МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Распознавание голосовых команд в информационных системах»

Исполнитель _____ Подолян Егор Юрьевич

(подпись) (фамилия, имя, отчество)

Руководитель _____ Переспелов Анатолий Витальевич

(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____ Лепешкин Олег Михайлович

(подпись) (фамилия, имя, отчество)

«_____» _____2026 г.

Санкт-Петербург

2026

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ Лепешкин Олег Михайлович

(подпись) (фамилия, имя, отчество)

«_____»_____ 20__ года

Задание

на выпускную квалификационную работу

студенту: Подоляну Егору Юрьевичу

(фамилия, имя, отчество)

1. Тема Распознавание голосовых команд в информационных системах

закреплена приказом ректора Университета от «___» _____20___ года, № _____

2. Срок сдачи законченной работы «___» _____20___ года

3. Исходные данные к выпускной квалификационной работе:

_____

4. Перечень вопросов, подлежащих разработке (краткое содержание работы:

Введение: Актуальность темы, цели и задачи ВКР

Глава 1 Анализ технологий распознавания речи и методов поведенческой идентификации

_____

(наименование главы)

Глава 2 Разработка модели угроз и формализация требований к защищенной системе голосового управления

(наименование главы)

Глава 3 Проектирование архитектуры системы идентификации по поведенческим признакам

(наименование главы)

Заключение: Выводы по работе в целом. Дальнейшие пути развития

5. Перечень материалов, представляемых к защите:

- Пояснительная записка;

6. Дата выдачи задания: «___» _____ 20___ года

Руководитель выпускной квалификационной работы

Переспелов Анаталий Витальевич _____

(фамилия, имя, отчество) (подпись)

Задание принял к исполнению «___»_____20___ года

Студент Подолян Егор Юрьевич _____

(фамилия, имя, отчество, учебная группа) (подпись)

РЕФЕРАТ

Дипломная работа: ___ с., ___ рис., ___ табл., ___ источников литературы.

РАСПОЗНАВАНИЕ ГОЛОСОВЫХ СИГНАЛОВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ.

Объект исследования - системы голосового управления в корпоративных информационных системах и системах управления доступом.

Предмет исследования - методы и средства биометрической идентификации пользователя на основе поведенческих признаков в речевом сигнале.

Цель исследования - разработка архитектурной модели системы распознавания голосовых команд с двухфакторной биометрической верификацией для повышения безопасности информационных систем.

Задачи исследования:

1. Провести анализ угроз безопасности и исследовать методы поведенческой идентификации по голосу.
2. Проанализировать нормативно-правовую базу РФ в области обработки биометрических данных.
3. Разработать модель угроз и формализовать требования к системе безопасности.
4. Спроектировать архитектуру и алгоритмическое ядро системы, интегрирующей распознавание команд и поведенческую верификацию.
5. Оценить эффективность предложенной модели и сформулировать рекомендации по ее практическому применению.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современный этап цифровизации экономики и социальной сферы Российской Федерации характеризуется повсеместным внедрением интеллектуальных систем управления и человеко-машинных интерфейсов. Голосовое управление, как один из наиболее естественных и эффективных способов взаимодействия, находит применение в критически важных областях: от систем «умного» дома и корпоративных информационных систем до элементов управления объектами критической информационной инфраструктуры. Однако интеграция голосовых технологий в ответственные контуры управления порождает комплекс серьёзных угроз информационной безопасности. Традиционные системы, ориентированные исключительно на распознавание семантики команды, остаются уязвимыми к атакам на подмену диктора, что создаёт риски несанкционированного доступа и реализации противоправных действий в информационной среде.

Актуальность настоящего исследования обусловлена необходимостью преодоления ключевого противоречия: между растущим удобством голосового управления и требуемым уровнем доверия к субъекту, отдающему команду. Стандартные методы голосовой биометрии, основанные на анализе статических спектральных характеристик (отпечатка голоса), демонстрируют растущую уязвимость перед современными методами речевого спуфинга, включая синтез речи и технологии глубокого фейка. В этой связи перспективным направлением представляется усиление процедуры верификации за счёт анализа поведенческих, или динамических, признаков, присущих манере речи конкретного пользователя. Эти признаки, такие как индивидуальные просодические паттерны, лексико-стилистические привычки и контекстные модели поведения, сложнее для целенаправленной имитации и могут служить дополнительным устойчивым фактором идентификации.

Целью данной выпускной квалификационной работы является разработка архитектурной модели системы распознавания голосовых команд с интегрированным механизмом многофакторной биометрической верификации, основанной на анализе как статических, так и поведенческих признаков голоса, для повышения безопасности информационных систем. Достижение поставленной цели требует последовательного решения ряда задач. В первую очередь необходимо провести аналитическое исследование современных систем распознавания речи и существующих угроз их безопасности, а также детально изучить теоретические основы и практические методы поведенческой идентификации по голосу. Во-вторых, требуется проанализировать действующую нормативно-правовую базу Российской Федерации, регламентирующую использование биометрических данных и обеспечение защиты информации. На основе этого анализа предстоит формализовать модель угроз и сформулировать комплекс требований к безопасности проектируемой системы. Ключевой задачей является непосредственное проектирование архитектуры системы, включая описание логики взаимодействия модулей распознавания команд, извлечения статических и поведенческих признаков, а также принятия решений. Завершающим этапом станет определение методики и критериев для оценки эффективности и безопасности предложенного решения.

Объектом исследования выступают процессы биометрической аутентификации и управления в информационных системах с использованием голосовых команд. Предметом исследования являются методы и модели идентификации пользователя на основе поведенческих признаков, проявляющихся в речевом канале.

Научная новизна работы заключается в систематизации поведенческих признаков голоса применительно к задачам контроля доступа в информационных системах и в разработке на этой основе концепции двухфакторной голосовой верификации, сочетающей проверку «что сказано»

и «как сказано». Практическая значимость результатов состоит в том, что разработанная модель может служить концептуальной основой для создания защищённых голосовых интерфейсов, соответствующих требованиям российских стандартов и регуляторов в области защиты информации, включая ФСТЭК России, и применимых, в том числе, для систем, обрабатывающих информацию ограниченного доступа.

Теоретической и методологической базой исследования послужили труды отечественных и зарубежных специалистов в области речевых технологий и биометрии, материалы научных конференций, а также положения ключевых нормативных документов: Федеральных законов №152-ФЗ и №187-ФЗ, стандартов серии ГОСТ Р ИСО/МЭК 27000 и ГОСТ Р 57580-2017, методических документов ФСТЭК России.

Структура работы отражает логику проведённого исследования. Работа состоит из введения, трёх основных глав, заключения, списка использованных источников и приложений. Первая глава посвящена аналитическому обзору технологий и угроз. Во второй главе осуществляется моделирование угроз и формирование требований. Третья глава содержит проектирование архитектуры системы. В заключении подводятся итоги и формулируются основные выводы.

