телекоммуникационных систем, а также при разработке решений в области информационной безопасности с акцентом на подтверждение подлинности субъектов управления.

Положения, выносимые на защиту:

1) Метод непрерывно-дискретной биометрической аутентификации, основанный на применении глубокого обучения (CNN) для автоматического извлечения пространственно-временных признаков динамики мыши. Метод обеспечивает устойчивую верификацию цифрового профиля в режиме реального времени с точностью (Accuracy) до 98,50% в сценарии одиночных движений и минимальным уровнем половинной частоты ошибок (HTER = 0,0120) при обработке комплексных поведенческих паттернов (координатно-временных траекторий перемещения, наведения и кликов). При этом вычислительный алгоритм характеризуется низким уровнем ресурсоемкости, обеспечивая суммарную нагрузку на компоненты пользовательской системы в пределах 7,1%, что не снижает общую производительность среды функционирования.

2) Многоуровневая модель информационного процесса удалённого доступа, включающая уровни взаимодействия, анализа поведенческого контекста и потоковой оценки цифровых признаков, что позволяет снизить число ложно-положительных событий в 1,5 раза по сравнению с аналогами.

3) Архитектура системы биометрической аутентификации на основе сверточных нейронных сетей, учитывающая динамику и структуру поведенческих сигналов непрерывно-дискретного поведенческого потока при удаленной работе с режимом адаптивного обучения, повышает устойчивость

биометрических систем к колебаниям пользовательского поведения до 15% в эксперименте с контрольными группами.

Работа состоит из введения, четырёх глав и заключения. Список использованной литературы содержит 189 наименований, отражающих историю и текущее состояние исследований в данной области.

Во введении обоснована актуальность исследования, определены объект и предмет исследования, сформулированы цель и задачи работы. Особое внимание уделено созданию точных и высокопроизводительных систем биометрической аутентификации, цель которых – повысить защищённость и устойчивость распределённых информационных систем.

В первой главе раскрываются теоретические аспекты информационных процессов биометрической аутентификации. Раскрыта сущность биометрии и история её развития применительно к задаче устойчивости информационных систем. Специфика неизменности состояния сеанса работы пользователя рассмотрена отдельно: идентификация пользователя определяется как инвариант на всём протяжении транзакционного цикла. В главе также разбираются тенденции и перспективы нейросетевых технологий при переходе от дискретных методов проверки к моделям непрерывного контроля.

Вторая глава посвящена исследованию возможностей использования стандартных средств ввода-вывода в информационных процессах аутентификации. В ней представлена разработанная многоуровневая модель информационного процесса, описывающая прохождение данных от аппаратного уровня до принятия решения о подлинности субъекта. В рамках модели предложен новый метод биометрической аутентификации, основанный на методах цифровой обработки сигналов и анализе индивидуальных признаков, выделяемых в потоке данных компьютерной мыши. Описываются ключевые принципы построения данной модели, алгоритмы фильтрации и преобразования биометрических сигналов, а также реализация процесса непрерывной верификации для обеспечения инвариантности сеанса работы пользователя.

Третья глава посвящена разработке программно-алгоритмического обеспечения и экспериментальной оценке предложенных решений. В ней определяются критерии эффективности информационных процессов аутентификации, проводятся расчеты показателей надежности нейросетевых алгоритмов, а также осуществляется сравнительный анализ разработанного метода с существующими аналогами.

Четвертая глава посвящена исследованию прикладного потенциала, девиаций и долгосрочных перспектив развития разработанной технологии непрерывно-дискретной аутентификации. В рамках главы определены ключевые направления практического применения модели в различных отраслевых сценариях, а также предложены модификации алгоритмической базы, направленные на повышение эффективности распознавания поведенческих паттернов за счет расширения пространства извлекаемых признаков. Формализованы принципы построения масштабируемых гибридных систем безопасности, функционирующих в условиях синергетического взаимодействия нескольких модальностей биометрии. Дополнительно обоснованы требования к стандартизации интерфейсов обмена информацией и обеспечению нормативно-правового соответствия процессов обработки конфиденциальных данных.

В заключении подводятся итоги исследования, отражающие вклад автора в область биометрической аутентификации. Особое внимание уделяется результатам разработки эффективной модели на основе методов цифровой обработки сигналов, применяемой в разнообразных телекоммуникационных системах. Подчёркивается значимость данной работы для дальнейшего развития и улучшения систем биометрической аутентификации.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

1.1 Специфика функционирования распределенных информационных систем и проблема инвариантности сеанса пользователя

Переход к децентрализованным архитектурам и гетерогенным (разнородным) облачным вычислениям существенно усложняет ландшафт угроз, смещая фокус безопасности с периметра защиты на легитимность транзакций внутри самой системы. В данных условиях центральным элементом обеспечения надежности становится контроль сессионной активности пользователей [85].

Системное разрешение проблемы инвариантности (неизменности и защищенности) пользовательского сеанса невозможно без обращения к фундаментальной теории информационных процессов. Именно она формирует математический аппарат и логический базис, необходимые для декомпозиции механизмов управления доступом и последующего моделирования доверенной среды в распределенных средах.

Исторически и методологически механизмы криптографической защиты и контроля доступа опираются на классическую теорию связи, заложенную Клодом Шенноном в его фундаментальной работе 1948 года «Математическая теория связи» [86]. Модель Шеннона, по праву признанная научным сообществом «Великой хартией вольностей информационной эры», абстрагируется от семантического и прагматического значения передаваемых сообщений, фокусируясь исключительно на пропускной способности канала, уровне шума и математической энтропии источника. В рамках данной теории фундаментальной единицей информации становится бит, а процесс взаимодействия рассматривается через призму кодирования, передачи и декодирования дискретных сигналов. В контексте информационной безопасности эта парадигма легла в основу традиционных шлюзовых

(дискретных) методов контроля доступа. Фундаментальный изъян современных систем безопасности заключается в ограничении проверки личности лишь этапом ввода пароля. Подобная разовая аутентификация не защищает канал связи от последующего перехвата.

Несмотря на фундаментальную значимость и математическую строгость концепции идентификации по Альсведе [90], процесс верификации источника рассматривается как дискретное, фиксированное во времени событие, при переносе которой на архитектуру распределенных информационных систем, возникает критическая уязвимость. Шлюзовые проверки эффективны на входе, но совершенно несостоятельны для защиты длинных дистанционных сессий.

Как справедливо указывали Дж. Виега (J. Viega) и Г. Макгроу (G. McGraw) в своей работе «Building Secure Software: How to Avoid Security Problems the Right Way» [52; 137], опора исключительно на периметральную защиту является концептуальной ошибкой. Развивая идеи Сальтцера и Шредера [147], они постулировали: безопасность обязана быть непрерывной, а выдача долгосрочного мандата после разовой проверки недопустима. С позиции теории информационных процессов это означает, что система формирует состояние абсолютного доверия к каналу связи, игнорируя тот факт, что энтропия системы и вероятность компрометации клиентского узла возрастают с каждой секундой поддержания активного сеанса.

Современные распределенные вычислительные системы характеризуются множественностью гетерогенных узлов, высокой степенью асинхронности взаимодействия и полным отсутствием единого, физически контролируемого периметра доверия (рисунок 1). В таких архитектурных условиях понятие «сеанс связи» становится основным логическим шаблоном, определяющим границы доверенного взаимодействия между клиентским терминалом и сервером. Поскольку факт принадлежности субъекта к доверенному множеству устанавливается сервером лишь однократно в момент входа, основная информационная нагрузка по обеспечению живучести и

устойчивости системы неизбежно переносится на постаутентификационную фазу.

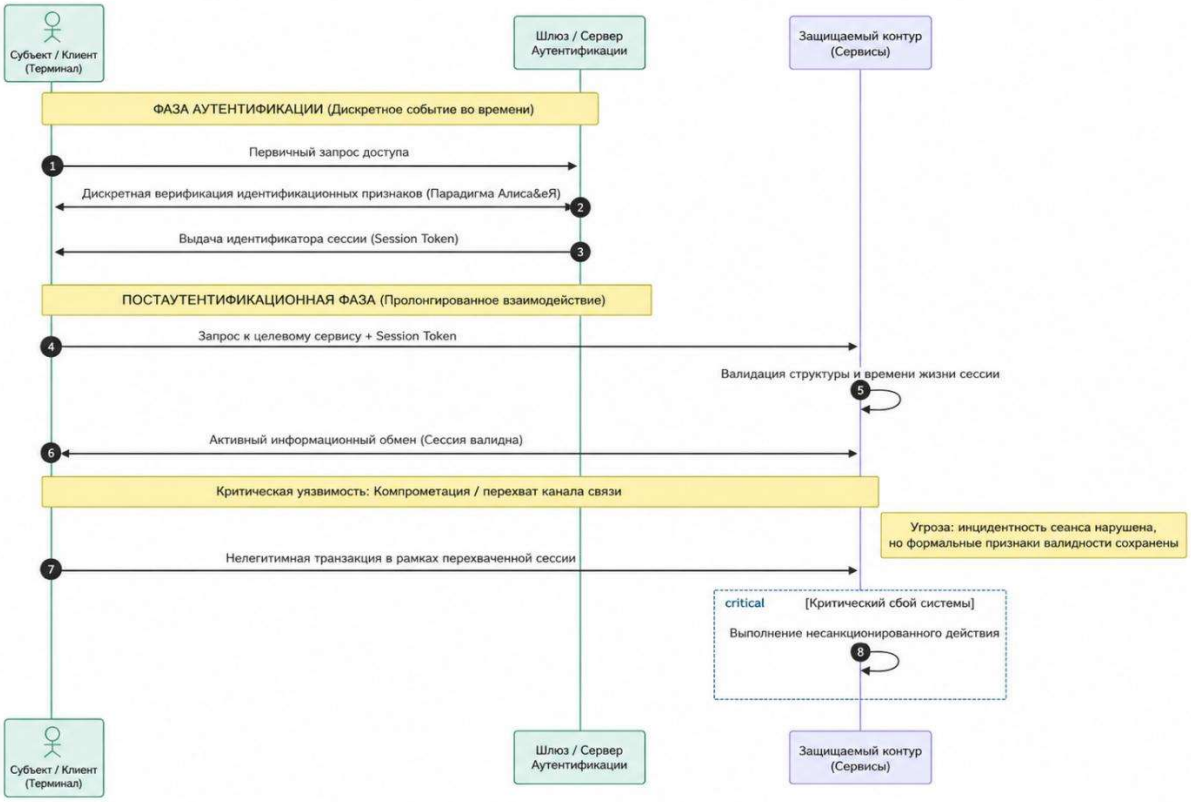

Рисунок 1 – Схема временной декомпозиции процессов аутентификации и сессионного взаимодействия в распределенных информационных системах

Основным вектором нарушения устойчивости распределенных комплексов в настоящее время является не столько аппаратный отказ узлов (проблема, успешно решаемая алгоритмами консенсуса и византийской отказоустойчивости), сколько скрытая компрометация самого сеанса легитимного субъекта. В работах М. Вальтера [163], посвященных оценке безопасности распределенных систем и алгоритмам защиты облачных инфраструктур, подчеркивается критическая важность обеспечения безопасности непосредственно на уровне сессий. Злоумышленник, преодолевший или обошедший этап первичной криптографической аутентификации, получает доступ к защищенным ресурсам от имени легитимного пользователя, при этом сама система, опирающаяся на валидные сессионные маркеры, остается в полном неведении относительно подмены субъекта.

Наличие централизованного сервера аутентификации в децентрализованной инфраструктуре (включая микросервисные архитектуры и среды Интернета вещей) детерминирует специфические, но уже ставшие классическими векторы атак. С точки зрения теории систем, любое несанкционированное вмешательство в постаутентификационную фазу представляет собой деструктивное внешнее воздействие, нарушающее штатное протекание информационного процесса поддержания доверенного состояния. В терминах информационной безопасности данная девиация (отклонение) переводит систему из целевого (легитимного) состояния в критическое, при котором формальные признаки валидности сеанса сохраняются при фактической утрате контроля над каналом связи.

Данный класс деструктивных воздействий подробно классифицирован и описан в международной базе знаний Common Attack Pattern Enumeration and Classification (CAPEC), поддерживаемой корпорацией MITRE. Детальный анализ зафиксированных паттернов позволяет формализовать строгую модель угроз для постаутентификационной фазы информационного обмена.

Традиционные механизмы контроля логических сессий (такие как веб-файлы cookie, токены доступа OAuth, идентификаторы сеансов) подвержены обширному классу деструктивных воздействий, объединенных в категорию «Exploitation of Trusted Identifiers» (CAPEC-21). Рассмотрим наиболее критичные паттерны нарушения информационной безопасности, эксплуатирующие концептуальные слабости дискретной модели и приводящие к потере инвариантности сеанса пользователя.

1) Атака подмены контекста и перехвата сеанса (Session Hijacking – CAPEC-593). Данный высокоуровневый паттерн атаки (CAPEC-593) представляет собой эксплуатацию уязвимостей в механизмах обработки сессионных данных приложением. Злоумышленник получает возможность украсть или манипулировать активным сеансом легитимного пользователя для получения несанкционированного доступа к системе. Процесс реализации атаки (Execution Flow) традиционно разделяется на фазу разведки (Explore) и

фазу эксплуатации (Exploit). На этапе разведки злоумышленник выявляет механизмы передачи незащищенных токенов сессии. Захват сессионного токена осуществляется несколькими путями: через межсайтовый скриптинг (XSS), путём пассивного перехвата незашифрованного сетевого трафика (Session Sidejacking – CAPEC-102), а также через межсайтовую трассировку (Cross Site Tracing, XST – CAPEC-107), которая обходит атрибут httpOnly за счёт эксплуатации HTTP-метода TRACE. Далее, уже на этапе эксплуатации, нарушитель использует захваченный криптографический токен для взаимодействия с целевым приложением от имени жертвы. Парадигма однократной проверки, на которую опирается центральный сервер аутентификации, не позволяет выявить подмену контекста: с математической точки зрения предъявленный токен валиден. По оценкам аналитиков MITRE, вероятность успешной реализации такой атаки в гетерогенных сетях относится к категории High, а типовая тяжесть последствий – Very High; в итоге профиль пользователя оказывается полностью скомпрометирован [178].

2) Атака повторного использования идентификаторов (Session Replay – CAPEC-60). Атака повторного воспроизведения сеанса (CAPEC-60) нацелена на повторное использование действующего идентификатора сеанса для спуфинга целевой системы. В отличие от классического перехвата активной (текущей) сессии, в данном случае злоумышленник пытается внедрить в канал связи перехваченный ранее идентификатор (полученный во время предыдущей легитимной транзакции). На этапе взаимодействия с целевым хостом злоумышленник обнаруживает, что для отслеживания пользователей применяются статические или предсказуемые идентификаторы. После кражи такого идентификатора у действительного пользователя осуществляется попытка получить доступ к системе с привилегиями первоначального владельца. Этот вектор атаки является прямым следствием отсутствия механизмов непрерывной криптографической или биометрической ротации ключей в рамках распределенной системы связи [174].

3) Фиксация сеанса (Session Fixation – CAPEC-61). Атака фиксации сеанса (CAPEC-61) представляет собой инвертированный подход к компрометации доверенной среды. Вместо того чтобы пытаться перехватить сгенерированный сервером маркер, злоумышленник превентивно навязывает клиенту (жертве) идентификатор сеанса, который был заранее сгенерирован или получен самим атакующим. Как только легитимный пользователь, ничего не подозревая, успешно проходит процедуру авторизации в целевом программном обеспечении (соответственно, повышая привилегии привязанного к нему идентификатора), злоумышленник начинает параллельно использовать этот же, теперь уже привилегированный идентификатор сеанса в своих собственных транзакциях. Успех атаки базируется на фундаментальном недостатке логики работы серверного ПО: система либо слепо доверяет генерируемым клиентом идентификаторам, либо не обновляет идентификатор сеанса после успешного прохождения проверки подлинности (привилегированной эскалации). [175]

4) Фальсификация учетных данных сеанса (Session Credential Falsification – CAPEC-226). Данный паттерн атак (CAPEC-226) заключается в ручной алгоритмической манипуляции существующими учетными данными сеанса (например, файлами cookie или JWT-токенами) с целью повышения привилегий или подмены пользователя. Если сессионный токен содержит атрибуты, указывающие на права доступа пользователя, и при этом не защищен надлежащим криптографическим механизмом обеспечения целостности (таким как MAC-подпись или надежный серверный state-контроль), злоумышленник может модифицировать эти поля на стороне клиента. В отличие от фальсификации путем криптоаналитического предсказания (когда вычисляется алгоритм генерации новых токенов), здесь модифицируются легитимно выданные сервером данные. Данная уязвимость, классифицируемая также как CWE-565 (Reliance on Cookies without Validation and Integrity Checking), наглядно демонстрирует деградацию атрибутов

субъекта, о которых централизованный сервер остается неосведомленным до следующего планового запроса. [177]

5) Временные уязвимости и гонки состояний (TOCTOU – CAPEC-29). Атаки класса Time-of-Check and Time-of-Use (CAPEC-29) нацелены на так называемое «состояние гонки» (race condition), возникающее между моментом проверки системой состояния ресурса или атрибутов субъекта (time of check) и моментом фактического использования этого мандата (time of use). В контексте дискретной аутентификации «проверка» происходит исключительно в момент входа, а «использование» предоставленного мандата растягивается на весь период активного сеанса. Именно в этот длительный временной промежуток злоумышленник может изменить системную конфигурацию, подменить субъекта за терминалом (например, физически сев за разблокированный компьютер) или модифицировать критические данные, заставляя приложение вести себя непредсказуемо [173].

6) Эксплуатация отладочных интерфейсов (CAPEC-121). Дополнительным критическим вектором компрометации защищенного периметра в постаутентификационной фазе является обнаружение и эксплуатация непроизводственных, тестовых или отладочных интерфейсов, ошибочно оставленных в рабочей среде (CAPEC-121). Такие интерфейсы по умолчанию не проектировались с учетом строгих политик безопасности, редко обладают адекватными механизмами контроля доступа (что соотносится с уязвимостью CWE-1302: Missing Security Identifier) и могут предоставлять злоумышленнику широкие административные функции управления системой в обход любой стандартной процедуры аутентификации [176].

В таблице 1 систематизированы описанные выше угрозы логическому сеансу пользователя в распределенных информационных системах, иллюстрирующие исчерпанность ресурса традиционных методов защиты.

Таблица 1 – Классификация атак на логический сеанс пользователя (на базе таксономии MITRE CAPEC)

Идентификатор CAPEC	Наименование угрозы	Вектор и механизм эксплуатации	Тяжесть последствий	Свойство нарушаемой безопасности
CAPEC-593	Session Hijacking (Перехват сеанса)	Захват криптографически валидного токена доступа через уязвимости среды передачи (XSS, Sidejacking) и его использование от имени жертвы.	Очень высокая (Very High)	Конфиденциальность, Доступность, Целостность
CAPEC-60	Session Replay (Повторное использование ID)	Повторное воспроизведение в канале связи ранее перехваченного валидного идентификатора в рамках новой транзакции.	Высокая (High)	Конфиденциальность, Авторизация
CAPEC-61	Session Fixation (Фиксация сеанса)	Превентивное навязывание жертве известного злоумышленнику идентификатора до прохождения ею легитимной процедуры входа.	Высокая (High)	Авторизация, Идентификация
CAPEC-226	Session Credential Falsification	Прямая алгоритмическая манипуляция клиентскими атрибутами сессии (cookie/токен) для несанкционированного повышения локальных привилегий.	Средняя (Medium)	Целостность, Разграничение доступа
CAPEC-29	Time-of-Check and Time-of-Use (TOCTOU)	Эксплуатация временного окна между дискретной проверкой прав сервером и фактическим исполнением системной команды клиентом.	Высокая (High)	Целостность, Синхронизация логики

Анализ указанных векторов атак показывает, что их фундаментальной первопричиной является семантический разрыв между криптографическим

доверием и реальным физическим поведением актора. Как только факт принадлежности субъекта установлен сервером однократно, центральный узел аутентификации фактически утрачивает контроль над физическим терминалом и логическим каналом управления. Классическая парадигма порождает специфические векторы, критически значимые для децентрализованных узлов, где между моментом проверки подлинности и моментом исполнения критической команды субъект может быть заменен без повторного обращения к серверу.

Снижение эффективности традиционных парольных и токенных политик с течением времени также подтверждается экспериментальными исследованиями в области управления рисками. В трудах М. Хуба (M. Hub) и К. Пржиходовой (K. Příhodová) [126; 142], посвященных влиянию глобализации на безопасность данных (2018–2021 гг.), математически доказана стремительная деградация устойчивости парольной аутентификации к современным вычислительным атакам (включая брутфорс и атаки по словарям, усиленные распределенными вычислениями). Авторы прямо указывают на острую необходимость внедрения многофакторных биометрических характеристик для верификации субъектов в реальном времени.

Для преодоления ограничений дискретного «шлюзового» контроля теоретически необходимо ввести непрерывную функцию доверия (модель перманентного доверия). Однако практическая алгоритмизация такой функции сталкивается с фундаментальной научно-технической проблемой, которая в современной международной практике в области информационной безопасности и машинного обучения (Machine Learning) классифицируется как проблема обеспечения непрерывной аутентификации (Continuous Authentication) в условиях временного дрейфа концепта (Concept Drift) поведенческих шаблонов субъекта [117; 145].

Данная проблема обусловлена высокой нестационарностью признакового пространства (динамики манипулятора «мышь», клавиатурного

почерка), из-за чего математические модели глубокого обучения теряют устойчивость («инвариантность») на длительных интервалах наблюдения.

С концептуальной точки зрения архитектуры информационной безопасности, инвариантность сеанса означает способность системы гарантировать, что физический субъект, инициировавший логический сеанс в начальный момент времени T_0, тождественно равен субъекту, выполняющему транзакции в любой последующий дискретный момент времени T_n. В условиях традиционных систем, лишенных механизмов непрерывного контроля, инвариантность сеанса не обеспечивается криптографически или алгоритмически, а лишь предполагается на основе априорного доверия к валидности токена.

С позиции интеллектуального анализа данных и биометрической идентификации проблема инвариантности сеанса приобретает принципиально иной, сугубо математический смысл. При разработке алгоритмов поведенческой или сложной физиологической биометрии (например, на основе анализа электроэнцефалограмм, ЭЭГ) исследователи часто совершают методологическую ошибку, опираясь на наборы данных, собранные в рамках одного короткого непрерывного сеанса взаимодействия [110; 117]. Оценка производительности систем машинного обучения на таких ограниченных выборках приводит к ложноположительным выводам об их высокой эффективности (достижение точности распознавания 98-99%). На практике же такие нейросетевые модели склонны переобучаться на специфических, зависящих от конкретного сеанса признаках (характеристиках аппаратного обеспечения, уровне электромагнитного шума канала, временном психоэмоциональном фоне субъекта, освещенности или влажности), а не на истинных, уникальных для конкретного субъекта особенностях [158].

Достижение истинной алгоритмической инвариантности сеанса требует создания генератора признаков или математической функции преобразования, способной отфильтровывать особенности, специфичные для локального контекста сессии, и оставлять лишь перманентную, устойчивую информацию

в латентном пространстве признаков. В передовых исследованиях по глубокому обучению для поведенческой биометрии эта задача решается посредством методов обучения инвариантных представлений с применением состязательных сетей. Идеальная прогностическая модель непрерывной аутентификации должна обладать устойчивостью сразу к трем видам дисперсии:

1) Субъектная инвариантность – способность модели вычленять и абстрагироваться от общих шумовых признаков, присущих всем людям, для выделения строгой индивидуальной сигнатуры. Также этот параметр важен для генерации синтетических данных, очищенных от признаков субъекта (используется для балансировки обучающих выборок).

2) Инвариантность к сеансам – способность алгоритма корректно классифицировать цифровой профиль пользователя при изменении условий сбора данных (времени суток, степени когнитивной усталости оператора, смене периферийного оборудования) без деградации точности. Эксперименты показывают, что при обучении моделей на аппаратно-независимых и многосессионных наборах данных половина общей частоты ошибок (HTER) снижается, и система перестает быть зависимой от локального технического контекста.

3) Инвариантность классов – математическая устойчивость модели к неизбежному дисбалансу классов в потоковом наборе поведенческих данных (когда действий "кликов" может быть в сотни раз меньше, чем "перемещений курсора").

Проблема инвариантности сеанса является краеугольным камнем разработки надежных биометрических систем. Специфика функционирования распределенных информационных систем диктует безальтернативную необходимость не просто проведения однократной аутентификации, а обеспечения инвариантности сеанса в режиме реального времени. В противном случае любые дорогостоящие меры защиты криптографического или сетевого уровня, включая специализированные решения защиты

информации в проводных каналах связи [185], будут легко нивелированы атаками на прикладной и сессионный уровни взаимодействия.

Единственным научно обоснованным ответом на описанные выше угрозы компрометации логических сеансов и концептуальные ограничения дискретных моделей является системный переход к парадигме непрерывной аутентификации (Continuous Authentication, CA). В отличие от дискретного «шлюзового» контроля, непрерывная аутентификация представляет собой особый, высокотехнологичный класс информационных процессов, реализующих функцию потокового мониторинга и верификации подлинности субъекта на всем протяжении активной фазы его взаимодействия с информационной системой.

Непрерывная аутентификация полностью устраняет проблему «временного разрыва», перманентно перепроверяя валидность пользователя во время активного сеанса без прерывания его основной интеллектуальной или операционной деятельности. Это достигается путем агрегации и интеллектуального анализа данных о поведенческих действиях пользователя, его физиологических реакциях и контекстной информации окружения. Исследователь Р. Савукинас (R. Savukynas) [149] в серии научных работ (2020–2024 гг.), посвященных безопасности устройств Интернета вещей и смарт-систем, доказывает, что постоянный фоновый мониторинг обладает значительными, фундаментальными преимуществами как с точки зрения эргономики, так и с позиции комплексной безопасности по сравнению с активными методами, требующими от пользователя постоянного ручного ввода PIN-кодов, паролей или периодического прикладывания пальца к дактилоскопическому сканеру.

Информационный процесс непрерывного контроля принципиально отличается от классической передачи данных. Он характеризуется потоковой природой, асинхронностью, зашумленностью и высокой энтропией исходных биометрических признаков. Результатом такого процесса является не жесткий бинарный статус (Доступ Разрешен / Доступ Запрещен), а непрерывная,

динамически изменяющаяся функция доверия. При падении значения этой математической функции ниже заранее установленного порогового уровня система информационной безопасности может автоматически применить гибкие политики реагирования: незаметно запросить дополнительный фактор аутентификации, временно ограничить права доступа к критическим модулям, заблокировать транзакцию или принудительно терминировать сессию (рисунок 2).

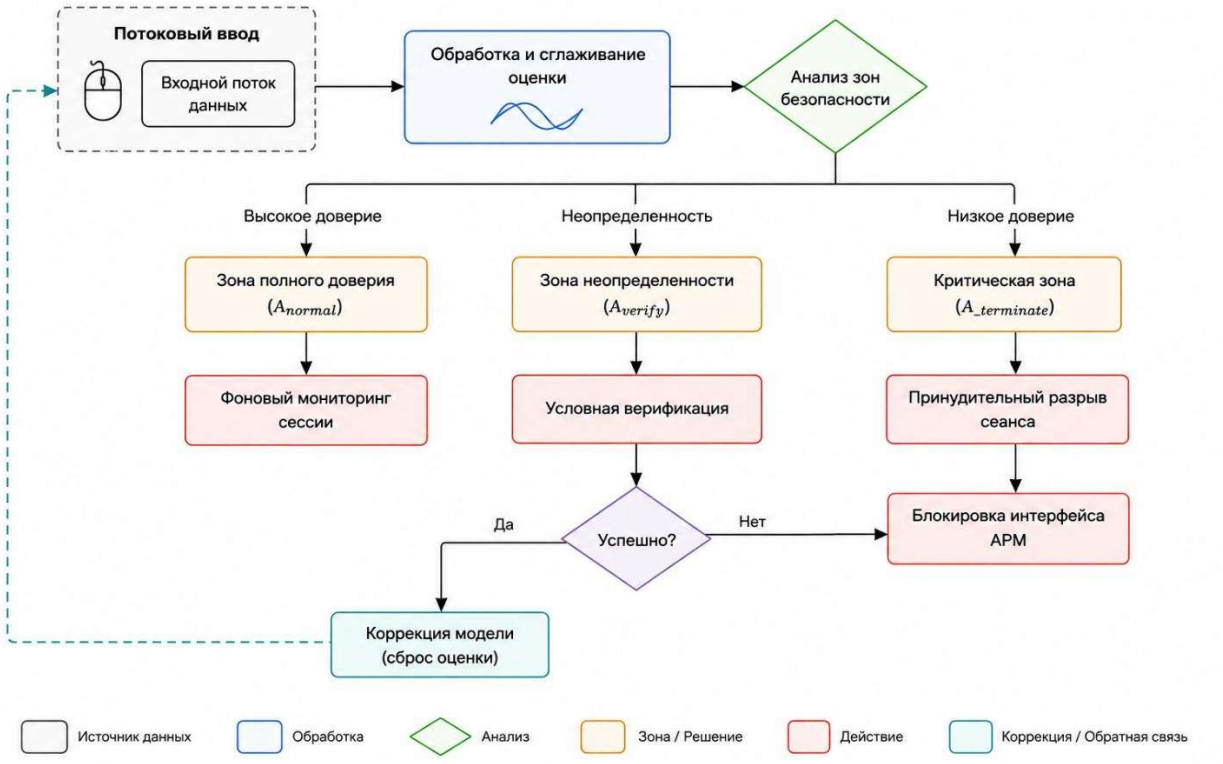

Рисунок 2 – Алгоритм функционирования процесса непрерывного адаптивного контроля доступа на основе рекуррентного расчета функции доверия

Безопасность, обеспечиваемая биометрическими системами, решает следующие задачи. Она предназначена для определения, кто находится перед системой − зарегистрированный пользователь или постороннее лицо. При этом должна быть минимальна вероятность введения системы в заблуждение посторонними лицами. В противном случае может возникнуть ложноположительная аутентификация. Естественно, необходимо исключить ситуации, когда система неправильно распознает образец и, таким образом,

препятствует доступу зарегистрированного пользователя. Следовательно, система должна быть максимально надежной и безошибочной. [150]

Итак, биометрические технологии оцениваются с различных позиций. Имеет значение стоимость организации подобной системы контроля за доступом, ее удобство, а также показатели, связанные с надёжностью, а именно управлением ошибками ложного доступа (FAR – False Acceptance Rate, ошибка 1-го рода) или же с ложным отказом (FRR – False Rejection Rate, ошибка 2-го рода).

FAR, или ошибка 1-го рода, относится к вероятности неправильного принятия системой ложного сигнала или ложного допуска неавторизованного пользователя. То есть это вероятность того, что система ошибочно принимает неавторизованного субъекта за правомерного пользователя. (Предположим, для проверки биометрической системы безопасности необходимо протестировать 100 пар биометрических образов. Если система ошибочно допустит к доступу 10 пользователей (неавторизованных), то FAR составит 10%).

FRR, или ошибка 2-го рода, относится к вероятности неправильного отклонения системой правомерного пользователя или неправильного отказа в доступе. То есть, это вероятность того, что система неверно отклонит человека, который на самом деле является правомерным пользователем. (Аналогично если в примере выше 1 авторизованный пользователь будет отклонён, FRR будет равен 1%).

HTER (Half Total Error Rate) – половина общей частоты ошибок.

$$FAR = \frac{Number\ of\ accepted\ imposters}{Total\ number\ of\ imposters} \quad (1)$$

$$FRR = \frac{Number\ of\ rejected\ genuines}{Total\ number\ of\ genuines} \quad (2)$$

$$HTER = \frac{FAR + FRR}{2} \quad (3)$$

Оба показателя, FAR и FRR, являются важными в контексте биометрии, поскольку они позволяют оценить работоспособность и надежность системы аутентификации. Так, для системы доступа к особо охраняемым объектам, таким как банки, правительственные учреждения или военные объекты, требуется меньшая возможность ложного доступа, так как даже один случай допуска нежелательного пользователя способен привести к серьезным последствиям. С другой стороны, для системы разблокировки смартфона, где пользователь имеет возможность легко повторить попытку ввода пароля, более высокая доля ложного отказа является приемлемой.

В общем случае, чем меньше FAR и FRR, тем эффективнее система аутентификации, однако, баланс между двумя метриками должен достигаться с учетом конкретных требований и ограничений используемой системы. [146]

Для создания эффективной системы контроля доступа недостаточно просто высоких значений FAR и FRR. Например, невозможно представить систему контроля доступа на основе анализа ДНК, несмотря на то что при таком методе аутентификации указанные коэффициенты стремятся к нулю. Однако, у такой системы возрастает время аутентификации, увеличивается влияние человеческого фактора, а стоимость системы становится неоправданно высокой.

Значения FAR и FRR для самых популярных методов биометрической аутентификации представлены в таблице 2.

Таблица 2 – Значения FAR и FRR популярных методов биометрической аутентификации

Биометрическая система использует	FAR	FRR
Отпечаток пальца	0,001%	0,6%

Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

FAR и FRR взаимно дополняют друг друга, потому что изменение одного из параметров приводит к изменению другого. Например, если увеличить порог распознавания в биометрической системе, чтобы уменьшить FAR, можно заставить систему отказывать в доступе большей доли пользователей, чьи данные распознаны неправильно, что увеличит FRR. [129]

Повышение точности лицевой биометрии достигается за счет камер высокого разрешения и адаптации к освещению. Значительный прирост надежности дает многокритериальный анализ – например, синергия распознавания лица и отпечатков. Агрегация результатов от ансамбля алгоритмов и обучение с подкреплением минимизируют ложные отказы. Оптимальный подход всегда зависит от аппаратных возможностей и требований к системе [108].

Для верификации эффективности классификаторов традиционно применяются ROC-кривые, демонстрирующие устойчивость модели при разных пороговых значениях. Кривая ROC отображает истинную положительную скорость (TPR) в сравнении с ложноположительной скоростью (FPR) [145]. Для целей оценки производительности использовались следующие выражения [111]: TP: истинно положительный, TN: истинно отрицательный, FP: ложноположительный, FN: ложноотрицательный, FAR: коэффициент ложного принятия, FRR: коэффициент ложного отклонения и HTER: половина общей частоты ошибок:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

$$TPR = \frac{TP}{TP + FN} \quad (5)$$

$$TNR = \frac{TN}{TN + FP} \quad (6)$$

$$FPR = \frac{FP}{FP + FN} \quad (7)$$

$$FNR = \frac{FN}{FN + TP} \quad (8)$$

1.2 Понятие и сущность биометрической аутентификации как инструмента обеспечения устойчивости сеанса

Исследования в области аутентификации пользователей выделяют три основные группы средств: аутентификация на основе биометрических данных, аутентификация на основе обладания информацией, и аутентификация на основе знаний [87; 88; 96]. Наиболее перспективной из них считается аутентификация на базе биометрических характеристик человека, так как она обеспечивает высокую надежность и удобство использования [53].

Биометрия – это автоматизированное или полуавтоматизированное распознавание людей по их физическим, поведенческим или психофизиологическим признакам [11].

В настоящее время большинство систем используют простые решения на основе пар логин-пароль или более сложные на основе двухфакторной аутентификации с использованием мобильных устройств [20]. Однако возможно применение биометрических средств защиты, которые обладают более высокой степенью надежности [146].

Биометрические технологии, основанные на измерении уникальных характеристик человека, включают врожденные (например, отпечатки

пальцев, ДНК [29]), приобретенные (например, почерк) и изменяемые (например, голос) признаки [25; 28]. Они находят применение в сферах, где требуется безопасный доступ к защищенным данным и надёжное подтверждение личности, включая финансовые услуги, государственные учреждения, медицину, транспорт. С развитием электронных устройств и компьютерного зрения в середине XX века, биометрия стала широко использоваться для обеспечения безопасности, медицинской диагностики, управления персоналом и др. В литературе также рассматриваются нестандартные направления биометрической идентификации, включая идентификацию животных по индивидуальным морфологическим признакам [99].

Как уже говорилось, повседневная жизнь также широко применяет указанный инструментарий, чтобы контролировать допуск. Чтобы разблокировать смартфон, необходимо пройти аутентификацию по точкам, например. Если человек оплачивает покупки посредством электронного платежного средства, также требуется подтвердить личность. Схожим образом обстоят дела с эксплуатацией банкоматов. Кроме того, граждане могут получить биометрические паспорта. С таким документом можно пересечь границу, находиться на территории какой-либо страны. Они признаются равноправными традиционным документам, удостоверяющим личность. Коммерческая сфера занимается внедрением нейросети. Достаточно фото в паспорте, чтобы личность человека была установлена. С помощью технологии IDX можно доказать, что человек является зарегистрированным пользователем и не выдает себя за третье лицо. [92; 128; 179]

Преимущества биометрических технологий в системах безопасности выражаются в следующих факторах:

– Высокая надежность и точность, поскольку уникальность физиологических и поведенческих признаков сводит к минимуму риск подделки или ошибочной аутентификации.

– Удобство для пользователей, так как устраняется необходимость запоминать пароли или носить ключи, а сама процедура проверки занимает секунды.
– Защита от утери и кражи, ведь биометрические данные невозможно потерять или передать третьим лицам, что снижает риск несанкционированного доступа.
– Высокая скорость идентификации, благодаря чему системы оперативно обрабатывают данные, что критично для объектов с большим потоком людей.
– Автоматизация процессов, что минимизируется человеческий фактор и снижает нагрузку на персонал службы безопасности.
– Простая интеграция, ввиду чего технологии легко совмещаются со сторонними системами (СКУД, видеонаблюдение, учет рабочего времени).
– Аудит и контроль, за счет чего обеспечивается точное отслеживание активности пользователей и создание надежного цифрового следа.
– Гибкость и масштабируемость, что позволяет легко адаптировать системы под меняющиеся потребности и масштабы организации.
– Превосходство над традиционными методами, так как они обеспечивают принципиально более высокий уровень защиты по сравнению с паролями, картами или ключами [96].

Основным компонентом любого метода для его реализации в реальном использовании является биометрический алгоритм и биометрический сканер.

Биометрический алгоритм – последовательность команд, позволяющая биометрической системе решить ту или иную задачу. Примечание: число операций в биометрическом алгоритме должно быть конечным. Подобные алгоритмы используются в программном обеспечении биометрических систем с целью выполнения верификации или идентификации личности при сравнении биометрических контрольных шаблонов [12].

Устройство сбора биометрических данных – биометрический сканер – устройство, регистрирующее биометрические характеристики и преобразующее их в зарегистрированный биометрический образец. [12]

Для биометрической аутентификации используются различные типы аппаратных и программных ресурсов. Сканер отпечатков пальцев определяет уникальные папиллярные характеристики пользователей [16; 22; 23; 26], при этом современные системы сравнения на основе искусственного интеллекта достигают точности распознавания более 99% при работе с большими базами данных [32; 39; 45; 51]. В системах распознавания лиц, для которых стандартизованы форматы обмена данными изображения лица [24], обработка видеопотока камерами достигает 30 кадров в секунду с помощью алгоритмов компьютерного зрения, а точность идентификации приближается к 99,8%. [98; 165] Сканеры сетчатки и радужной оболочки глаза анализируют соответствующие индивидуальные рисунки органов зрения с целью верификации субъекта [15].

Голосовое распознавание базируется на уникальных характеристиках голоса, таких как частота и интонация; даже в шумной обстановке точность данного метода составляет порядка 90%. [19; 166]. При обработке голосовых данных в шумной среде применяются методы повышения качества и выделения речевого сигнала [135]. Сканер вен, в свою очередь, исследует уникальный подкожный орнамент сосудов пользователя [18]. Смежным направлением являются мультимодальные методы распознавания по признакам кисти руки, объединяющие несколько характеристик ладони и пальцев [122]. Отдельный класс составляют поведенческие методы аутентификации, опирающиеся на анализ динамических характеристик человека: походки, стиля письма, подписи или динамики использования координатных устройств ввода при работе с автоматизированным рабочим местом (АРМ). Поведенческая биометрия в реальных условиях эксплуатации показывает точность до 95%. [161]

На практике применяются сканеры разных типов – главным образом оптические и кремниевые. Оптические устройства считаются надежными, но у них есть слабое место: их легко обмануть имитацией из латекса или силикона. Такие материалы позволяют искусственно поменять текстуру кожи или вообще деформировать черты лица, что приводит к ошибкам аутентификации.

Любая биометрическая система опирается на программный алгоритм и устройство захвата. Она превращает «сырой» сигнал в цифровой шаблон и сверяет его с эталоном. Информативность данного цифрового шаблона и техническая эффективность системы напрямую зависят от качества сенсора, освещенности и позиционирования. Как следствие, снижение точности на этапе захвата неизбежно ведет к росту вероятности ошибок первого и второго рода.

Минимизировать указанные риски помогают следующие технологические подходы:

- Интеллектуальный анализ: алгоритмы принимают во внимание изменение формы и текстуры кожи при разном освещении.
- Мультимодальная верификация: совместное использование физических, химических и биометрических методов выявления инородных материалов.
- Компьютерное зрение: отслеживание микродинамики глаз, губ и иных частей лица для подтверждения «живости» (liveness detection) пользователя.
- Расширенное обучение: тренировка нейросетей на наборах данных, включающих изображения лиц в масках и накладках.

Светоизлучающие датчики можно рассматривать как одно из наиболее перспективных решений в данной группе методов. Их преимущество связано с высокой скоростью работы и устойчивым качеством сканирования в условиях слабого освещения, температурных колебаний либо изменения влажности кожи, в том числе при ее пересушенности или повышенной

влажности. При этом ни одна из биометрических систем не обеспечивает абсолютной точности, а применение имитационных материалов остается значимой проблемой для автоматизированного распознавания. Внедрение биометрии поэтому требует баланса между защищенностью и приватностью данных. Наибольшую устойчивость к физической фальсификации, согласно рассматриваемым источникам, демонстрируют системы сканирования радужной оболочки и рисунка вен [127]. В качестве примера можно привести терминал HBOX (EyeLock)[1], выполняющий верификацию по радужке менее чем за секунду с расстояния до 60 см. Бесконтактный режим снижает санитарные риски, а надежность и возможность интеграции со СКУД делают HBOX применимым в правительственных и финансовых организациях.

Разработчики уверяют, что технология легко интегрируется в любую стандартную систему безопасности. Это значит, что устройство перспективно для городской, производственной среды, где требуется обеспечение безопасности и контроль доступа.

Биометрический образ – образ человека, полученный с выходов первичных измерительных преобразователей физических величин, подвергающийся далее масштабированию и иной первичной обработке с целью извлечения из него контролируемых биометрических параметров человека. [13]

Процесс сбора биометрических образов обычно предполагает применение специальных датчиков и сенсоров для получения данных о физиологических и поведенческих характеристиках. [55]

Тем важнее качественно, с технической точки зрения, фиксировать паттерн, чтобы впоследствии понять, кому они принадлежат. Качество фиксации – это один из важнейших аспектов, который влияет на точность

[1] https://www.eyelock.com/

биометрической аутентификации. Он описывает, насколько хорошо биометрическое устройство захватывает информацию о характеристиках лица или другие типы биометрических данных. Чем выше качество захвата, тем точнее будет аутентификация.

Кроме того, правильная фиксация имеет решающее значение в качестве биометрической аутентификации. Недостаточное качество фиксации приводит к тому, что частичная или неполная информация будет считываться, что уменьшает точность аутентификации. Точность распознавания детерминирована внешними факторами: освещением, ракурсом и качеством программной обработки. Фундаментальную роль играет разрешающая способность сенсора [119; 127].