ГЛАВА 1. АНАЛИТИЧЕСКОЕ ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ РАСПОЗНАВАНИЯ РЕЧИ И МЕТОДОВ ПОВЕДЕНЧЕСКОЙ ИДЕНТИФИКАЦИИ

1.1. Технологии распознавания голосовых команд и актуальные угрозы информационной безопасности

Современный этап развития информационных систем характеризуется активной интеграцией речевых интерфейсов, что обусловлено стремлением к естественности человеко-машинного взаимодействия и повышению оперативности управления. Системы распознавания голосовых команд (СРГК) нашли применение в широком спектре областей — от пользовательских мобильных приложений и «умного» дома до корпоративных систем управления технологическими процессами и элементами критической информационной инфраструктуры. Исторически развитие технологий распознавания речи прошло путь от статистических методов, основанных на скрытых марковских моделях, до современных нейросетевых архитектур, включая глубокие рекуррентные сети и трансформеры. Ключевым трендом стало распространение end-to-end моделей, таких как DeepSpeech от Mozilla или Whisper от OpenAI, которые минимизируют количество этапов предобработки, напрямую преобразуя акустический сигнал в текстовую последовательность. В Российской Федерации также ведется активная разработка в данной области; среди заметных решений можно выделить платформу SOVA.speech от компании ЦРТ, модель Silero от сообщества OpenVoice, а также оффлайн-движок Vosk, что свидетельствует о наличии научно-технического задела для создания суверенных речевых интерфейсов.

Однако повсеместное внедрение голосового управления в контуре ответственных информационных систем вскрывает серьезные проблемы в области информационной безопасности. Основная уязвимость классических

СРГК заключается в их функциональной ориентации исключительно на семантику произнесенной команды, при полном игнорировании аутентичности источника голоса. Данный недостаток формирует благоприятную среду для реализации широкого спектра угроз. К канальным угрозам относится перехват и анализ голосового трафика, передаваемого по открытым или недостаточно защищенным сетям, что может привести к компрометации конфиденциальной информации, содержащейся в командах. Наиболее критичными являются угрозы целостности, связанные с подменой легитимного диктора. К ним относятся атаки с использованием предварительно записанных образцов голоса (речевой спуфинг), синтез команд с помощью современных текст-в-речь систем, а также создание глубоких фейков голоса с применением методов генеративно-состязательных сетей. Отдельный класс составляют адверсариальные атаки, направленные непосредственно на модель машинного обучения. Путем внесения в аудиосигнал незаметных для человеческого слуха искажений злоумышленник может добиться кардинально иного результата распознавания, что открывает возможности для скрытого управления системой. Таким образом, безопасность голосовых интерфейсов не может быть обеспечена в рамках парадигмы простого распознавания текста и требует обязательного включения надежного механизма верификации говорящего.

1.2. Эволюция голосовой биометрии: от статических отпечатков к анализу поведенческих паттернов

Для решения задачи установления подлинности диктора традиционно применяется голосовая биометрия, основанная на анализе уникальных физиологических особенностей речевого тракта человека. Данные особенности, такие как размер и форма гортани, резонансные свойства носовой и ротовой полостей, формируют статический спектральный отпечаток голоса. Для его описания используются такие признаковые пространства, как мел-кепстральные коэффициенты, линейные

предсказательные коды и перцептуальные линейные предсказания. Несмотря на длительную историю применения и относительно высокую точность в контролируемых условиях, статическая биометрия демонстрирует принципиальные уязвимости. Она высокочувствительна к изменениям состояния говорящего (простуда, стресс, усталость), качеству канала передачи и фоновым шумам. Главное же ограничение заключается в уязвимости к целенаправленным атакам подмены, поскольку физиологические параметры, хоть и сложно, но возможно воспроизвести или сымитировать с использованием современных технологий синтеза и преобразования голоса.

В этой связи в научном сообщении и практике защиты информации возрастает интерес к поведенческой, или динамической, биометрии. Ее фундаментальное отличие заключается в анализе не столько «материальных» характеристик голосового тракта, сколько индивидуальных паттернов, приобретенных человеком в процессе жизнедеятельности и отражающих его уникальную манеру речи. Эти паттерны обладают значительно более высокой устойчивостью к имитации, так как формируются на подсознательном уровне и тесно связаны с когнитивными процессами. Поведенческие признаки в речи можно условно разделить на несколько категорий. К просодическим признакам относятся индивидуальные особенности интонационного контура, привычный темп речи, характерное распределение пауз, динамика громкости и ритмический рисунок фразы. Лексико-стилистические признаки охватывают устойчивые модели словоупотребления, включая частоту использования определенных служебных слов, местоимений, профессионального жаргона, а также синтаксические предпочтения в построении фраз. Контекстуально-поведенческие признаки связаны с типичными для пользователя сценариями взаимодействия с системой: последовательностью подаваемых команд, временем суток для определенных действий, реакцией на системные события. Комбинированный анализ статических и поведенческих признаков формирует основу для

многофакторной голосовой верификации, где первый фактор отвечает на вопрос «кто говорит?», а второй — «как говорит?». Такой подход создает существенные барьеры для злоумышленника, вынуждая его не только скопировать голос, но и точно воспроизвести глубокие поведенческие шаблоны, что на современном уровне развития технологий представляется крайне сложной задачей.

1.3. Отечественный контекст: нормативное регулирование и состояние рынка

Разработка и внедрение систем голосового управления, особенно с элементами биометрической идентификации, на территории Российской Федерации должны осуществляться в строгом соответствии с национальным законодательством и нормативными требованиями в области защиты информации. Ключевым нормативным актом является Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», который классифицирует голос как биометрические персональные данные. Это накладывает на оператора ряд обязательств, включая необходимость получения письменного согласия субъекта на обработку, обеспечение конфиденциальности и безопасности данных на всех этапах их жизненного цикла, а также использование для их защиты сертифицированных средств. Если система голосового управления развернута на объекте критической информационной инфраструктуры, в силу вступают положения Федерального закона от 26.07.2017 №187-ФЗ, требующие обеспечения надежности и безопасности с применением средств защиты информации, имеющих положительное заключение ФСТЭК России.

Методическую основу для построения защищенных систем задают документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России). В частности, «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах

персональных данных» и «Методика оценки угроз безопасности информации» предоставляют структурированный подход к идентификации и анализу рисков. Национальный стандарт ГОСТ Р 57580-2017 «Биометрическая идентификация. Требования к системам контроля и управления доступом на основе биометрических данных» устанавливает прямые требования к надежности, достоверности и защищенности биометрических систем, включая целевые показатели вероятности ложного допуска и ложного отказа. Игнорирование данной нормативной базы на этапе проектирования делает систему не только уязвимой, но и нелегитимной для использования в большинстве корпоративных и государственных сегментов.

Что касается состояния российского рынка, наблюдается активное развитие отечественных речевых технологий в рамках политики импортозамещения. Помимо уже упомянутых коммерческих и открытых решений для распознавания речи, ведутся исследования в области голосовой биометрии. Крупные технологические компании, научные институты и университеты публикуют результаты работ в рецензируемых журналах, индексируемых в РИНЦ, и выступают с докладами на профильных конференциях, таких как «Информационная безопасность» и «Речевые технологии». Однако анализ публикационной активности показывает, что тема поведенческой биометрии в голосе, особенно в прикладном аспекте обеспечения безопасности информационных систем, освещена фрагментарно. Существующие работы зачастую фокусируются либо на фундаментальных аспектах выделения просодических признаков, либо на задачах банковской удаленной идентификации. Таким образом, сохраняется значительный пробел в области систематизации поведенческих признаков применительно к задаче контроля доступа в системах голосового управления и разработки соответствующих архитектурных решений, что подтверждает актуальность и научную новизну настоящего исследования.

1.4. Сравнительный анализ методов и средств поведенческой идентификации в речевом канале

Развитие технологий голосовой биометрии привело к формированию отдельного научно-практического направления, ориентированного на идентификацию личности по динамическим, поведенческим признакам, проявляющимся в речи. В отличие от статической биометрии, опирающейся на относительно неизменные физиологические параметры голосового тракта, поведенческий анализ рассматривает речь как сложный когнитивно-моторный акт, подверженный влиянию привычек, эмоционального состояния и контекста деятельности. Уникальность поведенческих паттернов, их сложность для целенаправленной имитации и устойчивость к прямому копированию делают это направление ключевым для создания надежных систем аутентификации. Однако сама природа поведенческих признаков — их высокая вариативность, зависимость от множества внешних и внутренних факторов — предъявляет особые требования к методам их анализа, извлечения и сравнения. Данный раздел посвящен систематическому анализу и сравнению существующих подходов к поведенческой идентификации по голосу, оценке их алгоритмической базы, а также рассмотрению фундаментальных проблем, связанных с формированием и эксплуатацией поведенческих профилей.

1.4.1. Классификация подходов к анализу поведенческих признаков

Многообразие методов поведенческой идентификации можно классифицировать по типу обрабатываемых данных, принципам лежащих в их основе алгоритмов и конечной цели анализа. Первый крупный класс составляют просодические методы, ориентированные на извлечение супрасегментных характеристик речи. К ним относятся анализ интонационного контура (моделирование динамики основного тона), ритмической организации (распределение ударений, длительностей сегментов

и пауз) и темпоральных паттернов (скорость речи, ее изменения). Эти признаки отражают глубинную манеру говорения, часто неосознаваемую самим диктором. Второй класс — лингво-стилистические методы — работает с семантико-синтаксическим уровнем. Сюда входит анализ лексического выбора (характерный словарный запас, частота использования определенных частей речи, профессиональный жаргон), синтаксических конструкций (сложность предложений, порядок слов) и дискурсивных маркеров. Данные признаки сильно зависят от образования, профессиональной среды и когнитивных особенностей личности. Третий класс, контекстуально-поведенческие методы, выходит за рамки анализа единичного высказывания. Он рассматривает речевую деятельность как часть более широкого поведенческого сценария, учитывая такие параметры, как типичное время суток для определенных команд, последовательность операций, привычные реакции на системные события. Этот класс методов наиболее тесно связан с предметной областью конкретной информационной системы.

С алгоритмической точки зрения методы можно разделить на статистические, спектрально-временные и нейросетевые. Статистические методы, такие как анализ гистограмм распределения длительностей фонем, вычисление математического ожидания и дисперсии основного тона, отличаются простотой реализации и низкими вычислительными затратами. Их основной недостаток — неспособность улавливать сложные временные зависимости и динамические паттерны, что ограничивает их применение в системах с высокими требованиями к надежности. Спектрально-временные методы, например, анализ формантных траекторий с использованием алгоритма динамического выравнивания временных рядов, позволяют более точно моделировать изменчивость речевого сигнала, но требуют качественной предобработки данных и значительных ресурсов. Нейросетевые методы, в частности, использование рекуррентных сетей с долгой краткосрочной памятью для обработки последовательностей акустических или

лингвистических признаков, демонстрируют наивысшую точность при решении задач классификации и обнаружения аномалий. Однако они являются «черным ящиком», требуют большого объема размеченных данных для обучения и сложны в интерпретации, что может быть критично при расследовании инцидентов безопасности. В современных исследованиях, включая отечественные работы, представленные в Российском индексе научного цитирования (РИНЦ), все чаще предлагаются гибридные подходы, комбинирующие преимущества разных методов для достижения баланса между точностью, производительностью и объяснимостью.

1.4.2. Обзор алгоритмических решений и инструментальных средств

В области алгоритмической поддержки поведенческой идентификации можно выделить несколько ключевых направлений, получивших развитие как в мировых, так и в российских исследованиях. Для обработки просодии широко применяются алгоритмы, основанные на скрытых марковских моделях, адаптированных для работы с непрерывными параметрами, и методы векторного квантования, позволяющие сравнивать интонационные контуры. В работах российских ученых, например, в исследованиях, публикуемых в журнале «Речевые технологии», предлагается использование адаптивных пороговых алгоритмов, настраиваемых под индивидуальный диапазон вариативности каждого пользователя, что позволяет снизить количество ложных отказов.

Для лингво-стилистического анализа базовым аппаратом являются методы статистической обработки текста. К ним относятся анализ N-грамм (биграмм, триграмм слов), вычисление TF-IDF меры для выявления характерной лексики, а также применение синтаксических парсеров для построения деревьев зависимостей и последующего сравнения структур. В российской практике активно используются библиотеки для обработки естественного языка, такие как pymorphy2 и Natasha, которые обеспечивают

морфологический анализ и лемматизацию для русского языка, что является необходимым этапом перед извлечением стилистических признаков. Следует отметить, что большинство зарубежных аналогов (например: NLTK, spaCy) имеют ограниченную или неполную поддержку морфологически богатого русского языка, что делает отечественные разработки предпочтительными для реализации подобных систем в национальном контуре.

В части контекстуального анализа и моделирования поведения перспективными являются алгоритмы, заимствованные из области Data Mining, в частности, алгоритмы поиска ассоциативных правил (Apriori, FP-Growth) для выявления типичных последовательностей команд. Для моделирования нормального поведения и обнаружения отклонений применяются методы, основанные на машине Больцмана или автоэнкодерах, способных обучаться представлениям, характеризующим стандартные сценарии работы пользователя. Важно подчеркнуть, что в соответствии с требованиями безопасности и положениями 152-ФЗ, все алгоритмы обработки биометрических данных, особенно те, что связаны с машинным обучением, должны обеспечивать возможность аудита и контроля принимаемых решений. Это накладывает дополнительные ограничения на использование сложных нейросетевых архитектур и повышает ценность гибридных, частично интерпретируемых моделей.

1.4.3. Проблема формирования, адаптации и дрейфа поведенческого профиля

Одной из фундаментальных проблем поведенческой биометрии является нестационарность эталонного образа. Поведенческие признаки не являются константой; они закономерно изменяются под влиянием усталости, стресса, долговременных изменений голоса, смены профессионального контекста или просто эволюции привычек пользователя. Это явление, известное как концептуальный дрейф, приводит к постепенному расхождению

между сохраненным профилем и текущим поведением, что влечет за собой рост уровня ложных отказов и снижение удобства использования системы.

Процесс первичного формирования профиля становится критически важным этапом. Для сбора репрезентативной начальной выборки поведения требуется не просто произнесение нескольких калибровочных фраз, а имитация реальных рабочих сценариев в различном эмоциональном и физиологическом состоянии. В исследованиях, например, в работах, представленных на конференциях по биометрии в МГТУ им. Н.Э. Баумана, предлагаются методики многосессионного обучения с обязательным включением в обучающую выборку данных, полученных в неидеальных условиях (при фоновом шуме, в состоянии легкого стресса).

Для противодействия дрейфу применяются стратегии адаптивного обновления профиля. Наиболее распространенным является метод экспоненциального взвешенного скользящего среднего, при котором параметры профиля постепенно обновляются данными из успешных сеансов аутентификации. Однако такая стратегия несет в себе риск медленной компрометации, когда злоумышленник, имеющий частичный доступ или ведущий наблюдение, может постепенно «подстроить» профиль под свои поведенческие характеристики. Поэтому современные подходы, описанные в отечественных научных публикациях, предусматривают двухуровневую систему обновления: быстрое обновление краткосрочных, более лабильных параметров (текущего темпа речи) и крайне консервативное, контролируемое обновление долгосрочных, устойчивых паттернов (лексико-стилистического ядра). Любое обновление профиля должно сопровождаться строгим аудитом и, при значительных изменениях, может требовать дополнительного подтверждения личности через другой канал аутентификации. Таким образом, управление жизненным циклом поведенческого профиля представляет собой непрерывный поиск компромисса между устойчивостью к атакам,

адаптивностью к законным изменениям пользователя и соответствием принципам безопасности, закрепленным в стандартах ФСТЭК России.