Алгоритм работы биометрической системы выглядит следующим образом:

1) Человек предоставляет сканеру свои биометрические данные.

2) Захваченный биометрический образ преобразуется в цифровой формат.

3) На этапе регистрации данных создается эталонный образ, который является уникальным шаблоном биометрического образа человека и сохраняется в базе данных системы.

4) Захваченный цифровой образ сравнивается с эталонным образом в базе данных системы, чтобы определить, совпадают ли они.

5) На основе полученных результатов сравнения (будь то верификация «один к одному» или идентификация «один ко многим») система принимает окончательное решение о подлинности субъекта. Если захваченный образ признается валидным и соответствующим эталону, аутентификация считается успешной, и пользователю предоставляется санкционированный доступ к ресурсам или правам, закрепленным за данной личностью. [119]

Биометрический шаблон – это блок данных, содержащий параметры преобразователя, биометрия-код доступа.

Скорость поиска биометрического шаблона зависит от многих факторов, включая объем данных, эффективность алгоритма поиска, производительность сервера, качество входных данных, количество конкурентных запросов и уровень безопасности.

В свою очередь, скорость обработки биометрических данных зависит от различных факторов. Некоторые из них включают в себя:

1) Качество биометрических данных: чем выше качество биометрических данных, тем меньше времени потребуется на их обработку. Правильная съемка отпечатка пальца, сканирование лица или сетчатки глаза, акустическое считывание звуковых характеристик голоса и правильное съемка других типов данных помогает ускорить процесс обработки.

2) Аппаратное обеспечение: эффективная обработка биометрических данных зависит от современной и производительной техники. Биометрические системы должны иметь быстродействующие процессоры, адекватную оперативную память и достаточную пропускную способность каналов передачи данных между устройствами.

3) Комплексность алгоритмов обработки: хорошо разработанные алгоритмы обработки данных, учитывающие все возможные варианты искажения биометрических данных, помогают в быстрой аутентификации пользователя.

4) Объем базы данных: чем больше БД, тем больше требуется времени на поиск и сопоставление биометрических данных.

5) Способность сети обработки данных: обработка биометрических данных замедляется ввиду нерегулярности потока данных, слабого сигнала сети, на территории которой находятся биометрические датчики или наличия сбоев в оборудовании.

Обычно ускорение обработки биометрических данных достигается путем использования интеграции аппаратных ресурсов, повышения эффективности алгоритмов обработки или использования новых линий

передачи данных для улучшения пропускной способности. Однако все зависит от конкретной биометрической системы и ситуации использования.

Для каждого вида характеристики используется свой набор биометрических данных, например, если для доступа использовать отпечаток пальцев, то основными показателями здесь выступают точки начала и конца бороздок, раздвоение бороздок и их общая форма [103]. Необходимо тщательно выбирать, какие параметры будут использоваться в системе и какой алгоритм будет применяться для их обработки, в связи с тем, что необходимо решить проблему, связанную со скоростью поиска необходимого биометрического шаблона, который используется в схеме биометрической аутентификации. [59]

Наиболее перспективным способом обучать программу распознавать образы, что особенно важно в процессе распознавания лиц или других форм биометрической аутентификации, выступают алгоритмы нейронных сетей. Эти алгоритмы перспективны не только для анализа статических изображений, но и для выявления скрытых пространственно-временных зависимостей в высокоэнтропийных телеметрических потоках, генерируемых устройствами ввода.

Процедура аутентификации предполагает сопоставление предъявленных данных с данными клиента, которые были заранее сохранены в базе данных. При этом алгоритм переводит биометрические данные в цифровой формат и сравнивает их с шаблоном, который заранее был записан в базе данных. При совпадении происходит аутентификация.

При верификации ставится задача доказать, что человек, предъявляющий данные, является тем, кто он утверждает, что он таковым является. В этой процедуре нейронные сети также получают на вход данные от субъекта, переводят их в цифровой формат, а на выходе обучаются сопоставлять его с базой данных и, если совпадение произошло, допускают субъекта к запрашиваемому ресурсу. Подобный классический алгоритм

решает задачу начального разграничения доступа, но не обеспечивает защиту постаутентификационной фазы.

Несмотря на практические преимущества, биометрические технологии на этапах формирования, внедрения и эксплуатации связаны с рядом ограничений. [96; 119; 148] Наряду с проблемами создания цифровых эталонов возникают риски, характерные для последующего использования биометрии в системах контроля доступа. [65; 139; 150] Даже заявляемая разработчиками высокая точность аутентификации не устраняет технологических факторов, которые могут снижать фактическую надежность защитных решений. К основным проблемам применения биометрических образов относятся следующие. Отдельным направлением снижения таких рисков являются схемы защиты биометрических шаблонов и отменяемой биометрии [63; 148].

1) Недостаточная универсальность. Отдельные биометрические признаки могут быть нестабильны либо недоступны для части пользователей, что ограничивает область применения технологии. Например, папиллярный узор может быть поврежден вследствие физического труда или травм, а черты лица изменяются с возрастом. Если система опирается только на одну модальность, например на отпечатки пальцев, пользователи с такими особенностями фактически исключаются из контура биометрической аутентификации.

2) Возможность подделки. Уникальность биометрических характеристик не исключает попыток имитации или мошенничества. Часть методов подделки технически сложна, однако их реализация возможна, особенно с применением современных технологий. Так, системы распознавания лиц могут быть обмануты с помощью 3D-печати маски, созданной на основе сканирования лица реального пользователя. [116; 169]

3) Защита и хранение данных. Биометрические данные относятся к чувствительной персональной информации, поэтому их хранение и обработка требуют защиты от несанкционированного доступа и утечек. Нарушение

безопасности таких данных влечет серьезные последствия для приватности пользователя. [65; 130; 139; 150]

4) Стандарты и совместимость. Разнообразие биометрических технологий и устройств затрудняет взаимодействие между системами. Отсутствие единых стандартов осложняет обмен данными и может снижать эффективность аутентификации.

В целом проблема состоит в том, что скомпрометированные биометрические данные могут быть использованы злоумышленниками для доступа к защищенным системам или информации. Например, они служат основой для создания поддельных подписей при мошеннических транзакциях. Также возникает риск незаконного доступа, позволяющий проникать на охраняемую территорию, в здания и на пользовательские устройства (телефоны, планшеты). При каждой верификации данные фиксируются в виде биометрического шаблона. В случае получения доступа к нему злоумышленник компрометирует систему, формируя фальшивые шаблоны для обхода механизмов защиты.

Безопасное хранение и использование биометрической информации обеспечивается комплексом следующих мер:

– Шифрование данных: конфиденциальная информация, передаваемая по сети (в частности, между биометрическим сканером и ЭВМ), шифруется для исключения перехвата или использования третьими лицами.

– Безопасный доступ к данным: возможность работы со сведениями ограничивается исключительно авторизованными пользователями (сотрудниками служб безопасности или IT-специалистами) с применением паролей, смарт-карт и иных методов аутентификации.

– Физическая защита: серверы и аппаратное оборудование защищаются с помощью систем видеонаблюдения, датчиков движения, замков и ключевых карт.

– Аудит доступа и мониторинг: журналы доступа подлежат регулярной проверке для контроля действий пользователей и выявления

подозрительной активности. Более детальное наблюдение опирается на интеллектуальные системы аналитики поведения.

Дополнительно учитываются требования национальных законодательств, регулирующих оборот биометрических данных, а также вероятность технологических ошибок при сборе и обработке информации, связанных с недостаточной точностью отдельных модальностей.

Биометрия, как правило, применяется в сочетании с иными средствами – например, смарт-картами. Иногда она выступает в качестве основной защиты, активируя встроенные в карту криптографические ключи (сложные цифровые секреты для защиты транзакций и доступа). При такой схеме биометрический шаблон надежно изолирован на самой карте. [100]

Для защиты собираемых персональных данных и предотвращения их подделки широко внедряется многофакторная аутентификация (МФА). [88; 141] Данный метод безопасности основан на одновременном использовании двух и более независимых способов проверки подлинности субъекта (пароль, СМС-код, отпечаток пальца, голос). На сегодняшний день наиболее перспективными для защиты информационных систем признаются двухфакторные биометрические решения, сочетающие в себе высокую безопасность, простоту и удобство.

Однако подобные комплексы отличаются высокой стоимостью. При выборе конкретной системы необходимо сопоставлять уровень защищенности и сопутствующие финансовые затраты, включающие расходы на разработку, закупку оборудования, обучение персонала и техническое обслуживание. При этом существует возможность переноса архитектуры в сугубо программную плоскость, что радикально снижает затраты за счет внедрения систем поведенческой биометрии.

Под эффективностью в данном контексте понимается соотношение между результатом корректной аутентификации и ресурсами, затраченными на ее проведение. Для реализации биометрических процедур обычно задействуются:

1) Специализированные биометрические устройства (сканеры папиллярных узоров, камеры распознавания лиц и др.).
2) Программное обеспечение для обработки, анализа и распознавания конкретных модальностей (лиц, радужки, отпечатков).
3) Распределенные или централизованные базы данных, применяемые для верификации и индексации.
4) Специализированные серверы (включая облачные вычисления для обеспечения масштабируемости).
5) Сетевые протоколы приема-передачи данных (TCP/IP, HTTPS, специализированные API).
6) Квалифицированный персонал, осуществляющий разработку, настройку и поддержку систем с соблюдением регламентов разграничения доступа.

Современные исследовательские усилия направлены на повышение точности биометрических систем и снижение уровня ошибок. Так, в работе [98] предложен метод снижения вероятности ложного подтверждения в системах распознавания лиц посредством внедрения нового алгоритма оценки качества. В исследовании [93] описан метод локализации радужной оболочки глаза, направленный на повышение точности распознавания. Внедрение профильных международных стандартов (в частности, ISO/IEC 19794) содействует обеспечению технологической совместимости и корректному обмену данными между разнородными информационными системами.

В настоящее время активно ведется работа по стандартизации форматов обмена данными и программных интерфейсов приложений. Биометрические технологии в современных условиях позиционируются как средство достижения повышенного уровня защищенности, ранее характерного преимущественно для систем специального назначения, а в настоящее время получившего массовое распространение. Указанная трансформация сопровождается обострением этико-правовой проблематики применения данных технологий.

В рамках обозначенной проблематики представляется обоснованным выделение нескольких предметных областей:

1) Обеспечение конфиденциальности персональных данных. Сбор, хранение и обработка биометрических данных несут в себе риски нарушения приватности. Проблема обостряется при обработке информации без юридически оформленного согласия субъекта. Это обусловливает необходимость жесткого правового регулирования для предотвращения утечек и неправомерного использования данных.

2) Уязвимость биометрических систем аутентификации. Несанкционированный доступ к таким системам выходит за рамки локального инцидента. Поскольку биометрические параметры неизменяемы (в отличие от паролей), их компрометация носит необратимый характер, что создает долгосрочные риски использования данных в противоправных целях [151].

3) Алгоритмическая дискриминация. Программное обеспечение для биометрического распознавания нередко обладает системными ошибками (алгоритмической предвзятостью/bias). Это приводит к снижению точности идентификации и ложным срабатываниям при обработке лиц разной расовой, этнической или гендерной принадлежности.

4) Ограничение гражданских свобод. Внедрение биометрического мониторинга в общественных пространствах может нарушать право на личную свободу. Риск заключается в масштабном скрытом наблюдении за гражданами без их ведома и согласия.

Важно обеспечить соблюдение принципов прозрачности и справедливости при сборе и обработке биометрических данных, а также защиту личной жизни и прав граждан на конфиденциальность и защиту личных данных. Исследование, проведенное Европейским парламентом, выделяло важность законодательного регулирования и обеспечения прозрачности в использовании биометрических технологий с учетом этических норм и прав человека. [94; 134; 139]

Резюмируя вышеизложенное, наиболее распространенными и технологически проработанными на данный момент остаются дискретные статические методы биометрической аутентификации (отпечатки пальцев, геометрия лица, радужная оболочка). Применение биометрических методов обеспечивает существенно более высокий уровень надёжности первичного разграничения доступа в сопоставлении с традиционными парольными политиками.

Вместе с тем классическая статическая парадигма аутентификации обладает принципиальным ограничением применимости: постаутентификационная фаза сеанса фактически не охватывается контролем со стороны системы. После завершения верификации доверие к субъекту обычно распространяется на весь жизненный цикл логического сеанса. Это создает условия для атак типа «перехват сеанса» (Session Hijacking), а также для несанкционированного доступа к АРМ, временно оставленному пользователем без контроля.

Для повышения защищенности и сохранения инвариантности сеанса требуется переход от разовой дискретной проверки при входе к непрерывному мониторингу подлинности. В программной реализации такой подход целесообразно связывать с методами поведенческой биометрии, основанными на обработке высокоэнтропийных телеметрических потоков, формируемых координатными устройствами ввода. Это формирует концептуальный базис для разработки алгоритмов непрерывно-дискретной биометрической аутентификации» или «алгоритмов непрерывного контроля подлинности без привлечения дополнительного аппаратного обеспечения.

1.3 Нормативно-правовая база и стандартизация методов биометрической аутентификации

Существует несколько организаций, которые занимаются стандартизацией в области биометрии, вот некоторые из них:

– Международная организация по стандартизации (ISO) имеет ряд стандартов и технических рекомендаций, связанных с биометрией, включая стандарты для геометрических параметров лица, биометрических шаблонов и биометрических систем исследования и оценки[2].

– Международная ассоциация биометрики (IBG) является главным профессиональным органом в области биометрии и устанавливает наиболее актуальные и важные принципы и методы в этой области.

– Американский национальный институт стандартов и технологии (NIST) также играет важную роль в определении стандартов и тестировании биометрических технологий и приложений[3].

– Европейский комитет по стандартам электронной коммерции и аутентификации (CEN), и Европейский комитет по стандартизации (CENELEC) также задействованы в создании стандартов, связанных с биометрией[4].

К ключевым стандартам биометрической аутентификации относятся:

– *ГОСТ Р 58624.2-2019 (ИСО/МЭК 30107-2:2017) Информационные технологии (ИТ). Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных.* Данный стандарт описывает методы и процедуры выявления атак на биометрические представления, то есть попыток обмана с использованием фальсифицированных биометрических данных. Его назначение состоит в повышении безопасности биометрических систем и предотвращении атак, связанных с применением фотографий, поддельных отпечатков пальцев и иных манипуляций [17].

– *ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента*

[2] https://www.iso.org/home.html
[3] https://www.nist.gov/
[4] https://www.cencenelec.eu/

информационной безопасности. Требования. Документ устанавливает требования и рекомендации к созданию, внедрению, поддержке и постоянному улучшению систем управления информационной безопасностью. Стандарт применим к различным областям, включая биометрическую аутентификацию, поскольку затрагивает надежность, конфиденциальность и доступность биометрических данных и систем. Использование профильных стандартов позволяет выстроить комплексную защиту в системах сбора, хранения и обработки биометрической информации [30].

– *ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство.* Внедрение стандарта обеспечивает систематизацию процессов управления рисками, связанными с безопасностью и надежностью биометрических систем. Это позволяет снизить их уязвимость и повысить общую эффективность защитных механизмов [21].

– *ГОСТ Р МЭК 31010-2021. Надежность в технике. Методы оценки риска.* Применение данного стандарта совместно с ISO/IEC 17025:2017 гарантирует высокую компетентность испытательных лабораторий [10; 31]. Это обеспечивает верификацию биометрических данных, валидность результатов тестирования и, как следствие, повышает уровень доверия к биометрическим системам.

– *ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация.* Регламентирует базовые нормативно-технические требования и правила, обязательные для учета при проектировании и эксплуатации систем контроля и управления доступом (СКУД).

– *ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018) Информационные технологии (ИТ). Биометрия. Общие положения и примеры применения.* Содержит концептуальные основы и примеры внедрения биометрических технологий [14].

– *ГОСТ ИСО/МЭК 19794-1-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными.* Стандартизирует

структуры данных для обеспечения технологической совместимости между разнородными биометрическими системами. В рамках серии стандартов ИСО/МЭК 19794 отдельно регламентируется представление данных геометрии контура кисти руки как самостоятельной биометрической модальности [27].

Несмотря на очевидные преимущества биометрических технологий, их внедрение сопряжено с рядом существенных проблем, в первую очередь – с вопросами обеспечения конфиденциальности и безопасности хранения персонализированных биометрических данных. В этой связи особое значение приобретают как разработка комплексных мер защиты, так и соблюдение действующих нормативно-правовых актов и международных стандартов обработки указанных данных. [130]

Правовое регулирование применения биометрических технологий в различных юрисдикциях имеет свою специфику. В ряде государств биометрические данные отнесены к специальным категориям персональных данных, в отношении которых применяются повышенные требования по обеспечению защиты, хранения и обработки. Характерным примером является правовая система Европейского Союза, в которой действует Общий регламент по защите данных (General Data Protection Regulation, GDPR), классифицирующий биометрические характеристики как чувствительные персональные данные, подлежащие особому режиму защиты.

Кроме того, в разных странах могут существовать дополнительные законы и нормативные акты, которые регулируют конкретные аспекты использования биометрических технологий, такие как возрастные ограничения на использование таких технологий, обязательность получения согласия субъекта данных на использование его биометрических данных и т.д. Однако уровень регулирования и защиты биометрических данных в разных странах значительно различается. [130; 159]

Обработка биометрических данных в России регулируется Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных

данных" (далее – ФЗ-152). [2] Ниже приведены основные особенности обработки биометрических данных в соответствии с этим законом:

1) Определение биометрических данных. Согласно закону, к биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека. Именно на основании этих особенностей можно установить личность человека, и они используются оператором для установления личности субъекта персональных данных.

2) Отсутствие строгой категоризации в 152-ФЗ. В самом Федеральном законе "О персональных данных" отсутствует классификация биометрии на подгруппы (генетические, фотографические и т.д.). Регулирование конкретных видов биометрии (таких как изображение лица и запись голоса) осуществляется отдельными законами, например, законодательством о Единой биометрической системе.

3) Согласие на обработку. По общему правилу, биометрические персональные данные могут обрабатываться только при наличии согласия субъекта персональных данных в письменной форме. Важной гарантией является то, что предоставление биометрических данных не может быть обязательным. Оператор не вправе отказывать человеку в обслуживании, если тот отказался предоставить биометрию или дать согласие на ее обработку (за исключением прямо установленных законом случаев).

4) Обработка без согласия. Закон устанавливает строгий и исчерпывающий перечень ситуаций, когда биометрия обрабатывается без согласия человека. К таким исключительным случаям относятся:

- реализация международных договоров РФ о реадмиссии;
- осуществление правосудия и исполнение судебных актов;
- проведение обязательной государственной дактилоскопической или геномной регистрации;

- случаи, предусмотренные законодательством об обороне, безопасности, противодействии терроризму и коррупции, об оперативно-разыскной деятельности, а также о государственной службе;
- реализация уголовно-исполнительного законодательства, законодательства о порядке въезда/выезда из РФ, гражданстве РФ и о нотариате.

5) Особые требования к безопасности. Оператор обязан принимать необходимые организационные и технические меры для защиты персональных данных (в том числе биометрических) от неправомерного или случайного доступа, копирования и распространения. Использование и хранение биометрических данных вне информационных систем разрешается только на таких материальных носителях и с применением таких технологий, которые обеспечивают их надежную защиту.

6) Хранение и уничтожение данных. Хранение биометрических данных не должно длиться дольше, чем этого требуют цели их обработки. По достижении целей обработки (или в случае утраты необходимости в их достижении) данные подлежат уничтожению или обезличиванию. *(Примечание: сроки хранения в Единой биометрической системе, составляющие не менее 50 лет, устанавливаются не 152-ФЗ, а отдельным приказом Минцифры России № 453).*

7) Трансграничная передача данных. К биометрическим данным применяются общие правила трансграничной передачи. Оператор обязан до начала передачи уведомить Роскомнадзор о своем намерении. В целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, а также обеспечения обороны и безопасности государства трансграничная передача данных может быть ограничена или запрещена.

К отечественным нормативным актам, связанным с вопросом биометрической аутентификации, относятся:

– Вышеупомянутый ФЗ-152 является основным в сфере защиты прав субъектов персональных данных. Аналогично предыдущему пункту

согласие является частью пользовательского соглашения или политики конфиденциальности.

– Федеральный закон "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ.

– Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ [4].

– Гражданский кодекс РФ запрещает использовать изображение человека без его согласия [1]. Статья 152.1. Охрана изображения гражданина. В большинстве случаев, для сбора и использования биометрических данных (таких как отпечатки пальцев, сканирование лица и т.д.), пользователь должен дать свое явное согласие на обработку этих данных. Согласие является частью пользовательского соглашения или политики конфиденциальности. Статья 152.1 Гражданского кодекса РФ применяется в случае, если использование изображения нарушает частную жизнь или честь и достоинство гражданина. Однако в случае биометрической аутентификации, изображение используется исключительно для процесса аутентификации и не обязательно публикуется или распространяется в общедоступных источниках.

– Приказ ФСБ РФ от 16 декабря 2016 г. N 771, Об утверждении порядка получения, учета, хранения, классификации, использования, выдачи и уничтожения биометрических персональных данных об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека, позволяющих установить его личность, получения биологического материала и осуществления обработки геномной информации в рамках осуществления пограничного контроля. Общим результатом влияния данного приказа на биометрическую аутентификацию является более жесткое регулирование и контроль за сбором, использованием и защитой биометрических данных, а

также повышение эффективности пограничного контроля с использованием биометрических технологий [6].

– Приказ ФСТЭК от 14 марта 2014 года N 31, Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды. В зону влияния данного приказа можно отнести повышение уровня безопасности и контроля на критически важных объектах, а также использование биометрических методов для обеспечения защиты информации и контроля доступа [8].

– Приказ ФСТЭК от 18 февраля 2013 года N 21, Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Этот приказ предоставляет правовую основу и стандарты для обеспечения безопасности персональных данных, включая те, которые используются в биометрической аутентификации.

– Приказ ФСТЭК от 11 февраля 2013 года N 17, Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Положения данного приказа охраняют информацию, не являющуюся государственной тайной, путем установления стандартов и мер безопасности, которые обеспечивают конфиденциальность, целостность и доступность данных, а также защиту от различных угроз. [9]

Важно отметить, что в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 12 мая 2023 г. N 453 «О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, центрального банка Российской федерации в случае прохождения им

аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц» [3] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации одобрило новые правила обработки биометрических данных физических лиц.

Согласно новым правилам, обработка биометрических данных будет проводиться в единой биометрической системе (ЕБС) и ее региональных сегментах, а также в информационных системах государственных органов, Центрального банка Российской Федерации, организаций, осуществляющих аутентификацию на основе биометрии. Для этого предполагается использование информационных технологий и технических средств, получивших подтверждение соответствия установленным требованиям. Подтверждение соответствия будет проводиться Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в течение 60 рабочих дней после получения необходимых документов и сведений.

С целью обеспечения безопасности обработки биометрических данных и векторов, предусматривается использование средств защиты информации, которые помогут предотвратить актуальные угрозы.

При этом стоит отметить, что возможно реализовать систему биометрической аутентификации, избегая классификации используемых данных пользователей как персональных. Необходимо использовать набор данных, который не позволяет однозначно деанонимизировать личность пользователя за пределами конкретной информационной системы, что нивелирует риски нарушения конфиденциальности. И если поведенческий паттерн не деанонимизирует личность глобально, то он не попадает под жесткие требования передачи в государственную ЕБС (как лицо или голос).

1.4 Концепция непрерывно-дискретного мониторинга сеанса на основе высокоэнтропийных поведенческих данных

Традиционные методы, основанные на статических физиологических характеристиках, и перспективные поведенческие подходы обладают

различными границами применимости, что отражено в сравнительной таблице 3.

Таблица 3 – Сравнительный анализ методов биометрической аутентификации

Метод аутентификации	**Преимущества**	**Недостатки**	**Необходимость в дополнительном оборудовании для клиентской АРМ**
Отпечатки пальцев	- Высокая достоверность - Относительно низкая стоимость сканеров - Простая и быстрая процедура сканирования	- Возможность повреждения папиллярного узора (механические травмы, ожоги) - Уязвимость к подделке (изображения, латексные копии) - Ограниченная применимость в агрессивных средах (грязь, влага)	Да. Требуется дооснащение АРМ внешним USB-сканером или закупка специализированных клавиатур/ноутбуков со встроенным дактилоскопическим датчиком.
Радужка глаза	- Высокая статистическая стойкость алгоритмов - Возможность бесконтактного сканирования на разных расстояниях (от нескольких сантиметров до нескольких метров) - Высокая защищённость от повреждений и подделок	- Высокая стоимость оборудования и реализации системы - Ограниченная доступность готовых решений на рынке - Возможность ошибок при изменении освещения и положении глаз	Да. Требуется установка специализированных инфракрасных (IR) камер высокого разрешения. Обычные веб-камеры для данной задачи неприменимы.
3D-геометрия лица	- Отсутствие необходимости в специальном взаимодействии пользователя с системой - Стабильность к внешним факторам (например, изменение освещения)	- Высокая стоимость оборудования и вычислительных мощностей - Подверженность влиянию мимики, аксессуаров и других временных изменений лица	Да. Требуются датчики глубины (Time-of-Flight), инфракрасные проекторы точек (структурированный свет) или стереокамеры. Обычная штатная веб-камера АРМ не обеспечивает построение 3D-модели.

	- Высокий уровень надёжности		
Узоры вен на руках	- Отсутствие физического контакта со сканером - Высокая надёжность (уникальность венозного рисунка)	- Чувствительность к освещению (неприемлемо использование солнечного или галогенного света) - Ограниченное распространение технологии на рынке	Да. Требуется закупка и интеграция узкоспециализированных инфракрасных сканеров вен (ближний ИК-диапазон).
Сетчатка глаза	- Высокая статистическая достоверность (индивидуальность структуры)	- Длительное время обработки данных - Высокая стоимость системы - Недостаточная популярность и интенсивность развития метода	Да. Требуется дорогостоящее медицинское/оптическое оборудование контактного или сверхближнего действия. Развертывание на массовых клиентских АРМ практически невозможно.
Голосовые данные (речь)	- Возможность удалённой аутентификации без физического контакта - Удобство использования - Низкая стоимость оборудования	- Подверженность влиянию фонового шума, простудных заболеваний и возрастных изменений - Высокая вероятность имитации голоса и атак с использованием синтеза речи	Минимальная. Требуется наличие микрофона или офисной гарнитуры, которые как правило уже входят в стандартную комплектацию рабочего места.
Анализ ДНК	- Абсолютная уникальность и высокая точность - Генетическая неизменность в течение жизни	- Высокая стоимость анализа и длительность процедуры - Этические и конфиденциальные риски (возможность утечки данных)	Да. Метод требует физического забора биоматериала и лабораторного оборудования. Абсолютно неприменим для потоковой аутентификации на АРМ.
Поведенческие признаки	- Постоянный (ненавязчивый) контроль пользователя - Низкая стоимость интеграции - Применимость для онлайн-сред	- Подверженность изменениям в поведении (усталость, стресс, болезни) - Возможность ложных срабатываний и	Нет. Используются исключительно штатные устройства ввода (стандартная компьютерная мышь, тачпад, клавиатура), являющиеся неотъемлемой частью любого АРМ. Метод

		недостаточная точность	является программно-определяемым (Software-defined) и не требует аппаратного дооснащения.

Обобщение результатов анализа рассмотренных методов позволяет сделать следующий вывод: преобладающая часть высокоточных статических решений сталкивается с принципиальным барьером внедрения, обусловленным необходимостью масштабного аппаратного дооснащения клиентских автоматизированных рабочих мест. Статические биометрические признаки ориентированы на дискретную процедуру верификации (так называемая «шлюзовая модель»), вследствие чего система остаётся уязвимой по отношению к атакам подмены контекста на постаутентификационной фазе.

Переход к парадигме непрерывного мониторинга обеспечивается применением методов поведенческой биометрии. Использование стандартных координатных манипуляторов типа «мышь» позволяет перевести задачу обеспечения безопасности в программную плоскость. Это обеспечивает повышение эффективности защиты на сессионном уровне в распределённых информационных системах при сохранении конфиденциальности пользователя и исключении дополнительных финансовых затрат на модернизацию инфраструктуры. Таким образом, интеграция нейросетевых методов анализа динамики устройств ввода является наиболее рациональным путем развития систем обеспечения подлинности в современных информационных процессах.

Переход к модели непрерывного контроля требует пересмотра критериев оценки эффективности информационных процессов. В отличие от дискретных систем, где показатели надежности вычисляются однократно при аутентификации, непрерывный мониторинг функционирует перманентно. Вследствие этого механизмы защиты становятся активными фоновыми задачами, создающими постоянную вычислительную нагрузку на аппаратные ресурсы клиентского узла.

В данных условиях критическими критериями функциональной пригодности системы выступают утилизация центрального процессора и объем потребляемой оперативной памяти. Поскольку алгоритмы анализа поведенческих факторов (включая инференс нейросетевых моделей) работают в режиме реального времени, их вычислительная сложность не должна вызывать деградацию производительности целевого ПО и снижать общую эргономику рабочего процесса.

Другим детерминирующим фактором безопасности является латентность, определяемая как время принятия решения. В условиях непрерывной аутентификации временной интервал между возникновением аномалии в поведении (например, при захвате управления злоумышленником) и срабатыванием блокировки сессии определяет окно уязвимости системы [95].

Эффективность защиты контура напрямую зависит от скорости обнаружения аномалий, однако непрерывная аутентификация по-прежнему сталкивается с серьезными аппаратными и математическими ограничениями. Переход от концептуальных моделей к массовому внедрению сдерживают три ключевых фактора:

1) Вычислительная избыточность и сетевая латентность: Непрерывный сбор, векторизация и нейросетевой анализ биометрических данных в реальном времени перегружают клиентские узлы и каналы связи. Чтобы предотвратить деградацию пользовательского опыта в распределенных системах, необходимы облегченные алгоритмы классификации и оптимизированные протоколы передачи – например, на базе концепции односторонней аутентификации по одному сообщению (OM-UEA).

2) Риски раскрытия конфиденциальных данных. Постоянный мониторинг телеметрии позволяет косвенно определять возраст, пол или психоэмоциональное состояние субъекта, что входит в прямое противоречие с регуляторными требованиями (GDPR, ФЗ-152). Для компромисса между безопасностью и приватностью применяются криптографические протоколы

частичного гомоморфного шифрования и забывчивой передачи (oblivious transfer). Они позволяют серверу валидировать результаты вычислений, не раскрывая исходную биометрию.

3) Дисбаланс метрик FAR/FRR и ложные срабатывания. Будучи вероятностной, система неизбежно допускает ошибки первого и второго рода: ложный допуск (FAR) и ложный отказ (FRR). Критически важная для практики стабильность достигается точной настройкой порогов классификации. В качестве базового ориентира обычно используется точка равной частоты ошибок (EER), а итоговое качество системы оценивается через полувзвешенный коэффициент (HTER).

Эксперименты с классическими алгоритмами машинного обучения – такими как Random Forest, k-ближайших соседей (KNN) и метод опорных векторов (SVC) – подтверждают перспективность непрерывного мониторинга, хотя их точность все еще требует оптимизации для реальных сценариев. Классификация действий пользователя по сенсорной динамике методом опорных векторов даёт среднюю точность около 90% – это хороший базовый показатель, но для критической инфраструктуры его недостаточно.

В таблице 4 приведено комплексное концептуальное сравнение парадигм дискретной и непрерывной аутентификации в контексте обеспечения безопасности сессионного уровня современных распределенных систем.

Таблица 4 – Сравнительный анализ парадигм дискретной и непрерывной аутентификации

Критерий оценки информационного процесса	**Дискретная (шлюзовая) аутентификация**	**Непрерывная (потоковая) аутентификация**
Периодичность контроля	Однократно при установлении логического соединения (в момент T=0)	Непрерывно в течение всего активного сеанса (в моменты T=0...N)

Информационная модель (по Шеннону-Альсведе)	Конечная передача, предъявление и валидация секретного маркера	Динамическое формирование и непрерывная вероятностная оценка высокоэнтропийного паттерна
Устойчивость к атакам перехвата сессии (CAPEC-593, CAPEC-61)	Фактически отсутствует. Система слепо доверяет украденному криптографическому токену.	Высокая. Аномалии в поведении нарушителя мгновенно снижают функцию доверия, блокируя сессию.
Эргономика и влияние на пользователя (Usability)	Высокая (не требует никаких действий после успешного входа)	Крайне высокая (процесс протекает абсолютно прозрачно в фоновом режиме, passive mode).
Требования к вычислительным ресурсам (Load)	Минимальные (разовая отправка хеша или JWT-токена)	Значительные (требует повышения эффективности алгоритмов извлечения признаков на стороне клиента).
Гарантия инвариантности сеанса (Session Invariance)	Предполагается априорно (на основании неизменности IP или токена)	Доказывается эмпирически через постоянный анализ физиологических и поведенческих метрик.

С учетом выявленной специфики функционирования гетерогенных децентрализованных сетей, где изначальное доверие к конечным узлам (клиентским АРМ) не может быть абсолютным, а требования к производительности аппаратуры остаются предельно жесткими, одним из наиболее перспективных направлений поведенческой биометрии выступает анализ динамики взаимодействия пользователя с классическим компьютерным манипулятором типа «мышь».

Данный подход органично вписывается в концепцию непрерывной фоновой аутентификации и обладает рядом фундаментальных, неоспоримых преимуществ при проектировании защищенных архитектур:

1) Отсутствие необходимости аппаратной модернизации: Подавляющее большинство традиционных высокоточных решений сопряжено с критическим барьером внедрения. В отличие от интеграции дактилоскопических сканеров отпечатков пальцев, считывателей рисунка вен ладони или инфракрасных 3D-камер для радужки глаза, требующих дорогостоящего оснащения рабочих мест специализированными аппаратными средствами, обычная компьютерная мышь является унифицированным, стандартизированным и неотъемлемым устройством ввода. Использование ее сигналов переводит глобальную задачу обеспечения безопасности исключительно в программную плоскость, полностью решая проблему гетерогенности и масштабируемости парка рабочих станций.

2) Решение проблемы конфиденциальности и защиты ПДн: Математическая модель движения мыши генерирует высокоэнтропийный поток пространственно-временных координат (X, Y), угловых скоростей, ускорений и временных таймстемпов кликов. Этот информационный процесс достаточен для поддержания непрерывной функции доверия и высокоточного индивидуального распознавания пользователя в рамках конкретной, локальной информационной системы. Однако, в отличие от геометрии лица или ДНК, эти данные не позволяют однозначно деанонимизировать личность субъекта за пределами этой инфраструктуры (в глобальном интернете). Это позволяет соблюдать этические нормы и строгие требования законодательства по защите персональных данных.

3) Ненавязчивость и прозрачность (Frictionless UX). Сбор координат курсора, анализ частоты кликов и паттернов скроллинга происходят параллельно с процессами операционной системы. Мониторинг не прерывает работу пользователя, реализуя принцип «пассивной непрерывной аутентификации» (passive continuous authentication).

4) Устойчивость к спуфингу и высокая энтропия поведения. Динамику мелкой моторики, особенности хвата мыши и нейромышечные реакции человека крайне сложно имитировать программно или воспроизвести

физически. Даже если злоумышленник перехватит сессию (Session Hijacking / CAPEC-593) или украдет JWT-токен, его биомеханический почерк при управлении интерфейсом будет другим, что позволит системе обнаружить подмену. Система непрерывного контроля зафиксирует критическое расхождение пространственно-временных паттернов (то есть зафиксирует грубое нарушение инвариантности сеанса) и мгновенно обнулит функцию доверия, заблокировав скомпрометированный сеанс.

Однако прямая математическая обработка «сырых» потоков координат напрямую нейронной сетью кратно увеличивает размерность входного вектора, что зашумляет процесс выделения биометрических признаков и неоправданно завышает вычислительную сложность логического вывода (инференса). Для решения проблемы информационной избыточности в рамках рассматриваемой системы применяется метод упрощения кривой движения с использованием модифицированного алгоритма Дугласа-Пеккера. Данный алгоритмический подход позволяет радикально снизить количество производимых матричных вычислений и объем временно хранимых данных (за счет векторизации траектории) без малейшего ущерба для итоговой эффективности распознавания легитимного пользователя.

Выбор архитектуры глубокого машинного обучения, а именно сверточной нейронной сети (CNN), в качестве основного классификатора поведенческих признаков обусловлен её эталонной способностью автоматически извлекать скрытые пространственно-временные паттерны непосредственно из потоковых данных. В отличие от ансамблевых методов (например, Random Forest), требующих ручного, ресурсоемкого математического конструирования кинематических признаков, интеграция CNN позволяет осуществлять устойчивую классификацию цифрового профиля в режиме реального времени с точностью до 97%. При этом, благодаря предварительной фильтрации алгоритмом Дугласа-Пеккера, обеспечивается снижение вычислительной нагрузки на клиентский узел

(интегральная утилизация ресурсов CPU и RAM не превышает 7,1%), что полностью решает проблему деградации производительности.

Таким образом, специфика архитектуры распределенных информационных систем объективно требует парадигмального, научно обоснованного сдвига от разовых процедур дискретного контроля к непрерывным фоновым информационным процессам верификации. В условиях удаленного администрирования и отсутствия жесткого физического контроля над клиентской средой, классические векторы атак сессионного уровня (CAPEC-593, CAPEC-60, CAPEC-61) критически обесценивают любую традиционную парольную аутентификацию. С теоретической точки зрения, основная задача защиты сводится к созданию инновационных механизмов, гарантирующих алгоритмическую инвариантность сеанса пользователя в условиях шумовых и аппаратных дисперсий. Интеграция методов потоковой интеллектуальной обработки сигналов динамики компьютерной мыши на базе глубокого обучения позволяет создать непрерывно-дискретную биометрическую систему, формирующую надежный базис для динамической устойчивости защищенных сред к современным социотехническим и программным угрозам.

1.5 Тенденции и перспективы развития непрерывной биометрической аутентификации

Междисциплинарность направления биометрических технологий выражается в связях с биохимией, ИКТ. В настоящее время человека могут идентифицировать по внешности, при этом все признаки становятся основой для проведения компьютерного анализа. Теперь исследуются не только фотографии, но и видеозаписи.

При проектировании современных систем непрерывной аутентификации целесообразно использовать гибридную архитектурную модель, четко разграничивающую задачи клиентской и серверной сторон. Облачные ресурсы в данной парадигме играют ключевую роль на этапе

формирования и адаптации моделей машинного обучения: они предоставляют необходимые вычислительные мощности для обработки репрезентативных массивов данных и проведения ресурсозатратных процедур обучения сверточных нейронных сетей. Кроме того, централизованные сервисы позволяют эффективно управлять политиками безопасности и агрегировать деперсонализированную информацию для повышения эффективности алгоритмов распознавания. [101]

Биометрические устройства и варианты их использования были внедрены в разных странах как государственными, так и частными организациями независимо от политической или экономической структуры, размера и географии. Отдельные государственные проекты биометрической идентификации связаны с миграционным учетом и регулированием статуса временных резидентов [140]. Когда-то биометрия применялась только в криминалистике и правоохранительных органах [121; 136; 157], но теперь используется в смартфонах, компьютерах и мобильных устройствах, в которых существует несколько биометрических методов для мгновенной аутентификации [121; 136; 157]. Теперь люди мгновенно аутентифицируют свою личность несколько раз в день, разблокируя свои смартфоны или подтверждая мобильный платёж в банковском приложении. Эта мгновенная аутентификация происходит без необходимости понимания ее технических аспектов. [92]

Представленный на рисунке 3 график наглядно демонстрирует стабильный и динамичный восходящий тренд мирового годового дохода от биометрических данных за последние 10 лет (2015–2024 гг.): за этот период совокупный объем рынка вырос более чем в 6 раз — примерно с 2 млн до 12,6 млн долларов. Главным локомотивом этого роста выступает Азия (серый сегмент), показавшая наиболее стремительное увеличение доли, в то время как рынки Европы и Северной Америки сохраняют устойчивое и планомерное развитие, а Латинская Америка и страны Африки демонстрируют хоть и

меньшие в абсолютных цифрах, но также стабильно растущие показатели из года в год.

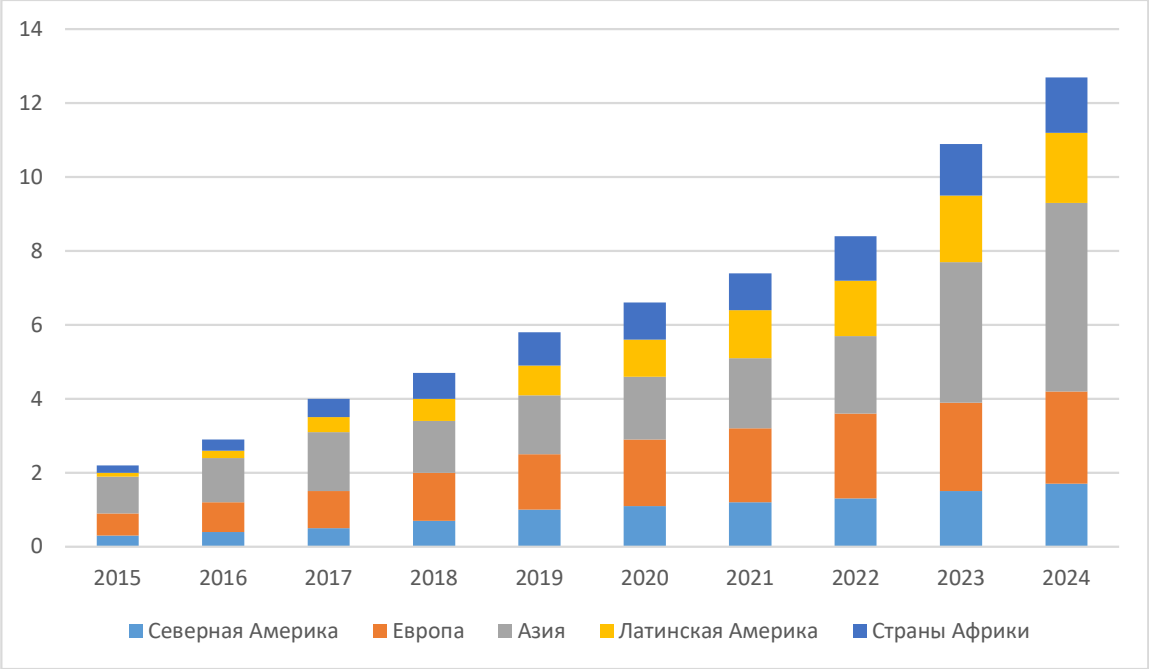

Рисунок 3 – Годовой доход от биометрических данных по регионам, млн. долл. [181]

Согласно последним исследованиям, рынок биометрических технологий продолжает демонстрировать значительный рост. К 2030 году общий рынок биометрии, как ожидается, достигнет 127,32 миллиарда долларов, что представляет собой увеличение с 34,95 миллиарда долларов в 2020 году при среднегодовом темпе роста (CAGR) 14%. Этот рост обусловлен потребностью в усиленной безопасности личных и корпоративных данных. Рынок биометрических сенсоров также показывает впечатляющие темпы роста, с прогнозируемым увеличением с 1,16 миллиарда долларов в 2020 году до 3,31 миллиарда долларов к 2030 году (CAGR 11,8%). Отдельное научно-практическое значение имеет динамика рынка автоматизированных дактилоскопических идентификационных систем (АДИС). Согласно прогнозным оценкам, к 2030 году данный сегмент достигнет объема в 68 миллиардов долларов при совокупном среднегодовом темпе роста (CAGR) 23,3%, что обусловлено интенсификацией спроса со стороны государственных

учреждений, а также банковского и финансового секторов. Кроме того, по данным аналитического агентства Transparency Market Research, к 2031 году совокупный объем мирового рынка биометрических технологий может составить 136,18 миллиарда долларов (CAGR 13,3%) на фоне его масштабирования в такие отрасли, как здравоохранение, финансовый сектор и автомобильная промышленность. [180: 181]

В контексте уменьшения затрат на мошенничество за счет использования биометрических технологий, важно учитывать следующие цифры:

- В 2017 году 16,7 миллиона американцев стали жертвами мошенничества, потеряв в общей сложности 16,8 миллиарда долларов.
- По оценкам ФБР, только мошенничество с карточками составило 28 миллиардов долларов, а дополнительные 32 миллиарда долларов были украдены онлайн.
- С тех пор как были собраны эти данные, наблюдается рост мошеннического использования украденных карт и банковских данных, что могло увеличить убытки примерно на 50%.

Большинство этих потерь возмещается клиентам их банками или кредиторами, но эти затраты возвращаются клиентам в виде комиссий, процентных ставок и инфляции. Расследования и судебные разбирательства также влекут за собой дополнительные расходы. Преступные доходы затем направляются в организованную преступность, наркоторговлю и терроризм, что приводит к дополнительным человеческим и финансовым затратам.

Благодаря массовому производству, строительные блоки биометрических систем дешевеют, а новые участники предлагают очень конкурентоспособные цены. Рост внедрения биометрических систем и датчиков привел к увеличению объема производства и снижению себестоимости, что, в свою очередь, позволило компаниям производить их в больших количествах и снижать цены на продукцию. Также факторами, которые способствовали снижению цен на запасные части, могут быть

изменения в технологиях производства, увеличение конкуренции на рынке и увеличение числа производителей и поставщиков на запасные части. Технологические усовершенствования и внедрение нового оборудования также снижают цены на предыдущие версии [49; 172].

Глобальный ландшафт биометрической аутентификации продолжает развиваться, что обусловлено развитием технологий и растущим спросом на повышенные меры безопасности в быстро меняющемся мире. Рост отрасли проявляется не только в рыночных показателях, но и в патентной активности крупнейших патентных ведомств, отражающей технологическую конкуренцию в сфере биометрии [131].

В последние годы российский рынок биометрических технологий начинает выходить из государственного сектора и появляются новые перспективные коммерческие акторы.

На рынке производителей биометрического оборудования выделяются несколько ключевых игроков, каждый из которых вносит свой уникальный вклад в развитие технологий и решений.

1) **Anviz** – глобальный лидер в сфере биометрической и бесконтактной аутентификации (RFID). Компания известна своими инновационными, эффективными и надежными решениями, которые находят применение в различных областях безопасности.

2) **ProSoft** – часть группы компаний «Прософт-Системы», основана в 2006 году. Компания специализируется на продуктах, обеспечивающих техническую и информационную безопасность с акцентом на биометрическую аутентификацию.

3) **BioLink Solutions** – эксперт и лидер российского рынка биометрических систем с многолетним опытом. Компания разрабатывает, поставляет и предоставляет биометрические решения и системы, демонстрируя постоянное развитие в этой сфере. [171]

Спрос на биометрические технологии вырастет в разных секторах, в первую очередь в финансовой сфере, где безопасность и защита интересов

клиентов критически важны [180; 181; 128; 141]. По мере появления новых технологий и роста точности аутентификации биометрические системы будут шире применяться в различных областях, повышая эффективность и безопасность процессов аутентификации личности. [181; 128; 141]

Перспективы развития биометрической аутентификации в ближайшем будущем [96; 108; 145; 168]:

1) Биометрическая аутентификация по поведенческим признакам. Поведенческие биометрические системы определяют человека по уникальным поведенческим характеристикам – ритму набора текста на клавиатуре, стилю взаимодействия с сенсорными устройствами, образцу движения мыши, характеристикам голоса. В таких системах задействованы сложные алгоритмы машинного обучения для анализа и интерпретации данных, и они эффективны в финансовой безопасности и контроле доступа. У поведенческих биометрических систем есть потенциал непрерывной и ненавязчивой аутентификации с более высоким уровнем безопасности, чем у традиционных методов. Они требуют более глубокого анализа приватности и этических аспектов: сбор и анализ поведенческих данных вызывает опасения за конфиденциальность и личные свободы.

2) Биометрическая аутентификация по походке/силуэту. Распознавание по походке и силуэту – интересная перспектива развития биометрических систем.

3) Биометрическая аутентификация по рисунку вен на ладони. Рисунок кровеносных сосудов на ладони уникален для каждого человека и сохраняется неизменным на протяжении жизни. Метод обеспечивает высокий уровень надёжности и с трудом поддаётся подделке.

Биометрическая аутентификация и далее демонстрирует свой потенциал в обеспечении безопасности, удобства и надёжности. Развитие биометрических технологий продолжится, новые методы внедрят в различные сферы деятельности, улучшая жизнь и повышая защиту персональных данных.

Традиционные методы аутентификации – пароли и двухфакторная аутентификация – характеризуются относительно низкой стоимостью внедрения. Однако их эффективность снижается пропорционально расширению множества актуальных угроз и уязвимостей. Высокоуровневые биометрические системы (в частности, системы распознавания лица и отпечатков пальцев) обеспечивают существенно более высокую степень защиты, однако требуют значительных финансовых вложений в специализированное аппаратное обеспечение, программные средства и инфраструктуру хранения и обработки данных. На данном фоне методика аутентификации, основанная на анализе динамики компьютерной мыши, представляет собой экономически целесообразное решение: она не предполагает применения дорогостоящего специализированного оборудования и не требует существенной модификации действующей ИТ-инфраструктуры. Эксплуатационные затраты традиционных биометрических систем формируются за счёт стоимости специализированного оборудования (сканеров отпечатков пальцев, камер для распознавания лиц) и затрат на обеспечение значительных вычислительных мощностей, требуемых для обработки биометрических данных.

Решение на основе анализа движений мыши использует уже имеющиеся ресурсы, что снижает стоимость внедрения и эксплуатации. Методика позволяет экономить на технической поддержке и обслуживании системы. Анализ движений мыши работает на программном уровне и встраивается в существующие системы без серьёзных модификаций, поэтому затраты на поддержание остаются минимальными. В итоге растёт точность аутентификации пользователей и оптимизируются бюджетные расходы на безопасность – это делает решение экономически привлекательным.

Дешевизна и скорость новых технологий биометрической аутентификации особенно ценны в образовательной сфере – для задач прокторинга и оценки поведения учащихся. Видеонаблюдение и машинное обучение для анализа видеоматериалов затратны и технически сложны в

реализации. Поведенческая биометрия на основе динамики движений мыши или ритме нажатий клавиш – более доступный и оперативный инструмент аутентификации. Подобные технологии встраиваются в образовательные платформы и системы дистанционного обучения без специализированного оборудования и дорогостоящего ПО. Ключевое преимущество поведенческого анализа – академическая честность при минимальных финансовых затратах, что важно для образовательных учреждений с ограниченными ресурсами. Такие методы воспринимаются пользователями как менее инвазивные на фоне визуального наблюдения, психологический дискомфорт ниже, качество образовательного процесса растёт. Интеграция поведенческих биометрических технологий формирует более прозрачную и справедливую образовательную среду.

1.6 Краткие выводы

Биометрическая аутентификация представляет собой фундаментальный элемент современных механизмов контроля доступа, обеспечивающий высокую надёжность идентификации за счёт анализа уникальных характеристик личности. Технологическая эволюция в этой сфере демонстрирует смещение фокуса в сторону нейросетевых алгоритмов, способных обнаруживать скрытые закономерности в высокоэнтропийных потоках данных. Точность распознавания и устойчивость систем к внешним помехам растут. Переход к программно-определяемым методам защиты (Software-defined security) поднимает эффективность внедрения и снимает необходимость в дорогостоящем аппаратном дооснащении рабочих мест.

Анализ нормативно-правовой базы и совокупности международных стандартов (прежде всего ISO/IEC 19794) подтверждает приоритет задач защиты биометрических шаблонов и обеспечения конфиденциальности субъектов персональных данных. При этом действующие нормативные требования и классические технические решения ориентированы преимущественно на однократную статическую процедуру верификации

подлинности на этапе входа в систему. Несмотря на наличие в арсенале современных методов статической биометрии (распознавание лица, радужной оболочки глаза), нейросетевых классификаторов высокой точности и протоколов многофакторной аутентификации, фундаментальная задача обеспечения инвариантности и устойчивости сеанса пользователя на протяжении всего периода работы остаётся нерешённой. Классическая парадигма не охватывает постаутентификационную фазу, что формирует векторы реализации атак типа «перехват сеанса» (Session Hijacking). В децентрализованных системах эта уязвимость становится критической: из-за отсутствия доверенной аппаратной среды на удаленных узлах риски атак сессионного уровня возрастают многократно. Это повышает риск атак сессионного уровня. В качестве решения предлагается концепция непрерывно-дискретной биометрической аутентификации, при которой поток данных от компьютерной мыши используется для скрытого фонового мониторинга подлинности субъекта без дополнительных аппаратных датчиков. Такой подход усиливает защиту постаутентификационной фазы логического сеанса и формирует адаптивный контур контроля, соответствующий требованиям безопасности распределенных сред.

В первой главе проведен анализ теоретических аспектов информационных процессов аутентификации в распределенных системах. Рассмотрены особенности функционирования таких систем и проблема сохранения инвариантности пользовательского сеанса. Результаты данной главы легли в основу следующих публикаций автора:

- Уймин, А. Г. Интеллектуальный анализ динамики трехпозиционного графического манипулятора типа "мышь" как элемента поведенческой биометрии / А. Г. Уймин // Системы управления и информационные технологии. – 2022. – № 2(88). – С. 92-96. – DOI 10.36622/VSTU.2022.88.2.018. – EDN XGHBWO.

- Никитин, О. Р. Инфраструктура JSON Web Token. Реализация основных типов атак / О. Р. Никитин, А. Г. Уймин // Перспективы науки. – 2023. – № 2(161). – С. 28-34. – EDN VOHMOG.
- Уймин, А. Г. Поведенческая биометрическая аутентификация и ее применимость в системах с комплексной дискретно-непрерывной передачей данных / А. Г. Уймин, А. В. Белоусов // Системы управления, связи и безопасности. – 2025. – № 4. – С. 1-26. – DOI 10.24412/2410-9916-2025-4-001-026. – EDN WAOURY.
- Уймин, А. Г. Оценка возможностей применения поведенческой биометрии: анализ движений компьютерной мыши для защиты сеансов удаленного администрирования / А. Г. Уймин, А. В. Белоусов // Computational Nanotechnology. – 2025. – Т. 12, № 3. – С. 170-177. – DOI 10.33693/2313-223X-2025-12-3-170-177. – EDN BULODR.
- Уймин, А. Г. Онлайн аутентификация: предварительная обработка данных / А. Г. Уймин // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VI Региональной научно-технической конференции, посвященной 100-летию М.М. Ивановой, Москва, 19–21 сентября 2022 года. – Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, 2022. – С. 1146-1147.
- Уймин, А. Г. Практическое применение элементов поведенческой биометрии / А. Г. Уймин, И. М. Морозов // Обеспечение информационной безопасности: вопросы теории и практики : Сборник статей Всероссийской научно-практической конференции, Ижевск, 29 мая 2023 года / Науч. редакторы Г.Г. Камалова, В.Г. Ившин, Г.А. Решетникова. – Ижевск: Издательский дом "Удмуртский университет", 2023. – С. 156-162. – EDN SLXNPB.

Материалы главы формируют фундаментальную постановку задачи и создают необходимые предпосылки для разработки метода непрерывно-

дискретной аутентификации (Положение 1) и многоуровневой модели удаленного доступа (Положение 2).

ГЛАВА 2 МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ НЕПРЕРЫВНО-ДИСКРЕТНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ПО ПОВЕДЕНЧЕСКИМ ПРИЗНАКАМ

2.1. Принципы и критерии построения многоуровневой модели информационного процесса удалённого доступа

Построение системы биометрической аутентификации (БИ) пользователя по движению мыши требует учета различных критериев, обеспечивающих качество работы и использования системы. В соответствии с ГОСТ Р ИСО/МЭК 25010-2015 «Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов» основными критериями, которые необходимо учитывать при построении такой системы, являются:

1. функциональная пригодность;
2. производительность;
3. совместимость;
4. удобство использования;
5. надёжность;
6. защищённость;
7. сопровождаемость;
8. переносимость.

Рассмотрим каждый из них подробнее в контексте биометрической аутентификации:

1. Функциональная пригодность включает в себя три ключевых аспекта, которые характеризуют способность продукта выполнять свои функции в полном объеме в соответствии с поставленными задачами и потребностями

пользователей: функциональная полнота, функциональная корректность и функциональная целесообразность.

Функциональная полнота определяет охват всех заявленных функций для выполнения задач. Применительно к БИ функциональная полнота показывает, в какой мере система обеспечивает весь необходимый функционал для задач аутентификации:

1.1) способность собирать данные (отпечатки пальцев, изображения лица, голос) – наличие соответствующих устройств ввода;

1.2) оперативная передача данных для обработки;

1.3) механизм сравнения с эталонными данными в базе (с учётом начального наполнения базы);

1.4) доступность использования в задаче верификации (подтверждения личности) или аутентификации (поиск личности в базе данных);

1.5) защита данных;

1.6) предотвращение подделки.

Функциональная корректность определяет, насколько точно и безошибочно система выполняет свои функции при биометрической аутентификации. Сюда относится правильность сбора данных (отсутствие искажений при сканировании отпечатка пальца), точность обработки (корректный анализ биометрических шаблонов), достоверность сравнения (минимизация ложноположительных и ложноотрицательных результатов) [127]. Важный аспект корректности – минимизация ошибок первого (False Acceptance Rate, FAR) и второго рода (False Rejection Rate, FRR), что прямо влияет на доверие к системе. [129]

Будем считать систему функционально корректной, если она надёжно определяет личность, соответствующую предоставленным данным (FAR < 0,5%; FRR < 0,5%), даже в условиях наличия проскальзывания датчика (курсора), отрыва устройства ввода от поверхности и т.д., влияющих на набор данных не более чем на 10% от выборки.

Наконец, функциональная целесообразность отражает степень, до которой функции системы действительно удовлетворяют потребности пользователей и соответствуют целям её использования. Будем считать систему целесообразной, если:

– начальное наполнение модели занимает до 5 мин времени пользователя;

– время отклика системы составляет до 1 с;

– система может быть оперативно (8 час) развернута в компьютерных классах до 100 устройств на оборудовании среднего ценового сегмента (см. требования к производительности).

2. Производительность охватывает аспекты, связанные с эффективностью работы продукта в реальных условиях использования. Она включает временные характеристики (насколько быстро продукт выполняет свои операции), использование ресурсов (насколько эффективно система использует доступные вычислительные мощности) и потенциальные возможности (как система справляется с увеличением нагрузки) системы.

Применительно к БИ производительность оценивается временем (скорости) аутентификации, задержками при обработке и доступностью модели в режиме реального времени [69]. Косвенно она характеризует эффективность использования ресурсов системы: процессорное время, расход памяти, загрузку ЦПУ, время отклика, пропускную способность, задержку.

Успешная биометрическая аутентификация невозможна без эффективной обработки данных и соответствующей производительности системы.

Оценка и повышение производительности обеспечивают быстрое и точное выполнение операций аутентификации, что отвечает потребностям пользователей.

Чтобы добиться заявленной эффективности и обеспечить минимальную ресурсоёмкость на конечных узлах, аппаратная архитектура разрабатываемой системы строго разделена на серверную часть (обучение моделей,

формирование эталонных шаблонов) и клиентскую (сбор телеметрии, фоновый инференс). При выборе вычислительного узла для развёртывания ядра системы учитывается баланс между скоростью обработки многомерных массивов данных и стоимостью решения.

Требования к серверному оборудованию определяются следующим образом:

- Процессор (CPU): многоядерная архитектура, не менее шести ядер и двенадцати потоков; базовая тактовая частота не ниже 3,5 ГГц, частота в турбо-режиме до 4,5 ГГц; поддержка современных наборов инструкций векторных вычислений (AVX, AVX2).
- Оперативная память (RAM): 16–32 ГБ DDR4, частота 3000–3200 МГц, двухканальный режим работы. Данный объем памяти позволяет загружать и удерживать в ОЗУ требуемые массивы поведенческих биометрических признаков.
- Графический процессор (GPU): поддержка технологии CUDA; объём видеопамяти не менее 12 ГБ; совместимость с программными средами TensorFlow и PyTorch.
- Накопитель: твердотельный накопитель типа SSD NVMe объёмом от 500 ГБ до 1 ТБ; скорости чтения и записи – не ниже 3000 МБ/с.

Состав указанных характеристик определён задачей обеспечения рационального соотношения производительности системы и её стоимости и гарантирует устойчивое функционирование алгоритмов глубокого обучения как на этапе инициализации, так и при последующем обновлении цифровых профилей пользователей.

Ключевым эксплуатационным преимуществом разработанной системы является её полная независимость от аппаратных ограничений автоматизированных рабочих мест (АРМ). По вычислительным ресурсам достаточно стандартного процессора офисного класса и 4 ГБ оперативной памяти. Из устройств ввода требуется стандартный координатный манипулятор типа «мышь». Специализированное аппаратное биометрическое

оборудование не нужно. Интегральная вычислительная нагрузка на клиентский узел снижена благодаря выносу процесса обучения на сервер. Анализ поведенческих паттернов (инференс) выполняется локально в фоновом режиме и обеспечивает непрерывную аутентификацию без заметной деградации производительности целевой операционной системы.

Совместимость показывает способность продукта взаимодействовать с другими системами и компонентами без потери функциональности. Сюда входят сосуществование и интероперабельность. Сосуществование означает, что продукт работает параллельно с другими программами или системами без конфликтов. Интероперабельность оценивает эффективность обмена данными с другими системами, а также совместное выполнение задач и бесшовную интеграцию в комплексные решения. В контексте БИ совместимость системы с аппаратным обеспечением – это работа с разными типами устройств: сканерами отпечатков пальцев, камерами для распознавания лица, микрофонами для голосовой аутентификации, сенсорами для анализа радужной оболочки глаза. Сюда же относится поддержка стандартных интерфейсов подключения оборудования и минимальные требования к характеристикам устройств.

Совместимость с аппаратной частью делает систему гибкой и адаптируемой к широкому спектру оборудования. На уровне ПО совместимость означает интеграцию системы биометрической аутентификации с операционными системами, существующими приложениями и базами данных. Сюда относится поддержка стандартных протоколов передачи данных (HTTPS, MQTT) и индустриальных форматов данных (ISO/IEC 19794 для биометрических данных).

Интероперабельность особенно актуальна в сценариях, где используются мультибиометрические системы, объединяющие несколько методов аутентификации.

4. Удобство использования включает множество характеристик, определяющих качество взаимодействия пользователя с продуктом. Основные

из них – это определимость пригодности, изучаемость, управляемость, защищённость от ошибок, эстетика интерфейса и доступность.

Доступность (простота) является ключевым фактором в создании положительного пользовательского опыта. Простота использования включает в себя легкость установки и настройки системы, понятный интерфейс пользователя и интуитивно понятные инструкции. Чем более проста модель или алгоритм, тем легче их принимать и использовать в реальных условиях [113].

5. Надёжность отражает способность системы стабильно выполнять функции в течение длительного времени. В биометрических системах надёжность оценивает способность модели или алгоритма справляться с вариациями и поддерживать высокую точность аутентификации независимо от них. Устойчивость к вариациям измеряется анализом производительности модели в различных условиях и при изменениях биометрических данных [57].

6. Защищённость показывает уровень защиты данных и предотвращения несанкционированного доступа. Сюда входят конфиденциальность, целостность, неподдельность, отслеживаемость, подлинность. Защищённость модели оценивают анализом её стойкости к различным видам атак – подделке биометрических данных, взлому системы. Шифрование и защита данных – важный аспект безопасности биометрической аутентификации.

7. Сопровождаемость характеризует трудоёмкость внесения изменений, обновлений и поддержки программного продукта. Применительно к системе биометрической аутентификации (БИ) данный показатель оценивает гибкость модели или алгоритма в части включения новых биометрических признаков или расширения существующего функционала. К таким признакам относятся: траектория движения, паузы и остановки, угол наклона и направление, силовая динамика, частота нажатий или касаний, временные зависимости, комбинации движений. По мере развития технологий и появления новых методов аутентификации модель должна обладать способностью к адаптации и интеграции инновационных решений. Сопровождаемость отражает

способность модели к обновлению с целью улучшения её характеристик либо устранения ошибок.

Реализация некоторых моделей биометрической аутентификации напрямую зависит от специализированного аппаратного обеспечения – сканеров дактилоскопии, камер распознавания лиц или микрофонов. Подобная гетерогенность оборудования требует гибких механизмов его обновления и адаптации под конкретные условия эксплуатации.

Для решения этой задачи программный комплекс проектируется на основе модульной архитектуры. Декомпозиция системы на независимые компоненты не только упрощает их модернизацию или повторное использование в смежных проектах, но и повышает общую анализируемость кода, облегчая локализацию неисправностей. Кроме того, модульный подход снижает трудоемкость внесения изменений (модифицируемость) и упрощает верификацию их корректности (тестируемость).

8. Переносимость определяет способность программного продукта работать в различных средах. Она включает адаптацию к разным аппаратным и программным платформам. Биометрическая система должна функционировать как на высокопроизводительных корпоративных серверах, так и на компактных вычислительных устройствах, включая смартфоны и планшеты. Отсюда следует необходимость оптимизации алгоритмов для устройств с ограниченными ресурсами, а также поддержки разных операционных систем и аппаратных конфигураций. Система должна иметь средства понятной настройки сканеров, камер и микрофонов, поддерживать стандартные драйверы и интерфейсы. Существенным свойством переносимости является взаимозаменяемость: возможность заменить текущую биометрическую систему альтернативной без значительных временных и материальных затрат. Это достигается за счет стандартизированных протоколов и форматов данных, в частности ISO/IEC 19794 (формат обмена биометрическими данными). Благодаря этому обеспечивается совместимость между различными решениями и упрощается

переход на новую систему, например, при масштабировании или обновлении технологии.

В контексте биометрической аутентификации, масштабируемость будет значима, если система должна обслуживать большое количество пользователей или использоваться в различных масштабных сценариях [58].

Помимо требований к качеству следует выделить экономическую целесообразность: критерий экономической целесообразности оценивает соотношение стоимости разработки, внедрения и поддержки модели биометрической аутентификации к ее эффективности и практической ценности. Учет экономической эффективности включает анализ затрат на разработку и внедрение модели, а также ресурсов, необходимых для поддержки и обновления. Основной статьей затрат в расчете экономической эффективности будет выступать оплата квалифицированных разработчиков.

Из рассмотрения перечисленных критериев можно сделать вывод, что кючевые факторы, определяющие эффективность биометрической аутентификации, – это функциональная пригодность, производительность точность, время принятия решения и нагрузка на систему пользователя, т.е. функциональная пригодность, так как именно эти три компонента напрямую влияют на удобство использования системы, её надежность и применимость в реальных условиях. Точность обеспечивает корректность аутентификации, время отклика – оперативность работы системы, а низкая нагрузка на систему пользователя гарантирует её доступность и эффективность в любых условиях эксплуатации.

В настоящей работе фокус делается на динамике манипуляций с компьютерной мышью как ключевом поведенческом признаке. Анализ этой динамики предоставляет возможность глубокого понимания способов взаимодействия пользователя с компьютерной системой с целью выявления потенциала поведенческой биометрии в современных технологических приложениях.

Достоинством использования движений мыши для биометрической аутентификации является возможность непрерывной аутентификации. [107] Пока пользователь взаимодействует с компьютером, система должна периодически анализировать его движения, чтобы убедиться, что управление осуществляется одним и тем же пользователем, чтобы в случае значительных отклонений запросить повторную аутентификацию или принять другие меры безопасности. [143] В рамках программной реализации количественными показателями качества анализа выступают параметры, представленные на рисунке 4.

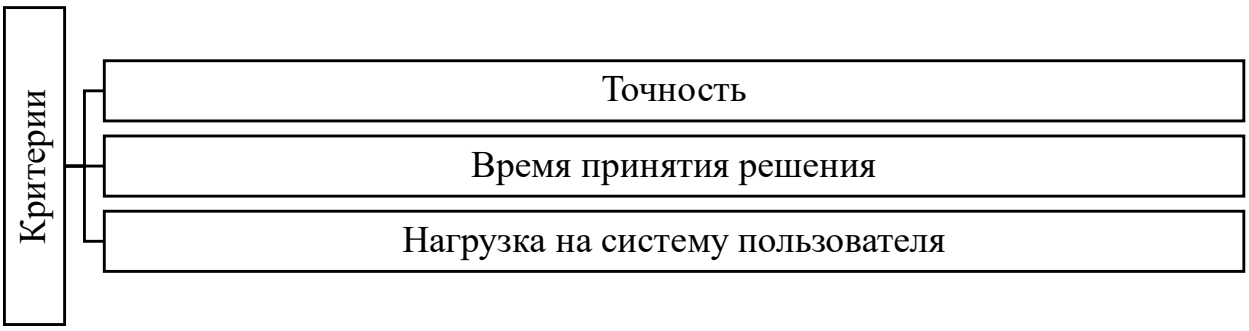

Рисунок 4 – Критерии качества системы биометрической аутентификации

Точность аутентификации измеряется с помощью вероятности ложного положительного срабатывания (FAR) и вероятности ложного отрицательного срабатывания (FRR).

Время принятия решения T_d можно рассматривать как сумму нескольких компонентов:

1) Сбор данных $T_{collect}$: время, необходимое для сбора необходимых данных (например, последовательности координат движения мыши).

2) Передача данных $T_{transmit}$: время, затраченное на формирование пакета данных и его отправку на сервер для обработки.

3) Обработка данных $T_{process}$: включает время, необходимое для предобработки данных, извлечения признаков и выполнения классификации.

4) Погрешности сети $T_{network}$: задержки из-за загруженности сети и возможных помех.

5) Сравнение и ответ $T_{compare}$: время, необходимое для сравнения извлеченных признаков с эталонными данными и выдачи решения.

Таким образом, общее время принятия решения можно выразить как:

$$T_d = T_{collect} + T_{transmit} + T_{process} + T_{network} + T_{compare} \quad (9)$$

Целью является минимизация T_d так, чтобы оно не превышало 1-2 секунды.

Нагрузка на систему пользователя L может быть оценена через следующие параметры:

— CPU Usage: загрузка центрального процессора.

— Memory Usage: загрузка оперативной памяти.

— Disk Operations: нагрузка на дисковую систему.

Для получения безразмерной величины L, необходимо учитывать, что разные типы нагрузки (CPU, память, диск) могут действовать параллельно и их нельзя просто суммировать напрямую. Одним из подходов к интегральной оценке разнородных типов вычислительной нагрузки является нормализация с последующим взвешенным суммированием, при которой учитывается вклад каждой компоненты в суммарную нагрузку. Введём следующие весовые коэффициенты для нормализации каждого типа нагрузки:

— w_{CPU}: вес для нагрузки на CPU

— w_{Memory}: вес для нагрузки на память

— w_{Disk}: вес для нагрузки на диск

Расчётная формула принимает вид:

$$L = w_{\mathrm{CPU}} \cdot \mathrm{CPU} + w_{\mathrm{Memory}} \cdot \mathrm{Memory} + w_{\mathrm{Disk}} \cdot \mathrm{Disk} \quad (10)$$

Значения весовых коэффициентов для различных систем определяются с учётом следующих факторов.

1) Тип и назначение системы. Для серверов баз данных приоритетное значение имеют дисковая подсистема и оперативная память. Для веб-серверных комплексов критическими ресурсами являются CPU и оперативная память. На рабочих станциях все три ресурса имеют равнозначное значение.
2) Мониторинг производительности: тесты производительности применяются для выявления узких мест в системе; мониторинг реальных условий эксплуатации – для выявления критических ресурсов.
3) Экспертная оценка: консультации с системными администраторами и инженерами для определения важности каждого ресурса.

Экспериментальным путём на ресурсах, описанных в пункте 2.2 определено, что чувствительность задержек начинается с 50% загрузки.

Соблюдение этих критериев позволит создать биометрическую систему аутентификации пользователей по движению мыши, которая будет эффективно сочетать точность, скорость и оптимальную нагрузку.

2.2 Методы потоковой обработки и экстракции цифровых признаков динамики компьютерной мыши

Передвижение по экрану компьютерной системы курсора компьютерной мыши представляет собой последовательный набор дискретных данных, записываемых в память компьютера.

Единичный элемент рассматриваемого набора данных представляет собой вектор параметров, включающий пространственные координаты курсора манипулятора («мыши») на экране, метку системного времени и текущее состояние кнопок устройства. В рамках поведенческого анализа динамика взаимодействия с манипулятором описывается

последовательностью элементарных событий, ключевыми из которых являются перемещение курсора и фиксация нажатий в определенных точках координатной сетки дисплея. Указанные пространственно-временные характеристики составляют основу динамической поведенческой биометрии, исследующей индивидуальные паттерны управления периферийными устройствами ввода в режиме реального времени.

При этом детальному анализу подлежат такие кинематические и динамические показатели, как траектория движений, мгновенная и средняя скорость перемещения курсора, векторы ускорения, а также специфический стиль и длительность удержания кнопок при кликах. Совокупность данных параметров формирует уникальный цифровой профиль поведения конкретного пользователя. При проведении аутентификации регистрируемый в текущей сессии поведенческий паттерн математически сопоставляется с предварительно сформированным эталоном для верификации подлинности субъекта [123].

Для достижения максимального уровня защищенности информационных систем метрики динамики управления манипулятором целесообразно интегрировать в контур многофакторной или непрерывной аутентификации. Так, если процедура первичного доступа базируется на традиционном вводе пароля или сканировании папиллярных узоров пальца, фоновый анализ координатно-временных характеристик мыши выступает в качестве дополнительного проверяющего фактора, что существенно снижает риски компрометации активной сессии в процессе работы.

Кривая движения курсора, скорость нажатия клавиш мыши, частота нажатий, бесцельные нажатия на клавиши, скорость перемещения курсора зависят от физиологических и психологических факторов, отождествимых только с одним уникальным пользователем компьютерной системы.

Показатели использования компьютерной мыши являются биометрическими данными: они зависят от физиологических признаков человека и однозначно определяют пользователя.

Целью сбора биометрических данных является их последующий анализ с целью подтверждения личности пользователя. Анализ биометрических данных позволяет подтверждать личность пользователя путем сравнения предоставленных биометрических характеристик с ранее сохраненными эталонами или шаблонами в базе данных.

При выполнении задачи сбора и анализа биометрических данных в общем виде можно выделить следующие этапы:

1) Сбор необработанных (так называемых «сырых» данных).
2) Передача «сырых» данных на устройство хранения.
3) Хранение «сырых» данных.
4) Выделение ключевых характеристик «сырых» данных.
5) Обучение решающего математического аппарата, функционирующего, как правило, на основе использования нейронных сетей и машинного обучения (далее – решающий аппарат).
6) Хранение состояний решающего аппарата.
7) Классификация действий пользователей при помощи решающего аппарата.
8) Определение пользователей с использованием решающего аппарата.

Обработка поступающих «сырых» данных в системах биометрической аутентификации реализуется в двух парадигмах. Первая – серверная: все собранные события передаются на центральный узел без предварительной фильтрации по информативности, где выполняются нормализация, агрегация и вычисление признаков. Вторая – потоковая (в реальном времени): ключевые характеристики извлекаются непосредственно на стороне сбора, после чего на сервер отправляются только информативные представления, что сокращает объём передаваемых данных и ускоряет последующий анализ [36].

В биометрической аутентификации по поведенческим признакам работы с компьютерной мышью индивидуальный стиль взаимодействия пользователя рассматривается как устойчивый маркер личности [144]. В

качестве наблюдаемых характеристик используются динамика перемещения курсора, частотные и временные параметры нажатий, доля спонтанных (контекстно не обусловленных) перемещений, траектория (паттерн) движения, а также распределение действий по кнопкам мыши. Скорость перемещения трактуется как изменение координат курсора во времени; для аутентификации сопоставляются статистические и модельные описания этой динамики с эталонным профилем пользователя. Частота и ритмика нажатий рассматриваются как элементы поведенческого почерка: анализируются средняя интенсивность кликов, вариативность и сезонность во времени, длительность удержания кнопок, повторяющиеся последовательности и контекстная изменчивость при выполнении разных задач или работе в различных приложениях. Траектория движения курсора (его геометрия и кинематика) описывает направления, скорости, микропаузирование и структуру навигации; по совокупности этих признаков формируется многомерный профиль, сопоставляемый с базой эталонных образцов методами статистического вывода и машинного обучения. Практически значимым считается интегральный подход, в котором перечисленные характеристики оцениваются совместно, поскольку их комбинация повышает устойчивость к имитации и точность распознавания.

В классических системах аутентификации указанные поведенческие признаки сопоставляются с заранее сформированным эталонным профилем пользователя. Такой подход повышает надёжность процедуры входа и усложняет подделку поведенческого паттерна при попытках несанкционированного доступа.

Построение признаков перемещения, наведения и щелчков требует предварительной обработки событийных логов и их преобразования в непрерывные временные ряды (рисунок 5) [77; 162]. В качестве временной оси используется Unix timestamp (далее – временная метка). Данные группируются по временным меткам таким образом, что каждой метке соответствует одна или несколько записей; для каждой уникальной метки вычисляются

агрегированные координаты, например средние значения по осям X и Y для всех событий, попавших в данное окно. На этапе извлечения выбирается целевой класс событий (перемещение либо клики), после чего выполняется агрегирование, формирующее равномерно отсэмплированный ряд. Затем применяется ресэмплирование (укрупнение или, при необходимости, интерполяция), обеспечивающее непрерывность и сопоставимость временных рядов между сессиями и пользователями, что является необходимым условием для устойчивого обучения и валидации моделей.

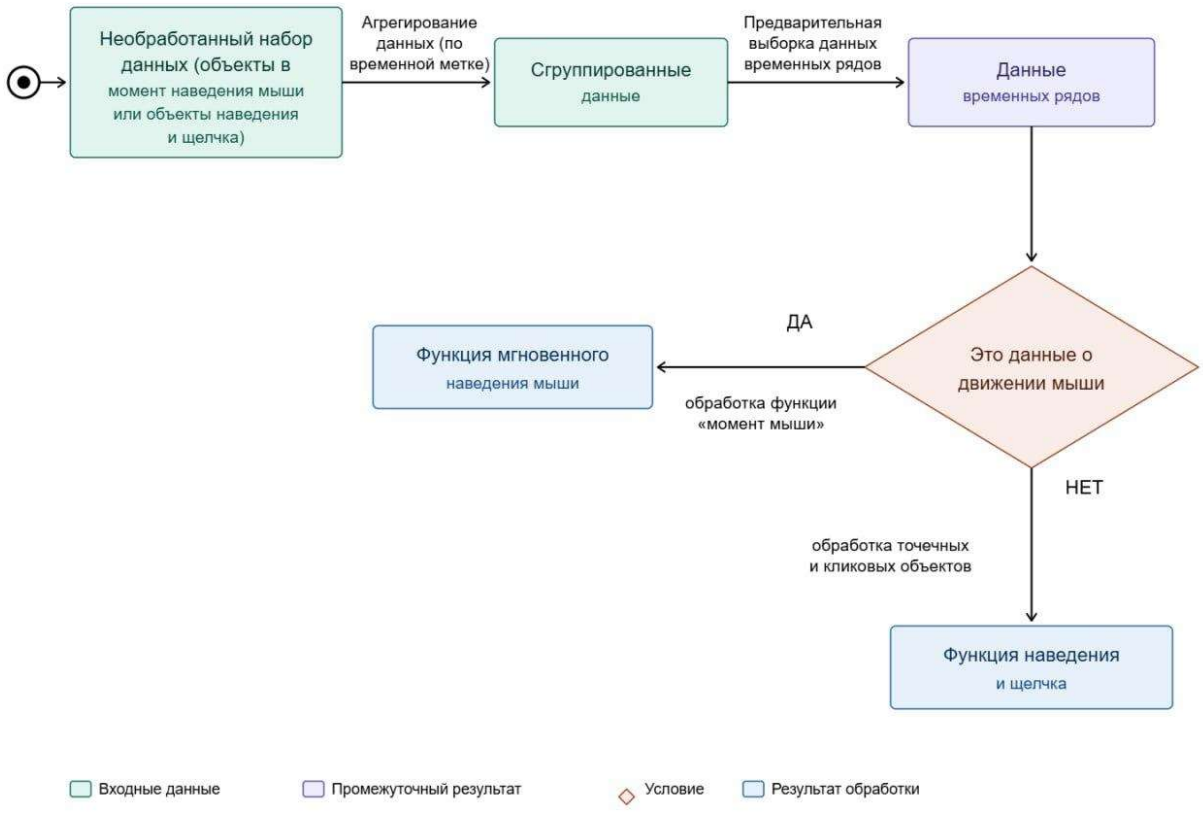

Рисунок 5 – Схема действий по предварительной обработке данных

Действие перемещения мыши представляет собой непрерывную последовательность действий пользователя, заключающуюся в смещении курсора между двумя позициями на экране. Каждое событие содержит информацию о координатах в момент фиксации. На рисунке 6 показано, как

действие перемещения может быть представлено в виде последовательности точек {P1, P2, P3, …, Pn}, каждая из которых соответствует фиксированному положению указателя [91; 118].

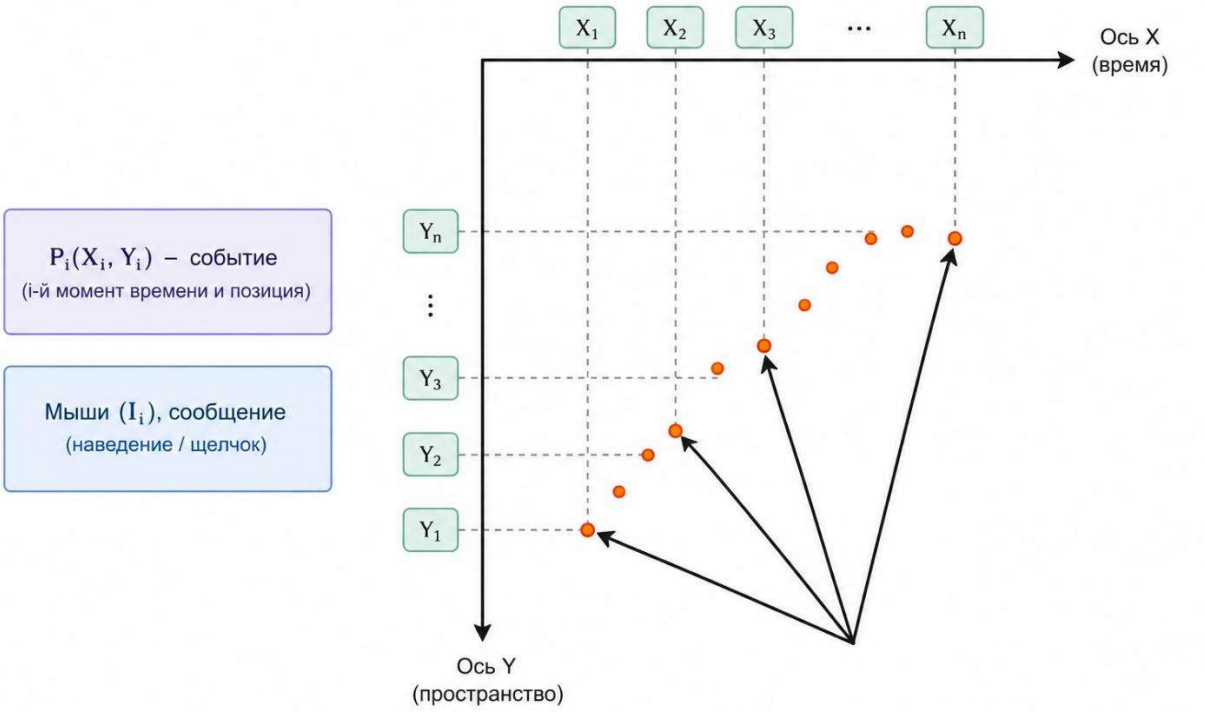

Рисунок 6 – Перемещение мыши между сериями расположения экрана

На основе анализа литературы выделяют три типа действий мыши: MM, PC и DD [91]. MM описывает перемещение указателя между двумя позициями на экране, PC характеризует процесс наведения курсора на объект и последующего нажатия одной из кнопок мыши, тогда как DD отражает действие перетаскивания, начинающееся с удержания кнопки и завершающееся её отпусканием. В рамках данного исследования набор данных был разделён на две укрупнённые категории: перемещение курсора (категория 1) и действия наведения с щелчком (категория 2). Действие классифицируется как PC, если за событием «нажатие кнопки» следует событие «отпускание кнопки»; в противном случае оно интерпретируется как последовательность типа MM.

Из временного ряда можно извлечь ряд функций. Скорость определяется как отношение приращения координат к интервалу времени (11-13):

$$v(x,t) = \frac{\Delta x}{\Delta t} \tag{11}$$

$$v(y,t) = \frac{\Delta y}{\Delta t} \tag{12}$$

$$v(pixels,t) = \sqrt{v(x,t)^2 + v(y,t)^2} \tag{13},$$

угловая скорость – как (14)

$$W = (\Delta\theta/\Delta t) \tag{14}$$

Ускорение вычисляется как изменение скорости за единицу времени (15-17):

$$a(x,t) = \frac{\Delta v(x)}{\Delta t} \tag{15}$$

$$a(y,t) = \frac{\Delta v(y)}{\Delta t} \tag{16}$$

$$a(x,y,t) = a(pixels,t) = \sqrt{a(x,t)^2 + a(y,t)^2} \tag{17}$$

Рывок определяется как изменение ускорения (18-20):

$$jerk(x,t) = \frac{\Delta a(x)}{\Delta t} \tag{18}$$

$$jerk(y,t) = \frac{\Delta a(y)}{\Delta t} \tag{19}$$

$$jerk(x,y,t) = \sqrt{jerk(x,t)^2 + jerk(y,t)^2} \tag{20}$$

Угловое перемещение θ вычисляется как (21):

$$\theta = atan\ (\Delta y/\Delta x) \quad (21),$$

где функция atan возвращает значения в диапазоне (−π,π)(-π, π)(−π,π).

Пройденное расстояние выражается через приращения координат (22):

$$Travelled(pixels) = \sqrt{(\Delta x)^2 + (\Delta y)^2} \quad (22)$$

Кривизна определяется через изменение угла касательной к длине пути (23):

$$Angle\ o\ f\ Curvature(\mathrm{c}) = \frac{\Delta\theta}{\Delta L} \quad (23),$$

а скорость изменения кривизны – как (24)

$$Curvature\ change\ rate(c) = \frac{\Delta C}{\Delta L} \quad (24)$$

При нормализации направлений используется методика Ahmed и Traore [91], где выделяются восемь базовых направлений (рисунок 7).