1.4.4. Сравнительные выводы и выбор базового подхода для проектируемой системы

Проведенный анализ позволяет сделать вывод о том, что не существует универсального метода поведенческой идентификации, пригодного для всех сценариев использования. Выбор конкретных алгоритмов и их комбинации должен определяться требованиями к безопасности, допустимым временем отклика, доступностью вычислительных ресурсов и необходимостью обеспечения аудируемости.

Для проектируемой системы распознавания голосовых команд в корпоративных информационных системах, обрабатывающих информацию ограниченного доступа, целесообразно ориентироваться на гибридную модель. В ее основе должен лежать статистический аппарат для первичной, высокопроизводительной оценки базовых просодических и контекстуальных параметров. Этот слой обеспечит отсев грубых аномалий и атак низкой сложности. Для глубокого анализа сложных поведенческих паттернов, таких как интонационные контуры и лингво-стилистические особенности, следует предусмотреть возможность применения более ресурсоемких, но точных методов, например, основанных на машинном обучении, с обязательным обеспечением логирования и объяснимости промежуточных решений. При этом алгоритмическое ядро должно быть спроектировано с учетом необходимости постоянной адаптивной коррекции профиля при одновременной реализации защитных механизмов, препятствующих его медленной компрометации. Такой многоуровневый и сбалансированный подход, опирающийся на анализ отечественных исследований и требований регуляторов, позволит создать не просто теоретическую модель, а практичный

фундамент для разработки реальных защищенных систем голосового управления.

1.5. Этические аспекты использования поведенческой биометрии

Внедрение систем поведенческой биометрии, особенно в корпоративной и государственной сфере, сопряжено не только с техническими, но и с серьезными этическими вызовами. Эти системы оперируют глубоко персональными данными, которые отражают не только физиологические особенности, но и подсознательные поведенческие модели, что создает новые риски для приватности и автономии личности.

1.5.1. Проблемы приватности и согласия пользователей.

- Глубина собираемых данных: В отличие от отпечатка пальца, поведенческий профиль голоса может неявно раскрывать информацию о психоэмоциональном состоянии (стресс, усталость), здоровье (неврологические нарушения), культурном бэкграунде и даже чертах личности. Обработка таких «расширенных» биометрических данных находится в «серой зоне» с точки зрения трактовки 152-ФЗ.

- Информированное согласие: В соответствии со ст. 9 152-ФЗ, обработка биометрических данных требует письменного согласия субъекта. Однако является ли пользователь в полной мере информированным, понимает ли он, какие именно поведенческие паттерны (просодия, лексика, паттерны взаимодействия) будут извлекаться, анализироваться и храниться? Существует риск «согласия по умолчанию» в корпоративной среде, где отказ от использования системы может повлечь ограничение доступа к рабочему месту.

- Целевое использование и вторичная обработка: Возникает риск использования собранных поведенческих профилей не по прямому назначению (контроль доступа), а для скрытого мониторинга

продуктивности сотрудников, анализа их лояльности или эмоционального состояния без их ведома. Необходимы четкие технические и организационные меры, исключающие такую возможность, и прозрачная политика обработки данных.

1.5.2. Риски дискриминации и манипуляций на основе поведенческих данных.

- Систематическая ошибка и дискриминация: Алгоритмы машинного обучения, лежащие в основе поведенческой биометрии, могут унаследовать смещения из обучающих данных. Например, система может менее точно идентифицировать людей с определенными диалектами, речевыми особенностями (заикание), или представителей меньшинств, если они недостаточно представлены в обучающей выборке. Это может привести к несправедливо высокому проценту ложных отказов (FRR) для отдельных групп и, как следствие, к дискриминации при доступе.

- Манипуляции и давление: Знание того, что система анализирует поведение, может привести к изменению естественного поведения пользователя «эффект наблюдателя». Более того, работодатель может оказывать давление на сотрудника, чтобы тот «говорил более уверенно» или «соблюдал корпоративные речевые стандарты», что является формой манипуляции и ущемления свободы личности.

- Угроза профилирования и манипуляций: Детализированный поведенческий профиль представляет высокую ценность для злоумышленников, маркетологов или политических технологов. В случае утечки такие данные могут быть использованы для:

1. Гиперперсонализированного фишинга или социальной инженерии, где злоумышленник имитирует не только голос, но и стиль общения жертвы.
2. Создания манипулятивного контента, например, для влияния на мнение человека, чей речевой и поведенческий паттерн был скомпрометирован.

- Проблема «цифрового бессмертия»: Созданный поведенческий профиль, особенно если он включает лингво-стилистическую модель, теоретически может быть использован для синтеза речи, неотличимой от речи оригинального пользователя, даже после его смерти, что поднимает новые этико-правовые вопросы.

Использование поведенческой биометрии требует выхода за рамки формального соответствия 152-ФЗ и внедрения принципов защиты конфиденциальности и этического проектирования. Разработчикам и операторам таких систем необходимо:

1. Обеспечивать максимальную прозрачность в отношении того, какие именно признаки извлекаются и как используются.
2. Реализовывать минимально необходимый сбор данных, избегая избыточного профилирования.
3. Проводить обязательный аудит алгоритмов на предмет смещений и публиковать результаты проверок на дискриминацию.
4. Внедрять строгие технические меры, исключающие использование данных не по назначению (сильное шифрование, разграничение доступа, чистые журналы аудита).
5. Разрабатывать четкие этические кодексы и регламенты для внутреннего использования систем поведенческой идентификации в организациях.

Таким образом, этические риски являются не побочным эффектом, а неотъемлемой частью проектирования систем поведенческой биометрии. Их игнорирование может привести не только к репутационным потерям и судебным искам, но и к подрыву базового доверия к технологии, что в конечном итоге сведет на нет все ее преимущества в области безопасности.

1.6. Выводы по главе

Проведенный анализ позволяет сделать ряд основополагающих выводов. Во-первых, современные системы распознавания голосовых команд, основанные на передовых нейросетевых архитектурах, достигли высокого уровня точности, но при этом обладают фундаментальными уязвимостями с точки зрения информационной безопасности, поскольку не осуществляют верификацию источника команды. Во-вторых, традиционная статическая голосовая биометрия, опирающаяся на физиологические признаки, не обеспечивает необходимого уровня устойчивости к целенаправленным атакам подмены с использованием современных технологий синтеза и преобразования голоса. В-третьих, перспективным направлением для создания надежного контура безопасности является многофакторная верификация, дополняющая анализ статического отпечатка исследованием поведенческих паттернов речи, которые значительно сложнее поддаются имитации. В-четвертых, разработка и внедрение подобных систем в Российской Федерации должны осуществляться с учетом комплексных требований нормативно-правовой базы, регулирующей обработку биометрических данных и защиту информации, что накладывает специфические ограничения и определяет архитектурные особенности. Синтез этих выводов формирует теоретический и методологический фундамент для последующего моделирования угроз и проектирования архитектуры системы, сочетающей распознавание команд и поведенческую идентификацию.