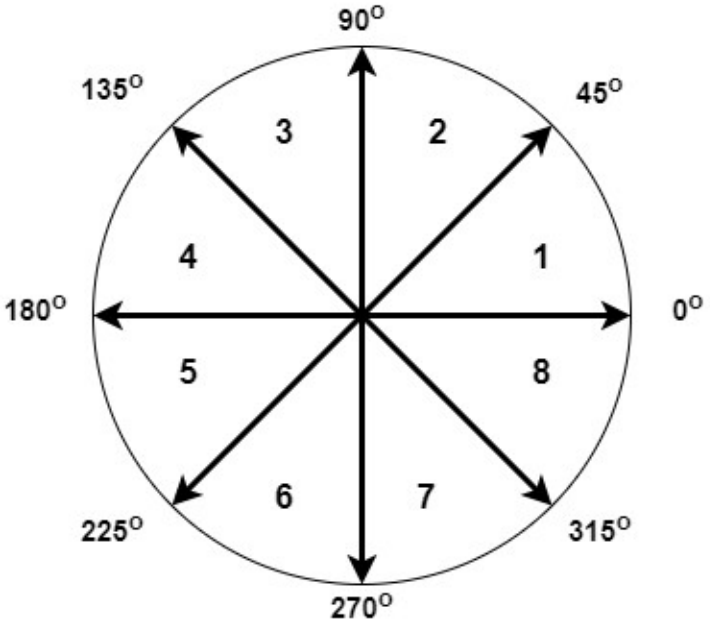

Рисунок 7 – Восемь направлений. Углы между 0 и 45 падают в направлении 1

Для вычисления дополнительных характеристик используются следующие соотношения. Полное угловое перемещение определяется суммированием угловых приращений вдоль траектории (25):

$$Total\ Angular\ Movement\ = \sum_{i=1}^{n} \theta_i \tag{25}$$

Абсолютное расстояние между начальной и конечной точками траектории описывается как (26):

$$Absolute\ Distance = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \tag{26}$$

Длина траектории представляет собой сумму евклидовых расстояний между последовательными точками (27):

$$\text{Длина траектории} = \sum_{i=1}^{n-1} \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2} \quad (27)$$

Прямолинейность пути определяется как отношение абсолютного расстояния к длине траектории (28):

$$Straightness = \frac{Absolute\ distance}{Length} \quad (28)$$

Время выполнения действия вычисляется как разность между моментом отпускания и моментом нажатия кнопки мыши (29):

$$T = T_{release} - T_{press} \quad (29)$$

Помимо перечисленных признаков, из выборок извлекаются статистические характеристики: среднее значение, минимум, максимум, стандартное отклонение и дисперсия [115] (30-34):

$$Mean = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (30)$$

$$Std = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - Mean)^2} \quad (31)$$

$$Min = \min(x_1, \dots, x_n) \quad (32)$$

$$Max = \max(x_1, \dots, x_n) \quad (33)$$

$$Variance = Std^2 \quad (34)$$

Анализ наведения и щелчков выделяет два набора данных: сегменты «ON KEY» (при нажатии) и «OFF KEY» (при отпускании). Для каждого сегмента рассчитываются перечисленные параметры движения, а также интегральные показатели: длина траектории, общее угловое перемещение и прямолинейность.

Эти характеристики применяются в разных задачах: от идентификации и аутентификации [91; 118; 123; 144] до анализа эмоционального состояния [104; 132; 161] и пользовательского опыта в виртуальных средах [132; 161; 170], усталости [125], физических параметров [114], концентрации внимания и удобства интерфейсов [44; 113; 133]. Использование этих сведений накладывает на разработчиков строгие юридические обязательства, включая соблюдение ФЗ-152 и получение явного согласия пользователей. Параллельно возникает необходимость технической защиты каналов от несанкционированного перехвата и сбора информации [2; 5; 7; 130; 139].

Для эффективной классификации жестов исходная траектория курсора преобразуется в ломаную, шаг дискретизации которой оптимизируется алгоритмом Дугласа–Пекера [77; 156; 162] (допустимый порог среднеквадратичной ошибки – 5%). Алгоритм извлекает 33 ключевые точки; полученные в результате 32 сегмента транслируются в нормализованные от -1 до 1 косинусы углов наклона к осям координат. Полученный вектор признаков поступает на вход многослойного персептрона [97]. Выбор данного способа аппроксимации обусловлен компактностью и масштабной инвариантностью результирующих данных, хотя он и не гарантирует сохранение топологии линии (возможны самопересечения). Схема описанного конвейера вычислений приведена на рисунке 8.

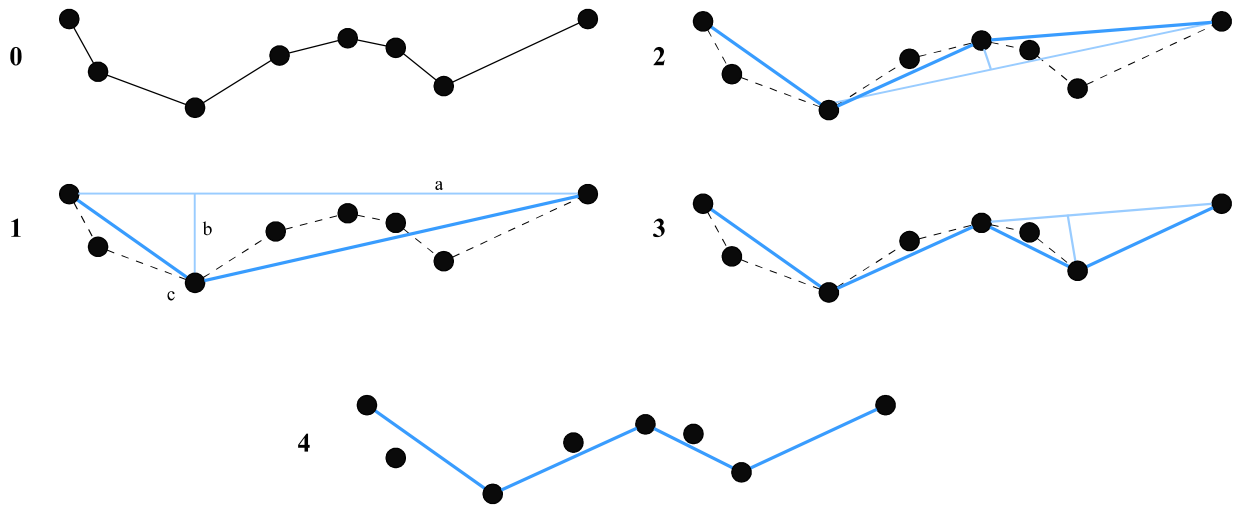

Рисунок 8 – Процесс упрощения ломаной

Алгоритм Дугласа–Пекера широко применяется для аппроксимации ломаных линий и редукции избыточных опорных точек при сохранении ключевых морфологических особенностей траектории. Входными параметрами алгоритма являются пороговое значение расстояния tol и исходная ломаная $\Lambda = \{V0, V1, \dots, Vn-1\}$, содержащая n вершин. На начальном этапе фиксируются крайние точки вектора траектории V_0 и V_{n-1}, после чего запускается рекурсивная процедура упрощения. Она последовательно оценивает отклонение промежуточных вершин от отрезка, соединяющего базовые крайние точки. Если максимальное перпендикулярное расстояние превышает установленный порог tol, соответствующая вершина признается локальным экстремумом (значимой точкой). Исходная линия дробится в этой точке, а процедура рекурсивно повторяется для двух вновь образованных подотрезков. Результатом работы алгоритма является сжатая ломаная $\Omega = \{W_0, W_1, \dots, W_{m-1}\}$, содержащая лишь ортогонально значимые подмножества исходных точек.

Ключевой операцией алгоритма является вычисление кратчайшего расстояния от точки до отрезка, для реализации которой целесообразно использовать параметрическое уравнение прямой. Если прямая L задана двумя точками P_0 и P_1, то её уравнение имеет вид (35):

$$P(t) = P_0 + tv_L = P_0 + t(P_1 - P_0) = (1 - t)P_0 + tP_1 \quad (35)$$

где $t \in R$ – действительный параметр. При $0 < t < 1$ точка $P(t)$ принадлежит отрезку P_0P_1 причём параметр t определяет отношение расстояний (36):

$$t = \frac{d\big(P_0, P(t)\big)}{d(P_0, P_1)} \quad (36)$$

Для определения расстояния $d(P, L)$ от произвольной точки P до прямой L находится ортогональная проекция точки P на данную прямую. Пусть $P(b)$ – основание перпендикуляра. В этом случае вектор $P_0P(b)$ является проекцией вектора P_0P на направляющий вектор отрезка. Обозначив $v_L = P_1 - P_0$ и $w = P - P_0$, значение параметра b для точки проекции можно выразить через скалярное произведение (37):

$$b = \frac{d\big(P_0, P(b)\big)}{d(P_0, P_1)} = \frac{|w| cos\,\theta}{|v_L|^2} = \frac{w \cdot v_L}{|v_L|^2} = \frac{w \cdot v_L}{v_L \cdot v_L} \quad (37)$$

Тогда искомое расстояние до прямой вычисляется как длина вектора ортогональной составляющей:

$$d(P, L) = |P - P(b)| = \|w - bv_L\| = \|w - (w \cdot u_L)u_L\|, \quad (38)$$

где $u_L = \frac{v_L}{\|v_L\|}$ - единичный направляющий вектор прямой L. Если проекция $P(b)$ выходит за пределы отрезка, то кратчайшим расстоянием считается расстояние от точки P до ближайшей из граничных точек P_0 или P_1. [77; 162]

При декомпозиции упрощенной ломаной направляющий вектор каждого сегмента нормализуется и представляется через направляющие

косинусы: $u_L = (\cos\theta_1, \cos\theta_2)$, где θ_1 и θ_2 – углы наклона сегмента к осям координат x и y соответственно. Данное компактное представление векторов траектории является инвариантным к масштабу и используется для формирования входного слоя искусственных нейронных сетей.

Практический базис применения алгоритма Дугласа–Пекера для предобработки биометрических данных в рамках настоящего исследования подробно раскрыт в третьей главе.

Помимо оптимизации входных признаков, способность нейросетевой модели к аппроксимации сложных поведенческих зависимостей определяется выбором функций активации. Рассмотрим применимость их классических вариантов.

Пороговая функция Хевисайда (39) имеет вид (рисунок 9):

$$\theta(x) = \begin{cases} 0, x < 0 \\ 1, x \geq 0 \end{cases} \quad (39)$$

Из-за нулевой производной на всей области определения (за исключением точки разрыва $x = 0$) данная функция не позволяет использовать градиентные методы обучения, что исключает ее применение в глубоких архитектурах.

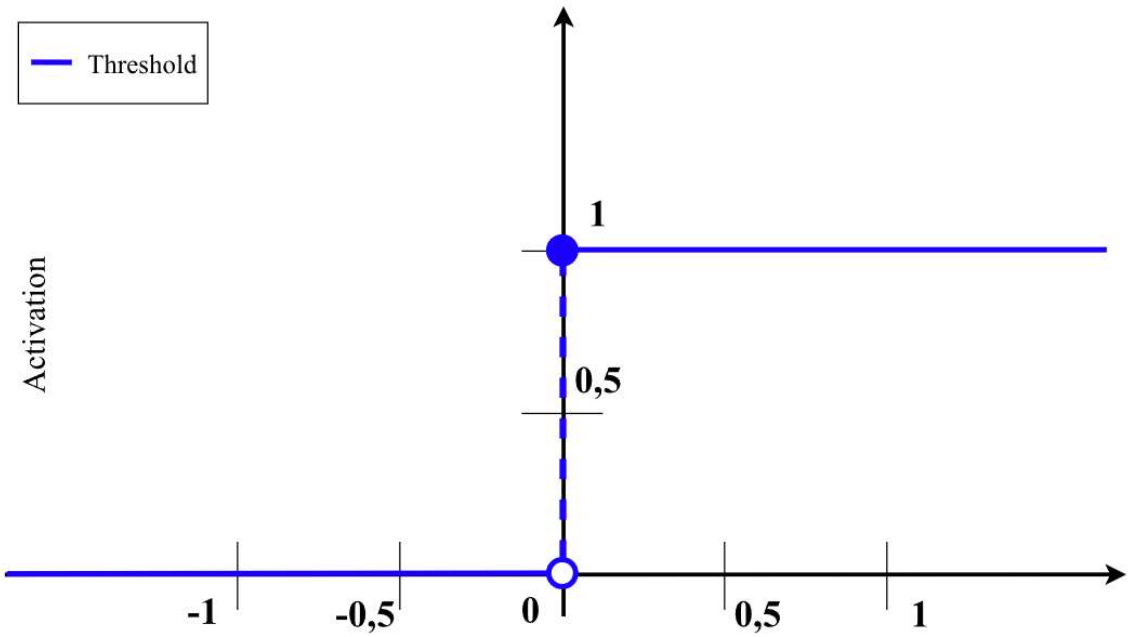

Рисунок 9 – Пороговая функция активации

Линейная функция активации (40) сохраняет входной сигнал без нелинейных преобразований (рисунок 10):

$$F(x) = x \tag{40}$$

Ввиду отсутствия нелинейности ее область применения ограничена преимущественно выходными слоями сетей, решающих задачи регрессии.

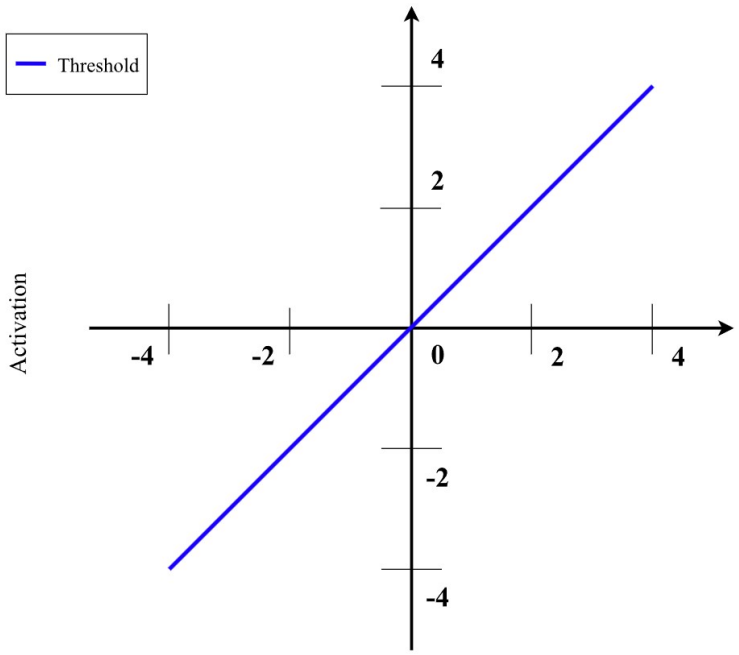

Рисунок 10 – Линейная функция активации

Сигмоидная (логистическая) функция (41) (рисунок 11)

$$F(x) = \frac{1}{1 + e^{-x}} \tag{41}$$

широко применяется в бинарной классификации, так как преобразует значения в диапазон $[0, 1]$. Недостатком является затухание градиента на больших $| x |$.

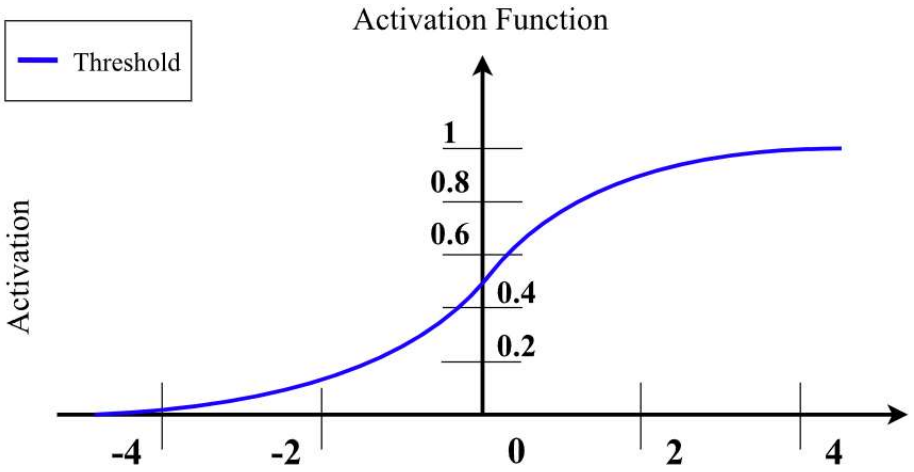

Рисунок 11 – Сигмоидная функция активации

Гиперболический тангенс (42) (рисунок 12)

$$tanh(x) = \frac{\exp(x) - \exp(-x)}{exp(x) + \exp(-x)} \tag{42}$$

ограничивает значения в диапазоне $[-1, 1]$ и имеет более высокий градиент вблизи нуля. Его производная вычисляется как (43):

$$1 - tanh^2(x) \tag{43}$$

тогда как у сигмоиды как (44)

$$f(x) * (1 - f(x)) \tag{44}$$

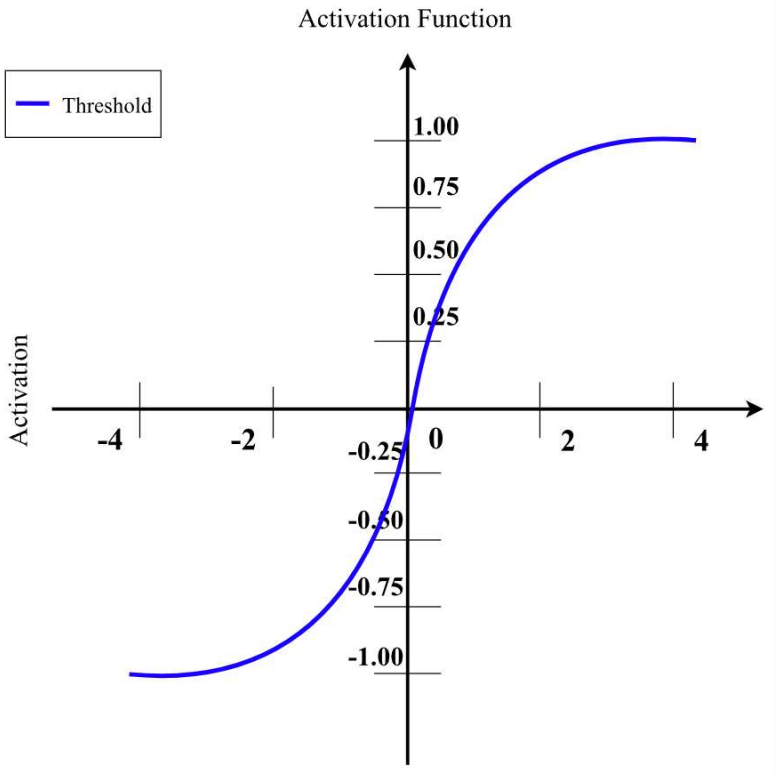

Рисунок 12 – Гиперболический тангенс

Однако и в случае tanh сохраняется эффект затухания градиента при увеличении числа слоёв.

Таким образом, несмотря на историческую роль сигмоидных и гиперболических функций активации, их использование в глубоких нейронных сетях ограничено. Именно поэтому современные архитектуры чаще опираются на функции ReLU и её модификации, которые позволяют избежать описанных проблем.

5. Используемая нами в функция активации ReLU

ReLU (Rectified Linear Unit) – одна из самых популярных функций активации, используемых как в сетях с низким числом слоёв, так и в моделях deep learning (рисунок 13).

Формула ReLU(45):

$$f(x) = max(0, x) \tag{45}$$

где x – входной сигнал, а f(x) – выходной.

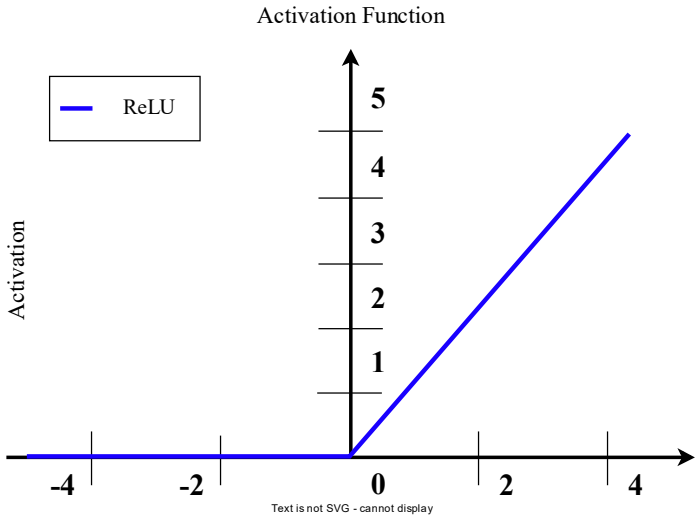

Рисунок 13 – Функция активации ReLU

Эта функция активации (равно как и существующие ее модификации) устраняет проблемы с исчезающим градиентом. Градиенты для значений

больше нуля остаются ненулевыми, что обеспечивает эффективное распространение градиентов и обновление весов в процессе тренировки.

У модифицированных функций Leaky ReLU, Parametric ReLU (PReLU) и Exponential Linear Unit (ELU) тоже есть свойства, которые способствуют предотвращению затухания градиента. Например, Leaky ReLU добавляет небольшой наклон для отрицательных значений, а у ELU есть экспоненциальная зависимость отрицательных значений (рисунок 14).

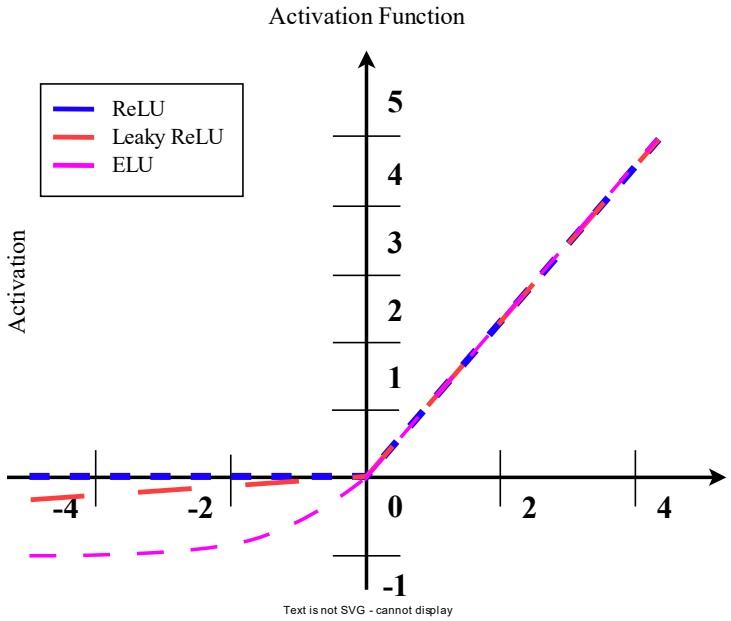

Рисунок 14 – Сравнение функции активации ReLU с ее модификациями

Функция универсальна и пригодна для любых задач, не требуя больших вычислительных мощностей. Все отрицательные значения функция заменяет на ноль и передает положительные значения без изменений. Градиенты для положительных значений остаются ненулевыми, что позволяет эффективно распространять градиенты и обновлять веса во время обучения.

Недостатком функции является то, что часть ReLu представляет из себя горизонтальную линию (для отрицательных значений x), градиент на этой части равен 0. Из-за равенства нулю градиента, веса не будут корректироваться во время спуска. Это означает, что пребывающие в таком состоянии нейроны не будут реагировать на изменения в ошибке входных

данных (просто потому, что градиент равен нулю, ничего не будет меняться). Такое явление называется проблемой умирающего ReLu (Dying ReLu problem). Из-за этой проблемы некоторые нейроны просто выключатся и не будут отвечать, делая значительную часть нейросети пассивной. Однако существуют вариации ReLu, которые помогают эту проблему избежать. Например, имеет смысл заменить горизонтальную часть функции на линейную. Если выражение для линейной функции задается выражением y = 0,01*x для области $x < 0$, линия слегка отклоняется от горизонтального положения. Существует и другие способы избежать нулевого градиента. Основная идея здесь – сделать градиент неравным нулю и постепенно восстанавливать его во время тренировки.

2.3 Разработка метода непрерывного контроля подлинности на основе анализа индивидуальных поведенческих паттернов

Биометрическая модальность зависит от совокупности факторов: конкретного биометрического признака, используемого сенсора, алгоритмов извлечения и манипулирования биометрическими атрибутами. Исследовательское сообщество [108] уделяет повышенное внимание биометрическим системам, о чем свидетельствуют научные работы. Биометрические данные, получаемые с помощью сенсоров, обрабатываемые алгоритмами и дифференцируемые на основе категорий или образцов признаков, вносят свой вклад в повышение точности распознавания в рамках биометрической системы. [168]

В рамках данного исследования были достигнуты следующие результаты:

1. Определены основные программные средства, предназначенные для сбора данных о действиях мыши.
2. Разработана методика, в рамках которой собирается и уточняется набор данных на основе данных о манипуляциях мышью с основными закономерностями.

3. Распространены проекты моделей глубокого обучения для когнитивной аналитики и обнаружения аномалий, что способствует тестированию пользователями.

Главная сложность при работе с данными от манипулятора – их извлечение. Необходимо получить данные, пригодные для обучения моделей машинного обучения (МОО) или альтернативного аналитического анализа. Сложность объясняется разнообразием форматов и структур, снижением качества или искажениями данных, ошибками при передаче. Не исключены шумы или помехи, которые затрудняют либо искажают извлечение информации. Поэтому важно использовать соответствующие алгоритмы и методы для обработки данных и их трансформации в понятный и полезный вид.

Для решения этой задачи используется схема предварительной обработки, которая преобразует необработанные данные в хорошо структурированный набор данных. В первую очередь временные метки преобразуются в стандарт UNIX, что обеспечивает их уникальность. Затем по оси времени выполняется повторная выборка, чтобы заполнить все недостающие записи, соответствующие отсутствующим временным меткам в диапазоне данных. Для этого используется функция из библиотеки Python pandas[5].

Существует несколько основных причин, по которым выбирают стандарт UNIX для временных меток:

1) Универсальность: стандарт UNIX используется на многих операционных системах и платформах, включая Linux, macOS, Solaris и другие. Это обеспечивает совместимость и переносимость временных меток между различными системами.

[5] https://pandas.pydata.org

2) Простота использования: стандарт UNIX определяет временные метки как количество секунд, прошедших с 1 января 1970 года. Это позволяет легко считать и сравнивать временные метки, а также выполнять математические операции с ними.

3) Точность: временные метки UNIX представляют время с очень высокой точностью - в миллисекундах или даже микросекундах, в зависимости от системы. В рамках работы нам достаточно точности порядка микросекунд.

4) Поддержка международной даты и времени. Временные метки UNIX дают возможность представлять локальное время и координированное всемирное время (UTC). Благодаря этому возможна работа с различными часовыми поясами и конвертация временных значений между ними.

При повторной выборке применяется линейная интерполяция, формирующая непрерывный временной ряд данных, пригодный для сложного анализа временных рядов[6]. [77; 162] Для подготовки набора данных применяются две техники – передискретизация и интерполяция.

Методы повторной выборки (передискретизации) формируют новые наборы данных за счёт повторения элементов исходного набора с определённым весом. На выходе получается более репрезентативная выборка, лучше отражающая характеристики генеральной совокупности.

Интерполяция же заполняет пробелы в наборе данных по информации из соседних точек. Интерполяция может быть использована для заполнения пропущенных значений в временных рядах данных или для восстановления недостающих значений в пространственных данных.

[6] Временные ряды – это последовательности точек данных, измеренных в последовательные временные интервалы. Они обычно используются для анализа и прогнозирования данных, которые изменяются со временем.

При работе с данными, полученными от манипулятора, одна из основных проблем заключается в их извлечении и подготовке. Важно получить данные, пригодные для обучения моделей машинного обучения (ML).

Важно, чтобы данные, подвергаемые анализу временных рядов, содержали либо записанные, либо интерполированные точки данных. Различные методики изучения временных рядов, в том числе AROMA/ARIMA[7] (и обучение нейронных сетей на основе LSTM[8] [112], предусматривают обязательное наличие чистых наборов данных, не содержащих временных разрывов. Наложение неполных наборов данных с временными лакунами приведёт к искаженным или ошибочным аналитическим результатам.

Если перейти к экспериментальному обоснованию, то на первый план выходит архитектура свёрточной нейронной сети (CNN). Эта парадигматическая нейросетевая структура начинается с начального слоя, включающего 64 фильтра, затем следует следующий слой, состоящий из 32 фильтров. Завершающим слоем является конфигурация, содержащая всего 16 фильтров. Каждый из трех слоёв опирается на ядро размером 1 × 1 пиксель. Для борьбы с опасностью перебора между последовательными стратами вводится отсев с вероятностью p = 0,05. Интеграция объединяющих слоёв обеспечивает извлечение признаков на различных иерархических уровнях, что способствует более полному раскрытию структуры входных данных для нейронной сети.

---

[7] AROMA (AutoRegressive Moving Average) и ARIMA (AutoRegressive Integrated Moving Average) – это две модели, используемые в статистическом анализе временных рядов для прогнозирования и понимания данных, которые изменяются со временем.

[8] LSTM, что расшифровывается как Long Short-Term Memory, представляет собой вид рекуррентных нейронных сетей (RNN), разработанный для решения проблемы исчезающего градиента, свойственной традиционным RNN. LSTM способен запоминать информацию на длительные периоды времени, что делает его идеальным для задач, где важно улавливать долгосрочные зависимости в данных

Итоговые вероятностные значения, формируемые на полностью связанном слое, отражают оценку нейронной сетью характеристик и атрибутов каждого пользователя по входным данным. Сеть формирует обоснованные прогнозы или классификации с адаптацией к конкретным пользователям.

Интеграция объединяющих слоев (pooling layers) обеспечивает извлечение признаков на различных иерархических уровнях, что позволяет нейронной сети эффективно декодировать пространственную или временную структуру входных данных. В качестве функции активации скрытых слоев применяется выпрямленный линейный блок (ReLU). Использование ReLU способствует формированию разреженных представлений (sparse representations) и повышает способность модели к аппроксимации сложных нелинейных взаимосвязей, параллельно снижая риск переобучения [138]. На выходе нейросети полносвязный слой (fully connected layer) формирует вектор вероятностей, определяющий результат классификации или аутентификации конкретного субъекта.

Функционирование разработанной модели непрерывного мониторинга базируется на сквозном конвейере обработки информации, включающем следующие этапы:

– Сбор и первичная агрегация данных: непрерывное накопление телеметрических параметров взаимодействия пользователя с интерфейсом.

– Извлечение и векторизация признаков: выделение информативных биометрических характеристик и формирование векторов признаков.

– Предобработка и разбиение выборки: в рамках каждой эпохи обучения агрегированные векторы признаков подвергаются процедуре случайного перемешивания (shuffling) для декорреляции данных. Сформированный массив разделяется в классическом соотношении: 80% векторов направляется в обучающее подмножество (train set) для настройки весовых коэффициентов модели, а оставшиеся 20% – в валидационную

выборку (validation set) для верификации обобщающей способности нейронной сети. Для исключения смещения классификатора соблюдается постоянство, обеспечивающее неизменное равновесие между обучающим и оценочным наборами на протяжении всех экспериментальных итераций.

– Этап выбора классификатора. Множество классификаторов, таких как DT (Decision Trees)[9], RF (Random Forest)[10], KNN (K-Nearest Neighbors)[11] и CNN (Convolutional Neural Networks)[12], используются для того, чтобы подчеркнуть эффективность предлагаемой модели в определении подлинных пользователей от злоумышленников на основе данных потока кликов пользователя.

Алгоритм межкомпонентного взаимодействия на этапах предобработки данных, обучения и оценки прогностической модели представлен на рисунке 15.

[9] **DT (Decision Trees)**: Деревья решений – это модели принятия решений, представляющие решения и их возможные последствия в виде древовидной структуры. Они просты в понимании и интерпретации, легко визуализируются и могут работать как с категориальными, так и с числовыми данными.

[10] **RF (Random Forest)**: Случайный лес – это метод ансамблевого обучения, основанный на агрегировании результатов множества деревьев решений для улучшения точности и устойчивости классификации. RF эффективен в снижении переобучения и способен обрабатывать большие наборы данных с высокой размерностью признаков.

[11] **KNN (K-Nearest Neighbors)**: Метод ближайших соседей – это простой, но мощный алгоритм классификации, основанный на предположении, что похожие объекты находятся в близком пространстве друг к другу. KNN не требует обучения на этапе обучения, но вычислительно требователен на этапе классификации, особенно для больших наборов данных.

[12] **CNN (Convolutional Neural Networks)**: Свёрточные нейронные сети относятся к типу глубоких нейронных сетей и особенно эффективны при анализе изображений. CNN используют слои свертки, которые автоматически извлекают признаки из визуальных данных; поэтому такие сети применяются для распознавания образов, классификации изображений и обработки видео. пользователей от злоумышленников на основе данных потока кликов пользователя.

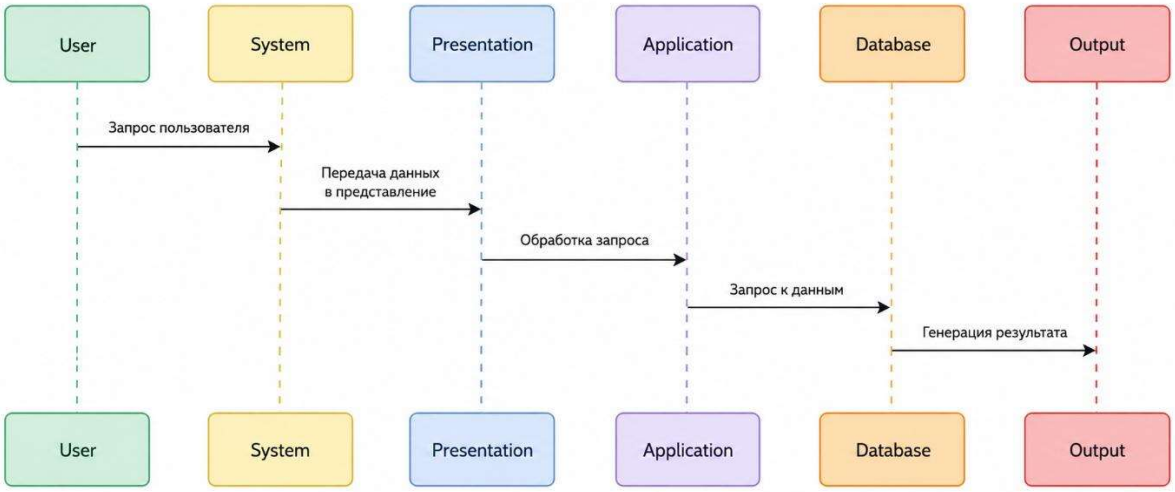

Рисунок 15 – Схема последовательности процессов обработки данных и обучения модели

После первичной предварительной обработки данных, включая преобразование временных меток и заполнение пропущенных записей, необходимо устранить проблемы, связанные с неполнотой набора данных. Для этого применяются методы повторной выборки и интерполяции. Их сочетание позволяет получить целостный и непрерывный временной ряд, пригодный для дальнейшего анализа.

2.4 Формализация и алгоритмизация процесса принятия решения в условиях асинхронного информационного потока

Процедура биометрической аутентификации пользователя формализуется в виде последовательного выполнения следующих взаимосвязанных этапов:

1) Сбор данных вида $T = \{(x_i, y_i, t_i)\}_{i=1}^{n}$ – последовательность точек траектории мыши, где x_i и y_i - координаты точки в момент времени t_i.

2) Предобработка данных: применение алгоритма Дугласа-Пекера для упрощения траектории, результатом чего является уменьшение количества точек траектории при сохранении её основных характеристик.

Входной информацией для задачи распознавания жестов мыши с использованием нейронной сети является путь мыши, который представляет

собой ломаную линию, состоящую из конечного числа точек. Перед подачей записанного пути мыши на вход нейронной сети целесообразно выполнить определенное преобразование ломаной, подробно описанное в разделе 2.2.

Упрощение ломаной дает возможность выделить точки, количество которых соответствует числу входов сети.

Таким образом, входной информацией используемой нейронной сети являются косинусы углов наклона отрезков, соединяющих наиболее значимые точки пути мыши.

3. Извлечение признаков:

– Общая длина траектории (L) – вычисляется как сумма евклидовых расстояний между смежными точками дискретизированного трека (46):

$$L = \sum_{k=1}^{m-1} \sqrt{(x_{k+1} - x_k)^2 + (y_{k+1} - y_k)^2} \tag{46}$$

– Абсолютное смещение (D) – определяет евклидово расстояние между начальной и финальной точками зафиксированной траектории (47):

$$D = \sqrt{(x_m - x_1)^2 + (y_m - y_1)^2} \tag{47}$$

– Суммарное угловое перемещение (Θ) – отражает интегральную кривизну (извилистость) движения и рассчитывается как сумма модулей разностей углов наклона смежных сегментов (48):

$$\Theta = \sum_{k=1}^{m-1} \left| \tan^{-1}\left((y_{k+1} - y_k)/(x_{k+1} - x_k)\right) - \tan^{-1}\left((y_k - y_{k-1})/(x_k - x_{k-1})\right) \right| \tag{48}$$

– Коэффициент прямолинейности (R) – безразмерная величина, характеризующая степень отклонения реальной траектории от кратчайшего пути (интерпретируется как отношение абсолютного смещения к полной длине) (49):

$$R = \frac{D}{L} \tag{49}$$

– Общая продолжительность движения (Δt) – временной интервал, затраченный пользователем на выполнение перемещения (50):

$$\Delta t = t_m - t_1 \tag{50}$$

4. Архитектура нейросети (CNN):

— Входной слой: принимает на вход набор векторизованных признаков $v = [L, D, \Theta, R, \Delta t]$.

— Последующие за входным слоем одномерные сверточные слои (Conv1D): анализируют локальные зависимости между признаками.

Обозначим:

$W^{(k)}$– веса k-го сверточного слоя,

$b^{(k)}$ – смещения k-го сверточного слоя,

$z^{(k)}$ – выход k-го сверточного слоя.

Каждый элемент выхода i-го слоя можно вычислить как (51):

$$z^{(k)} * i = \sigma\left(\sum_j W_{ij}^{(k)} \cdot v_j + b_i^{(k)}\right) \tag{51}$$

где σ – функция активации ReLU, применяемая после каждого сверточного слоя для добавления нелинейности (52):

$$\sigma(x) = \max(0, x) \tag{52}$$

— Полносвязные слои (Dense): интегрируют информацию из предыдущих слоев и переходят к выходному слою.

Обозначим:

$W^{(d)}$ – веса d-го полносвязного слоя,

$b^{(d)}$ – смещения d-го полносвязного слоя,

$h^{(d)}$ – выход d-го полносвязного слоя.

Выход каждого элемента полносвязного слоя можно вычислить как (53):

$$h^{(d)} * i = \sigma\left(\sum_j W_{ij}^{(d)} \cdot z_j^{(k)} + b_i^{(d)}\right) \tag{53}$$

где σ – функция активации ReLU, аналогично предыдущим слоям.

— Выходной слой с одним нейроном и сигмоидной функцией активации: предсказывает вероятность того, что траектория принадлежит зарегистрированному пользователю.

Обозначим:

$W^{(o)}$ – веса выходного слоя,

$b^{(o)}$ – смещение выходного слоя,

$\hat{y}$ – выход нейросети, предсказывающий вероятность принадлежности траектории зарегистрированному пользователю.

Выходной слой вычисляется как (54):

$$\hat{y} = \sigma\left(\sum_i W_i^{(o)} \cdot h_i^{(d)} + b^{(o)}\right) \tag{54}$$

где σ – сигмоидная функция активации (55):

$$\sigma(x) = \frac{1}{1 + e^{-x}} \tag{55}$$

Таким образом, вся архитектура CNN последовательно обрабатывает входной вектор признаков, применяет конволюционные слои для анализа локальных зависимостей, полносвязные слои для интеграции информации и выходной слой для предсказания вероятности.

5. Классификация: принятие решения об аутентификации выполняется на основе порогового значения θ . Если $f(v;\Theta) \geq \theta$, пользователь аутентифицируется успешно; в противном случае, доступ отклоняется.

Число выходов используемой нейронной сети соответствует количеству жестов. Значения активационных функций нейронов выходного слоя позволяют судить о том, к какому эталонному жесту наиболее близок поданный на вход вектор.

Основу предложенной модели составляет сверточная нейронная сеть (CNN), адаптированная для обработки одномерных пространственно-временных рядов, полученных после векторизации динамики манипулятора. В отличие от классических полносвязных сетей (персептронов), сверточные слои позволяют автоматически извлекать локальные кинематические признаки, независимые от их точного положения во времени.

Пусть $x^{(l-1)}$– входная матрица признаков (карта признаков) для слоя l, где каждый столбец представляет временной отсчет, а строка – канал данных. Значение сигнала $z_j^{(l)}(t)$ для j-го фильтра в l-м сверточном слое в момент времени t вычисляется посредством операции одномерной свертки (56):

$$z_j^{(l)}(t) = \sum_{c=1}^{C_l - 1} \sum_{k=1}^{\mathrm{K}} W_{j,c}^{(l)}(k) \cdot x_c^{(l-1)}(t + k - 1) + b_j^{(l)} \tag{56}$$

где $C_l - 1$ – количество каналов на предыдущем слое;

K – размер ядра свертки;

$W_{j,c}^{(l)}(k)$ – весовой коэффициент j-го фильтра для c-го канала;

$b_j^{(l)}$ – смещение (bias) j-го фильтра.

Выходная матрица признаков сверточного слоя формируется путем применения нелинейной функции активации ReLU к полученному результату операции свертки (57):

$$a_j^{(l)}(t) = \mathrm{ReLU}\left(z_j^{(l)}(t)\right) = \max\left(0, z_j^{(l)}(t)\right) \quad (57)$$

Архитектура разработанной нейросети строится по иерархическому принципу глубокого извлечения признаков. Экстрактор включает три последовательных сверточных слоя с уменьшением количества фильтров: первый слой содержит 64 фильтра, второй – 32 фильтра, третий – 16 фильтров. Для снижения пространственной размерности карт признаков и обеспечения инвариантности к масштабу между сверточными слоями интегрированы операции субдискретизации (Pooling). С целью регуляризации модели и предотвращения переобучения в структуру сети встроен слой исключения нейронов (Dropout) с вероятностью зануления весов $p = 0{,}05$.

В компактной форме операторное преобразование входного вектора признаков в латентное представление на выходе экстрактора описывается выражением (58):

$$h = \psi_3(W^{(3)} * \psi_2(W^{(2)} * \psi_1(W^{(1)} * x))) \quad (58)$$

где $*$ обозначает операцию одномерной свертки, совмещенную с последующим пулингом, $W^{(i)}$ – матрицы весов соответствующих слоев, а ψ_i – нелинейные покомпонентные функции активации скрытых слоев.

Предложенная сверточная архитектура экстракции признаков заменяет классическую полносвязную топологию на этапе предобработки, что

обеспечивает существенное снижение вычислительной сложности и сокращает нагрузку на клиентский узел распределенной системы.

Выходное значение нейросети интерпретируется не как принадлежность к изолированному дискретному «жесту», а как апостериорная вероятность соответствия текущего поведенческого паттерна профилю легитимного пользователя (задача бинарной классификации). Для генерации указанной метрики на финальном полносвязном слое применяется логистическая функция активации (Sigmoid), имеющая вид (59):

$$y = (z) = \frac{1}{1 + e^{-z}} \tag{59}$$

Если вычисленная вероятность y превышает установленный порог безопасности (например, $\tau = 0{,}5$), текущая сессия признается легитимной. При падении метрики ниже порогового значения система идентифицирует аномалию и инициирует превентивные процедуры защиты сеанса связи.