ГЛАВА 2. РАЗРАБОТКА МОДЕЛИ УГРОЗ И ФОРМАЛИЗАЦИЯ ТРЕБОВАНИЙ К ЗАЩИЩЕННОЙ СИСТЕМЕ ГОЛОСОВОГО УПРАВЛЕНИЯ

2.1. Методологическая основа моделирования угроз и идентификация критических активов

Проектирование любой защищенной информационной системы, в особенности обрабатывающей биометрические данные, должно начинаться с систематического анализа угроз ее безопасности. Для обеспечения соответствия отечественным нормативным реалиям в качестве методологической основы выбрана адаптированная версия методологии OCTAVE Allegro, согласующаяся с принципами, изложенными в документах ФСТЭК России, таких как «Методика оценки угроз безопасности информации». Данный подход фокусируется на активах, их уязвимостях и вероятных сценариях реализации угроз, что идеально соответствует задаче построения модели для сложной системы, интегрирующей речевые технологии и биометрию.

Первым и фундаментальным шагом является идентификация и ранжирование активов системы. Под активами понимаются ресурсы, представляющие ценность для организации и требующие защиты. В контексте проектируемой системы распознавания голосовых команд с поведенческой идентификацией ключевые активы могут быть классифицированы следующим образом:

Информационные активы:

- Биометрические персональные данные пользователей (статические голосовые шаблоны и динамические поведенческие профили).
- Семантика распознаваемых голосовых команд, которая может содержать конфиденциальную информацию.

- Журналы аудита и системные логи, содержащие историю доступа и попыток верификации.

Программно-аппаратные активы:

- Серверные компоненты системы (модули распознавания, верификации, базы данных).
- Каналы передачи аудиоданных между клиентским устройством и обработчиком.
- Клиентские устройства (микрофоны, специализированные терминалы).
- Целевые информационные системы, управляемые посредством голосовых команд.
- Репутационные и процессные активы:
- Доступ к критическим бизнес-функциям, предоставляемый через голосовой интерфейс.
- Репутация организации как оператора, обеспечивающего конфиденциальность биометрических данных.
- Непрерывность бизнес-процессов, зависящих от доступности системы голосового управления.

На основе выявленных активов формулируются профили потенциальных злоумышленников с указанием их мотивации, возможностей и предполагаемых точек атаки. В рамках исследования рассматриваются два базовых профиля: внешний нарушитель, целью которого является получение несанкционированного доступа или нарушение работоспособности системы, и внутренний нарушитель (инсайдер), обладающий легитимными привилегиями и нацеленный на компрометацию данных или скрытое управление.

2.2. Построение и документирование модели угроз

На основании идентифицированных активов и профилей злоумышленников осуществляется построение структурированной модели угроз. Модель фиксирует взаимосвязь между активом, его уязвимостями, конкретными угрозами и потенциальными последствиями их реализации. Для наглядности и удобства анализа угрозы группируются по объекту посягательства в соответствии с триадой КИБ (конфиденциальность, целостность, доступность).

Таблица 2.1 - Фрагмент модели угроз для системы голосового управления с поведенческой идентификацией

Угроза	Уязвимость / Вектор атаки	Возможные последствия
Кража или утечка эталонных биометрических данных.	Уязвимости СУБД, недостаточное шифрование данных на rest, доступ инсайдера.	Необратимая компрометация биометрического идентификатора пользователя; нарушение требований 152-ФЗ.

Перехват голосового трафика.	Отсутствие сквозного шифрования (например, TLS).	Раскрытие биометрических признаков и содержания команд; анализ для последующего спуфинга.
Атака подмены диктора (спуфинг) с использованием синтезированной речи (TTS).	Недостаточная устойчивость статического биометрического модуля к высококачественному синтезу.	Несанкционированный доступ для злоумышленника, имитировавшего голос, но не поведенческие паттерны.
Целенаправленная адаптация под поведенческие паттерны целевого пользователя.	Возможность длительного наблюдения и анализа легитимных сеансов пользователя.	Постепенное снижение эффективности поведенческого модуля, риск ложного допуска.
Адверсариальная атака на модель ИИ: подача скрытой (неслышимой) команды.	Чувствительность нейросетевых моделей к специально сгенерированным искажениям в аудиосигнале.	Скрытое исполнение команды, не предполагаемой пользователем, для которой не требуется верификация.

Атака типа «Отказ в обслуживании» (DoS/DDoS) на интерфейс приема запросов.	Ограниченная пропускная способность каналов или вычислительных ресурсов.	Полная или частичная недоступность системы голосового управления, сбой бизнес-процессов.

2.3. Формулирование и структурирование требований к системе

Результаты моделирования угроз служат прямым входом для формирования комплекса требований к проектируемой системе. Требования структурируются по трем основным категориям.

1. Функциональные требования (Определяют, что должна делать система):

- Система должна осуществлять прием аудиосигнала с заданной частотой дискретизации и разрядностью.
- Система должна выполнять двухэтапную обработку запроса: распознавание семантики команды и многофакторную верификацию диктора.
- Модуль верификации должен формировать интегральную оценку достоверности на основе взвешенного анализа статического отпечатка голоса и динамического поведенческого профиля.
- Система должна принимать решение о разрешении/запрете выполнения команды на основании интегральной оценки и заданного порогового значения.

- Система должна вести детализированный журнал аудита всех событий (принятый аудиосигнал, результаты распознавания и верификации, принятое решение).

2. Требования по безопасности (Определяют, как система должна противостоять выявленным угрозам):

- Обеспечение конфиденциальности передаваемых данных путем применения сквозного шифрования голосового трафика с использованием алгоритмов, одобренных ФСБ России.
- Безопасное хранение биометрических шаблонов в зашифрованном виде с использованием криптографических средств, сертифицированных ФСТЭК/ФСБ России.
- Реализация механизма обнаружения аномалий в поведенческих паттернах для противодействия целенаправленной адаптации злоумышленника.
- Обеспечение устойчивости системы к базовым атакам спуфинга (запись, TTS) с целевыми показателями вероятности ложного допуска (FAR) не более 0.01%.
- Техническая реализация процедуры получения и подтверждения информированного согласия пользователя на обработку биометрических ПДн в соответствии со ст. 11 152-ФЗ.

3. Нефункциональные требования (Определяют качественные характеристики системы):

- Производительность - время отклика системы (от конца произнесения команды до принятия решения) не должно превышать 2 секунд для 95% запросов.

- Масштабируемость - архитектура системы должна позволять горизонтальное масштабирование для обслуживания увеличения числа пользователей.
- Надежность - коэффициент готовности системы должен составлять не менее 99.5%.
- Адаптивность - система должна корректно функционировать при уровне фонового шума до -20 дБ относительно полезного сигнала.

2.4. Методика оценки рисков для биометрических систем

Разработанная модель угроз (раздел 2.2) является необходимым, но недостаточным основанием для построения системы защиты. Следующим критическим шагом является оценка рисков — определение вероятности реализации угроз и масштаба возможного ущерба. Для биометрических систем, обрабатывающих особые категории персональных данных и выполняющих функции контроля доступа, данный процесс должен быть формализован, измерим и соотнесен с отечественными методическими рекомендациями.

2.4.1. Количественная и качественная оценка рисков на основе модели угроз.

В практике информационной безопасности применяются два взаимодополняющих подхода к оценке рисков.

- Качественная оценка является наиболее применимой на этапе проектирования. Она опирается на экспертные мнения и ранжирование рисков по шкалам «вероятность» и «влияние». Для каждого сценария угрозы из модели (Таблица 2.1) проводится оценка:

- Вероятность (P): Низкая / Средняя / Высокая. Определяется на основе доступности средств атаки, уровня квалификации предполагаемого нарушителя и наличия базовых мер защиты.
- Влияние / Ущерб (I): Низкий / Средний / Высокий / Критический. Оценивается по триаде КИБ: масштаб компрометации данных, финансовые потери, ущерб репутации, нарушение бизнес-процессов.
- Уровень риска (R) определяется по матрице рисков: $R = P \times I$. На выходе получается приоритезированный список рисков (например, «Высокий», «Средний», «Низкий»).

- Пример качественной оценки для угроз из Таблицы 2.1:
  - Угроза: «Атака подмены диктора с использованием TTS». P=Средняя (инструменты доступны), I=Высокий (несанкционированный доступ). Уровень риска = Высокий.
  - Угроза: «Целенаправленная адаптация под поведенческие паттерны». P=Низкая (требует глубокого анализа и времени), I=Критический (полный обход системы). Уровень риска = Средний/Высокий.
- Количественная оценка стремится выразить риск в числовых показателях (денежный ущерб, годовая вероятность реализации). Хотя она сложнее в применении на этапе проектирования, для критических систем она может быть полезна. Формула базового количественного риска: $R = A \times V \times C$, где:
  - A (Asset Value) - стоимость актива (можно оценить через затраты на восстановление, штрафы по 152-ФЗ, стоимость упущенной выгоды).

- V (Vulnerability) - коэффициент уязвимости (вероятность успешной эксплуатации уязвимости, от 0 до 1).
- C (Threat Capability) - сила угрозы (частота или вероятность атаки за определенный период, например, в год).

- Для биометрической системы ключевым метрическим показателем является Интегральный показатель риска биометрической аутентификации, который может учитывать целевые показатели FAR/FRR, стоимость инцидента ложного допуска и годовую предполагаемую атакуемость (AR - Attack Rate).

2.4.2. Рекомендации по выбору мер защиты в зависимости от уровня риска.

Полученная классификация рисков служит основой для экономически обоснованного выбора и внедрения мер защиты (контролей). Принцип состоит в том, что затраты на защиту не должны превышать возможный ущерб.

- Для рисков «Критический» и «Высокий» применяются обязательные, комплексные и часто избыточные меры:
  - Технические: Внедрение многофакторной аутентификации (статический + поведенческий анализ + дополнительный фактор), строгое сквозное шифрование трафика и данных на rest (с использованием сертифицированных СКЗИ), аппаратная изоляция и защита баз биометрических шаблонов, регулярное тестирование на проникновение и оценка устойчивости к спуфингу.
  - Организационные: Обязательное получение явного письменного согласия, назначение ответственных за биометрические данные, проведение регулярного аудита и анализа логов SIEM-системой,

разработка и отработка плана реагирования на инциденты с биометрическими данными.

- Правовые: Включение соответствующих положений в договоры с сотрудниками и контрагентами, страхование киберрисков.

- Для рисков «Средний» применяются стандартные, проверенные меры, соответствующие лучшим отраслевым практикам:
  - Технические: Реализация базовой криптографической защиты, настройка систем обнаружения аномалий (например, на уровне поведенческого модуля), регулярное обновление ПО и моделей ИИ.
  - Организационные: Периодическая переоценка рисков, обучение пользователей, назначение умеренных сроков хранения аудиологов.
- Для рисков «Низкий» могут применяться базовые или отложенные меры:
  - Принятие риска на основе решения руководства с регулярным пересмотром.
  - Внедрение простых организационных контролей (политики паролей, базовое логирование).

Формализованная методика оценки рисков, интегрирующая как качественные экспертные оценки, так и, где это возможно, количественные метрики, позволяет перейти от простого перечисления угроз к управлению безопасностью на основе рисков. Для биометрических систем акцент должен делаться на оценке ущерба от компрометации эталонных данных и ложного допуска, что напрямую связано с репутационными и финансовыми потерями, а также с юридической ответственностью по 152-ФЗ. Результирующая карта

рисков с указанием приоритетов служит прямым техническим заданием для проектирования архитектуры системы, определяя, какие security-контроли должны быть реализованы в первую очередь и с какой строгостью.

2.5. Выводы по главе

В результате проведенной работы была разработана комплексная модель угроз безопасности для системы голосового управления с поведенческой идентификацией. Модель построена на методологической основе, согласующейся с отечественными подходами к оценке угроз, и документирована в структурированном виде, что включает:

- Идентификацию и классификацию критически важных активов, среди которых ключевое место занимают биометрические данные и процессы верификации.
- Детальное описание профилей злоумышленников и сценариев реализации угроз, с особым акцентом на атаки, направленные на обход биометрических проверок.
- Формализацию угроз в виде структурированной таблицы, устанавливающей четкую связь между активом, уязвимостью, угрозой и последствиями.

На основании данной модели был сформулирован полный и структурированный перечень требований к системе, разделенный на функциональные, security-требования и нефункциональные характеристики. Этот перечень носит конкретный и измеримый характер, акцентирует необходимость криптографической защиты данных, соответствия законодательству РФ и обеспечения заданных показателей надежности и устойчивости к атакам. Полученные модель угроз и перечень требований образуют законченный аналитический фундамент, который является обязательным и достаточным основанием для перехода к следующему этапу

работы — проектированию архитектуры системы, удовлетворяющей всем установленным критериям безопасности и эффективности.

ГЛАВА 3. ПРОЕКТИРОВАНИЕ АРХИТЕКТУРЫ СИСТЕМЫ РАСПОЗНАВАНИЯ КОМАНД С ИНТЕГРИРОВАННОЙ ПОВЕДЕНЧЕСКОЙ ИДЕНТИФИКАЦИЕЙ

На основании результатов аналитического исследования и сформулированных требований, представленных в предыдущих главах, осуществляется ключевой этап работы — проектирование архитектуры системы. Целью данной главы является разработка концептуальной модели, которая интегрирует механизм распознавания семантики голосовой команды с двухфакторной биометрической верификацией, основанной на анализе статических и поведенческих признаков голоса. Проектирование ведется с учетом выявленных угроз безопасности и строгого соблюдения нормативных требований Российской Федерации.

3.1. Концептуальная архитектура и принципы построения системы

Архитектура проектируемой системы строится по модульному принципу, что обеспечивает гибкость, масштабируемость и возможность независимого совершенствования отдельных компонентов. Фундаментальным принципом является разделение ответственности: модули, отвечающие за обработку аудиосигнала, биометрическую верификацию, принятие решений и логирование, функционируют относительно независимо, взаимодействуя через четко определенные программные интерфейсы. Общая логическая схема системы представляет собой последовательно-параллельный конвейер обработки запроса, где параллельно выполняются задачи распознавания команды и многофакторной верификации, а итоговое решение принимается на основе агрегированных результатов.

Концептуально система разделена на три основных логических уровня: уровень представления (клиентский интерфейс), уровень обработки и бизнес-логики (серверные модули) и уровень данных. Клиентский уровень представлен специализированным приложением или веб-интерфейсом,

основной задачей которого является захват аудиосигнала с микрофона пользователя, его первичная обработка и безопасная передача на сервер. Уровень обработки является ядром системы и включает в себя все модули, описанные в последующих разделах. Уровень данных обеспечивает безопасное хранение эталонных биометрических профилей, политик безопасности и журналов аудита, для чего предполагается использование сертифицированных СУБД и средств криптографической защиты информации.