При оптимизации весовых коэффициентов модели в качестве обучающей выборки использовались наборы данных, размеченные на два комплементарных класса: «легитимный пользователь» $(d_i = 1)$ и «злоумышленник / аномалия» $(d_i = 0)$.

Для обучения сети используется алгоритм обратного распространения ошибки, адаптированный под бинарную кросс-энтропию (Binary Cross-Entropy, BCE), которая является оптимальной целевой функцией для задач аутентификации. Целевая функция потерь $Q(W)$ для N обучающих наблюдений имеет вид (60):

$$Q(W) = -\frac{1}{N}\sum_{i=1}^{N}[d_i \log(y_i) + (1 - d_i)\log(1 - y_i)] \to min \tag{60}$$

Градиент целевой функции по выходному значению сети (61):

$$\frac{Q}{y_i} = -\frac{d_i}{y_i} + \frac{1 - d_i}{1 - y_i} \tag{61}$$

С учетом производной сигмоидной функции, локальный градиент (ошибка) на выходном слое $\delta^{(out)}$ вычисляется как (62):

$$\delta^{(out)} = y_i - d_i \tag{62}$$

Корректировка весовых коэффициентов полносвязного слоя (63):

$$\frac{\delta Q}{\delta W_{ij}^{(dense)}} = \delta_i^{(out)} \cdot h_j \tag{63}$$

Для сверточных слоев ошибка распространяется в обратном направлении через операцию «полной свертки» (full convolution) транспонированной матрицы весов с матрицей ошибок следующего слоя. Корректировка весов фильтров вычисляется как свертка входов слоя с его градиентами (64):

$$\frac{Q}{W_j^{(l)}} = x^{(l-1)} \cdot \delta_j^{(l)} \tag{64}$$

Обновление весов на итерации m осуществляется по методу градиентного спуска (на практике используются адаптивные оптимизаторы, такие как Adam) (65):

$$W(m+1) = W(m) - \eta \cdot Q(W) \tag{65}$$

где η – гиперпараметр скорости обучения.

Инициализация весовых коэффициентов сверточных слоев производилась по методу He (He Initialization), что является стандартом для сетей с функцией активации ReLU, обеспечивая дисперсию, пропорциональную $\frac{2}{n_{in}}$ (где n_{in} – количество входов нейрона). Максимально допустимая ошибка обучения принималась равной 10^{-4}. Установленная величина представляет собой эмпирически обоснованный компромисс между требованиями к целевой точности классификации и вычислительной скоростью сходимости алгоритма.

Центральным элементом алгоритма принятия решения в разрабатываемой системе непрерывно-дискретной аутентификации является динамически вычисляемая функция доверия (рисунок 16). Необходимость её введения обусловлена тем, что мгновенные выходы нейросетевого классификатора могут содержать флуктуации, вызванные случайными аномалиями в движении манипулятора (ошибки позиционирования, внешние отвлечения пользователя). Опора исключительно на мгновенные значения неизбежно приведет к высокому уровню ложных отказов в доступе (FRR).

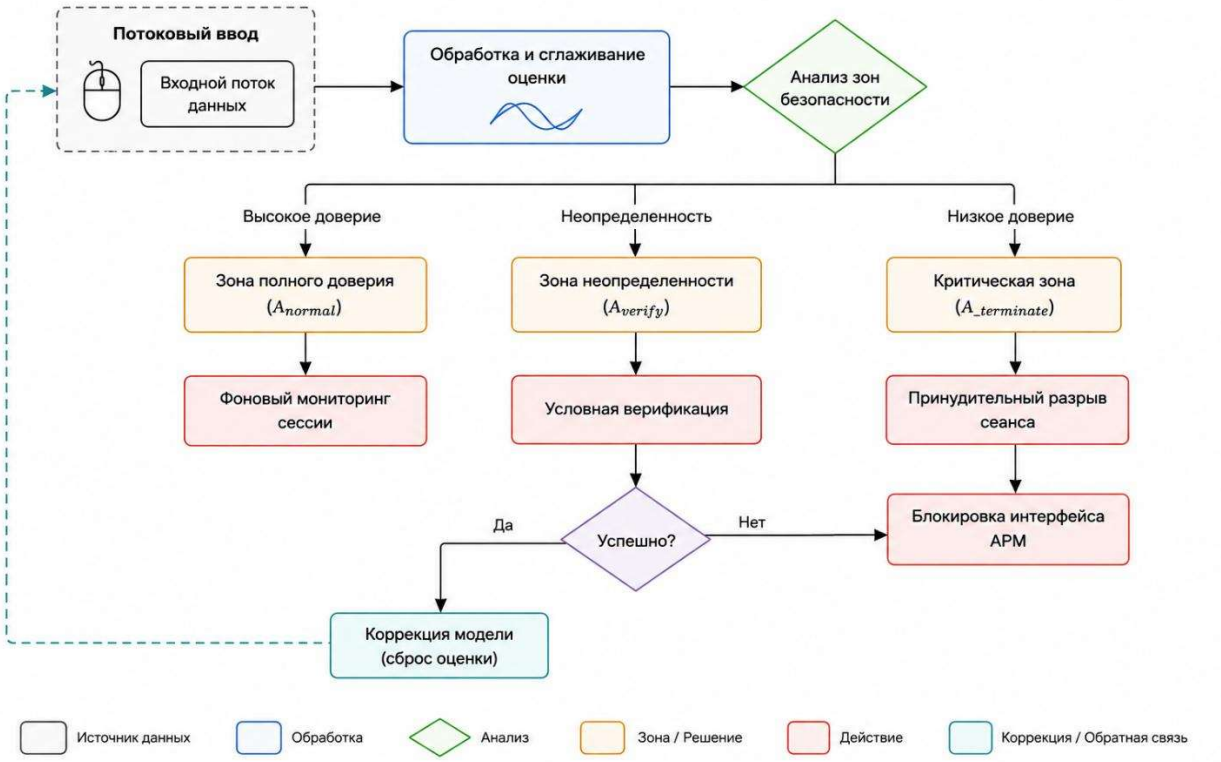

Рисунок 16 – Алгоритм функционирования процесса непрерывного адаптивного контроля доступа на основе рекуррентного расчета функции доверия

Функция доверия TR_k представляет собой скалярную величину, определяющую текущий уровень легитимности сеанса связи на шаге k. Для обеспечения плавности изменения уровня доверия и учета исторического контекста сессии, функция вычисляется на основе экспоненциального скользящего среднего (Exponential Moving Average, EMA) от выходных вероятностей нейросети.

В динамическом режиме рекуррентное вычисление функции доверия для k-го временного окна (или дискретного события) описывается выражением (66):

$$TR_k = \alpha \cdot p_k + (1 - \alpha) \cdot TR_{k-1}, \quad (66)$$

где $p_k \in [0;1]$ – апостериорная вероятность легитимности текущего паттерна, формируемая на выходе логистической функции активации полносвязного слоя нейросети на k-м шаге; TR_{k-1} – значение функции доверия на предыдущем шаге мониторинга; $\alpha \in [0;1]$ – коэффициент адаптации (параметр экспоненциального сглаживания), определяющий весовой вклад новых измерений по отношению к накопленной ретроспективной истории сеанса.

Начальное значение функции при успешном прохождении процедуры первичной дискретной аутентификации инициализируется как $TR_0 = 1$.

Поскольку область значений функции доверия строго ограничена интервалом $[0;1]$, для управления состояниями защищаемого контура вводятся два пороговых значения: порог подтверждения (θ_{auth}) и порог блокировки (θ_{block}), удовлетворяющие условию: $0 < \theta_{block} < \theta_{auth} < 1$.

Политика безопасности и соответствующий алгоритм реагирования системы формализуются с помощью следующих граничных условий:

1) Зона устойчивого доверия ($TR_k > \theta_{auth}$): система функционирует в штатном фоновом режиме. Текущие действия субъекта верифицируются как легитимные, управляющие воздействия не генерируются.

2) Зона неопределенности ($\theta_{block} \leq TR_k < \theta_{auth}$): уровень доверия снижается вследствие кумулятивного накопления аномальных поведенческих признаков. Мониторинг переходит в режим повышенной готовности: инициируется латентная или явная дискретная проверка (например, запрос контекстной капчи или повторный ввод учетных данных). Данное состояние позволяет системе адаптироваться к флуктуациям психофизиологического состояния легитимного пользователя без принудительной деградации сеанса.

3) Критическая зона ($TR_k < \theta_{block}$): текущий поведенческий профиль демонстрирует критическое расхождение с эталоном, что классифицируется как несанкционированная подмена пользователя (Session Hijacking). Защитное действие включает в себя незамедлительную терминацию сессии, блокировку интерфейса автоматизированного рабочего

места (АРМ) и генерацию уведомления в адрес службы информационной безопасности.

Значения коэффициента α и порогов $\theta_{auth}, \theta_{block}$ являются настраиваемыми гиперпараметрами. Их рациональный выбор позволяет оптимизировать баланс между уровнем защищенности распределенной системы (минимизация FAR) и критериями информационной эргономики (минимизация FRR) в зависимости от специфики и критичности защищаемого контура.

2.5 Предобработка биометрических признаков и обоснование среды имитационного моделирования постаутентификационных процессов

В соответствии с классификацией, предложенной в работе [153], регистрируемый поток телеметрии манипулятора типа «мышь» дифференцируется на три дискретных класса элементарных моторных актов: ММ (движение мыши), ПК (наведение и нажатие) и ДД (перетаскивание). ММ подразумевает перемещение курсора мыши между двумя точками на экране. ПК подразумевает наведение курсора и выполнение щелчка при нажатии одной из кнопок мыши. Наконец, ДД означает перетаскивание − движение, которое начинается при нажатии основной кнопки мыши и завершается при ее отпускании.

В исследовании данные о действиях мыши классифицируются по двум основным категориям: «Категория 1», представляющая движение мыши, и «Категория 2», включающая действия наведения и нажатия. Определение типа действия основывается на том, состоит ли предшествующее событие мыши из нажатия вниз и последующего нажатия вверх, что распознается как наведение и нажатие (ПК). Напротив, если предыдущее событие не соответствует этому шаблону, данные классифицируются как действие движения мыши (ММ).

Для наглядного представления на рисунке 17 показано поведение пользователей во время движения манипулятора, сопровождаемого

действиями наведения и нажатия. Движения нормированы относительно центра в окне браузера по шкалам X(-200;200) и Y(-10;10).

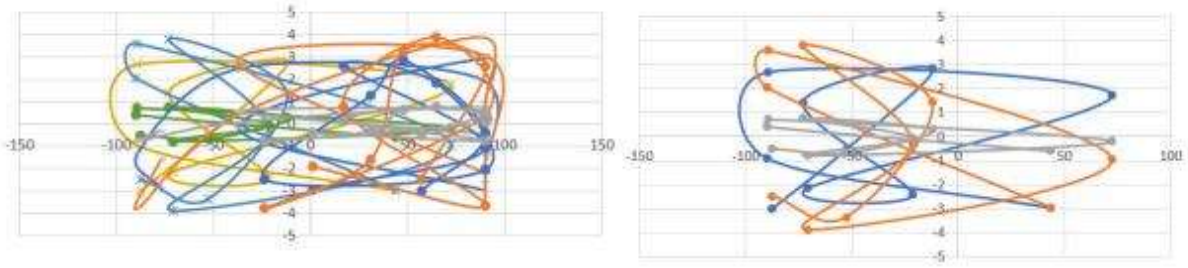

Рисунок 17 – (а) Поведение пользователя при движении манипулятора и действий по наведению курсора и щелчку. (б) Движение мыши, действия наведения курсора и щелчки манипулятора у трех пользователей.

Придерживаясь вышеупомянутой схемы предварительной обработки, мы можем преодолеть эти проблемы и создать полный набор данных, пригодный для последующего анализа [74]. Этот тщательно обработанный набор данных служит основой для применения передовых аналитических методов, способствуя получению точных выводов и принятию обоснованных решений.

Для объективной оценки эффективности предложенной архитектуры данных и обученных моделей глубокого обучения требуется их верификация в средах, имитирующих реальное удаленное взаимодействие.

Важнейшим аспектом верификации разработанной архитектуры сверточной нейронной сети является подтверждение её инвариантности к переменным факторам эксплуатации, которые в реальных условиях удаленного взаимодействия неизбежно вносят искажения в биометрический поток. Речь идет о необходимости раздельного измерения и анализа устойчивости модели к смене аппаратного обеспечения (разрешение сенсора мыши, частота опроса), времени суток и физиологическому состоянию пользователя (усталость, эмоциональный фон). Без учета этих факторов

точность аутентификации может существенно деградировать при переходе от лабораторных данных к промышленной эксплуатации.

Обоснование необходимости таких измерений диктуется природой поведенческой биометрии: в отличие от статических признаков, динамика манипулятора подвержена краткосрочным флуктуациям. Применение свёрточных нейронных сетей (CNN) позволяет осуществлять извлечение глубоких структурных паттернов движений, теоретически обладающих свойством стабильности. Для подтверждения данной гипотезы в рамках имитационного моделирования требуется проведение стресс-тестирования модели. По результатам стресс-тестирования формируется количественная оценка «запаса прочности» алгоритма, обеспечивающая верификацию того, что система идентифицирует именно индивидуальный стиль управления, а не специфические характеристики конкретного устройства ввода или временное состояние пользователя [64; 66].

Современные технологии моделирования и симуляции занимают центральное место в исследованиях, направленных на повышение эффективности сложных систем различных классов – от промышленных производственных процессов и сетевой инфраструктуры до распределённых вычислительных сред. Анализ существующих инструментов показывает: многие из них не отвечают требованиям к разработке прототипов систем биометрической аутентификации. Основное ограничение – отсутствие встроенных механизмов верификации, обеспечивающих проверку соответствия модели фактическим процессам. Моделируемые решения проявляют эффективность в контролируемых условиях, однако не гарантируют корректность при реальной эксплуатации [68; 71; 72; 73; 82].

Существенным барьером на пути адаптации выпускников к условиям реального производства является разрыв между дидактическими свойствами учебных симуляторов и архитектурой корпоративного ПО. Если образовательные среды, как правило, оперируют упрощенными цифровыми моделями для решения узкоспециализированных задач, то современный

промышленный контур требует применения крупномасштабных интегрированных платформ [68; 71; 72; 73; 82]. Отсутствие преемственности между этими классами систем приводит к девальвации сформированных у студентов базовых умений и вынуждает предприятия инвестировать в ресурсоемкое переобучение молодых специалистов.

Особое внимание следует уделить точности моделирования. Для киберфизических систем, распределённых сетей и облачных платформ даже незначительные расхождения между моделью и реальными параметрами могут приводить к критическим последствиям: перегрузке сети, уязвимостям в системе безопасности или неоптимальному распределению вычислительных ресурсов. При этом большинство существующих решений ограничивается построением логических схем и сетевых топологий, не предоставляя инструментов для проверки соответствия смоделированных процессов реальному поведению системы [71; 72; 82].

Проблему усугубляет фрагментация программных средств: каждое из них решает локальные задачи (мониторинг, анализ трафика, выявление уязвимостей), однако отсутствует универсальная интегрированная платформа, объединяющая моделирование, администрирование и верификацию. В результате организации вынуждены использовать множество разрозненных инструментов, что усложняет интеграцию, повышает стоимость сопровождения и снижает эффективность цифровой трансформации. Образовательные учреждения, в свою очередь, опираются на доступные симуляторы, которые не поддерживают интеграцию с корпоративными ИТ-инфраструктурами и промышленными объектами. Это приводит к несоответствию компетенций выпускников реальным требованиям рынка [78].

Дополнительные трудности связаны с совместимостью. Различные программные решения опираются на собственные протоколы и архитектурные подходы, что затрудняет формирование единой цифровой экосистемы. Примером может служить несовместимость систем мониторинга

одной компании с аналитическими платформами другой, что вынуждает организации разрабатывать промежуточное программное обеспечение и постоянно адаптировать инфраструктуру [68; 71; 72; 78].

В современных условиях одной из ключевых задач становится создание универсального инструмента, объединяющего моделирование, администрирование, верификацию и мониторинг. Такой инструмент должен быть применим как в образовательных, так и в корпоративных средах, обеспечивать возможность проектирования виртуальных топологий и их проверки на соответствие реальным системам, интеграцию с существующими инфраструктурами и высокий уровень безопасности [68; 71; 72; 78; 82]. Ключевым фактором является автоматизация: инструмент должен не только отображать структуру и параметры модели, но и предлагать конфигурации, повышающие эффективность, выявлять потенциальные проблемы и минимизировать трудоёмкость процесса.

Современные программные средства моделирования характеризуются рядом принципиальных ограничений: отсутствием встроенных механизмов верификации; несоответствием между учебными и промышленными решениями; недостаточной точностью симуляции; наличием проблем совместимости. Преодоление указанных ограничений предполагает разработку комплексных платформ нового поколения, объединяющих моделирование, эксплуатацию, анализ и управление в единую экосистему, отвечающую требованиям цифровой трансформации.

2.6 Краткие выводы

Анализ ключевых принципов и критериев аутентификации позволил формализовать модель биометрической аутентификации. Процесс её построения включает ряд этапов: выбор релевантных биометрических характеристик, обеспечение требуемого уровня точности и надёжности, учёт эргономических требований и требований к защите персональных данных.

Особое внимание уделено вопросам обработки сигналов от устройств ввода – этапам преобразования, фильтрации и нормализации.

В работе рассмотрен процесс аутентификации личности на основе методов цифровой обработки сигналов, генерируемых манипулятором. Показано, каким образом данные, получаемые от устройства ввода, подвергаются преобразованию и используются для построения профиля пользователя. Подробно обсуждаются алгоритмы точного распознавания и сопоставления биометрических характеристик.

Представлена модель системы биометрической аутентификации, включающая архитектуру, ключевые компоненты и принципы взаимодействия между ними. Сделан акцент на её функциональности, масштабируемости и устойчивости к эксплуатационным рискам. Проанализирована структура алгоритма аутентификации, включающая последовательные этапы – от сбора данных до сравнения признаков с эталоном и принятия решения о подтверждении личности пользователя.

Во второй главе решена задача математического и алгоритмического моделирования информационных процессов непрерывно-дискретной биометрической аутентификации. Результаты данной главы легли в основу следующих публикаций автора:

- Уймин, А. Г. Применение алгоритма Дугласа-Пеккера в вопросах онлайн-аутентификации инструментов удалённой работы при подготовке специалистов укрупнённой группы специальностей 10.00.00 "Информационная безопасность" / А. Г. Уймин, В. С. Греков // Электронные библиотеки. – 2024. – Т. 27, № 4. – С. 679-694. – DOI 10.26907/1562-5419-2024-27-4-679-694. – EDN QYROFU.
- Уймин, А. Г. Моделирование телекоммуникационной сети средствами сетевых инструментов Linux: инструменты создания цифровых двойников / А. Г. Уймин, О. Р. Никитин // I-methods. – 2023. – Т. 15, № 2. – EDN NFJDVH.

- Уймин, А. Г. Оценка безопасности wine с использованием методологии stride: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164-170. – DOI 10.37882/2223-2982.2023.6-2.40. – EDN HYCKNP.
- Уймин, А. Г. Предобработка данных манипулятора "мышь" для использования в анализе поведенческой биометрии / А. Г. Уймин // Научно-технический вестник Поволжья. – 2022. – № 7. – С. 94-97. – EDN NJNUTH.
- Formalization of Computational Process Using Informative Coloring of User Resource Requests in a Local Area Network Node / O. Demidenko, V. N. Kulinchenko, A. I. Kucharau, Y. Nikityuk, D. S. Sych, A. G. Uymin // 9th International Conference on Information, Control, and Communication Technologies (ICCT), Gomel, Belarus, 2025, pp. 1-4, DOI 10.1109/ICCT67028.2025.11427516.
- Uymin, A. G. Applying the Douglas–Peucker Algorithm in Online Authentication of Remote Work Tools for Specialist Training in 10.00.00 “Information Security” Integrated Group of Specialties / A. G. Uymin, V. S. Grekov // Automatic Documentation and Mathematical Linguistics. – 2024. – Vol. 58, No. S4. – P. S265-S268. – DOI 10.3103/S0005105525700323. – EDN CJXWPX.
- Уймин, А. Г. Концепция экспериментального анализа уязвимостей процесса аутентификации через манипуляции с манипулятором «мышь» / А. Г. Уймин // Актуальные проблемы защиты информации: современность и перспективы : Материалы II Научно-практической конференции, Москва, 09–10 апреля 2024 года. – Москва: федеральное государственное бюджетное образовательное учреждение высшего образования "Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)", 2025. – С. 29-36. – EDN PQHHWE.

- Уймин, А. Г. Система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши / А. Г. Уймин // Проблемы управления безопасностью сложных систем : Материалы XXXII международной конференции, посвященной памяти Владимира Васильевича Кульбы, Заслуженного деятеля науки РФ, д-ра техн. наук, профессора, Москва, 13 ноября 2024 года. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2024. – С. 273-278. – EDN JCZCJI.

В рамках главы теоретически обосновано и полностью раскрыто второе положение, выносимое на защиту – разработана многоуровневая модель информационного процесса удалённого доступа. Кроме того, заложен алгоритмический фундамент метода непрерывно-дискретной биометрической аутентификации, что является концептуальной основой для первого положения.

ГЛАВА 3 ПРОГРАММНАЯ РЕАЛИЗАЦИЯ И ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА СИСТЕМЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

3.1 Требования к программной системе и её архитектурное построение

Данная глава посвящена разработке прототипа системы биометрической аутентификации, описанию её архитектуры и анализу экспериментальных результатов. Реализация осуществлялась в соответствии с требованиями и метриками, сформулированными в главе 2, а также с учётом принципов функциональности, надёжности и масштабируемости. Представлены результаты апробации разработанного решения и проведён сравнительный анализ с существующими аналогами.

Система БИ, требования к которой были сформулированы ранее, реализована в виде программно-аппаратного комплекса. Архитектура системы включает три ключевых уровня: клиентский, серверный и прикладной.

Клиентский уровень обеспечивает взаимодействие пользователя с системой. Основой клиентского устройства является персональный компьютер, выполняющий функции клиентской части программного комплекса и обрабатывающий пользовательские запросы. В качестве устройств ввода используются манипулятор «мышь» (основной источник биометрических данных), а также клавиатура, применяемая для ввода текстовой информации и управляющих команд. Отображение интерфейса и аналитических данных осуществляется посредством монитора, который выполняет функции устройства вывода.

Серверный уровень отвечает за централизованную обработку, хранение и управление данными. В его состав входят сервер баз данных, обеспечивающий хранение структурированных записей и эталонных профилей пользователей, сервер приложений, реализующий бизнес-логику и

обработку поступающих запросов, а также сетевые интерфейсы, поддерживающие взаимодействие между клиентскими и серверными компонентами.

Программный комплекс реализует прикладную функциональность системы БИ и состоит из клиентской и серверной частей. Клиентская часть включает графический пользовательский интерфейс (GUI), предоставляющий пользователю доступ к функциям системы и визуализацию результатов анализа, модуль взаимодействия с сервером, обеспечивающий передачу данных по сети, а также локальные инструменты обработки, выполняющие кэширование, предварительную фильтрацию и агрегацию информации. Серверная часть включает модуль обработки запросов, агрегирующий поступающие данные и формирующий отчёты, модуль управления базами данных, осуществляющий извлечение, обновление и удаление информации, модуль безопасности, отвечающий за аутентификацию, авторизацию и контроль доступа, а также интерфейсы интеграции (API), которые обеспечивают взаимодействие с внешними системами.

Таким образом, реализованный прототип системы БИ представляет собой многоуровневую архитектуру, сочетающую аппаратные и программные компоненты, обеспечивающую сбор, обработку, хранение и анализ биометрических данных. В последующих разделах главы будут рассмотрены особенности реализации отдельных модулей, результаты экспериментальной оценки эффективности прототипа и его сравнительный анализ с существующими решениями.

3.2 Реализация прототипа системы на базе платформы Remote Topology

Для реализации прототипа системы биометрической аутентификации была использована исследовательская платформа RemoteTopology, изначально разработанная автором для организации и проведения учебных

мероприятий и соревнований в области операционных систем и сетевых технологий. [68; 71; 72; 73; 78; 182; 183].

Приложение RemoteTopology представляет собой комплексную систему для мониторинга и управления распределёнными вычислительными системами. Оно предназначено для контроля состояния и производительности сетевых устройств и сервисов. Основная задача приложения заключается в повышении эффективности процессов мониторинга и управления сетевой инфраструктурой, включая серверы, маршрутизаторы, коммутаторы и другие сетевые компоненты. RemoteTopology предоставляет пользователям инструменты удалённого доступа для диагностики и администрирования, что повышает оперативность реагирования на возникающие проблемы. Важной функцией системы является обеспечение сетевой безопасности за счёт управления доступом и мониторинга уязвимостей.

Платформа RemoteTopology разработана в ответ на потребность в универсальном инструментальном средстве для решения задач мониторинга, управления и обучения в области операционных систем и сетевых технологий. Современные информационные системы предъявляют высокие требования к уровню автоматизации администрирования, особенно в условиях распределённой инфраструктуры, в которой мониторинг и управление вручную не обеспечивают требуемой эффективности. Платформа RemoteTopology решает указанную проблему посредством применения централизованных инструментальных средств контроля, диагностики и анализа сетевой инфраструктуры [41].

Дополнительной предпосылкой создания платформы является её образовательная направленность. Современные учебные заведения и профессиональные курсы по сетевому администрированию нуждаются в тренажёрах и симуляторах, обеспечивающих условия, приближённые к реальной эксплуатации. Платформа RemoteTopology обеспечивает указанную среду: студенты и специалисты получают возможность работы с виртуальными и физическими устройствами, моделирования топологий,

отработки сценариев администрирования. Таким образом, платформа удовлетворяет ряду ключевых потребностей: обеспечение безопасности, удобство администрирования, повышение квалификации специалистов [79].

Приложение реализует ряд ключевых функций – мониторинг состояния сети, диагностику сетевых устройств, управление топологией сети, удалённое администрирование. Функция мониторинга отображает в реальном времени параметры всех сетевых узлов – серверов, коммутаторов, маршрутизаторов. Система отслеживает загрузку процессора, использование памяти, сетевой трафик, активность дисковой системы. Для контроля состояния инфраструктуры предусмотрена система уведомлений о критических событиях – аппаратных сбоях, перегрузке сетевых каналов. Реализован механизм сбора исторических данных с возможностью анализа: выявляются потенциальные проблемы, прогнозируется развитие сети.

Управление топологией сети – одна из ключевых возможностей RemoteTopology. Приложение предлагает инструменты автоматического построения сетевой карты с актуальными данными о подключённых устройствах и их соединениях. Пользователи в ручном режиме меняют структуру сети, добавляют новые узлы и настраивают параметры взаимодействия. Встроенные средства визуализации наглядно представляют топологию, упрощают контроль за состоянием сети и повышает эффективность администрирования. Предусмотрены механизмы автоматического обнаружения новых устройств с их последующим включением в топологическую модель.

Функция удалённого управления обеспечивает администраторам возможность настройки и обслуживания сетевых узлов без необходимости физического доступа к оборудованию. Платформа RemoteTopology поддерживает удалённые подключения к устройствам через виртуальные консоли, предоставляет средства конфигурирования сетевых параметров, обновления прошивок и управления политиками безопасности. Централизованное администрирование обеспечивает оперативное

реагирование на инциденты, сокращение времени простоя сети, снижение объёма ручных операций администратора. Для защиты передаваемых данных приложение задействует многоуровневую систему безопасности, включающую механизмы аутентификации и авторизации. Поддерживается двухфакторная аутентификация; передача данных осуществляется с применением современных алгоритмов шифрования. Существенным элементом защиты является ведение журналов операций: история изменений подвергается анализу, при этом обеспечивается выявление несанкционированных попыток доступа или модификации конфигурации.

RemoteTopology интегрируется с внешними сервисами и платформами обработки данных и мониторинга. Приложение поддерживает стандартные сетевые протоколы – SNMP, NetFlow, Syslog, и это обеспечивает совместимость с существующей инфраструктурой. Предоставляется API для автоматизации администрирования и взаимодействия с другими программными продуктами.

Архитектура RemoteTopology состоит из серверной части, клиентских интерфейсов, подсистем взаимодействия. Сервер обрабатывает запросы, хранит данные, выполняет аналитические операции. В базе данных хранится информация о сети, её текущем состоянии, истории событий. Доступ к системе обеспечивают интерфейсы: веб-приложение, мобильный клиент, консольная утилита для опытных администраторов. Модули взаимодействия собирают данные с устройств и передают их в центральную систему для дальнейшего анализа.

RemoteTopology с самого начала разрабатывалась как модульная система, так как такая архитектура обладает рядом ключевых преимуществ:

1. Гибкость и масштабируемость – новые функции добавляются без переписывания всей платформы. Это важно в сетевом администрировании, где требования быстро меняются.

2. Разделение функциональности – каждый модуль отвечает за свою область, что даёт возможность разрабатывать, тестировать и обновлять их

независимо. Модуль мониторинга обновляется без затрагивания модуля администрирования.

3. Повышенная отказоустойчивость – сбой в одном модуле не выводит из строя всю систему. Временный выход из строя модуля визуализации не повлияет на сбор и анализ сетевых данных.

4. Удобство кастомизации – пользователи включают или отключают модули в зависимости от своих задач. Это важно для образовательных программ, где набор инструментов варьируется в зависимости от курса или чемпионата.

Функциональный состав платформы подтверждён свидетельствами о регистрации соответствующих программных модулей [182; 183; 187; 188; 189].

В составе платформы RemoteTopology выделены ключевые модули, каждому из которых соответствует определённый функциональный круг задач:

1) Модуль авторизации RemoteTopology реализует одну из критически значимых задач: обеспечение регистрации и аутентификации пользователей, гарантирование информационной безопасности и контроля доступа в системе. Автоматическая генерация ключей доступа обеспечивает снижение вероятности компрометации данных за счёт исключения влияния человеческого фактора на этапе формирования паролей. На стадии регистрации пользователь вводит адрес электронной почты, фамилию, имя и отчество, а также формирует уникальный пароль, что обеспечивает системе возможность однозначной идентификации каждого участника.

Существенной особенностью данного модуля является его интеграция с остальными компонентами платформы RemoteTopology. Авторизация требуется не только для доступа к интерфейсу управления, но и для функционирования различных подсистем: симулятора, инструментов администрирования, топологических схем. Таким образом формируется единая экосистема, в которой пользователь обеспечивает бесшовный переход

между функциональными модулями с использованием единых учётных данных. Помимо стандартного ввода логина и пароля, модуль поддерживает дополнительные механизмы безопасности: двухфакторную аутентификацию и привязку к биометрическим данным (при условии установки соответствующего браузерного расширения). Указанные меры обеспечивают защиту системы от несанкционированного доступа и повышение уровня кибербезопасности. [189; 186]

2) Модуль RemoteTopology-Администрирование обеспечивает администраторам возможность дистанционного управления сетевыми устройствами – как физическими, так и виртуальными.

В рамках функционирования модуля администраторы осуществляют создание новых учётных записей, редактирование их параметров, распределение пользователей по группам, привязку к определённым чемпионатам или образовательным программам. Указанный модуль обладает особой ценностью для образовательных организаций и корпоративных сред, в которых требуется централизованное управление доступом и контроль образовательного или соревновательного процесса.

Поддерживается массовый импорт пользователей и стендов посредством файлов формата CSV, что обеспечивает упрощение работы при развёртывании системы в крупных инфраструктурах.

Интерфейс RemoteTopology-Администрирование спроектирован с учётом требований к удобству и интуитивности навигации: обеспечивается оперативный доступ ко всем ключевым функциям, а администраторам предоставляется возможность эффективного управления топологиями, пользователями и сетевыми ресурсами. Сфера применения модуля не ограничена образовательными целями – он применим для повседневного администрирования реальных сетей, обеспечивая гибкость и автоматизацию соответствующих процессов. [187]

3) Программный модуль-тренажёр для подготовки к демонстрационному экзамену. Указанный модуль представляет собой

тренажёр для обучения студентов среднего профессионального образования по специальности «Системное и сетевое администрирование». Он обеспечивает подготовку к экзаменам в условиях, максимально приближенных к реальным. Программа совместима с ПЭВМ стандарта IBM PC, функционирует под управлением операционной системы Windows x32/64. [184].

В состав RemoteTopology входит симулятор-тренажёр для подготовки студентов к демонстрационному экзамену по специальности «Системное и сетевое администрирование». Модуль формирует виртуальную среду, максимально приближенную к реальным условиям эксплуатации сетевых систем. Пользователь выполняет стандартные операции по настройке сетевого оборудования, диагностике и устранению неисправностей – таким образом закрепляются теоретические знания и приобретается практический опыт. Интерфейс тренажёра интуитивно понятен; в его функционал входят выполнение сценарных заданий, моделирование сетевых топологий, работа с виртуальными устройствами – полезный инструмент для образовательных учреждений и тренировочных программ.

Возможности тренажёра не сводятся только к образовательным целям. Платформа RemoteTopology обеспечивает интеграцию модуля с реальной сетевой инфраструктурой – подключение к физическим устройствам через сетевой интерфейс. Инструмент применяется не только в симуляционном режиме, но и для практического администрирования существующих сетей. Гибкость даёт возможность использовать систему в корпоративной среде для тестирования конфигураций, анализа сетевых проблем, подготовки специалистов к работе с реальными сетевыми объектами. Платформа поддерживает работу с различными протоколами взаимодействия, и это обеспечивает совместимость с распространёнными типами сетевого оборудования.

После подключения к реальной сети все функции RemoteTopology сохраняются доступными – мониторинг, управление, анализ сетевого трафика.

Администраторы действуют через единый интерфейс, получают актуальную информацию о состоянии системы, настраивают оборудование, устраняют сбои. RemoteTopology – это не только удобный образовательный инструмент, но и мощное средство управления сетевой инфраструктурой; область его применения простирается от обучения студентов до профессиональной эксплуатации в крупных организациях.

4) Модуль RemoteTopology-Интерфейс пользователя представляет собой визуальный компонент системы, обеспечивающий удобство взаимодействия с функционалом платформы RemoteTopology. Основным элементом интерфейса является выпадающее меню, отображающее доступные чемпионаты и соответствующие им модули.

В зависимости от текущего задания или сценария соревнования пользователь выбирает требуемый модуль, после чего система формирует запрос к программно-аппаратной части, возвращающей соответствующую сетевую топологию. Процесс навигации построен на принципах логической связности и интуитивности, что обеспечивает удобство ориентации пользователя в системе. Загружаемая в интерфейсе топология содержит полную информацию о сетевой инфраструктуре. Визуализация включает изображения сетевых устройств (серверов, коммутаторов, маршрутизаторов, рабочих станций), их наименования, а также данные о связях между элементами сети.

Модуль RemoteTopology-Интерфейс пользователя выполняет существенную роль в обеспечении удобства взаимодействия с системой – как для администраторов, так и для обучающихся. Указанный модуль обеспечивает упрощение работы с топологиями, ускорение доступа к функциональным модулям, наглядное представление сетевой структуры. В сочетании с другими модулями системы интерфейс формирует целостную рабочую среду, пригодную для решения задач образовательного характера, проведения соревнований и профессионального администрирования реальных сетей. [188]

5) Клиент-серверное браузерное расширение RemoteTopology представляет собой специализированный модуль, предназначенный для повышения уровня безопасности системы посредством механизма биометрической аутентификации. В отличие от традиционных методов аутентификации (логин и пароль) данный компонент осуществляет анализ поведения пользователя и фиксацию его уникальных характеристик. Указанный подход обеспечивает повышение уровня защиты системы и минимизацию вероятности несанкционированного доступа.

Принцип функционирования расширения заключается в сборе и обработке биометрических данных, формируемых в процессе взаимодействия пользователя с интерфейсом. К параметрам анализа относятся: характеристики движения мыши, ритм и скорость набора текста, частота и последовательность нажатий клавиш. На основе указанных данных формируется уникальный профиль поведения пользователя, выступающий в качестве дополнительного фактора аутентификации. При обнаружении системой отклонений от типового поведения инициируется повторная аутентификация либо блокировка доступа, что обеспечивает предотвращение атак.

Архитектура разработанного решения RemoteTopology представляет собой трёхуровневую структуру, обеспечивающую организацию информационного процесса непрерывной биометрической аутентификации в распределённой вычислительной среде (рисунок 18). Клиентская часть включает браузерное расширение RT Extensions с интегрированными модулями Hook Manager (на базе pyHook/Windows API) и Connection Manager, обеспечивающими перехват и регистрацию событий манипулятора с шагом дискретизации 0,5 с в формате CSV-лога. Локальный модуль предобработки реализует алгоритм Дугласа-Пекера для упрощения траектории и фоновый инференс CNN-классификатора с интегральной утилизацией ресурсов CPU и RAM не более в заданных пределах. Структурная схема решения RemoteTopology показана на рисунке N

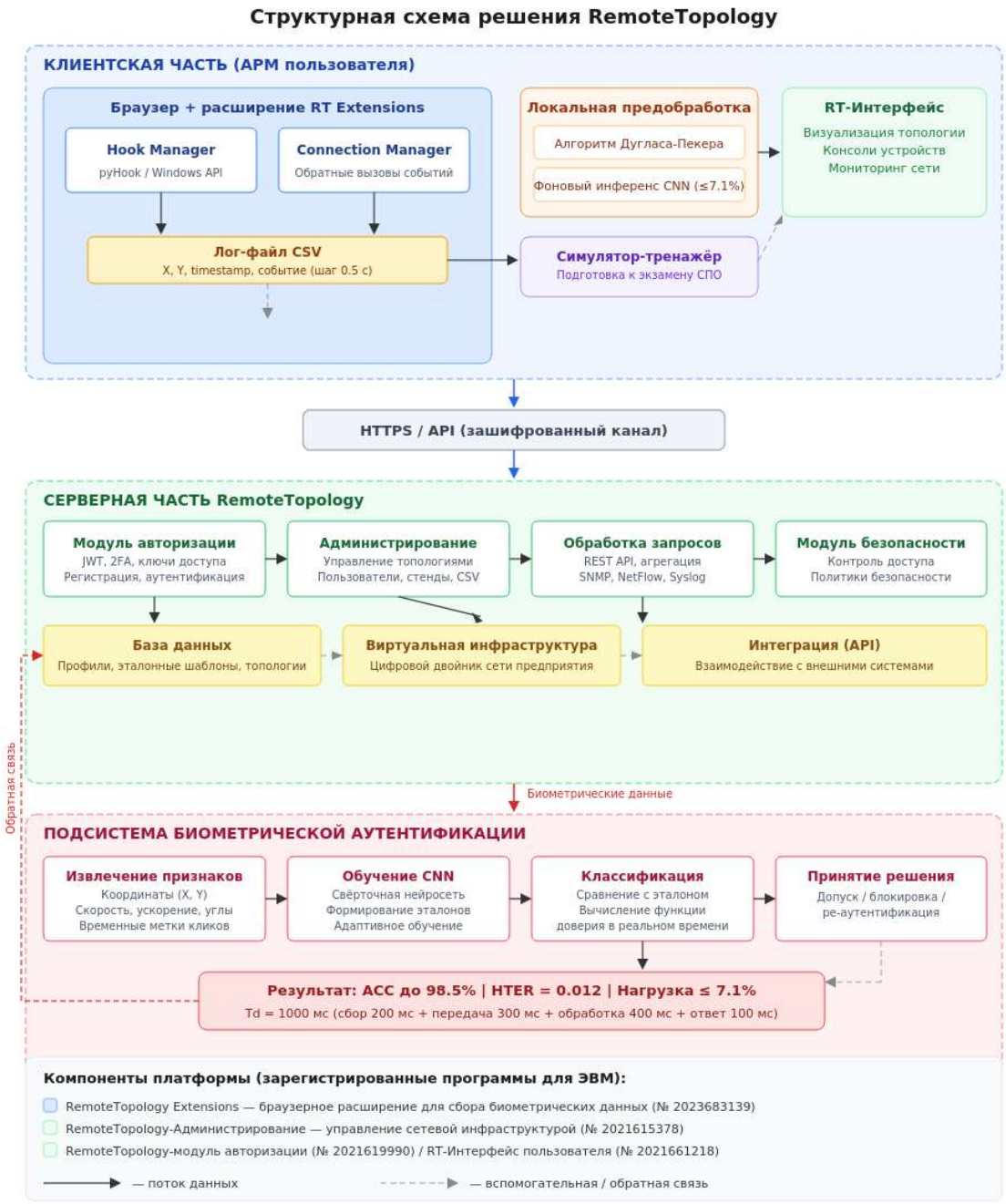

Рисунок 18 – Структурная схема решения RemoteTopology

Серверная часть содержит модуль авторизации (JWT, 2FA), модуль администрирования топологиями и пользователями, подсистему обработки запросов (REST API, SNMP, NetFlow), базу данных эталонных поведенческих шаблонов и модуль управления виртуальной сетевой инфраструктурой (цифровой двойник). Подсистема биометрической аутентификации реализует последовательное извлечение пространственно-временных признаков,

обучение свёрточной нейронной сети и принятие решения о допуске, ре-аутентификации или блокировке сеанса на основе динамически вычисляемой функции доверия TR(k).

Расширение функционирует в клиент-серверном режиме: обработка данных и их защищённое хранение осуществляются централизованно. Передача информации производится по защищённым каналам, что исключает возможность перехвата и подмены. Интеграция с другими модулями платформы RemoteTopology обеспечивает биометрической аутентификации статус важного элемента общей системы безопасности: идентификация пользователей осуществляется на основе поведенческих характеристик, что обеспечивает снижение риска компрометации учётных записей. Указанное решение одновременно выступает в качестве инструмента повышения безопасности и средства автоматического контроля доступа в распределённых вычислительных средах. [186].

Для обеспечения взаимодействия операционной системы с RemoteTopology была проведена дополнительная разработка модуля сбора данных. Модуль обладает обширным набором возможностей для сбора параметров, собираемых на основе движений компьютерной мыши. Параметры включают в себя не только данные, связанные с траекторией движения мыши, но и периодическую регистрацию нажатий пользователя в контролируемом цифровом пространстве. В основе модуля находится инструмент pyHook[13], предоставляющий необходимый функционал для сбора данных.

Стандартные средства ОС, применяемые в эксперименте:

[13] https://pypi.org/project/pyHook/

1) Использование Windows Hooking API[14] (Application Programming Interface) для взаимодействия с компьютерной мышью на уровне операционной системы.

2) Компоненты Hook Manager и Connection Manager для управления и сбора событий манипулятора. Hook Manager отвечал за запись событий, а Connection Manager облегчал их сбор посредством обратных вызовов. API выступает в качестве канала, обеспечивающего взаимодействие с базовой системой путем предоставления набора готовых функций, методов и процедур. По сути, Hook Manager выступает в качестве основы для регистрации всего спектра событий манипулятора.

Реализованный аппаратно-программный комплекс позволяет с заданной периодичностью фиксировать и записывать события в обновляющийся с той же периодичностью лог-файл, сохраняемый в формате CSV. В рамках исследования в качестве шага фиксации выступало время в 0.5 секунд, поскольку данное значение обеспечивает баланс между точностью мониторинга и нагрузкой на систему[15].

Процесс сбора данных осуществлялся на эталонном персональном компьютере, на котором было установлено программное обеспечение для перехвата действий мыши.

Зарегистрированное программное обеспечение приведено в Приложении А.