3.2. Детализация функциональных модулей системы

3.2.1. Модуль приема и предобработки аудиопотока

Данный модуль выполняет роль шлюза, обеспечивающего входной контроль и подготовку данных для последующей обработки. Его ключевые функции включают валидацию входящего аудиопотока (проверка формата, частоты дискретизации), автоматическое подавление шума и эхо-компенсацию с использованием адаптивных цифровых фильтров, а также сегментацию непрерывного потока на отдельные речевые фразы (Voice Activity Detection - VAD). Предобработанный аудиофрагмент, соответствующий одной голосовой команде, нормализуется по амплитуде и передается одновременно в модуль распознавания команд и в модули биометрической верификации.

3.2.2. Модуль распознавания речевых команд

Данный модуль отвечает за преобразование акустического сигнала в текстовую команду, понятную управляемой информационной системе. Учитывая российскую специфику и требование к возможному импортозамещению, в качестве базовой технологии рассматривается использование открытых нейросетевых моделей, обученных на русскоязычных корпусах, таких как Silero или аналогов. Архитектура модуля

предполагает возможность поддержки контекстно-зависимых грамматик для ограниченного набора команд в корпоративных системах, что повышает точность. Результатом работы модуля является текстовое представление команды и оценка уверенности распознавания, которые передаются в модуль принятия решений.

3.2.3. Модуль статической биометрической верификации

Целью данного модуля является проверка того, что предъявленный голос соответствует зарегистрированному статическому отпечатку (шаблону) пользователя. Процесс верификации включает два этапа. На этапе извлечения признаков из предобработанного аудиосигнала вычисляются мел-кепстральные коэффициенты и их производные, формирующие вектор статических признаков. На этапе сравнения этот вектор сопоставляется с эталонным шаблоном, хранящимся в защищенном хранилище. Для сравнения используются алгоритмы, основанные на Gaussian Mixture Models или нейросетях прямого распространения. Результатом является бинарное решение (совпадение/несовпадение) и числовая оценка сходства которая передается в модуль принятия решений.

3.2.4. Модуль анализа поведенческих признаков (концептуальное ядро системы)

Этот модуль реализует инновационную составляющую системы - верификацию на основе динамических паттернов речи. Его работа строится на анализе не физиологических, а приобретенных особенностей речевого поведения. Модуль состоит из трех взаимосвязанных подмодулей, каждый из которых анализирует свой аспект поведения.

- Подмодуль просодического анализа извлекает признаки, связанные с мелодикой и ритмом речи. К ним относятся: средняя и дисперсия основного тона (F0), темп речи (количество фонем в секунду),

длительность и распределение пауз между словами, динамика интенсивности сигнала. Эти признаки сравниваются с эталонным поведенческим профилем пользователя.

- Подмодуль лингво-стилистического анализа фокусируется на языковых привычках. Он работает с текстом, полученным от модуля распознавания, и анализирует частоту использования служебных слов, особенности синтаксиса (например, средняя длина предложения), использование специфической лексики или профессионального жаргона. Для этого могут применяться методы обработки естественного языка (NLP), включая n-gram модели и векторизацию текста.
- Подмодуль контекстуально-поведенческого анализа учитывает мета-информацию о сеансе. Он оценивает соответствие времени суток, дня недели и последовательности подаваемых команд типичным для данного пользователя сценариям работы. Например, команда на выполнение критической операции в нехарактерное время будет считаться аномалией.

Результаты работы всех подмодулей агрегируются в единую оценку поведенческого соответствия, которая отражает степень уверенности в том, что предъявленный голосовой образец произнесен в характерной для легитимного пользователя манере.

3.2.5. Модуль принятия решений и управления доступом

Данный модуль является центральным логическим узлом системы, ответственным за итоговую оценку риска и вынесение решения. Он получает на вход четыре ключевых параметра: текст команды, оценку уверенности ее распознавания, результат статической верификации и интегральную оценку поведенческого соответствия. На основе предварительно настроенной политики безопасности, которая определяет весовые коэффициенты для каждого фактора и пороговые значения, модуль вычисляет общую оценку

достоверности сеанса. Политика может быть гибкой: для команд с низким уровнем привилегий может требоваться только успешная статическая верификация, в то время как для критических команд необходимо успешное прохождение как статической, так и поведенческой проверки. На основе расчета модуль выдает одно из трех решений: разрешить выполнение команды, отказать в выполнении или инициировать запрос на дополнительную аутентификацию. Управляющий сигнал направляется в целевую информационную систему.

3.2.6. Модуль регистрации и аудита

Данный модуль обеспечивает выполнение требований подотчетности и неизменяемости журналов. Он получает события от всех других модулей системы и записывает их в защищенную базу данных. Каждая запись в журнале включает временную метку, идентификатор сеанса, результаты работы каждого модуля, итоговое решение и контекстные данные (например, IP-адрес клиента). Журналы защищаются от модификации с помощью электронной подписи и используются для расследования инцидентов безопасности, анализа эффективности системы и периодической переоценки рисков.

3.3. Модель данных и структура эталонного профиля пользователя

Для эффективной работы системы необходима формализованная модель данных, описывающая эталонный профиль пользователя. Профиль представляет собой структурированный объект, состоящий из двух основных блоков.

- Блок статической биометрии: Содержит преобразованный и зашифрованный вектор MFCC-признаков, извлеченных из нескольких речевых образцов пользователя, полученных в эталонных условиях. Для

хранения используется необратимый шаблон (template), что минимизирует риски в случае утечки данных.

- Блок поведенческой биометрии (динамический профиль): Включает в себя:
    - Просодический дескриптор (средние значения и дисперсии для F0, темпа, пауз).
    - Лингво-стилистическую модель (например, частотный словарь характерных слов, n-gram модель).
    - Контекстуальные паттерны (типичное время и последовательность команд).

Профиль создается в процессе первоначальной адаптации, когда пользователь в контролируемых условиях произносит набор калибровочных фраз и выполняет типовые сценарии. Важным аспектом является возможность адаптивного обновления поведенческого блока профиля в процессе эксплуатации для учета естественной эволюции речевых привычек пользователя, при этом изменения должны проходить дополнительные проверки на аномальность.

3.4. Сценарий взаимодействия модулей и пример рабочего цикла

Для иллюстрации принципов работы системы рассмотрим типичный сценарий обработки голосовой команды.

1. Пользователь произносит команду «Открыть отчет за июнь».
2. Клиентское приложение захватывает аудио, выполняет первичную обработку и отправляет зашифрованный поток на сервер.
3. Модуль приема и предобработки принимает поток, выполняет шумоподавление и выделяет речевую фразу.
4. Очищенный аудиофрагмент параллельно передается в Модуль распознавания команд и в модули биометрической верификации (Статический и Поведенческий).

5. Модуль распознавания возвращает текст команды «открыть отчет за июнь».
6. Модуль статической верификации извлекает MFCC-признаки, сравнивает их с шаблоном пользователя и возвращает оценку сходства 0.85.
7. Модуль поведенческой верификации анализирует просодию, стиль речи и контекст. Результат: просодия соответствует на 92%, стиль речи типичен, но команда подана в необычно позднее время. Интегральная поведенческая оценка — 0.75.
8. Модуль принятия решений получает все результаты. Согласно политике для команды «открыть отчет» веса распределены как 40% — распознавание, 30% — статика, 30% — поведение. Итоговый скор рассчитывается. Учитывая контекстуальную аномалию, итоговый скор находится чуть ниже порога полного доверия. Модуль принимает решение запросить дополнительную аутентификацию.
9. Пользователь вводит код, аутентификация проходит успешно, команда исполняется. Модуль аудита фиксирует все шаги, включая аномалию и успешную двухфакторную аутентификацию.