3.3 Методика и условия проведения экспериментальных исследований

Эксперимент проходил по определенной схеме, которую можно кратко описать следующим образом:

[14] https://learn.microsoft.com/en-us/windows/win32/winmsg/hooks

[15] Соболев В. И. Характеристика латентных периодов и параметров вариабельности составных элементов простой зрительно-моторной реакции (электромиографическое исследование) //Физиология человека. – 2020. – Т. 46. – №. 4. – С. 30-43.

1) В качестве основы для эксперимента были выбраны проекты Asia-Pacific Best Practice Marathon (Марафон лучших практик Азиатско-Тихоокеанского региона), III Международный чемпионат Хабаровского края по стандартам WorldSkills и с участием стран ATR в дистанционном формате и чемпионат REASkills-2022.

2) Эксперимент был сосредоточен на компетенции «Сетевое и системное администрирование», участники были отобраны на основе их знаний в этой области, с учётом релевантности их опыта, степени профессионализма и мотивации.

3) Участникам была предоставлена свобода в определении их собственных рабочих мест. Ограничений на тип используемых устройств, их физическое размещение или факторы окружающей среды, такие как расположение мебели и освещение не предъявлялось. Однако минимальные требования к мебели, помещениям и техническому оборудованию были установлены на инфраструктурном листе компетенции.

4) Хабаровский краевой институт развития образования предоставил аппаратную базу, которая послужила физической и материально-технической инфраструктурой для проведения эксперимента.

5) В ходе эксперимента был собран набор данных, включающий 200 000 образцов движений манипулятора и 100 000 изображений действий наведения, сопровождаемых щелчками манипулятора. Данные были собраны в общей сложности у 400 участников чемпионатов.

6) Участники выполняли задания, используя интерфейс RemoteTopology (RT)[16]. Интерфейс состоял из топологии с графическими иконками, при нажатии на которые открывается доступ к устройству. Подключение производилось из разных точек мира, самая дальняя из которых

[16] Uymin A.G. (2022) Automatic marking of browser network traffic for analysis and classification using the example of the RemoteTopology platform. T-Comm, vol. 16, no.12, pp.17-22.

– Колумбия. Форма обеспечивала структурированную основу для выполнения заданий и фиксировала данные в ходе чемпионата.

7) На протяжении всего эксперимента участники выполняли широкий спектр действий, связанных с сетевым и системным администрированием. Участники сталкивались с сценариями и задачами, проверяющими их знания, навыки решения проблем и способность принимать решения. Разнообразный характер заданий позволил дать целостную оценку компетентности участников в этой области.

Сама экспериментальная среда была максимально близка к среде производственного процесса (рисунок 19). Ее функции и возможности соответствовали целям эксперимента, проводимого с помощью систем виртуализации и эмуляции [68; 71; 72; 73; 82].

Виртуальная сеть (цифровой двойник) реального предприятия построен на основе [68; 71; 72; 73; 82] с указанием результатов теста, описанных там же. Уровень безопасности системы оценен в [67]. Сетевая часть построена в соответствии с учётом результатов обзора [72; 73; 82] о средствах моделирования сетевой инфраструктуры. Акцент на практическом применении моделирования в образовательном процессе является ключевым для подготовки квалифицированных специалистов в данной области. Важность профессиональной подготовки с учетом стандартов «Worldskills Russia», освещенная, акцентирует внимание на необходимости современного и комплексного подхода в обучении специалистов и демонстрирует высокий уровень проработки экспериментальной среды (Уймин А.Г., 2021).

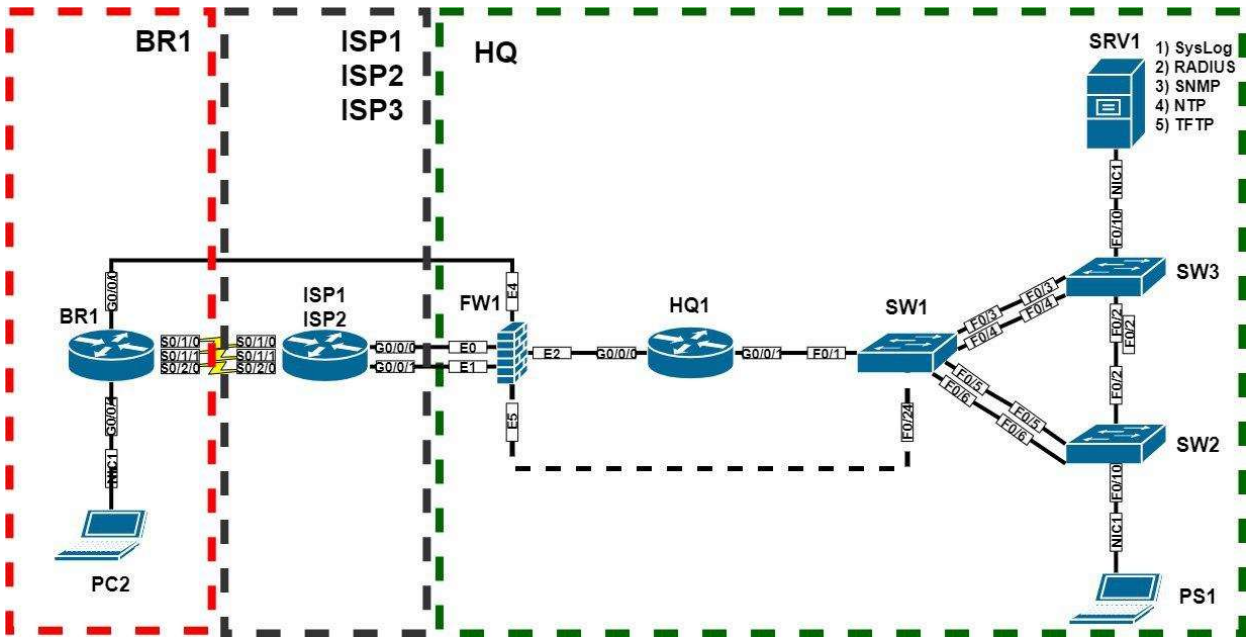

Рисунок 19 – RT при выполнении задания

После каждой сессии создается файл, содержащий строки данных, каждая из которых представляет собой записанное действие мыши. Эти события мыши включают в себя семь параметров, а именно: имя сообщения, идентификатор события, идентификатор сообщения, время, имя окна, ось X и ось Y (для разрешения 1024x768). Имя сообщения служит для описания характера самого события, например, направления движения (влево/вправо) или состояния нажатия (вниз/вверх).

В рамках исследования были проведены эксперименты для оценки эффективности различных методов машинного обучения:

- Классификаторы дерева решений (DT - Decision Trees),
- K-ближайших соседей (kNN – K-Nearest Neighbours),
- Случайный лес (RF - Random Forest) ,
- Свёрточная нейронная сеть (CNN - Convolutional Neural Network).

Наиболее широкое исследование с тестированием различных параметров модели касалось метода случайного леса ввиду зависимости его производительности от настройки гиперпараметров (fine-tuning) [54; 83]

С помощью библиотеки scikit-learn сравнение полученных моделей производилось на основе следующих метрик:

- Точность (ACC - Accuracy),
- Отзыв (Recall),
- Прецизионность (Precision),
- Оценка F1 (F1 Score).

Эксперименты включали две фазы: непрерывная аутентификация и обнаружение аномалий. Для каждой фазы классификаторы обучались и тестировались отдельно в трех сценариях:

1) Одно действие перемещения мыши.
2) Одно действие наведения и щелчка.
3) Набор действий перемещения мыши и наведения и щелчка.

Результаты оценивались с точки зрения:

- Точности классификации (ACC).
- Площади под кривой рабочих характеристик приемника (AUC).
- Частоты ложноположительных и ложноотрицательных срабатываний (FAR и FRR соответственно).
- Половины общей частоты ошибок (HTER).

Также оценивалась производительность систем обнаружения с помощью кривых ROC.

Работу прототипа модели для лучшего понимания можно разделить на следующие этапы (рисунок 20):

- Этап сбора данных: собираются исходные данные пользователей.
- Этап извлечения объектов: для извлечения объектов использовались библиотеки Pandas и numpy.
- Этап подготовки данных: на этапе обучения все данные пользователей были объединены и размещены в случайном порядке. Затем обучающий набор данных был разделен на две части: первая часть (80% данных) использовалась для обучения, а вторая часть (20% данных) использовалась для тестирования производительности модели. Для каждого эксперимента баланс обучающих наборов и оценочных наборов оставался неизменным, чтобы избежать смещения классификатора.

– Этап выбора классификатора: DT, RF, KNN и CNN были использованы, чтобы показать способность предлагаемой модели определять, был ли пользователь подлинным или злоумышленником по данным потока щелчков мыши пользователя.

– Этап обучающих данных: процесс обучения начался с считывания характеристик всех пользователей из обучающего набора данных и последующей загрузки их в четыре классификатора для обучения модели. Этот шаг был важным шагом, поскольку обучающие данные содержали само поведение пользователя и метку класса.

– Этап тестирования данных: после завершения этапа обучения модель была протестирована на новых данных, которые никогда не использовались для обучения, чтобы определить, был ли пользователь подлинным пользователем или злоумышленником.

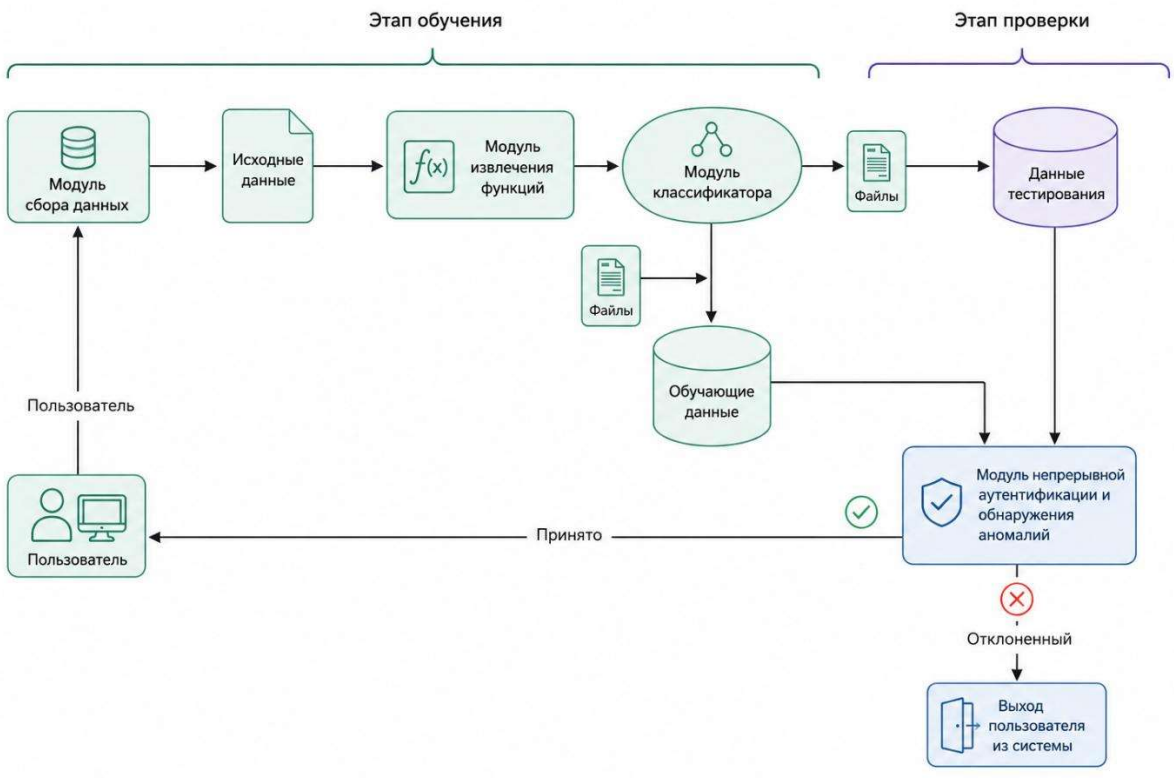

Рисунок 20 – Этапы работы прототипа модели

3.4 Сравнительный анализ нейросетевых архитектур и выбор модели классификатора

В контексте эффективности реализованной модели рассматривались показатели, выбор и обоснование которых приведено в главе 2.

Набор данных был разделен на две части: первая часть (80% данных) использовалась как описание подлинного пользователя для обучения моделей; вторая часть (20% данных) использовалась как действия пользователя, подлежащего аутентификации для тестирования производительности модели. На этом этапе были проведены эксперименты с использованием каждого из классификаторов (k-ближайшего соседа (KNN), дерева решений (DT), случайного леса (RF) и сверточной нейронной сети (CNN)) для всех пользователей с помощью одного действия движения мыши, одного действия наведения и щелчка, и набор действий по перемещению мыши и наведению, и щелчку. Сравнивая результаты, полученные во всех экспериментах, мы обнаружили, что сценарий 1 (действие с одним движением мыши) достиг наивысшей точности по сравнению со сценариями 2 и 3, со сценарием 1 KNN ACC: 97.0%, Recall: 95.25%, Precision: 97.0% и F1-score: 96.12%. Также было обнаружено, что модель CNN получила наивысшую точность, отзыв, точность и оценку F1: CNN ACC: 97.75%, отзыв: 95.25%, точность: 97% и оценка F1: 95.5%. Таблицы 5-7 иллюстрируют все достигнутые результаты.

Таблица 5 – Результаты непрерывной аутентификации для сценария 1: действие с одним движением мыши

Классификатор	KNN	DT	RF	CNN
Accuracy, %	96.5	94.5	94.0	97.0
Recall, %	92.75	92.5	93.25	95.25
Precision, %	95.0	92.0	95.0	97.0

F1-score, %	93.86	92.25	94.12	96.12

Таблица 6 – Результаты непрерывной аутентификации для сценария 2: действие с одним нажатием кнопки

Классификатор	KNN	DT	RF	CNN
Accuracy, %	81.75	82.25	95.0	94.25
Recall, %	89.25	81.75	94.25	94.50
Precision, %	80.0	80.50	92.75	93.25
F1-score, %	84.37	81.12	93.49	94.87

Таблица 7 – Результаты непрерывной аутентификации для сценария 3: набор действий по перемещению мыши, наведению и щелчку

Классификатор	KNN	DT	RF	CNN
Accuracy, %	94.75	93.25	96.25	96.0
Recall, %	90.25	89.25	96.25	93.5
Precision, %	92.25	92.75	92.5	91.25
F1-score, %	91.24	90.97	94.34	92.36

Основная идея системы обнаружения аномалий зависит от действий пользователя в системе. Когда система сравнивает текущее поведение пользователя с базой данных о поведении пользователя, система должна

разрешить пользователю продолжать работу, если в текущем поведении пользователя есть лишь небольшое отклонение; в противном случае система должна выйти из системы пользователя и потребовать статической аутентификации пользователя перед тем, как пользователь может продолжить работу. Для проверки осуществимости предложенных алгоритмов мы протестировали каждый из четырех классификаторов на трех сценариях: одно действие перемещения мыши (сценарий 1), одно действие наведения и щелчка (сценарий 2), а также комбинацию действий перемещения мыши и наведения с последующим щелчком (сценарий 3). Результаты продемонстрировали, что наивысшая точность была достигнута в сценарии 1 (перемещение мыши) с показателями: KNN ACC: 97.25%, DT ACC: 91.25%, RF ACC: 97.00% и CNN ACC: 98.50%. Среди всех классификаторов наилучшие результаты по точности, отзыву, точности предсказания и F1-оценке в сценарии 1 продемонстрировал классификатор CNN: ACC: 98.50%, Recall: 98.00%, Precision: 97.75%, F1-score: 97.87%. Подробные результаты представлены в таблицах 8–10.

Таблица 8 – Обнаружение аномалий приводит к сценарию 1: действие с одним движением мыши

Классификатор	KNN	DT	RF	CNN
Accuracy	97.25	91.25	97.00	98.50
Recall	96.75	89.75	95.25	98.00
Precision	93.00	89.75	96.00	97.75
F1-score	94.84	89.75	95.62	97.87

Таблица 9 – Обнаружение аномалий приводит к сценарию 2: действие с одним щелчком мыши

Классификатор	KNN	DT	RF	CNN
Accuracy	92.00	82.50	94.50	96.25

Recall	89.25	79.75	92.00	95.50
Precision	88.00	80.50	91.75	94.75
F1-score	88.62	80.12	91.87	95.12

Таблица 10 – Обнаружение аномалий приводит к сценарию 3: Набор движений мыши и действий по наведению и щелчку

Классификатор	KNN	DT	RF	CNN
Accuracy	88.50	73.00	91.00	94.50
Recall	86.25	71.25	90.00	93.75
Precision	85.75	70.75	91.50	93.50
F1-score	86.00	71.00	90.74	93.62

Результаты для сценариев 1 (одно движение мыши), 2 (наведение и щелчок мыши) и 3 (комбинация движения мыши и щелчка) были проанализированы с использованием показателей FAR, FRR, HTER и ROC-кривой. Получены соответствующие значения FAR, FRR и HTER. Во всех трех сценариях наименьшие значения FAR зафиксированы для классификатора CNN: сценарий 1 (0.0110), сценарий 2 (0.0100) и сценарий 3 (0.0080). Самые низкие значения FRR также наблюдаются у CNN: в сценарии 1 (0.0240), сценарии 2 (0.0200) и сценарии 3 (0.0160). Минимальные значения половины общей частоты ошибки (HTER) составили: сценарий 1 (CNN: 0.0175), сценарий 2 (CNN: 0.0150) и сценарий 3 (CNN: 0.0120). Подробные данные для показателей FAR, FRR и ERR представлены в таблицах 11–13.

Установлено, что для задачи непрерывной аутентификации (CA) классификатор CNN достиг наименьшего HTER, равного 0,0120, для сложного набора действий с перемещением мыши, наведением и щелчком (сценарий 3). Это подтверждает высокую способность сверточных сетей извлекать устойчивые пространственно-временные признаки из комплексных поведенческих паттернов.

Для всех трех сценариев, оцененных с использованием FAR, FRR, HTER и ROC-кривой, сценарий 1 (одно движение мыши) показал самые низкие значения HTER: KNN: 0.0800, DT: 0.1000, RF: 0.0650 и CNN: 0.0325. Полные результаты для всех сценариев приведены в таблицах 14–16. Итоговые данные демонстрируют, что для задачи аутентификации по одиночному движению мыши (AD) классификатор CNN достиг минимального значения HTER, равного 0,0325.

Таблица 11 – Оценка CA – сценарий 1 (действие с одним движением мыши): FAR, FRR и HTER

Классификатор	KNN	DT	RF	CNN
FAR	0.0150	0.0200	0.0120	0.0110
FRR	0.1850	0.2400	0.1280	0.0240
HTER	0.1000	0.1300	0.0700	0.0175

Таблица 12 – Оценка CA – сценарий 2: (действие с одним щелчком мыши): FAR, FRR и HTER

Классификатор	KNN	DT	RF	CNN
FAR	0.0250	0.0180	0.0150	0.0100
FRR	0.1550	0.2120	0.0650	0.0200
HTER	0.0900	0.1150	0.0400	0.0150

Таблица 13 – Оценка CA – сценарий 3: (набор действий по перемещению мыши, наведению и щелчку): FAR, FRR и HTER.

Классификатор	KNN	DT	RF	CNN

FAR	0.0300	0.0250	0.0200	0.0080
FRR	0.1900	0.1350	0.0900	0.0160
HTER	0.1100	0.0800	0.0550	0.0120

Таблица 14 – Оценка AD – сценарий 1 (действие с одним движением мыши): FAR, FRR и HTER

Классификатор	KNN	DT	RF	CNN
FAR	0.0180	0.0220	0.0160	0.0250
FRR	0.1420	0.1780	0.1140	0.0400
HTER	0.0800	0.1000	0.0650	0.0325

Таблица 15 – Оценка AD – сценарий 2 (действие с одним щелчком мыши): FAR, FRR и HTER

Классификатор	KNN	DT	RF	CNN
FAR	0.0200	0.0240	0.0180	0.0220
FRR	0.1600	0.1960	0.1220	0.0380
HTER	0.0900	0.1100	0.0700	0.0300

Таблица 16 – Оценка AD – сценарий 3 (набор действий по перемещению мыши, наведению и щелчку): FAR, FRR и HTER

Классификатор	KNN	DT	RF	CNN
FAR	0.0250	0.0280	0.0200	0.0180
FRR	0.1850	0.2220	0.1400	0.0320

HTER	0.1050	0.1250	0.0800	0.0250

Результаты доказывают способность предложенных подходов отличать легитимного пользователя от злоумышленника. Модель CNN выбрана в качестве финального классификатора, поскольку она продемонстрировала наилучшие комплексные результаты среди всех алгоритмов во всех сценариях, обеспечив максимальную точность (до 98.50%) и минимальный уровень ошибок (HTER до 0.0120) за счет эффективного извлечения пространственно-временных признаков из поведенческих паттернов. Мы изучили эффективность CA и AD с использованием различных алгоритмов ML и DL [83]. Для аутентификации пользователя мы рассмотрели три сценария: сценарий 1, действие с одним движением мыши; сценарий 2, действие с одним нажатием и щелчком мыши; и сценарий 3, набор движений мыши и действия с наведением и щелчком мыши.

Тем не менее, важно признать существующее ограничение проекта, которое ограничивает операции без возможности корректировки разрешения экрана.

Несмотря на это ограничение, записанные строки данных обладают огромным потенциалом для улучшения пользовательского опыта, совершенствования дизайна приложений и направления развития пользовательского интерфейса и практики взаимодействия.

Рассмотрим количественные критерии повышения эффективности модели, такие как точность, время принятия решения и нагрузку на систему пользователя для сопоставления их с оценкой, проведённой в главе 2.

Проведена серия из 100 тестов для оценки времени принятия решений. Результаты (среднее время) представлены ниже:

- Сбор данных $T_{collect}$ – 200±3.92 мс
- Передача данных $T_{transmit}$ – 300±5.88 мс (учитывая задержки и помехи в сети)

– Обработка данных $T_{process}$ – 400±7.84 мс (включая время работы нейросети)
– Сравнение и ответ $T_{compare}$ – 100±1.96 мс

Суммарное время принятия решения:

$T_d = 1000 \pm 10.73$ мс, что соответствует рамкам функциональной пригодности биометрической системы.

В рамках эксперимента на основе экспертной оценки веса были определены как:

- $w_{\text{CPU}} = 0.5$
- $w_{\text{Memory}} = 0.3$
- $w_{\text{Disk}} = 0.2$

Тогда при нагрузках:

- CPU: 10% (0.10 в долях)
- Память: 5% (0.05 в долях)
- Дисковая операция: 3% (0.03 в долях)

Нагрузка на систему:

$$L = 0.5 \cdot 0.10 + 0.3 \cdot 0.05 + 0.2 \cdot 0.03 = 0.05 + 0.015 + 0.006 = 0.071$$

Таким образом, итоговая нагрузка на систему L составляет 0.071 или 7,1%. Сравнив это с обычным использованием системы, где чувствительность задержек начинается с 50% загрузки, можно увидеть, что система работает в пределах, соответствующих функциональной пригодности системы.

Полученные значения предполагают, что система может эффективно справляться с задачами аутентификации, обеспечивая быстрое время отклика и умеренную нагрузку на ресурсы пользователя. Дальнейшие исследования и повышение эффективности могут помочь улучшить эти показатели, возможно, за счет более эффективного алгоритма предобработки данных или улучшенной архитектуры нейронной сети.

3.5 Анализ результатов оценки функциональной пригодности системы

Отдельный интерес представляет сравнение исследуемого метода цифровой обработки сигналов устройства ввода посредством манипулятора и других наиболее часто употребляемых методов биометрии.

1) Точность аутентификации, измеряемая с помощью вероятности ложного положительного срабатывания (FAR) и вероятности ложного отрицательного срабатывания (FRR).

Расчеты, представленные в таблице 17, выполнены на основе выборок объемом не менее $15 \cdot 10^3$ измерений; значимость полученных результатов подтверждается критерием Фишера ($p < 0,$ при 90%-м доверительном интервале).

Таблица 17 – Средние значения FAR и FRR[17]

Биометрическая СКУД использует:	FAR	FRR
Исследуемая динамическая система: Цифровая обработка сигналов устройства ввода посредством манипулятора (мыши)	0,1%	1,2%
Популярные статические системы		
Отпечаток пальца	0,001%	0,6%
Распознавание лица 2D	0,1%	2,5%
Распознавание лица 3D	0,0005%	0,1%
Радужная оболочка глаза	0,00001%	0,016%
Сетчатка глаза	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

[17] Источник: TECHNOPORTAL. Биометрическая идентификация. URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html

Данные таблицы 17 указывают на то, что разработанная система уступает большинству традиционных биометрических методов по критериям точности (FAR и FRR). Тем не менее, этот недостаток компенсируется ее высокой инфраструктурной доступностью. В отличие от специализированных аппаратных сканеров, координатный манипулятор «мышь» является штатным компонентом автоматизированных рабочих мест (АРМ). Это позволяет развернуть контур непрерывной аутентификации без модернизации существующей ИТ-инфраструктуры и дополнительных капиталовложений, что критически важно для объектов, где внедрение выделенных биометрических систем технически затруднено или экономически нецелесообразно.

2) Устойчивость к вариациям (воздействие окружающей среды).

Таблица 18 – Устойчивость к окружающей среде (в баллах, 10 – максимальная устойчивость)[18]

Популярные статические системы	Устойчивость к окружающей среде
Отпечаток пальца	10
Распознавание лица 2D	6
Распознавание лица 3D	8
Радужная оболочка глаза	9
Сетчатка глаза	10
Рисунок вен	7
Исследуемая динамическая система: Цифровая обработка сигналов устройства ввода посредством манипулятора (мыши)	10

[18] См. 17

Анализируя данные таблицы 18 следует отметить, что исследуемая система по данному показателю превосходит или не уступает большинству популярных биометрических СКУД.

3) Производительность (оценивается на основе скорости получения результата).

Современные системы аутентификации обладают временем получения результата 5 – 10 сек.

Таблица 19 – Скорость (в баллах, 10 – максимальная скорость, соответствует времени получения результата в 5 – 10 сек.)[19]

Популярные статические системы	Скорость
Отпечаток пальца	10
Распознавание лица 2D	10
Распознавание лица 3D	7
Радужная оболочка глаза	10
Сетчатка глаза	6
Рисунок вен	8
Исследуемая динамическая система: Цифровая обработка сигналов устройства ввода посредством манипулятора (мыши)	9

Анализируя данные таблицы 19 следует отметить, что исследуемая система по данному показателю почти не уступает самым быстрым популярным биометрическим СКУД.

4) Возможность расширения и использование большого количества данных.

[19] См. 17

Таблица 20 – Возможность расширения и использование большого количества данных (в баллах, 10 – максимальная способность)[20]

Популярные статические системы	Возможность расширения и использование большого количества данных
Отпечаток пальца	9
Распознавание лица 2D	8
Распознавание лица 3D	5
Радужная оболочка глаза	7
Сетчатка глаза	6
Рисунок вен	5
Исследуемая динамическая система: Цифровая обработка сигналов устройства ввода посредством манипулятора (мыши)	10

Анализируя данные таблицы 20 следует отметить, что исследуемая система по данному показателю превосходит (некоторые в 2 раза) все популярные биометрические СКУД.

5) Оставшиеся значимые критерии.

Наиболее важными из оставшихся критериев является простота использования, дешевизна аутентификации и стабильность признака аутентификации во времени.

Таблица 21 – Оставшиеся критерии (в баллах, больше - лучше)[21]

[20] См. 17
[21] См. 17

Популярные статические системы	Простота использования	Дешевизна аутентификации	Стабильность признака во времени	Оценка стоимости внедрения
Отпечаток пальца	9	10	9	9
Распознавание лица 2D	6	10	8	8
Распознавание лица 3D	10	5	10	5
Радужная оболочка глаза	8	7	10	3
Сетчатка глаза	6	6	9	2
Рисунок вен	9	9	7	6
Исследуемая динамическая система: Цифровая обработка сигналов устройства ввода посредством манипулятора (мыши)	10	10	10	10

Из данных таблицы 21 заключаем, что исследуемый метод имеет максимальную оценку по всем рассмотренным признакам.

Из анализа данных таблиц 17 – 21 следует, что система цифровая обработки сигналов устройства ввода посредством манипулятора (мыши) серьезно уступает по важнейшим показателям FAR и FRR почти всем

популярным СКУД, однако, значения этих показателей достаточны для использования в качестве системы биометрической аутентификации.

С другой стороны, по всем другим значимым показателям исследуемая система или не уступает (по скорости) или превосходит прочие СКУД, что вместе с низкой стоимостью системы и отсутствием дополнительных гаджетов (сканер отпечатков пальца, сетчатки глаза и т.п.) делает ее весьма привлекательной. Кроме того, существует возможность совершенствования программного обеспечения с целью улучшить FAR и FRR за счет использования более сложной нелинейной функции активации и, соответственно, снижения скорости аутентификации.

Исходя из анализа, проведенного выше, следует, что эффективность конкретного биометрического метода определяется использованным математическим алгоритмом обработки данных. В нашем случае исследуемого метода цифровой обработки сигналов устройства ввода посредством манипулятора (мыши) для обработки данных используется нейронная сеть с архитектурой CNN. Вследствие этого необходимо сравнить показатели эффективности нейронной сети с архитектурой CNN с показателями эффективности нейронных сетей с другими популярными архитектурами.

Для сравнения применяются следующие ключевые параметры нейронной сети, влияющие на работоспособность биометрической аутентификации:

– время ответа (S1) – время получения результата;

– продолжительность обучения (S2) – время обучения алгоритма до момента принятия решений;

– визуализация и сравнение производительности различных моделей биометрической аутентификации с учётом соотношения FAR и FRR при различных пороговых значениях;

– F1 метрика (S4) – характеризует качество распознавания спуфинг-атак (подмены биометрии одного человека на биометрию другого).

Распознавание спуфинга (подделки биометрии) – важный аспект кибербезопасности: биометрические технологии применяются для аутентификации людей в финансах, медицине, корпоративных системах, повседневных устройствах. Значимость борьбы с распознаванием спуфинга обусловлена рядом причин:

– Противодействие мошенничеству. Киберпреступники могут использовать активацию подделки биометрии для получения несанкционированного доступа к чужим аккаунтам, данным и ресурсам. Это может привести к потерям, утечке личной информации и другим видам мошенничества.

– Защита личных данных. Биометрические данные представляют собой особую чувствительную информацию для человека. Подделка биометрии может привести к утечке личных данных и нарушению конфиденциальности.

Теоретический вес, варьирующийся от 0 до 1, был дан каждому из указанных выше параметров, которые представляют его важность для решения проблемы биометрической аутентификации (62):

– время отклика: w1=0,2;
– продолжительность обучения: w2=0,2;
– ROC значение: w3=0,4;
– F1 метрика: w4 =0,2.
–

$$\sum_{i=1}^{4} w_i = 1 \qquad (62)$$

Таблица 22 – Сравнение показателей эффективности исследуемой сети CNN с показателями других нейронных сетей (при решении однотипных задач)

	S1	S2	S3	S4	$S = \sum_{i=1}^{4} w_i * S_i$

VGG-16	0,5	0,3	0,0842	0,94	0,44568
AlexNet	0,7	0,2	0,0768	0,917	0,46582
SquezeeNet	0,4	0,7	0,0816	0,96	0,47064
CNN	0,6	0,6	0,0864	0,946	0,49836

Как видно из результатов, представленных в таблице 22, CNN является наиболее эффективной архитектурой нейронной сети для решения проблемы биометрической аутентификации.

3.6 Краткие выводы

Разработанная модель ориентирована на обеспечение требований безопасности, точности, эффективности и адаптации к различным типам биометрических данных. Практическая применимость модели подтверждена результатами экспериментальной апробации. В ходе тестирования применялись стандартизированные методы оценки точности, скорости и надёжности в различных условиях. Анализ включал верификацию корректности аутентификации, оценку скорости обработки, исследование устойчивости к попыткам обхода системы. Сопоставление с действующими стандартами подтвердило высокий уровень точности, быстродействия и надёжности модели. Дополнительно проведена оценка её эффективности в контексте обработки данных от устройств цифрового ввода; установлена зависимость качества аутентификации от характеристик входных данных.

Разработанная система сочетает эффективность и безопасность, что делает его перспективным для применения в сферах, требующих высокой точности биометрической аутентификации.

В третьей главе осуществлена программная реализация предложенных моделей и проведена их полномасштабная экспериментальная оценка. Результаты данной главы легли в основу следующих публикаций автора:

- Уймин, А. Г. Сравнение производительности алгоритмов классификации в рамках сетевой инфраструктуры / А. Г. Уймин, О. Р.

Никитин // Наукоемкие технологии в космических исследованиях Земли. – 2023. – Т. 15, № 2. – С. 33-40. – DOI 10.36724/2409-5419-2023-15-2-33-40. – EDN ELOYEH.

- Уймин, А. Г. Эмпирическая оценка методов машинного обучения в задачах онлайн-аутентификации / А. Г. Уймин // Вестник компьютерных и информационных технологий. – 2022. – Т. 19, № 8(218). – С. 49-57. – DOI 10.14489/vkit.2022.08.pp.049-057. – EDN EUAYKG.
- Uymin, A. Application of machine learning in the classification of traffic in telecommunication networks: working with network modeling systems / A. Uymin // E3S Web of Conferences : International Scientific Siberian Transport Forum - TransSiberia 2023, Novosibirsk, Russia, 16–19 мая 2023 года. Vol. 402. – Novosibirsk, Russia: EDP Sciences, 2023. – P. 03001. – DOI 10.1051/e3sconf/202340203001. – EDN ZMBVYO.
- Uymin, A. User identification and authentication in browser environments via machine learning / A. Uymin // E3S Web of Conferences. – 2024. – Vol. 549. – P. 08019. – DOI 10.1051/e3sconf/202454908019. – EDN NPJUNS.
- Свидетельство о государственной регистрации программы для ЭВМ № 2021619990 Российская Федерация. RemoteTopology-модуль авторизации : № 2021613424 : заявл. 09.03.2021 : опубл. 21.06.2021 / А. Г. Уймин, С. В. Любкин. – EDN KEDGKG.
- Свидетельство о государственной регистрации программы для ЭВМ № 2021615378 Российская Федерация. RemoteTopology-Администрирование : № 2021614090 : заявл. 16.03.2021 : опубл. 07.04.2021 / А. Г. Уймин. – EDN FTNONQ.
- Свидетельство о государственной регистрации программы для ЭВМ № 2021614803 Российская Федерация. Программный модуль-тренажер подготовки к демонстрационному экзамену профессионального мастерства для обучения студентов СПО по специальности "Системное и сетевое администрирование" : № 2021613749 : заявл. 24.03.2021 : опубл. 30.03.2021 / А. Г. Уймин, В. О. Антонов, Д. А. Шерунтаев, М. М.

Агафонова ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – EDN CNHXZQ.

- Свидетельство о государственной регистрации программы для ЭВМ № 2021614735 Российская Федерация. Программный интерфейс взаимодействия участников соревнований WorldSkills по компетенции 39 "Системное и сетевое администрирование" с удаленной сетевой инфраструктурой : № 2021613729 : заявл. 24.03.2021 : опубл. 29.03.2021 / А. Г. Уймин, М. М. Агафонова, Д. А. Шерунтаев, М. И. Костарев ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – EDN RNAFOG.
- Свидетельство о государственной регистрации программы для ЭВМ № 2021614613 Российская Федерация. Программная модель-симулятор сетевой инфраструктуры для обучения студентов ВПО и СПО по компетенции 39 "Системное и сетевое администрирование" WorldSkills : № 2021613770 : заявл. 24.03.2021 : опубл. 26.03.2021 / А. Г. Уймин ; заявитель Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – EDN FCAHFK.
- Свидетельство о государственной регистрации программы для ЭВМ № 2021661218 Российская Федерация. RemoteTopology-Интерфейс пользователя : № 2021613953 : заявл. 16.03.2021 : опубл. 07.07.2021 / А. Г. Уймин, Л. М. Черкашин. – EDN NQQVEK.
- Свидетельство о государственной регистрации программы для ЭВМ № 2023683139 Российская Федерация. Remote Topology extensions: Клиент-серверное браузерное расширение, обеспечивающие отслеживание

действий пользователя с целью проведения биометрической аутентификации : № 2023682110 : заявл. 25.10.2023 : опубл. 02.11.2023 / А. Г. Уймин. – EDN MSIISH.

- Греков, В. С. Оптимизация биометрической аутентификации через движения мыши: использование и настройка Random Forest для улучшения точности и эффективности / В. С. Греков, А. Г. Уймин // Современные цифровые технологии : Материалы II Всероссийской научно-практической конференции, Барнаул, 01 июня 2023 года / Под общей редакцией А.А. Беушев, А.С. Авдеев, Е.Г. Боровцов, А.Г. Зрюмова. – Барнаул: Алтайский государственный технический университет им. И.И. Ползунова, 2023. – С. 319-323. – EDN TAKTQB.
- Уймин, А. Г. Enhancing biometric authentication through the application of Relu and multilayer perceptrons in mouse movement analysis / А. Г. Уймин // Радиоэлектроника, электротехника и энергетика : Тезисы докладов Тридцатой международной научно-технической конференции студентов и аспирантов, Москва, 29 февраля – 02 2024 года. – Москва: Общество с ограниченной ответственностью "Центр полиграфических услуг " РАДУГА", 2024. – С. 275. – EDN LTNDUJ.

Результаты оценки функциональной пригодности аппаратно и программно доказывают первое положение, выносимое на защиту (достижение устойчивой классификации в реальном времени с точностью 97%). Также успешно верифицировано третье положение: обоснована и реализована архитектура системы с режимом адаптивного обучения.

ГЛАВА 4 АНАЛИЗ ВОЗМОЖНОСТЕЙ И ПЕРСПЕКТИВ ПРИМЕНЕНИЯ РАЗРАБОТАННОЙ МОДЕЛИ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ НА ОСНОВЕ МЕТОДОВ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ УСТРОЙСТВА ВВОДА

4.1 Практическое применение разработанной модели биометрической аутентификации на основе методов цифровой обработки сигналов устройства ввода

Применение этой модели варьируется от усиления безопасности в банковской сфере до улучшения контроля доступа в медицинских учреждениях. Это также включает усовершенствование паспортного контроля и повышение безопасности на промышленных объектах. Благодаря своей универсальности и эффективности, биометрическая аутентификация на основе методов цифровой обработки сигналов устройства ввода обладает значительным потенциалом в разнообразных областях применения. [76; 81; 109; 124; 141]

Направления применения разработанной модели биометрической аутентификации

Разработанная модель биометрической аутентификации, использующая цифровую обработку сигналов компьютерной мыши, имеет широкий спектр практических применений:

1) Аутентификация пользователя: использование уникальных биометрических характеристик, таких как движения мыши, для проверки личности при доступе к компьютерным системам.

2) Предотвращение несанкционированного доступа: блокировка доступа к системам при несовпадении биометрических данных обеспечивает повышение уровня безопасности.

3) Системы виртуальной реальности: повышение качества пользовательского взаимодействия за счёт отслеживания движений пользователя.

4) Медицинские информационные системы: обеспечение аутентификации пациентов и автоматизированного доступа к медицинским записям [56].

5) Финансовые транзакции: повышение уровня защиты онлайн-платежей и финансовых операций посредством применения биометрической аутентификации [102; 106].

6) Системы контроля доступа: управление доступом к зданиям, помещениям и информационным системам на основе биометрических данных; в специализированных средах такие решения могут дополнять технические комплексы контроля поведения лиц, находящихся под надзором [84].

7) Управление производственными процессами: контроль доступа работников к рабочим станциям и оборудованию на промышленных предприятиях.

Практическая значимость разработанной модели заключается в ее применимости для решения широкого спектра задач в гетерогенных информационных средах. Предложенный подход, базирующийся на фильтрации координатных треков и их последующем нейросетевом анализе, может быть экстраполирован с систем анализа движений мыши на смежные области: защиту сенсорных мобильных устройств и выявление мошеннической активности по поведенческим данным пользователя [155], аутентификацию жестов в IoT-системах и верификацию динамики рукописных подписей.

Вместе с тем, масштабирование метода накладывает требования по преодолению таких ограничений, как высокая вариативность индивидуальных признаков и сложность временной сегментации потока данных. Дальнейшее развитие теоретического базиса исследования в направлении цифровой

обработки сигналов устройств ввода позволит повысить робастность классификаторов к изменению внешних условий эксплуатации и психофизиологического статуса пользователя, обеспечивая сбалансированные показатели точности и эргономики защищаемого контура.

4.2 Рекомендации по дальнейшему развитию модели биометрической аутентификации

Развитие и практическая экспансия систем биометрической аутентификации требуют комплексного учета технологических, организационных и этико-правовых факторов. На глобальном уровне масштабирование таких решений детерминируется качеством международного сотрудничества, интенсивностью обмена научно-практическим опытом и темпами унификации нормативно-технических стандартов.

Особое значение приобретает этико-правовой базис: обеспечение конфиденциальности и защиты персональных данных граждан регламентируется строгим комплаенсом с требованиями профильных регуляторных актов. При этом успешность внедрения технологий в контур реальных предприятий напрямую зависит от уровня профессиональной подготовки обслуживающего персонала.

Повышение эффективности и информационной эргономики защищаемого периметра достигается за счет мультимодальной интеграции биометрической аутентификации со смежными системами безопасности (в частности, с комплексами интеллектуального видеонаблюдения). Автоматизация сквозного мониторинга, а также интенсификация обработки данных реализуются на основе методов машинного обучения, гарантирующих целевые показатели точности и скорости распознавания паттернов. Системная устойчивость разработанной архитектуры к возникающим угрозам поддерживается процедурами регулярного аудита рисков и оперативного устранения выявленных уязвимостей.

Многофакторная аутентификация, объединяющая различные биометрические модели, обеспечивает повышение надёжности аутентификации. Адаптация моделей к изменениям внешних условий и обучение на репрезентативных наборах данных обеспечивают повышение точности идентификации личности. Создание интуитивно понятных пользовательских интерфейсов обеспечивает упрощение взаимодействия пользователей с системой. Развитие биометрической аутентификации охватывает многофакторную аутентификацию, применение машинного обучения и искусственного интеллекта, обеспечение защиты приватности и конфиденциальности данных, эргономичные интерфейсы, соблюдение требований безопасности и законодательства.

Защита хранимых биометрических данных – ключевой аспект безопасности биометрической аутентификации, особенно при использовании облачной инфраструктуры обработки и хранения биометрических шаблонов [167].. Использование современных методов шифрования и механизмов контроля доступа предотвращает несанкционированный доступ и утечку данных. Безопасность предложенного метода непрерывной аутентификации достигается за счет реализации эшелонированной защиты информационного контура. Поведенческий анализ мыши выступает в качестве одного из независимых факторов в гетерогенных MFA-системах, эксплуатирующих также методы строгой аутентификации (токены, пароли) [81; 109; 154].

Архитектурная надежность сетевого сегмента программного комплекса требует детальной верификации [75]. На основе методов интеллектуального анализа данных целесообразно провести исследование инкапсулированного трафика на предмет его устойчивости к детекции и инъекциям ложных поведенческих сигналов [60; 67]. Оценку защищенности сессионных токенов при этом следует производить в соответствии со стандартами безопасности инфраструктуры JWT [61; 62]. В целях предотвращения угроз искусственной задержки пакетов (тайминг-атак), способных вызвать ложное срабатывание системы защиты, сетевой стек должен поддерживать жесткую классификацию

трафика с высоким приоритетом для аутентификационных сообщений [60; 67; 70; 80; 160].

Исключение рисков использования синтезированных биометрических шаблонов обеспечивается за счет внедрения алгоритмов проверки динамической подлинности потока. Обеспечение высокого качества исходной телеметрии минимизирует флуктуации метрик FAR/FRR, а открытость алгоритмических политик гарантирует правовой комплаенс в части обработки персональных данных пользователей.

Организации обязаны обеспечивать предоставление чётко сформулированных политик конфиденциальности и соблюдение нормативных требований. Для обеспечения надёжности функционирования систем у всех групп населения принципиально значим учёт разнообразия пользователей.

Обучение пользователей обеспечивает повышение эффективности и приемлемости биометрических технологий – пользователи становятся информированными о возможных рисках и мерах безопасности. Постоянное совершенствование моделей биометрической аутентификации, в том числе обновление технологий и алгоритмов, является необходимым условием адаптации к новым вызовам и угрозам. Регулярные обновления и обратная связь от пользователей обеспечивают улучшение пользовательского опыта и повышение безопасности систем. [44; 120; 127]

Применение биометрической аутентификации организациями и корпорациями расширяется в различных отраслях экономики – финансовой, транспортной, образовательной, в государственных учреждениях и муниципальных информационных системах, включая проекты биометрической актуализации данных избирателей [105]. К основным направлениям развития относятся повышение точности и надёжности биометрических моделей (отпечатки пальцев, распознавание лица, голосовая идентификация), внедрение новых технологий (сканирование радужной оболочки, генетическая аутентификация).

Организации применяют биометрическую аутентификацию в системах обеспечения безопасности и контроля доступа в качестве замены физических ключей, карт доступа и паролей. Это обеспечивает упрощение и усиление контроля доступа, в особенности в крупных офисных комплексах и на предприятиях. В сфере электронных транзакций и платежей биометрическая аутентификация обеспечивает повышение защиты данных и снижение рисков мошенничества.

Развитие систем видеонаблюдения с функцией распознавания лиц обеспечивает автоматическую идентификацию лиц в видеопотоке, что применяется для анализа данных о посетителях и работниках, выявления случаев несанкционированного доступа, проведения расследования преступлений.

Развитие биометрической аутентификации сопровождается возникновением проблем обеспечения безопасности и приватности данных. Организации принимают дополнительные меры защиты персональной информации от несанкционированного доступа или неправомерного использования.

Для обеспечения надёжности и защищённости систем организации осуществляют взаимодействие с экспертами в области информационной безопасности и специалистами по биометрии, проводят регулярные аудиты безопасности, участвуют в разработке международных стандартов. Многофакторная аутентификация рекомендуется в качестве дополнительного уровня обеспечения безопасности.

Доступ к биометрическим данным ограничивается сотрудниками, для которых он необходим в силу должностных обязанностей; пользователям предоставляется возможность контроля и удаления собственных данных. Компании готовы к инцидентам безопасности и располагают планами реагирования – назначение ответственных лиц, обучение сотрудников.

Дальнейшее развитие биометрической аутентификации поднимет надёжность, безопасность и удобство использования; компании активно

внедряют технологию с соблюдением требований безопасности и конфиденциальности. [127; 145; 168; 181]

Безопасность биометрической аутентификации – значимый аспект для компаний и организаций, использующих эту технологию. Регулярные обновления программного обеспечения и алгоритмов, физическая защита устройств и инфраструктуры, шифрование данных, ограничение доступа и прочие меры необходимы для предотвращения несанкционированного доступа и использования биометрических данных. Обучение пользователей, сотрудничество с экспертами, внедрение двухфакторной аутентификации, разработка политики безопасности, наличие плана реагирования на инциденты повышают уровень безопасности системы. В совокупности эти меры обеспечат надёжную защиту биометрической аутентификации и предотвратят возможные угрозы безопасности.

4.3 Анализ возможных модификаций моделей биометрической аутентификации

В рамках улучшения модели биометрической аутентификации на основе движений мыши ключевые цели – повышение точности и надёжности аутентификации. Их достижение охватывает разработку усовершенствованных алгоритмов обработки данных, улучшение качества и разнообразия собираемых данных, повышение эффективности процессов обучения и валидации модели. Улучшения должны поднять уровень защиты от несанкционированного доступа, увеличить скорость и точность аутентификации пользователя, укрепить доверие к системе биометрической аутентификации.

Разработка модели опирается на достижения предыдущих исследований (см. главу 2) в области анализа движений мыши и нейронных сетей. Прошлые работы показали значительный потенциал поведенческих биометрических данных, в том числе движений мыши, для надёжной аутентификации пользователей. Потребность в развитии методов сохраняется – это улучшение

точности, скорости обработки данных, устойчивости к попыткам мошенничества. Учитываются последние достижения в машинном и глубоком обучении: они открывают новые подходы к обработке и анализу биометрических данных.

Для повышения точности и надёжности модели биометрической аутентификации основные усилия концентрируются на разработке и внедрении усовершенствованных алгоритмов обработки данных. Разработанные алгоритмы ориентированы на многофакторный анализ кинематических характеристик координатного ввода, включая мгновенную скорость, ускорение, геометрию траектории, длительность пауз (фикций) и индивидуальный ритм взаимодействия. Для повышения селективных свойств модели и минимизации ошибок первого и второго рода (FAR/FRR) стандартный базис признаков целесообразно обогатить дополнительными параметрами: направляющими косинусами векторов перемещения, динамикой аппликации (нажатия) клавиш и пространственно-временными паттернами скроллинга. Интеграция данных признаков требует предварительной оценки их информативности и анализа вычислительной сложности, обусловленной ростом размерности пространства признаков.

Центральным вектором развития биометрической модели является оптимизация процедур ее обучения. Переход от классических алгоритмов к глубоким нейросетевым архитектурам (в частности, к одномерным сверточным сетям –1D CNN) позволяет эффективно декодировать скрытые нелинейные взаимосвязи и иерархические паттерны в зашумленных временных рядах поведенческой телеметрии. За счет этого достигается не только стабилизация метрик точности, но и повышается адаптивность системы к естественным флуктуациям индивидуального поведения субъекта в процессе долгосрочной эксплуатации (персонализация профиля). Дополнительным фактором робастности классификатора выступает модернизация конвейера сбора данных, где расширение объема и

гетерогенности обучающих выборок гарантирует устойчивость модели к вариативности стилей пользовательского интерфейса.

Сюда относится сбор данных в разных контекстах использования мыши – в играх, при навигации по интернету, при работе с офисным ПО. Разнообразие контекстов формирует более универсальную и надёжную модель, способную точно идентифицировать пользователя в различных сценариях. Помимо количества данных значимо и их качество – точность, последовательность, целостность собираемых данных. Качество сбора данных растёт благодаря более точным методам отслеживания движений мыши и улучшенному программному обеспечению для сбора данных. Принимаются во внимание вопросы конфиденциальности и безопасности данных: собранная информация используется исключительно в целях аутентификации и не подвергается риску несанкционированного доступа.

В контексте биометрической аутентификации обеспечение безопасности и защита от мошенничества являются критически значимыми аспектами. Для повышения уровня безопасности проведено усовершенствование механизмов обнаружения и предотвращения подделки данных. Указанное направление включает разработку алгоритмов, обеспечивающих распознавание нетипичных или подозрительных паттернов поведения, свидетельствующих о попытках манипуляции или имитации движений мыши. Внедряются многоуровневые системы безопасности, оснащённые дополнительными методами аутентификации для подтверждения личности пользователя при выявлении подозрительной активности. Анализ поведенческой телеметрии на основе машинного обучения позволяет обнаруживать аномальную активность, выявляя отклонения от типовых паттернов пользователя, что служит маркером попытки несанкционированного доступа. Практическое развертывание таких решений требует калибровки порогов классификации, чтобы минимизировать частоту ложных срабатываний при сохранении надежной защиты от угроз.

Надежность и точность биометрической модели верифицируются в рамках комплексного тестирования [120; 164] в различных операционных системах, под разной вычислительной нагрузкой и с использованием манипуляторов с отличающимися аппаратными характеристиками (разрешением сенсора и частотой опроса). Самостоятельным этапом проверки выступает стресс-тестирование системы, направленное на оценку ее устойчивости к попыткам обхода защиты, включая атаки воспроизведения и инъекции искусственно сгенерированных треков.

Для объективности и надёжности модели валидация проводится на разнообразных наборах данных, отражающих различные демографические и поведенческие характеристики пользователей. В результате модель эффективно работает для широкого спектра пользователей и адаптируется к разнообразным стилям взаимодействия. Параллельно проводится сравнительный анализ с другими существующими моделями биометрической аутентификации для оценки преимуществ и ограничений разработанной модели.

Описанные улучшения модели биометрической аутентификации на основе анализа движений мыши открывают новые горизонты в области безопасности и аутентификации. Усовершенствование алгоритмов обработки данных, повышение эффективности алгоритмов обучения, улучшение процесса сбора данных, повышение безопасности и защиты от подделок, тщательное тестирование и валидация модели формируют более точную, надёжную и безопасную систему аутентификации. Возможности дальнейшего развития модели включают интеграцию с другими биометрическими методами (распознавание лиц, отпечатков пальцев) для создания многофакторных систем аутентификации. Перспективным направлением является разработка адаптивных алгоритмов, способных самостоятельно обновляться при изменениях в поведенческих паттернах пользователей или при появлении новых угроз безопасности. Так формируется более

универсальная и устойчивая к внешним изменениям система, отвечающая современным требованиям безопасности и приватности.

4.4 Перспективы совершенствования технологии в общей системе алгоритмов биометрической аутентификации

В современном мире, где цифровая безопасность критически важна, интеграция инновационных технологий в области биометрической аутентификации становится неотъемлемой частью защиты личных данных и системных операций. Расширение для браузера, отслеживающее положения и движения мыши, открывает уникальную возможность углубить понимание пользовательского поведения. Применение нейросети методом CNN (Convolutional Neural Network) для обработки и анализа собранных данных существенно повышает эффективность систем биометрической аутентификации. Эта технология улучшает точность аутентификации личности и обеспечивает новый уровень защиты. Интеграция системы в общую структуру биометрических алгоритмов даёт возможность создавать более комплексные и надёжные методы аутентификации, адаптируемые к различным сценариям использования и потребностям пользователей.

Цель усовершенствования технологии в рамках системного подхода – более гибкая, безопасная и эффективная система биометрической аутентификации. Значимо обеспечение конфиденциальности и безопасности собираемых данных, для чего необходимо разрабатывать и внедреть строгие протоколы шифрования и хранения информации.

Совершенствование технологий аутентификации направлено на повышение их надежности, конфиденциальности и защищенности. Перспективным направлением развития систем информационной безопасности является интеграция мониторинга динамики движений мыши с традиционными статическими и поведенческими биометрическими методами, такими как дактилоскопия, распознавание лиц, голоса и клавиатурного почерка. Синергия разнородных параметров позволяет сформировать

многоуровневый контур безопасности. Мультибиометрический подход решает проблему отказов единичных каналов верификации за счет аппаратной и программной избыточности, а также существенно снижает риски успешных деструктивных воздействий (фишинга, несанкционированного доступа и мошенничества), поскольку одновременная компрометация или имитация нескольких уникальных характеристик пользователя злоумышленником маловероятна.

Ключевыми критериями эффективности внедрения технологии поведенческой биометрии в инфраструктуру корпоративного, банковского и государственного секторов являются масштабируемость и адаптивность. Для успешного функционирования в крупномасштабных системах разработанные алгоритмы должны обладать высокой вычислительной способностью при обработке больших массивов данных в режиме реального времени, устойчивостью к изменению внешних факторов (аппаратных характеристик устройств ввода, специфики операционных систем и пропускной способности каналов связи), а также способностью к непрерывному дообучению для своевременного реагирования на эволюционирующие киберугрозы. При этом возможность персонализации и гибкой настройки параметров под конкретные сценарии и группы пользователей позволяет повысить эргономичность системы без снижения уровня ее защищенности.

Интеграция метода отслеживания движений мыши в общую архитектуру безопасности требует строгой стандартизации. Разработка унифицированных протоколов обмена информацией и форматов представления биометрических шаблонов является необходимым условием для обеспечения кроссплатформенной совместимости решений. Соответствие разрабатываемых систем международным и национальным стандартам, в частности стандартам ISO/IEC в области информационных технологий и защиты данных, гарантирует легитимность процессов сбора, обработки и хранения конфиденциальной информации. В конечном итоге сопряжение предлагаемой технологии со спецификациями многофакторной

аутентификации позволяет создать гибридную экосистему безопасности, минимизирующую издержки при интеграции в существующие программные комплексы и повышающую общий уровень доверия к системе.

Одним из наиболее значимых аспектов внедрения новых технологий, в особенности в области биометрической аутентификации, является обеспечение безопасности и конфиденциальности собираемых данных. Применительно к технологии отслеживания движений мыши указанный аспект включает разработку и применение мер защиты данных от несанкционированного доступа, кражи или утечки. Принимается во внимание применение современных методов шифрования, безопасного хранения данных, регулярного обновления систем безопасности для противодействия новым угрозам. Сбор и обработка данных осуществляются с соблюдением законодательства в области защиты персональных данных.

Соответствие законодательным и этическим стандартам является неотъемлемой составляющей разработки и внедрения технологии биометрической аутентификации. Подразумевается соответствие нормативно-правовым актам и принятие этических принципов в области использования биометрических данных. Принимаются во внимание проблемы конфиденциальности и потенциальные риски для личной свободы и безопасности пользователей. Этический подход к применению биометрических данных включает обеспечение прозрачности процедур сбора, обработки и использования данных, предоставление пользователям контроля над их персональными данными. Указанный подход обеспечивает укрепление доверия пользователей к системе и способствует более широкому принятию технологии.

Одной из ключевых задач развития технологии отслеживания движений мыши в контексте биометрической аутентификации является определение перспективных направлений дальнейших исследований. К указанным направлениям относятся: углублённый анализ поведенческих биометрических данных; разработка усовершенствованных алгоритмов обработки и анализа

данных; исследование новых сфер применения технологии – в онлайн-банкинге, удалённой работе, системах безопасности. Существенным аспектом является исследование способов повышения точности и надёжности системы, в особенности в контексте разнообразных условий и сценариев применения. Исследования концентрируются на минимизации потенциальных ошибок аутентификации и обеспечении высокого уровня защиты данных.

Поиск инновационных решений в области биометрической аутентификации открывает широкие возможности технологических прорывов. Сюда относится разработка новых методов машинного обучения и искусственного интеллекта для более точной интерпретации данных, интеграцию с другими технологиями (искусственное зрение, глубинное обучение) для создания более комплексных систем аутентификации. Инновации касаются развития технологий для улучшения пользовательского опыта – например, создания более интуитивных и удобных интерфейсов. Рассматриваются вопросы удобства использования и доступности технологии для широкого круга пользователей, включая людей с ограниченными возможностями.

Интеграция технологии отслеживания движений мыши в области биометрической аутентификации открывает новые горизонты в обеспечении цифровой безопасности. Разработка и совершенствование технологии сформирует более надёжные, удобные и адаптивные системы аутентификации, интегрируемые в широкий спектр приложений. Стратегическое видение развития технологии включает техническое усовершенствование и учёт этических и законодательных аспектов обработки и защиты личных данных. Усилия концентрируются на исследованиях и разработках в направлении инновационных решений и улучшения интеграции технологии в общую систему биометрической аутентификации. Перспективы развития технологии обширны, её потенциал в повышении безопасности и удобства использования значителен. Продолжение работы в этом направлении

принесёт значительные улучшения в области цифровой безопасности и защиты персональных данных.

4.5 Краткие выводы

Модель биометрической аутентификации на основе анализа движений мыши демонстрирует значительные перспективы применения в областях, в которых требуются ненавязчивые и эргономичные методы аутентификации. Практическая значимость разработанной модели заключается в возможности ее интеграции в системы корпоративной безопасности, сервисы дистанционного банковского обслуживания и иные программные комплексы, требующие обеспечения повышенного уровня защищенности при сохранении исходного качества пользовательского взаимодействия. С целью повышения эффективности и надежности идентификации целесообразно внедрение адаптивных алгоритмов машинного обучения, способных динамически учитывать изменения индивидуальных поведенческих паттернов субъектов. Кроме того, необходимо проектирование специализированных механизмов фильтрации и компенсации мешающих факторов, обусловленных аппаратными различиями устройств ввода и вариативностью психофизиологического состояния пользователей. Проведенное исследование подтверждает высокий потенциал дальнейшей модернизации модели, в частности, за счет ее интеграции с комплементарными биометрическими методами для минимизации ошибок первого и второго рода, а также посредством разработки гибких конфигурационных профилей для различных эксплуатационных сценариев.

В долгосрочной перспективе технология аутентификации на основе движений мыши усовершенствуется за счёт продвинутых технологий искусственного интеллекта и машинного обучения. Это повысит точность аутентификации и сделает систему более устойчивой к попыткам подделки и мошенничества. Модель биометрической аутентификации на основе анализа поведенческих характеристик движений компьютерной мыши представляет

собой перспективное направление развития биометрических технологий с высоким потенциалом дальнейшей интеграции в системы аутентификации различного назначения.

Четвертая глава посвящена анализу возможностей масштабирования и перспектив применения разработанной биометрической модели. В основу предложенных рекомендаций, доказательств эффективности и масштабируемости архитектуры легли исследования автора, опубликованные в работах:

- Уймин, А. Г. Цифровые двойники сетевых инфраструктур: точность, методы и практические решения / А. Г. Уймин // Радиотехнические и телекоммуникационные системы. – 2023. – № 3(51). – С. 44-52. – DOI 10.24412/2221-2574-2023-3-44-52. – EDN QUSITK.
- Настройка виртуального сетевого стенда в режиме вложенной виртуализации / А. В. Воруев, О. М. Демиденко, Д. С. Сыч [и др.] // Известия Гомельского государственного университета имени Ф. Скорины. – 2025. – № 6(153). – С. 70-75. – EDN KQNSVY.
- Уймин, А. Г. Практическая адаптация педагогической методологии 4C/ID в рамках преподавания дисциплины «Сети и системы передачи информации» в системе профессионального образования / А. Г. Уймин // Russian Journal of Education and Psychology. – 2025. – Т. 16, № 5. – С. 46-76. – DOI 10.12731/2658-4034-2025-16-5-822. – EDN KPPBZQ.
- Уймин, А. Г. Методы машинного обучения при определении психического состояния на основе данных координатного устройства ввода информации / А. Г. Уймин // Психология и психотехника. – 2025. – № 3. – С. 207-223. – DOI 10.7256/2454-0722.2025.3.75214. – EDN UTXTAA.
- Уймин, А. Г. Применение отечественного сетевого оборудования Eltex и EcoRouter в рамках специальности 09.02.06 "Сетевое и системное администрирование". Вопросы импортозамещения и подготовки квалифицированных кадров в сетевом оборудовании / А. Г. Уймин, И.

М. Толмачев // Автоматизация и информатизация ТЭК. – 2025. – № 11(628). – С. 58-62. – EDN DMHQJU.

- Дегтярев, С. С. Оптимизация процесса разработки оценочных материалов для проведения государственной итоговой аттестации обучающихся СПО по специальности 09.02.06 «Сетевое и системное администрирование» в форме демонстрационного экзамена / С. С. Дегтярев, О. А. Терентьева, А. Г. Уймин // Russian Journal of Education and Psychology. – 2025. – Т. 16, № 3. – С. 211-236. – DOI 10.12731/2658-4034-2025-16-3-751. – EDN CEDMWH.
- Уймин, А. Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2024. – № 5(610). – С. 59-65. – EDN VSLWIA.
- Уймин, А. Г. Оценка эмоционально психологического состояния при дистанционном обучении. Инструментальные средства / А. Г. Уймин // Сборник материалов XVIII межвузовской конференции молодых ученых по результатам исследований в области психологии, педагогики, социокультурной антропологии, Москва, 18 апреля 2023 года. – Москва: Московский педагогический государственный университет, 2023. – С. 328-334. – EDN XWBCXU.
- Уймин, А. Г. Функционал обнаружения внутренних угроз, основанный на динамике мыши / А. Г. Уймин // Молодая наука Сибири. – 2024. – № 3(25). – С. 82-92. – EDN RPRZBM.

Глава подтверждает масштабируемость предложенной в третьем положении архитектуры, развивает ее потенциал и доказывает высокую практическую применимость результатов диссертационного исследования в образовательном процессе, тестировании систем безопасности и оценке состояния пользователей.

ЗАКЛЮЧЕНИЕ

В работе исследованы ключевые аспекты построения и применения модели биометрической аутентификации на основе методов цифровой обработки сигналов устройств ввода, в частности с применением данных, формируемых компьютерным манипулятором типа «мышь». Исследование охватывает теоретические основы алгоритмов биометрической аутентификации, в том числе анализ этапов развития и действующих стандартов, и вопросы стандартизации и повышения эффективности функционирования биометрических систем. Предложена и разработана структурная модель системы биометрической аутентификации, сочетающая традиционные подходы с инновационными методами цифровой обработки сигналов. Архитектура подтвердила свою гибкость и масштабируемость, обеспечивающие применимость в различных предметных областях.

Результаты программной реализации прототипа и последующей экспериментальной оценки подтвердили высокую точность, надежность и эффективность разработанной модели в условиях, приближенных к реальной эксплуатации. Полученные в ходе апробации данные обосновывают целесообразность внедрения предложенного решения в широкий спектр программных комплексов, критичных к сочетанию высокого уровня защищенности и эргономичности процесса верификации. На основе проведенного анализа сформулированы рекомендации по дальнейшей модернизации модели, направленные на повышение ее адаптивности и устойчивости к деструктивным внешним воздействиям. В целом исследование открывает новые научно-практические перспективы в области проектирования ненавязчивых систем биометрической аутентификации, что обусловливает необходимость продолжения изысканий по совершенствованию технологического базиса и расширению областей его практического применения в корпоративных и пользовательских инфраструктурах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Нормативные правовые акты и официальные документы

Нормативные правовые акты

1. Гражданский кодекс Российской Федерации. Часть первая : Федеральный закон от 30.11.1994 № 51-ФЗ : ст. 152.1 «Охрана изображения гражданина» [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

2. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ : ред. от 06.02.2023 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

3. О порядке обработки биометрических персональных данных и векторов единой биометрической системы : приказ Минцифры России от 12.05.2023 № 453 : зарегистрирован в Минюсте России 30.05.2023 № 73620 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

4. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ : ред. от 12.12.2023 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

5. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных : Федеральный закон от 29.12.2022 № 572-ФЗ [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об утверждении Порядка получения, учета, хранения, классификации, использования, выдачи и уничтожения биометрических персональных данных об особенностях строения папиллярных узоров пальцев и (или) ладоней рук человека : приказ ФСБ России от 16.12.2016 № 771 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

7. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их

обработке в информационных системах персональных данных : приказ ФСТЭК России от 18.02.2013 № 21 : ред. от 14.05.2020 : зарегистрирован в Минюсте России 14.05.2013 № 28375 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

8. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах : приказ ФСТЭК России от 14.03.2014 № 31 : ред. от 15.03.2021 : зарегистрирован в Минюсте России 30.06.2014 № 32919 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

9. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11.02.2013 № 17 : ред. от 28.05.2019 : зарегистрирован в Минюсте России 31.05.2013 № 28608 [Электронный ресурс]. – Доступ из справ.-правовой системы «КонсультантПлюс».

Стандарты

10. ГОСТ ISO/IEC 17025-2019. Общие требования к компетентности испытательных и калибровочных лабораторий. – Москва : Стандартинформ, 2021. – 32 с.

11. ГОСТ ИСО/МЭК 2382-37-2016. Информационные технологии. Словарь. Часть 37. Биометрия. – Москва : Стандартинформ, 2018. – 27 с.

12. ГОСТ ИСО/МЭК 19794-1-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 1. Структура. – Москва : Стандартинформ, 2018. – 32 с.

13. ГОСТ Р 52633.0-2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. – Москва : Стандартинформ, 2020. – 25 с.

14. ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018). Информационные технологии. Биометрия. Общие положения и примеры применения. – Москва : Стандартинформ, 2019. – 43 с.

15. ГОСТ Р 58295-2018. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза. – Москва : Стандартинформ, 2018. – 58 с.

16. ГОСТ Р 58298-2018. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальца. – Москва : Стандартинформ, 2018. – 98 с.

17. ГОСТ Р 58624.2-2019 (ИСО/МЭК 30107-2:2017). Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных. – Москва : Стандартинформ, 2019. – 20 с.

18. ГОСТ Р 58668.8-2019. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения сосудистого русла. – Москва : Стандартинформ, 2019. – 46 с.

19. ГОСТ Р 58668.11-2019. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Данные голоса. – Москва : Стандартинформ, 2019. – 28 с.

20. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения. – Москва : Стандартинформ, 2020. – 32 с.

21. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. – Москва : Стандартинформ, 2020. – 19 с.

22. ГОСТ Р ИСО/МЭК 19794-2-2013. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца – контрольные точки. – Москва : Стандартинформ, 2015. – 123 с.

23. ГОСТ Р ИСО/МЭК 19794-3-2009. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 3. Спектральные данные изображения отпечатка пальца. – Москва : Стандартинформ, 2011. – 44 с.

24. ГОСТ Р ИСО/МЭК 19794-5-2013. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица. – Москва : Стандартинформ, 2015. – 179 с.

25. ГОСТ Р ИСО/МЭК 19794-7-2017. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи. – Москва : Стандартинформ, 2019. – 91 с.

26. ГОСТ Р ИСО/МЭК 19794-8-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 8. Данные изображения отпечатка пальца – остов. – Москва : Стандартинформ, 2016. – 68 с.

27. ГОСТ Р ИСО/МЭК 19794-10-2010. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 10. Данные геометрии контура кисти руки. – Москва : Стандартинформ, 2019. – 24 с.

28. ГОСТ Р ИСО/МЭК 19794-11-2015. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 11. Обрабатываемые данные динамики подписи. – Москва : Стандартинформ, 2019. – 27 с.

29. ГОСТ Р ИСО/МЭК 19794-14-2017. Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 14. Данные ДНК. – Москва : Стандартинформ, 2017. – 45 с.

30. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва : Стандартинформ, 2021. – 28 с.

31. ГОСТ Р МЭК 31010-2021. Надежность в технике. Методы оценки риска. – Москва : Стандартинформ, 2021. – 94 с.

II. Специальная литература

Монографии, учебники, учебные пособия, диссертации

32. Арутюнов, В. В. Биометрия на службе защиты информации / В. В. Арутюнов. – Москва : Литера, 2012. – 108 с.

33. Введение в математическое моделирование / В. Н. Ашихмин [и др.]. – Москва : Логос, 2004. – 439 с.

34. Коробова, Л. А. Математическое моделирование. Практикум : учеб. пособие / Л. А. Коробова [и др.]. – Воронеж : ВГУИТ, 2017. – 112 с. – ISBN 978-5-00032-247-5.

35. Математическое моделирование / пер. с англ. ; под ред. Дж. Эндрюса, Р. Мак-Лоуна. – Москва : Мир, 1979. – 280 с.

36. Новейшие методы обработки изображений / А. А. Потапов [и др.] ; под ред. А. А. Потапова. – Москва : Физматлит, 2008. – 496 с.

37. Рейзлин, В. И. Математическое моделирование : учеб. пособие для вузов / В. И. Рейзлин. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2022. – 126 с. – ISBN 978-5-534-08475-7.

38. Самарский, А. А. Математическое моделирование: идеи, методы, примеры / А. А. Самарский, А. П. Михайлов. – 2-е изд., испр. – Москва : Физматлит, 2002. – 316 с. – ISBN 5-9221-0120-X.

39. Суомалайнен, А. Биометрическая защита: обзор технологии / А. Суомалайнен. – Москва : ДМК Пресс, 2019. – 104 с.

40. Тарасик, В. П. Математическое моделирование технических систем : учебник для вузов / В. П. Тарасик. – 2-е изд. – Минск : ДизайнПРО, 2004. – 640 с. – ISBN 985-452-080-3.

41. Уймин, А. Г. Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учеб.-метод. пособие для СПО / А. Г. Уймин. – 3-е изд., стер. – Санкт-Петербург : Лань, 2022. – 480 с. – ISBN 978-5-8114-9255-8. – URL: https://elibrary.ru/item.asp?id=50761885 (дата обращения: 20.05.2026).

42. Уймин, А. Г. Система непрерывно-дискретной биометрической аутентификации на основе анализа потока данных компьютерной мыши : автореф. дис. ... канд. техн. наук : 2.3.8, 2.3.6 / А. Г. Уймин. – Москва, 2026. – 39 с.

43. Яглом, И. М. Математические структуры и математическое моделирование / И. М. Яглом. – Москва : Советское радио, 1980. – 143 с.

44. Barnum, C. M. Usability testing essentials: ready, set... test! / C. M. Barnum. – 2nd ed. – Burlington : Morgan Kaufmann, 2020. – 448 p. – ISBN 978-0-12-816942-1.

45. Biometrics: theory, methods, and applications / ed. by N. V. Boulgouris, K. N. Plataniotis, E. Micheli-Tzanakou. – Hoboken : Wiley-IEEE Press, 2009. – 762 p.

46. Dym, C. Principles of mathematical modeling / C. Dym. – 2nd ed. – Burlington : Academic Press, 2004. – 303 p.

47. Gershenfeld, N. A. The nature of mathematical modeling / N. A. Gershenfeld. – Cambridge : Cambridge University Press, 1999. – 344 p.

48. Heinz, S. Mathematical modeling / S. Heinz. – Berlin ; Heidelberg : Springer, 2011. – 460 p.

49. Koltzsch, G. The External Firm Environment and Firm Success: A Qualitative Study in The German Biometrics Industry : dissertation / G. Koltzsch. – Guildford : University of Surrey, 2013. – 196 p.

50. Meerschaert, M. Mathematical modeling / M. Meerschaert. – 4th ed. – Waltham : Academic Press, 2013. – 676 p.

51. Reid, P. Biometrics for network security / P. Reid. – Upper Saddle River : Prentice Hall PTR, 2004. – 288 p. – ISBN 0-13-101549-4.

52. Viega, J. Building Secure Software: How to Avoid Security Problems the Right Way / J. Viega, G. McGraw. – Boston : Addison-Wesley Professional, 2002. – 528 p.

Научные статьи и материалы конференций

53. Брюхомицкий, Ю. А. Верификация динамических биометрических параметров личности на основе вероятностной нейронной сети // Известия Южного федерального университета. Технические науки. – 2020. – № 5 (215). – С. 52–60.

54. Греков, В. С. Оптимизация биометрической аутентификации через движения мыши: использование и настройка Random Forest для улучшения точности и эффективности / В. С. Греков, А. Г. Уймин // Современные цифровые технологии : материалы II Всерос. науч.-практ. конф., Барнаул, 01

июня 2023 г. – Барнаул : АлтГТУ, 2023. – С. 319–323. – URL: https://elibrary.ru/item.asp?id=54479927 (дата обращения: 20.05.2026).

55. Гусенкова, А. А. Применение систем видеонаблюдения и автоматизированных систем биометрической идентификации человека при производстве портретных экспертиз и исследований // Вестник Московского университета МВД России. – 2021. – № 6. – С. 86–90.

56. Зыков, В. Д. [и др.] Обеспечение защиты информации при обработке медицинских биометрических данных // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – № 2-2 (22). – С. 249–252.

57. Ибрагимов, Р. И. О. Биометрические системы аутентификации / Р. И. О. Ибрагимов, С. В. Чичахова // Инновации. Наука. Образование. – 2021. – № 32. – С. 1339–1352.

58. Кузнецова, Н. М. Анализ и применение методов биометрической аутентификации в автоматизированной системе защиты ресурсов промышленного предприятия / Н. М. Кузнецова, Т. В. Карлова, А. Ю. Бекмешов // Вестник Брянского государственного технического университета. – 2020. – № 8 (93). – С. 47–52. – DOI: 10.30987/1999-8775-2020-8-47-52. – URL: https://cyberleninka.ru/article/n/analiz-i-primenenie-metodov-biometricheskoy-autentifikatsii-v-avtomatizirovannoy-sisteme-zaschity-resursov-promyshlennogo (дата обращения: 25.05.2026).

59. Лекарь, Л. А. Новые технологические возможности нейросетевого искусственного интеллекта при решении задач быстрого поиска по большим базам биометрических данных / Л. А. Лекарь, А. И. Иванов // Развитие учения о противодействии расследованию преступлений и мерах по его преодолению в условиях цифровой трансформации. – 2021. – С. 199–207.

60. Махмудов, Р. Т. Анализ зашифрованного сетевого трафика с применением машинного обучения / Р. Т. Махмудов, А. Г. Уймин // Губкинский университет в решении вопросов нефтегазовой отрасли России : тез. докл. VI Регион. науч.-техн. конф., Москва, 19–21 сент. 2022 г. – Москва :

РГУ нефти и газа им. И. М. Губкина, 2022. – С. 1133–1134. – URL: https://elibrary.ru/item.asp?id=53007307 (дата обращения: 20.05.2026).

61. Монахов, М. Ю. Инфраструктура JSON Web Token. Инфраструктура защиты / М. Ю. Монахов, А. Г. Уймин // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 1. – С. 136–141. – DOI: 10.37882/2223-2966.2023.01.28. – URL: https://elibrary.ru/item.asp?id=53699750 (дата обращения: 20.05.2026).

62. Никитин, О. Р. Инфраструктура JSON Web Token. Реализация основных типов атак / О. Р. Никитин, А. Г. Уймин // Перспективы науки. – 2023. – № 2 (161). – С. 28–34. – URL: https://elibrary.ru/item.asp?id=53738296 (дата обращения: 20.05.2026).

63. Новопавловский, А. А. Обзор биометрических криптосистем и отменяемой биометрии / А. А. Новопавловский, К. Верейкин // Угрозы и риски финансовой безопасности в контексте цифровой трансформации. – 2021. – С. 407–412.

64. Самотуга, А. Е. [и др.] Обзор методов тестирования надежности биометрических систем с использованием синтетических образов // Цифровизация и кибербезопасность: современная теория и практика. – 2021. – С. 263–268.

65. Тихонова, Д. И. Системы биометрической идентификации и риски для конфиденциальности / Д. И. Тихонова, С. А. Грязнов // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе. – 2021. – С. 242–245.

66. Туреев, С. В. Использование эмбриона базы биометрических образов "чужой" для формирования большой тестовой базы с сохранением основных свойств корреляционной матрицы / С. В. Туреев, Е. А. Малыгина // Труды международного симпозиума "Надежность и качество". – 2019. – Т. 2. – С. 211–213.

67. Уймин, А. Г. Автоматическое маркирование сетевого трафика браузера для анализа и классификации на примере платформы

"RemoteTopology" // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 12. – С. 17–22. – DOI: 10.36724/2072-8735-2022-16-12-17-22. – URL: https://elibrary.ru/item.asp?id=49917706 (дата обращения: 20.05.2026).

68. Уймин, А. Г. Инструментальные средства обучения компьютерным сетям. Развёртывание на базе российского программного обеспечения / А. Г. Уймин, Г. И. Токарев // Системы управления и информационные технологии. – 2022. – № 4 (90). – С. 88–92. – DOI: 10.36622/VSTU.2022.90.4.019. – URL: https://elibrary.ru/item.asp?id=49894266 (дата обращения: 20.05.2026).

69. Уймин, А. Г. Интеллектуальный анализ динамики трёхпозиционного графического манипулятора типа "мышь" как элемента поведенческой биометрии // Системы управления и информационные технологии. – 2022. – № 2 (88). – С. 92–96. – DOI: 10.36622/VSTU.2022.88.2.018. – URL: https://elibrary.ru/item.asp?id=48558801 (дата обращения: 20.05.2026).

70. Уймин, А. Г. Классификация корпоративного трафика с использованием алгоритмов машинного обучения // Автоматизация и информатизация ТЭК. – 2023. – № 7 (600). – С. 22–29. – DOI: 10.33285/2782-604X-2023-7(600)-22-29. – URL: https://elibrary.ru/item.asp?id=54172274 (дата обращения: 20.05.2026).

71. Уймин, А. Г. Моделирование телекоммуникационной сети средствами сетевых инструментов Linux: инструменты создания цифровых двойников / А. Г. Уймин, О. Р. Никитин // i-methods. – 2023. – Т. 15, № 2. – С. 4. – EDN NFJDVH. – URL: http://intech-spb.com/wp-content/uploads/archive/2023/2/Uimin.pdf (дата обращения: 20.05.2026).

72. Уймин, А. Г. Обзор систем моделирования: анализ эффективности на примере чемпионата AtomSkills-2023 / А. Г. Уймин, В. С. Греков // Автоматизация и информатизация ТЭК. – 2023. – № 11 (604). – С. 25–34. – DOI: 10.33285/2782-604X-2023-11(604)-25-34. – URL: https://elibrary.ru/item.asp?id=54902985 (дата обращения: 20.05.2026).

73. Уймин, А. Г. Обзор средств моделирования сетевой инфраструктуры при подготовке специалистов по укрупнённым группам специальностей

09.00.00, 10.00.00 / А. Г. Уймин, Д. А. Мельников // Наука. Информатизация. Технологии. Образование : материалы XIV Междунар. науч.-практ. конф., Екатеринбург, 2021. – Екатеринбург, 2021. – С. 392–405.

74. Уймин, А. Г. Онлайн-аутентификация: предварительная обработка данных // Губкинский университет в решении вопросов нефтегазовой отрасли России : тез. докл. VI Регион. науч.-техн. конф., Москва, 19–21 сент. 2022 г. – Москва : РГУ нефти и газа им. И. М. Губкина, 2022. – С. 1146–1147. – URL: https://elibrary.ru/item.asp?id=53007316 (дата обращения: 20.05.2026).

75. Уймин, А. Г. Оценка безопасности Wine с использованием методологии STRIDE: математическая модель / А. Г. Уймин, И. М. Морозов // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2023. – № 6-2. – С. 164–170. – DOI: 10.37882/2223-2982.2023.6-2.40. – URL: https://elibrary.ru/item.asp?id=54390435 (дата обращения: 20.05.2026).

76. Уймин, А. Г. Практическое применение элементов поведенческой биометрии / А. Г. Уймин, И. М. Морозов // Обеспечение информационной безопасности: вопросы теории и практики : сб. ст. Всерос. науч.-практ. конф., Ижевск, 29 мая 2023 г. – Ижевск : Удмуртский университет, 2023. – С. 156–162. – URL: https://elibrary.ru/item.asp?id=54662260 (дата обращения: 20.05.2026).

77. Уймин, А. Г. Предобработка данных манипулятора "мышь" для использования в анализе поведенческой биометрии // Научно-технический вестник Поволжья. – 2022. – № 7. – С. 94–97. – URL: https://elibrary.ru/item.asp?id=49287252 (дата обращения: 20.05.2026).

78. Уймин, А. Г. Применение отечественного программного обеспечения для перестройки образовательного процесса вуза в рамках подготовки кадров цифровизации производства // Цифровая трансформация промышленности: новые горизонты : материалы 3-й Всерос. науч.-практ. конф., Москва, 10 нояб. 2022 г. – Москва : Русайнс, 2022. – С. 398–405. – URL: https://elibrary.ru/item.asp?id=49961491 (дата обращения: 20.05.2026).

79. Уймин, А. Г. Развитие профессиональной подготовки с учётом стандартов "WorldSkills Russia" // Вестник педагогических наук. – 2021. – № 1. – С. 42–51.

80. Уймин, А. Г. Сравнение производительности алгоритмов классификации в рамках сетевой инфраструктуры / А. Г. Уймин, О. Р. Никитин // Наукоёмкие технологии в космических исследованиях Земли. – 2023. – Т. 15, № 2. – С. 33–40. – DOI: 10.36724/2409-5419-2023-15-2-33-40. – URL: https://elibrary.ru/item.asp?id=54036953 (дата обращения: 20.05.2026).

81. Уймин, А. Г. Сравнительный анализ инструментов непрерывной онлайн-аутентификации и систем обнаружения аномалий для постоянного подтверждения личности пользователя / А. Г. Уймин, И. М. Морозов // T-Comm: Телекоммуникации и транспорт. – 2022. – Т. 16, № 5. – С. 48–55. – URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-instrumentov-nepreryvnoy-onlayn-autentifikatsii-i-sistem-obnaruzheniya-anomaliy-dlya-postoyannogo (дата обращения: 20.05.2026).

82. Уймин, А. Г. Цифровые двойники сетевых инфраструктур: точность, методы и практические решения // Радиотехнические и телекоммуникационные системы. – 2023. – № 3 (51). – С. 44–52. – DOI: 10.24412/2221-2574-2023-3-44-52. – URL: https://elibrary.ru/item.asp?id=54709845 (дата обращения: 20.05.2026).

83. Уймин, А. Г. Эмпирическая оценка методов машинного обучения в задачах онлайн-аутентификации // Вестник компьютерных и информационных технологий. – 2022. – Т. 19, № 8 (218). – С. 49–57. – DOI: 10.14489/vkit.2022.08.pp.049-057. – URL: https://elibrary.ru/item.asp?id=49345313 (дата обращения: 20.05.2026).

84. Федотов, О. В. Анализ перспективных направлений функционирования технических комплексов контроля за поведением условно осуждённых и лиц, условно-досрочно освобождённых из мест лишения свободы / О. В. Федотов [и др.] // Техника и безопасность объектов уголовно-

исполнительной системы : сб. материалов Междунар. науч.-практ. конф. – Воронеж : Воронежский институт ФСИН России, 2011. – С. 84–88.

85. Шелупанов, А. А. [и др.] Актуальные направления развития методов и средств защиты информации // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2017. – Т. 20, № 3. – С. 11–24.

86. Шеннон, К. Математическая теория связи / К. Шеннон // Работы по теории информации и кибернетике. – Москва : Изд-во иностранной литературы, 1963. – С. 243–332.

87. Шибанов, С. В. Сравнительный анализ современных методов аутентификации пользователя / С. В. Шибанов, Д. А. Карпушин // Математическое и программное обеспечение систем в промышленной и социальной сферах. – 2015. – № 1. – С. 33–37.

88. Юсупов, М. Н. Двухфакторная аутентификация // Актуальные вопросы теории и практики развития научных исследований. – 2022. – С. 180–182.

89. Ahlswede, R. [et al.] General Theory of Information Transfer and Combinatorics // Lecture Notes in Computer Science. – Berlin ; Heidelberg : Springer-Verlag, 2006. – Vol. 4123. – P. 1–45.

90. Ahlswede, R. Identification for sources / R. Ahlswede, B. Balkenhol, C. Kleinewachter // General Theory of Information Transfer and Combinatorics. – Berlin ; Heidelberg : Springer, 2006. – P. 51–61.

91. Ahmed, A. A. E. A new biometric technology based on mouse dynamics / A. A. E. Ahmed, I. Traore // IEEE Transactions on Dependable and Secure Computing. – 2007. – Vol. 4, No. 3. – P. 165–179.

92. Ahvanooey, M. T. [et al.] Modern authentication schemes in smartphones and IoT devices: An empirical survey // IEEE Internet of Things Journal. – 2021. – Vol. 9, No. 10. – P. 7639–7663.

93. Ak, T. A. [et al.] An iris recognition system using a new method of iris localization // International Journal of Open Information Technologies. – 2021. – Vol. 9, No. 7. – P. 67–76.

94. Albu, O. B. Three sides of the same coin: Datafied transparency, biometric surveillance, and algorithmic governmentalities / O. B. Albu, H. K. Hansen // Critical Analysis of Law. – 2021. – Vol. 8, No. 1. – P. 9–24.

95. Almalki, S. An empirical evaluation of online continuous authentication and anomaly detection using mouse clickstream data analysis / S. Almalki, N. Assery, K. Roy // Applied Sciences. – 2021. – Vol. 11, No. 13. – Art. 6083.

96. Alsaadi, I. M. Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review // International Journal of Science and Technology Research. – 2021. – Vol. 10, No. 1. – P. 15–21.

97. Andrean, A. Keystroke dynamics based user authentication using deep multilayer perceptron / A. Andrean, M. Jayabalan, V. Thiruchelvam // International Journal of Machine Learning and Computing. – 2020. – Vol. 10, No. 1. – P. 134–139.

98. Bah, S. M. An improved face recognition algorithm and its application in attendance management system / S. M. Bah, F. Ming // Array. – 2020. – Vol. 5. – Art. 100014.

99. Bello, R. W. [et al.] Cattle identification: the history of nose prints approach in brief // IOP Conference Series: Earth and Environmental Science. – 2020. – Vol. 594, No. 1. – Art. 012026. – DOI: 10.1088/1755-1315/594/1/012026.

100. Bharvada, K. Electronic Signatures, Biometrics and PKI in the UK // International Review of Law, Computers & Technology. – 2002. – Vol. 16, No. 3. – P. 265–275.

101. Bodepudi, A. Cloud-Based Biometric Authentication Techniques for Secure Financial Transactions: A Review / A. Bodepudi, M. Reddy // International Journal of Information and Cybersecurity. – 2020. – Vol. 4, No. 1. – P. 1–18.

102. Charumathi, N. 3D Security User Identification in Banking / N. Charumathi, N. Nithya // International Journal of Innovative Science and Research Engineering. – 2019. – Vol. 1, No. 2. – P. 72–78. – DOI: 10.5281/zenodo.2703057.

103. Chiroma, H. Deep learning algorithms-based fingerprint authentication: systematic literature review // Journal of Artificial Intelligence and Systems. – 2021. – Vol. 3, No. 1. – P. 157–197.

104. Chowdary, M. K. Deep learning-based facial emotion recognition for human-computer interaction applications / M. K. Chowdary, T. N. Nguyen, D. J. Hemanth // Neural Computing and Applications. – 2023. – Vol. 35, No. 32. – P. 23311–23328.

105. Coelho, G. G. R. Fiscal impacts of electoral abstention: a study on the electorate biometric update in Brazilian municipalities / G. G. R. Coelho, H. A. C. F. Hott, S. N. Sakurai // Local Government Studies. – 2023. – P. 1–36.

106. Cornelisse, J. No card, No Phone, No problem! Alipay: Pay with your face, A balance between convenience, security and privacy [Электронный ресурс] / J. Cornelisse // New Media M.A. Research Blog. – 2020. – 27 Sept. – URL: https://mastersofmedia.hum.uva.nl/blog/2020/09/27/no-card-no-phone-no-problem-alipay-pay-with-your-face-a-balance-between-convenience-security-and-privacy/ (дата обращения: 20.05.2026).

107. Dahia, G. Continuous authentication using biometrics: An advanced review / G. Dahia, L. Jesus, M. Pamplona Segundo // Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. – 2020. – Vol. 10, No. 4. – Art. e1365.

108. Dargan, S. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities / S. Dargan, M. Kumar // Expert Systems with Applications. – 2020. – Vol. 143. – Art. 113114. – DOI: 10.1016/j.eswa.2019.113114.

109. De Santis, A. [et al.] Continuous Entity Authentication in the Internet of Things Scenario // Applied Sciences. – 2023. – Vol. 13, No. 10. – Art. 5945.

110. Debie, E. Session invariant EEG signatures using elicitation protocol fusion and convolutional neural network / E. Debie, N. Moustafa, A. Vasilakos // IEEE Transactions on Dependable and Secure Computing. – 2021. – Vol. 19, No. 4. – P. 2488–2500.

111. Dimaratos, A. Evaluation Scheme to Analyze Keystroke Dynamics Methods / A. Dimaratos, D. Pohn // ICISSP 2023 : Proceedings of the 9th International Conference on Information Systems Security and Privacy. – 2023. – P. 357–365.

112. DiPietro, R. Deep learning: RNNs and LSTM / R. DiPietro, G. D. Hager // Handbook of Medical Image Computing and Computer Assisted Intervention. – Waltham : Academic Press, 2020. – P. 503–519.

113. Ellavarason, E. [et al.] Touch-dynamics based behavioural biometrics on mobile devices: a review from a usability and performance perspective // ACM Computing Surveys. – 2020. – Vol. 53, No. 6. – P. 1–36.

114. Ferrari, A. [et al.] On the personalization of classification models for human activity recognition // IEEE Access. – 2020. – Vol. 8. – P. 32066–32079.

115. Fisher, R. The analysis of variance with various binomial transformations // Biometrics. – 1954. – Vol. 10, No. 1. – P. 130–139.

116. Gallardo-Cava, R. [et al.] Creating Realistic Presentation Attacks for Facial Impersonation Step-by-Step // IEEE Access. – 2023. – Vol. 11. – P. 109257–109266. – DOI: 10.1109/ACCESS.2023.3313094.

117. Gama, J. [et al.] A survey on concept drift adaptation // ACM Computing Surveys. – 2014. – Vol. 46, No. 4. – P. 1–37.

118. Gamboa, H. A behavioral biometric system based on human-computer interaction / H. Gamboa, A. Fred // Biometric Technology for Human Identification : Proceedings of SPIE. – Bellingham : SPIE, 2004. – Vol. 5404. – P. 381–392.

119. Gayathri, M. A review on various biometric techniques, its features, methods, security issues and application areas / M. Gayathri, C. Malathy, M. Prabhakaran // Computational Vision and Bio-Inspired Computing: ICCVBIC 2019. – 2020. – P. 931–941.

120. Goldsack, J. C. [et al.] Verification, analytical validation, and clinical validation (V3): the foundation of determining fit-for-purpose for Biometric Monitoring Technologies (BioMeTs) // npj Digital Medicine. – 2020. – Vol. 3, No. 1. – Art. 55.

121. Gursel, Z. D. Bertillon, Ravachol and the Explosive Potential of Police Portraiture // History of Photography. – 2021. – Vol. 45, No. 3-4. – P. 245–263.

122. Haider, S. A. Enhanced multimodal biometric recognition based upon intrinsic hand biometrics / S. A. Haider, Y. Rehman, S. M. U. Ali // Electronics. – 2020. – Vol. 9, No. 11. – Art. 1916.

123. Hayashi, K. Proposal of user identification scheme using mouse / K. Hayashi, E. Okamoto, M. Mambo // Information and Communications Security : Proceedings of the 1st International Conference ICIS'97, Beijing, China, November 11-14, 1997. – Berlin ; Heidelberg : Springer, 1997. – P. 144–148.

124. Hernandez-de-Menendez, M. [et al.] Biometric applications in education // International Journal on Interactive Design and Manufacturing. – 2021. – Vol. 15. – P. 365–380.

125. Horberry, T. [et al.] Human-centered design for an in-vehicle truck driver fatigue and distraction warning system // IEEE Transactions on Intelligent Transportation Systems. – 2021. – Vol. 23, No. 6. – P. 5350–5359.

126. Hub, M. Impact of Globalization on Data Security: Authentication Issues / M. Hub, K. Prihodova // SHS Web of Conferences. – 2021. – Vol. 92. – Article 02024. – P. 1–8.

127. Jain, A. K. Biometrics: Trust, but verify / A. K. Jain, D. Deb, J. J. Engelsma // IEEE Transactions on Biometrics, Behavior, and Identity Science. – 2021. – Vol. 4, No. 3. – P. 303–323.

128. Kaul, S. D. Intelligent RFID biometric enabled dual security lock in the banking environment / S. D. Kaul, D. Hatzinakos // Journal of Banking and Financial Technology. – 2020. – Vol. 4. – P. 159–173.

129. Kaur, N. [et al.] A study of biometric identification and verification system // 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). – Piscataway : IEEE, 2021. – P. 60–64.

130. Kindt, E. A first attempt at regulating biometric data in the European Union // Regulating Biometrics: Global Approaches and Open Questions. – New York : AI Now, 2020. – P. 62–69.

131. Lee, J. W. Patenting trends in biometric technology of the Big Five patent offices / J. W. Lee, W. K. Lee, S. Y. Sohn // World Patent Information. – 2021. – Vol. 65. – Art. 102040.

132. Lietz, R. [et al.] Survey of mood detection through various input modes // Proceedings of the 12th ACM International Conference on PErvasive Technologies Related to Assistive Environments. – New York : ACM, 2019. – P. 28–31.

133. Lourenco, M. L. Usability Evaluation of Slanted Computer Mice / M. L. Lourenco, F. Lanhoso, D. A. Coelho // International Journal of Environmental Research and Public Health. – 2021. – Vol. 18, No. 8. – Art. 3854.

134. Lyon, D. Biometrics, identification and surveillance // Bioethics. – 2008. – Vol. 22, No. 9. – P. 499–508.

135. Martinek, R. [et al.] Voice communication in noisy environments in a smart house using hybrid LMS+ICA algorithm // Sensors. – 2020. – Vol. 20, No. 21. – Art. 6022.

136. Maxwell, A. Eugenics and photography in Britain, the USA and Australia 1870-1940 // Studies in History and Philosophy of Science. – 2022. – Vol. 92. – P. 71–85.

137. McGraw, G. Software Security / G. McGraw // IEEE Security & Privacy. – 2004. – Vol. 2, No. 2. – P. 80–83. – DOI: 10.1109/MSECP.2004.1281254.

138. Minaee, S. Biometrics recognition using deep learning: a survey / S. Minaee [et al.] // Artificial Intelligence Review. – 2023. – Vol. 56, No. 8. – P. 8647–8695. – DOI: 10.1007/s10462-022-10237-x.

139. North-Samardzic, A. Biometric technology and ethics: Beyond security applications // Journal of Business Ethics. – 2020. – Vol. 167, No. 3. – P. 433–450.

140. Pero, R. In the "service" of migrants: the temporary resident biometrics project and the economization of migrant labor in Canada / R. Pero, H. Smith // Geographies of Migration. – Abingdon : Routledge, 2018. – P. 191–202.

141. Prabakaran, D. Multi-factor authentication for secured financial transactions in cloud environment / D. Prabakaran, S. Ramachandran // CMC-Computers, Materials & Continua. – 2022. – Vol. 70, No. 1. – P. 1781–1798.

142. Prihodova, K. The impact of global changes on the security of password authentication / K. Prihodova, M. Hub // Globalisation and Its Socio-Economic Consequences : Proceedings of the 18th International Scientific Conference, Zilina, Slovak Republic, 2018. – Zilina, 2018. – P. 2061–2066.

143. Rahman, M. M. Identifying user authentication and most frequently used region based on mouse movement data: A machine learning approach / M. M. Rahman, S. Basak // 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). – Piscataway : IEEE, 2021. – P. 1245–1250.

144. Rashid, A. [et al.] Clicking Your Way to Security: A Review of Continuous Authentication with Mouse Dynamics // Journal of Computing Sciences in Colleges. – 2023. – Vol. 39, No. 4. – P. 39–49.

145. Ryu, R. [et al.] Continuous multimodal biometric authentication schemes: a systematic review // IEEE Access. – 2021. – Vol. 9. – P. 34541–34557.

146. Safie, S. I. Deep Learning Evaluation Using Receiver Operating Curve (ROC) for Footprint Biometric Authentication / S. I. Safie, R. Ramli, Z. Mohamad // 2022 IEEE 8th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA). – Piscataway : IEEE, 2022. – P. 26–29.

147. Saltzer, J. H. The protection of information in computer systems / J. H. Saltzer, M. D. Schroeder // Proceedings of the IEEE. – 1975. – Vol. 63, No. 9. – P. 1278–1308.

148. Sarkar, A. A review on performance, security and various biometric template protection schemes for biometric authentication systems / A. Sarkar, B. K. Singh // Multimedia Tools and Applications. – 2020. – Vol. 79. – P. 27721–27776.

149. Savukynas, R. Internet of Things information system security for smart devices identification and authentication // 2020 9th Mediterranean Conference on Embedded Computing (MECO). – Piscataway : IEEE, 2020. – P. 1–5.

150. Shopon, M. [et al.] Biometric systems de-identification: Current advancements and future directions // Journal of Cybersecurity and Privacy. – 2021. – Vol. 1, No. 3. – P. 470–495.

151. Singh, Y. N. A taxonomy of biometric system vulnerabilities and defences / Y. N. Singh, S. K. Singh // International Journal of Biometrics. – 2013. – Vol. 5, No. 2. – P. 137–159.

152. Skrypnikov, A. V. [et al.] Information security as the basis of digital economy // Russian Conference on Digital Economy and Knowledge Management (RuDEcK 2020). – Paris : Atlantis Press, 2020. – P. 149–153.

153. Stylios, I. C. [et al.] A review of continuous authentication using behavioral biometrics // Proceedings of the SouthEast European Design Automation, Computer Engineering, Computer Networks and Social Media Conference. – 2016. – P. 72–79.

154. Sudhakar, T. Cancelable biometrics using deep learning as a cloud service / T. Sudhakar, M. Gavrilova // IEEE Access. – 2020. – Vol. 8. – P. 112932–112943.

155. Sun, L. [et al.] KOLLECTOR: Detecting Fraudulent Activities on Mobile Devices Using Deep Learning // IEEE Transactions on Mobile Computing. – 2021. – Vol. 20, No. 4. – P. 1465–1476. – DOI: 10.1109/TMC.2020.2964226.

156. Sun, P. [et al.] An overview of moving object trajectory compression algorithms // Mathematical Problems in Engineering. – 2016. – Vol. 2016. – Article ID 6587309. – P. 1–13. – DOI: 10.1155/2016/6587309.

157. Teitelbaum, J. Alphonse Bertillon – Whose Legacy as a Pioneer in Criminal Identification Was Undone by Fingerprinting – May Have Solved the World's First Fingerprint Murder Case // Forensic Science Review. – 2020. – Vol. 32, No. 1. – P. 14–15.

158. Unlocking Security for Comprehensive Electroencephalogram-Based User Authentication Systems / J. A. Khalil [et al.] // Sensors. – 2024. – Vol. 24, Iss. 24. – Art. 7919.

159. Utegen, D. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models / D. Utegen, B. Z. Rakhmetov // Journal of Digital Technologies and Law. – 2023. – Vol. 1, No. 3. – P. 825–844.

160. Uymin, A. Application of machine learning in the classification of traffic in telecommunication networks: working with network modeling systems // E3S Web of Conferences. – 2023. – Vol. 402. – Art. 03001. – DOI: 10.1051/e3sconf/202340203001. – URL: https://www.e3s-conferences.org/articles/e3sconf/pdf/2023/39/e3sconf_transsiberia2023_03001.pdf (дата обращения: 20.05.2026).

161. Uymin, A. Instruments for student verification and assessment of his emotional and psychological state during remote work // Norwegian Journal of Development of the International Science. – 2022. – No. 96. – P. 98–101. – DOI: 10.5281/zenodo.7327249. – URL: https://elibrary.ru/item.asp?id=49826778 (дата обращения: 20.05.2026).

162. Uymin, A. Preprocessing data from the mouse manipulator for use in behavioral biometrics analysis // Norwegian Journal of Development of the International Science. – 2022. – No. 85. – P. 53–58.

163. Walter, M. Per-Session Security: Password-Based Cryptography Revisited / M. Walter [et al.] // Journal of Computer Security. – 2019. – Vol. 27, No. 1. – P. 75–111.

164. Wang, C. [et al.] A framework for behavioral biometric authentication using deep metric learning on mobile devices // IEEE Transactions on Mobile Computing. – 2021. – Vol. 22, No. 1. – P. 19–36.

165. Wang, M. Deep face recognition: A survey / M. Wang, W. Deng // Neurocomputing. – 2021. – Vol. 429. – P. 215–244.

166. Watt, D. [et al.] Forensic phonetics and automatic speaker recognition // The Routledge Handbook of Forensic Linguistics. – Abingdon : Routledge, 2020. – P. 400–415.

167. Yadav, B. P. [et al.] A Coherent and Privacy-Protecting Biometric Authentication Strategy in Cloud Computing // IOP Conference Series: Materials Science and Engineering. – 2020. – Vol. 981, No. 2. – Art. 022043.

168. Yang, W. [et al.] Biometrics for internet-of-things security: A review // Sensors. – 2021. – Vol. 21, No. 18. – Art. 6163.

169. Yang, X. Adversarial Attacks on Face Recognition / X. Yang, J. Zhu // Handbook of Face Recognition. – Cham : Springer International Publishing, 2023. – P. 387–404.

170. Zou, Z. Evaluating the effectiveness of biometric sensors and their signal features for classifying human experience in virtual environments / Z. Zou, S. Ergan // Advanced Engineering Informatics. – 2021. – Vol. 49. – Art. 101358.

Интернет-ресурсы

171. Производители биометрических систем [Электронный ресурс] // Био-профиль. – URL: https://biometricheskayasistema.rf/katalog/brands.html (дата обращения: 20.05.2026).

172. Breaking down the cost barrier with enhanced low-cost sensor technology and biometric-system-on-chip ASIC [Электронный ресурс] / IDEX Biometrics. – URL: https://www.idexbiometrics.com/breaking-down-the-cost-barrier-with-enhanced-low-cost-sensor-technology-and-biometric-system-on-chip-asic/ (дата обращения: 20.05.2026).

173. CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions [Электронный ресурс] / The MITRE Corporation. – URL: https://capec.mitre.org/data/definitions/29.html (дата обращения: 20.05.2026).

174. CAPEC-60: Reusing Session IDs (aka Session Replay) [Электронный ресурс] / The MITRE Corporation. – URL: https://capec.mitre.org/data/definitions/60.html (дата обращения: 20.05.2026).

175. CAPEC-61: Session Fixation [Электронный ресурс] / The MITRE Corporation. – URL: https://capec.mitre.org/data/definitions/61.html (дата обращения: 20.05.2026).

176. CAPEC-121: Privilege Abuse / Exploiting Debug Interfaces [Электронный ресурс] / The MITRE Corporation. – URL: https://capec.mitre.org/data/definitions/121.html (дата обращения: 20.05.2026).

177. CAPEC-226: Session Credential Falsification through Manipulation [Электронный ресурс] / The MITRE Corporation. – URL: https://capec.mitre.org/data/definitions/226.html (дата обращения: 20.05.2026).

178. CAPEC-593: Session Hijacking [Электронный ресурс] / The MITRE Corporation. – URL: https://capec.mitre.org/data/definitions/593.html (дата обращения: 20.05.2026).

179. History of Biometrics [Электронный ресурс] / Biometric Update. – URL: https://www.biometricupdate.com/201802/history-of-biometrics-2 (дата обращения: 20.05.2026).

180. Mobey Forum. Biometrics Survey Results [Электронный ресурс]. – URL: https://mobeyforum.org/biometrics-survey-results/ (дата обращения: 20.05.2026).

181. Total biometrics market to reach $127B by 2030, report forecasts [Электронный ресурс] / Biometric Update. – URL: https://www.biometricupdate.com/202203/total-biometrics-market-to-reach-127b-by-2030-report-forecasts (дата обращения: 20.05.2026).

Патенты и свидетельства о государственной регистрации программ для ЭВМ

182. Программная модель-симулятор сетевой инфраструктуры для обучения студентов ВПО и СПО по компетенции 39 «Системное и сетевое администрирование» WorldSkills : свидетельство о государственной регистрации программы для ЭВМ № 2021614613 Рос. Федерация / А. Г. Уймин ; заявка № 2021613770 ; заявл. 24.03.2021 ; зарегистр. 26.03.2021. – URL: https://www.fips.ru/registers-doc-

view/fips_servlet?DB=EVM&DocNumber=2021614613&TypeFile=html (дата обращения: 20.05.2026).

183. Программный интерфейс взаимодействия участников соревнований WorldSkills по компетенции 39 «Системное и сетевое администрирование» с удаленной сетевой инфраструктурой : свидетельство о государственной регистрации программы для ЭВМ № 2021614735 Рос. Федерация / А. Г. Уймин, М. М. Агафонова, Д. А. Шерунтаев, М. И. Костарев ; заявка № 2021613729 ; заявл. 24.03.2021 ; зарегистр. 29.03.2021. – URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=EVM&DocNumber=2021614735&TypeFile=html (дата обращения: 20.05.2026).

184. Программный модуль-тренажер подготовки к демонстрационному экзамену профессионального мастерства для обучения студентов СПО по специальности «Системное и сетевое администрирование» : свидетельство о государственной регистрации программы для ЭВМ № 2021614803 Рос. Федерация / А. Г. Уймин, В. О. Антонов, Д. А. Шерунтаев, М. М. Агафонова ; заявка № 2021613749 ; заявл. 24.03.2021 ; зарегистр. 30.03.2021. – URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=EVM&DocNumber=2021614803&TypeFile=html (дата обращения: 20.05.2026).

185. Способ защиты информации, принимаемой по проводным каналам связи, и система для его осуществления : пат. 2112319 Рос. Федерация / Э. И. Абалмазов [и др.] ; заявка № 97117276 ; заявл. 29.10.1997 ; опубл. 27.05.1998. – URL: https://patents.google.com/patent/RU2112319C1/ru (дата обращения: 20.05.2026).

186. Remote Topology extensions: клиент-серверное браузерное расширение, обеспечивающее отслеживание действий пользователя с целью проведения биометрической аутентификации : свидетельство о государственной регистрации программы для ЭВМ № 2023683139 Рос. Федерация / А. Г. Уймин ; заявка № 2023682110 ; заявл. 25.10.2023 ; опубл.

02.11.2023. – URL: https://fips.ru/EGD/10dd8ffc-2575-4667-a30b-a86cec846507 (дата обращения: 20.05.2026).

187. RemoteTopology-Администрирование : свидетельство о государственной регистрации программы для ЭВМ № 2021615378 Рос. Федерация / А. Г. Уймин ; заявка № 2021614090 ; заявл. 16.03.2021 ; зарегистр. 07.04.2021 ; опубл. 07.04.2021, Бюл. № 4. – 252 КБ. – URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=EVM&DocNumber=2021615378&TypeFile=html (дата обращения: 20.05.2026).

188. RemoteTopology-Интерфейс пользователя : свидетельство о государственной регистрации программы для ЭВМ № 2021661218 Рос. Федерация / А. Г. Уймин, Л. М. Черкашин ; заявка № 2021613953 ; заявл. 16.03.2021 ; зарегистр. 07.07.2021 ; опубл. 07.07.2021, Бюл. № 7. – 138 КБ. – URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=EVM&DocNumber=2021661218&TypeFile=html (дата обращения: 20.05.2026).

189. RemoteTopology-модуль авторизации : свидетельство о государственной регистрации программы для ЭВМ № 2021619990 Рос. Федерация / А. Г. Уймин, С. В. Любкин ; заявка № 2021613424 ; заявл. 09.03.2021 ; опубл. 21.06.2021. – URL: https://www.fips.ru/registers-doc-view/fips_servlet?DB=EVM&DocNumber=2021619990&TypeFile=html (дата обращения: 20.05.2026).

Приложение А Свидетельства о регистрации программы для ЭВМ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2023683139

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2023683139
Дата регистрации: **02.11.2023**
Номер и дата поступления заявки:
2023682110 25.10.2023
Дата публикации и номер бюллетеня:
02.11.2023 Бюл. № 11
Контактные реквизиты:
au-mail@ya.ru, +7(950)6320438

Автор(ы):
Уймин Антон Григорьевич (RU)
Правообладатель(и):
Уймин Антон Григорьевич (RU)

Название программы для ЭВМ:
Remote Topology extensions: Клиент-серверное браузерное расширение, обеспечивающие отслеживание действий пользователя с целью проведения биометрической аутентификации

Реферат:
Программа представляет собой реализацию алгоритма сбора данных о действиях пользователя в рамках браузера. Программа состоит из двух компонентов: клиента и сервера. 1. Функционал клиента: отправлять данные о текущих манипуляция пользователя внутри браузера. К таким данным относятся: движение мыши, нажатия на кнопки и переход на другие страницы. Кроме того, клиентская часть приложения имеет функционал перехвата определённых данных о трафике пользователя и перенаправление его на удаленный сервер. 2. Функционал сервера: принимать данные от клиентской части, обрабатывать их в соответствии с заложенным алгоритмом. Тип ЭВМ: IBM PC-совмест. ПК. ОС: ОС семейства MS Windows x32/64, ОС семейства Linux, ОС семейства UNIX.

Язык программирования: Python v.3.10, ECMAScript 2018, Html 5, Css 3, SQL

Объем программы для ЭВМ: 1 МБ

Стр.: 1

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2021614613

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2021614613
Дата регистрации: **26.03.2021**
Номер и дата поступления заявки:
2021613770 24.03.2021
Дата публикации и номер бюллетеня:
26.03.2021 Бюл. № 4

Автор(ы):
Уймин Антон Григорьевич (RU)
Правообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (RU)

Название программы для ЭВМ:
Программная модель-симулятор сетевой инфраструктуры для обучения студентов ВПО и СПО по компетенции 39 «Системное и сетевое администрирование» WorldSkills

Реферат:
Данная программная разработка представляет собой симулятор, позволяющий проводить занятия с целью обучения профессиональному мастерству студентов СПО и ВПО по компетенции WorldSkills 39 «Системное и сетевое администрирование» в условиях, максимально приближенных к реальным. Возможность удаленного доступа к единому серверному оборудованию позволяет обучать одновременно большое количество студентов без высоких требований к оборудованию в учебных заведениях. Тип ЭВМ: IBM PC-совмест. ПК; ОС: семейства MS Windows x32/64.

Язык программирования: PHP

Объем программы для ЭВМ: 27884 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2021614735

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2021614735
Дата регистрации: **29.03.2021**
Номер и дата поступления заявки:
2021613729 24.03.2021
Дата публикации и номер бюллетеня:
29.03.2021 Бюл. № 4

Автор(ы):
Уймин Антон Григорьевич (RU),
Агафонова Мария Михайловна (RU),
Шерунтаев Денис Александрович (RU),
Костарев Матвей Иванович (RU)
Правообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (RU)

Название программы для ЭВМ:
Программный интерфейс взаимодействия участников соревнований WorldSkills по компетенции 39 «Системное и сетевое администрирование» с удаленной сетевой инфраструктурой

Реферат:
Программа представляет собой платформу обеспечения доступа к удаленной модели сетевой инфраструктуры по протоколам TCP/IP. Служит для обеспечения проведения соревнований WorldSkills на удаленной платформе по компетенции 39 «Системное и сетевое администрирование» среди студентов СПО и ВПО. Тип ЭВМ: IBM PC-совмест. ПК. ОС: семейство Windows x32/64.

Язык программирования: PHP

Объем программы для ЭВМ: 20864 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2021614803

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2021614803
Дата регистрации: **30.03.2021**
Номер и дата поступления заявки:
2021613749 24.03.2021
Дата публикации и номер бюллетеня:
30.03.2021 Бюл. № 4

Автор(ы):
Уймин Антон Григорьевич (RU),
Антонов Вячеслав Олегович (RU),
Шерунтаев Денис Александрович (RU),
Агафонова Мария Михайловна (RU)

Правообладатель(и):
Федеральное государственное бюджетное образовательное учреждение высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (RU)

Название программы для ЭВМ:
Программный модуль-тренажер подготовки к демонстрационному экзамену профессионального мастерства для обучения студентов СПО по специальности «Системное и сетевое администрирование»

Реферат:
Данная программная разработка представляет собой тренажер, позволяющий проводить занятия с целью подготовки к демонстрационному экзамену студентов СПО по специальности «Системное и сетевое администрирование» в условиях, максимально приближенных к реальным. Тип ЭВМ: IBM PC-совмест. ПК; ОС: Windows x32/64.

Язык программирования: C#

Объем программы для ЭВМ: 23145 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2021615378

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2021615378
Дата регистрации: **07.04.2021**
Номер и дата поступления заявки:
2021614090 16.03.2021
Дата публикации и номер бюллетеня:
07.04.2021 Бюл. № 4
Контактные реквизиты:
au-mail@ya.ru

Автор(ы):
Уймин Антон Григорьевич (RU)
Правообладатель(и):
Уймин Антон Григорьевич (RU)

Название программы для ЭВМ:
RemoteTopology-Администрирование

Реферат:
Программа обеспечивает дистанционную работу с сетевыми устройствами: реальными, виртуальными. Программа предназначена для: создания сетевых устройств; добавления названия устройствам; создания связей между сетевыми устройствами; перемещения по рабочей области; масштабирования рабочей области с возможностью перехода к центру топологии; сохранения топологии в базу данных. Интерфейс администратора позволяет: создавать и редактировать данные пользователей (их имена, группы и чемпионаты); редактировать стенды (назначать их пользователям, изменять данные для подключения); добавлять пользователи и стенды группами с помощью CSV-файлов.

Язык программирования: Golang, JavaScript

Объем программы для ЭВМ: 252 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2021619990

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2021619990
Дата регистрации: **21.06.2021**
Номер и дата поступления заявки:
2021613424 09.03.2021
Дата публикации и номер бюллетеня:
21.06.2021 Бюл. № 7
Контактные реквизиты:
телефон: 89506320438 email: au-mail@ya.ru
telegram: @au_team

Автор(ы):
Уймин Антон Григорьевич (RU),
Любкин Сергей Васильевич (RU)
Правообладатель(и):
Уймин Антон Григорьевич (RU),
Любкин Сергей Васильевич (RU)

Название программы для ЭВМ:
RemoteTopology-модуль авторизации

Реферат:
Программа является частью проекта RemoteTopology, предназначена для регистрации и авторизации на ресурс. Функциональные возможности: автоматическая генерация ключей доступа для обеспечения безопасности; форма регистрации, содержащая email, ФИО и уникальный пароль пользователя.

Язык программирования: Golang, JavaScript

Объем программы для ЭВМ: 234 КБ

РОССИЙСКАЯ ФЕДЕРАЦИЯ

RU2021661218

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2021661218
Дата регистрации: **07.07.2021**
Номер и дата поступления заявки:
2021613953 16.03.2021
Дата публикации и номер бюллетеня:
07.07.2021 Бюл. № 7
Контактные реквизиты:
79506320438, au-mail@ya.ru

Автор(ы):
Уймин Антон Григорьевич (RU),
Черкашин Лев Михайлович (RU)
Правообладатель(и):
Уймин Антон Григорьевич (RU),
Черкашин Лев Михайлович (RU)

Название программы для ЭВМ:
RemoteTopology-Интерфейс пользователя

Реферат:
Визуальный интерфейс отображает список выпадающих меню чемпионатов, в которых содержатся модули. Количество модулей зависит от задания данного чемпионата. При нажатии на модуль отправляется запрос на программно-аппаратную часть, которая возвращает структуру топологии, а визуальный интерфейс перенаправляет пользователя на топологию. Топология содержит в себе: изображения сетевых устройств, таких как персональные компьютеры, коммутаторы, маршрутизаторы, сервера и т.д.; названия сетевых устройств; информации о связях между сетевыми устройствами.

Язык программирования: Golang, JS

Объем программы для ЭВМ: 138 КБ

Приложение Б Акты о внедрении

КОНСИСТ-ОС
РОСАТОМ
ОРГАНИЗАЦИЯ АО «КОНЦЕРН РОСЭНЕРГОАТОМ»
Акционерное общество
«КОНСИСТ – ОПЕРАТОР СВЯЗИ»
(АО «КОНСИСТ-ОС»)
Проектируемый проезд № 4062, д. 6, стр. 25,
Москва, 115432
Телефон/факс (499) 951-20-35
E-mail: info@consyst-os.ru
ОКПО 16990772, ОГРН 1027739236920
ИНН 7711077412, КПП 772501001

14.04.2022 № _____

На № _____ от _____

АКТ
Об использовании результатов научно-исследовательской работы
Уймина А.Г. программный продукт
«RemoteTopology-Администрирование» рег. номер №2021615378

Следующие результаты, полученные в научно-исследовательской работе Уймина А.Г., использованы в работах по обеспечению проведения VI дивизионального чемпионата профессионального мастерства «REASkills-2022» по компетенции «Сетевое и системное администрирование». Участие в чемпионате приняли ведущие специалисты: Белоярской АЭС, Нововоронежской АЭС, Курской АЭС и Центрального аппарата КОНСИСТ-ОС. Чемпионат прошел на базе ЦОД «Калининский» Тверская область, Удомельский городской округ, территория опорного ЦОД АО «Концерн Росэнергоатом»:

1. Разработанное программное обеспечение позволило обеспечить организацию непрерывной аутентификации пользователей системы, с отслеживанием паттернов работы;
2. Разработанные алгоритмы позволили в режиме реального времени отслеживать соответствие заявленного пользователя фактическому участнику, обеспечивать динамическое Администрирование пользователей;
3. Разработанные методики проведения дистанционной работы с использованием удаленной инфраструктуры позволили снизить технические требования к конечным площадкам проведения с сохранением заявленного уровня безопасности и управляемости инфраструктурой.

Руководитель управления по разработке государственной облачной платформы — М.А. Афанасьев

АО «КОНСИСТ-ОС» Для кадровых документов

Министерство образования и науки Хабаровского края

Краевое государственное автономное образовательное учреждение дополнительного профессионального образования

«ХАБАРОВСКИЙ КРАЕВОЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ» (КГАОУ ДПО ХК ИРО)

Уймину А.Г.

СПРАВКА

25.03.2022 № 10

г. Хабаровск

Об использовании результатов научно-исследовательской работы Уймина А.Г. программный продукт «RemoteTopology-модуль авторизации» рег. номер №2021619990

Следующие результаты, полученные в научно-исследовательской работе Уймина А.Г., использованы в работах по обеспечению проведения Asia-Pacific Best Practice Marathon (Марафона лучших практик на базе Хабаровского края с участием стран АТР и СНГ) по компетенции «Сетевое и системное администрирование» с участием:

Francisk Skorina Gomel State University	Belarus
WorldSkills Malaysia	Malaysia
Iran Technical and Vocational Training Organization (TVTO)	Iran
IT Team Services	India
Studying at Computics Lab	India
Khabarovsk Technical School of Technosphere Safety and Industrial Technologies	Russia
Komsomolsk-on-Amur College of Technologies and Services	Russia
Xiamen City University	China
Xiamen Technical College	China
Xiamen Nanyang College	China
Moscow Industrial College	Russia
Greenatom	Russia

Марафон прошел на базе краевого государственного автономного образовательного учреждения дополнительного профессионального образования «Хабаровский краевой институт развития образования»:

1. разработанное программное обеспечение позволило обеспечить организацию безопасного доступа к удаленной инфраструктуре;
2. разработанные алгоритмы позволили в режиме реального времени отслеживать соответствие заявленного пользователя фактическому

000367 ❄ Х. к. т. 2020 г. Зак. 2157. Тираж 1000 экз.

участнику; отсутствие интеграции неавторизованных сессий и сеансов в поток передачи данных;

3. разработанные методики проведения дистанционной работы с использованием удаленной инфраструктуры позволили снизить технические требования к конечным площадкам проведения с сохранением заявленного уровня безопасности.

Ректор Е.В. Гузман

Нестеренко Мария Сергеевна
46 14 18

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО
ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ (РИНХ)»
**ФАКУЛЬТЕТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
ул. Б.Садовая,69 ауд. 305
г. Ростов-на-Дону, 344002
тел. 8(863)240-24-92
e-mail: dianadekanat@yandex.ru

26.09.2024 № 22.05.02-25

АКТ об использовании результатов диссертационной работы Уймина А.Г. на тему «Система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши»

Настоящим актом подтверждается использование результатов диссертационной работы Уймина Антона Григорьевича на факультете Компьютерных технологий и информационной безопасности Ростовского государственного экономического университета (РИНХ).

В ходе диссертационного исследования разработана система биометрической идентификации, использующая данные о движениях компьютерной мыши для распознавания пользователей, основанная на методах цифровой обработки сигналов и машинного обучения, позволяющая эффективно выделять и анализировать уникальные паттерны поведения пользователей. Разработчик Уймин А.Г., старший преподаватель РГУ нефти и газа им. И.М. Губкина.

Система применена в учебном процессе кафедры информационных систем и прикладной информатики факультета компьютерных технологий и информационной безопасности для проведения текущей аттестации студентов бакалавриата по дисциплине «Инфокоммуникационные системы, сети и технологии».

Декан факультета КТ и ИБ Е.Н. Тищенко

Заведующий кафедрой ИС и ПИ С.М. Щербаков

ПЕРВОЕ ВЫСШЕЕ ТЕХНИЧЕСКОЕ УЧЕБНОЕ ЗАВЕДЕНИЕ РОССИИ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
САНКТ-ПЕТЕРБУРГСКИЙ ГОРНЫЙ УНИВЕРСИТЕТ ИМПЕРАТРИЦЫ ЕКАТЕРИНЫ II

"УТВЕРЖДАЮ"
Проректор по образовательной деятельности
_____Д.Г. Петраков
"25" 09 2024 г.

А К Т

о внедрении результатов диссертационной работы в учебный процесс

Настоящий акт составлен об использовании в учебном процессе разработки системы непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши.
(наименование разработки, объекта внедрения)

Разработка использована в учебном процессе института базового инженерного образования кафедры информационных систем и вычислительной техники и внедрена в учебный процесс 18.06.2024
(факультета, кафедры, время внедрения)

при выполнении практических работ по дисциплинам "Надежность информационных систем" и "Вычислительные системы", выполнении курсовой работы по дисциплине "Инструментальные средства информационных систем"
(подготовке / выполнении лабораторных, курсовых, дипломных работ, методик, обучающих программ, текстов лекций, учебников, кандидатских или докторских диссертаций[т] и т.д.)

и позволяет использовать разработанную технологию при изучении, проектировании и поддержке локальных вычислительных сетей.
(указать эффективность внедрения)

Описание объекта внедрения прилагается (на обороте) и является неотъемлемой частью Акта.

Директор института
базового инженерного образования _____А.Б. Маховиков
(подпись, фамилия)

Заведущий кафедрой ИСиВТ _____Е.Б. Мазаков
(подпись, фамилия)

Сотрудники, использующие разработку _____И.Г. Анкудинов
(подписи, фамилии)
_____О.Б. Соколов
(подписи, фамилии)
_____В.Е. Жуковский
(подписи, фамилии)

Описание объекта внедрения

Система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши.
(наименование разработки)

1. Краткая характеристика объекта внедрения и его назначения.

Результатом выполнения проекта является разработка и внедрение системы биометрической идентификации, использующей данные о движениях компьютерной мыши для распознавания пользователей. Система основана на методах цифровой обработки сигналов и машинного обучения, что позволяет эффективно выделять и анализировать уникальные паттерны поведения пользователей. Внедрение данной системы в учебный процесс позволяет принимать экзамены и проводить оценочные мероприятия дистанционно, обеспечивая высокую степень уверенности в том, что студент выполняет задания самостоятельно, и исключая возможность выполнения работы посторонними лицами. Кроме того, использование системы способствует улучшению практических навыков студентов в области информационной безопасности и биометрических технологий.

2. Разработчики:

Уймин А.Г., старший преподаватель РГУ нефти и газа им. И.М.Губкина
(фамилии, инициалы, должности и места работы разработчиков объекта внедрения)

3. Сотрудники, использующие разработку:

Анкудинов И.Г., доцент Санкт-Петербургского горного университета императрицы Екатерины II

Соколов О.Б., доцент Санкт-Петербургского горного университета императрицы Екатерины II

Жуковский В.Е. старший преподаватель Санкт-Петербургского горного университета императрицы Екатерины II
(фамилии, инициалы, должности сотрудников, использующих разработку в учебном процессе)

4. Начало использования объекта внедрения 18.06.2024
(месяц, год)

5. Число студентов (аспирантов, докторантов), пользующихся разработкой 48 студентов и 27 магистрантов

6. Дата и номер протокола заседания кафедры, на котором разработка рекомендована к внедрению в учебный процесс протокол № от 18.04.2023

Заведующий кафедрой ИСиВТ _____ Мазаков Е.Б.
(подпись, фамилия)

Разработчик _____ Уймин А.Г.
(подпись, фамилия)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКИЙ ГОРНО - МЕТАЛЛУРГИЧЕСКИЙ ИНСТИТУТ (ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ)»

«ЦÆГАТ КАВКАЗАГ ХÆХХОН - МЕТАЛЛУРГОН ИНСТИТУТ (ПАДДЗАХАДОН ТЕХНОЛОГОН УНИВЕРСИТЕТ)»

ул.Николаева, д.44, г.Владикавказ, Республика Северная Осетия-Алания, 362021, ОКПО 02069601, ОГРН 1031500350111,
ИНН 1501002522, тел.: (8672) 407-101 факс: (8672) 407-203 E-mail: info@skgmi-gtu.ru http://www.skgmi-gtu.ru

20.09.24 №2024-4/11
на № _____ от _____

АКТ

об использовании результатов диссертационной работы Уймина А.Г. «Система непрерывно-дискретной биометрической идентификации на основе анализа потока данных компьютерной мыши»

Настоящим актом подтверждается использование результатов диссертационной работы УЙМИНА Антона Григорьевича в ФГБОУ ВО «Северо-Кавказский горно-металлургический институт (государственный технологический университет)». Пилотирование системы идентификации пользователей проходило в целях осуществления дополнительного контроля в процедуре прокторинга обучающихся (на основе анализа потока данных компьютерной мыши) в сервисе оценки качества знаний Электронной информационно-образовательной среды вуза ФГБОУ ВО «СКГМИ (ГТУ)» (https://my.skgmi-gtu.ru).

Разработчик системы: Уймин А.Г., старший преподаватель РГУ нефти и газа им. И.М. Губкина.

Проректор по информатизации и цифровому развитию,
кандидат технических наук, доцент А.Г. Моураов

Исп. Бурдунова С. Э.
+7 8672 407-638

МІНІСТЭРСТВА АДУКАЦЫІ РЭСПУБЛІКІ БЕЛАРУСЬ

Установа адукацыі
«ГОМЕЛЬСКІ ДЗЯРЖАЎНЫ ЎНІВЕРСІТЭТ імя ФРАНЦЫСКА СКАРЫНЫ»

вул. Савецкая, 104, 246028, г. Гомель
Тэл. +(375 232) 51 00 73
Fax +(375 232) 51 00 71
official@mail.gsu.by
р/р BY31AKBB36329000001903000000
BY19AKBB36049000005223000000
ААТ «ААБ Беларусбанк»
БІК AKBBBY2X УНП 400011099

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«ГОМЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени ФРАНЦИСКА СКОРИНЫ»

ул. Советская, 104, 246028, г. Гомель
Тел. +(375 232) 51 00 73
Fax +(375 232) 51 00 71
official@mail.gsu.by
р/с BY31AKBB36329000001903000000
BY19AKBB36049000005223000000
ОАО «АСБ Беларусбанк»
БИК AKBBBY2X УНП 400011099

23.09.2024 № 10.39-20/6402

На от

Ректору РГУ нефти и газа (НИУ)
имени И.М. Губкина, профессору
Мартынову В.Г.

Ленинский проспект, д. 65
119991, г. Москва

Об использовании результатов
диссертационной работы

Настоящим письмом подтверждаем использование результатов диссертационной работы Уймина Антона Григорьевича старшего преподавателя РГУ нефти и газа (НИУ) имени И.М. Губкина в учреждении образования «Гомельский государственный университет имени Франциска Скорины».

Проректор по учебной работе Ю.В.Никитюк

10.39 Воруев 50 38 55
23.09.2024 Письма

Зак. 2057-10000