3.5. Оценка концептуальной эффективности и рекомендации по развитию

Качественная оценка эффективности предложенной архитектуры базируется на анализе ее способности парировать угрозы, выявленные в Главе 2. Внедрение поведенческого фактора создает дополнительный, трудноимитируемый барьер для атак подмены, особенно для внутреннего нарушителя, который может обладать записью голоса, но не знает поведенческих нюансов. Модульная архитектура и детальное логирование упрощают аудит и соответствие требованиям 152-ФЗ и стандартов ФСТЭК.

Для практической реализации данной концептуальной модели рекомендуется следующая последовательность действий: разработка прототипа на базе открытых русскоязычных речевых моделей (например Silero для распознавания), создание и верификация алгоритмов извлечения поведенческих признаков на синтезированных и реальных данных, интеграция с сертифицированными средствами криптографической защиты информации для шифрования каналов и хранилищ, а также проведение всесторонних испытаний на устойчивость к различным сценариям атак в специализированной лаборатории.

Перспективными направлениями дальнейшего развития системы являются: применение машинного обучения для автоматического обнаружения новых, ранее неизвестных аномалий в поведенческих паттернах; интеграция с системами анализа событий безопасности (SIEM) для корреляции голосовых инцидентов с другими угрозами; адаптация архитектуры для работы в распределенных и гибридных облачных средах с сохранением требований к суверенитету данных.

3.6. Выводы по главе

В третьей главе была разработана детализированная архитектурная модель системы распознавания голосовых команд с двухфакторной биометрической верификацией, являющаяся основным результатом данной выпускной квалификационной работы. Модель включает концептуальное описание модульной архитектуры, детальную спецификацию всех ключевых компонентов — от модуля предобработки до модуля принятия решений — с особым акцентом на инновационный модуль анализа поведенческих признаков. Разработана структура эталонного профиля пользователя, объединяющая статические и динамические биометрические данные. Описан типовой сценарий взаимодействия модулей, иллюстрирующий принципы работы системы в условиях выявления аномалии.

Предложенная архитектура носит концептуальный характер и готова к последующей детальной технической проработке и реализации. Она напрямую отвечает на выявленные в аналитической части работы угрозы, обеспечивая не только распознавание команды, но и надежную верификацию личности говорящего на основе уникального сочетания «что он сказал» и «как он это сказал». Данная модель служит конкретным практическим результатом, который может быть положен в основу создания защищенных голосовых интерфейсов для корпоративных и государственных информационных систем Российской Федерации.

ЗАКЛЮЧЕНИЕ

Проведенное исследование было посвящено решению актуальной задачи обеспечения безопасности информационных систем, использующих голосовые интерфейсы управления. Анализ современного состояния вопроса выявил ключевую проблему: традиционные системы распознавания голосовых команд, ориентированные исключительно на семантику высказывания, не обеспечивают надежную верификацию личности диктора, что создает серьезные риски несанкционированного доступа. В качестве основного пути решения данной проблемы была предложена концепция двухфакторной голосовой биометрической верификации, объединяющая проверку статического отпечатка голоса и анализ уникальных поведенческих речевых паттернов пользователя.

Целью работы являлась разработка архитектурной модели системы распознавания голосовых команд с интегрированным механизмом идентификации на основе поведенческих признаков. В ходе исследования данная цель была успешно достигнута путем последовательного решения комплекса взаимосвязанных задач.

В первой главе работы был осуществлен всесторонний аналитический обзор. Исследованы современные технологии распознавания речи и выявлен спектр присущих им угроз информационной безопасности, среди которых центральное место занимают атаки на подмену диктора. Проведен анализ эволюции голосовой биометрии, в результате которого обоснована недостаточная устойчивость статических методов к современным видам спуфинга и продемонстрирована перспективность использования поведенческих признаков, таких как индивидуальные просодические, лингво-стилистические и контекстуальные паттерны. Кроме того, детально изучена отечественная нормативно-правовая база, включая требования 152-ФЗ, 187-

ФЗ и стандартов ФСТЭК России, что заложило правовой фундамент для проектирования системы.

Во второй главе, на основе методологии, согласующейся с подходами российских регуляторов, была разработана комплексная модель угроз безопасности для проектируемой системы. Модель включает идентификацию критических активов, профилирование злоумышленников и детальное описание сценариев реализации угроз, сфокусированных на компрометации биометрических данных и обходе процедур аутентификации. На основании этой модели сформулирован структурированный перечень функциональных, security- и нефункциональных требований к системе, задающий четкие критерии ее защищенности, производительности и соответствия законодательству.

Результатом третьей, проектной главы, стала разработанная концептуальная архитектура системы. Архитектура построена по модульному принципу и включает в себя: модуль приема и предобработки аудиопотока; модуль распознавания речевых команд; модуль статической биометрической верификации; инновационный модуль анализа поведенческих признаков, состоящий из подмодулей просодического, лингво-стилистического и контекстуального анализа; модуль принятия решений (Orchestrator), реализующий взвешенную политику безопасности; а также модуль регистрации и аудита. Разработана модель данных и структура эталонного профиля пользователя, объединяющего статические и динамические биометрические дескрипторы. Продемонстрирован типовой сценарий работы системы, иллюстрирующий ее способность выявлять аномалии и запрашивать дополнительную аутентификацию.

Научная новизна работы заключается в систематизации поведенческих признаков голоса применительно к задачам контроля доступа в корпоративных информационных системах и в разработке на этой основе

целостной архитектурной модели, реализующей принцип многофакторной голосовой верификации «что сказано + как сказано».

Практическая значимость результатов состоит в том, что разработанная модель служит готовой концептуальной основой для создания защищенных голосовых интерфейсов. Результаты работы могут быть непосредственно использованы:

- Разработчиками программного обеспечения при проектировании систем голосового управления для государственных и коммерческих организаций.
- Специалистами по информационной безопасности для формирования требований к внедряемым голосовым решениям и проведения их оценки на соответствие российским стандартам.
- Научно-исследовательскими коллективами в качестве отправной точки для дальнейших прикладных исследований в области поведенческой биометрии и устойчивости речевых систем к атакам.

Перспективы дальнейших исследований связаны с развитием предложенной модели. Наиболее важными представляются следующие направления: детальная алгоритмическая проработка и машинное обучение моделей для извлечения и классификации русскоязычных поведенческих признаков; исследование устойчивости поведенческих паттернов к целенаправленной долгосрочной мимикрии; разработка и испытание действующего прототипа системы на базе открытых отечественных речевых технологий; а также интеграция концепции в стандарты и методики построения защищенных человеко-машинных интерфейсов для объектов критической информационной инфраструктуры.

Таким образом, в рамках выпускной квалификационной работы не только проведен глубокий анализ проблемы безопасности голосового управления, но и предложено конкретное, обоснованное и методически

завершенное архитектурное решение, способное стать основой для создания новых защищенных информационных систем, отвечающих вызовам цифровой эпохи и строгим требованиям национальной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 24.02.2024).
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 04.08.2023).
3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
5. ГОСТ Р 57580.1-2017. Национальный стандарт Российской Федерации. Безопасность финансовых (банковских) операций. Биометрическая идентификация. Требования к системам контроля и управления доступом на основе биометрических данных. Часть 1. Общие положения.
6. ГОСТ Р ИСО/МЭК 27001-2022. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
7. ГОСТ Р 53114-2008 (ИСО/МЭК 15408-1:2005). Защита информации. Обеспечение безопасности информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

8. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
9. Галатенко, В. А. Основы информационной безопасности: учебное пособие для вузов / В. А. Галатенко. – 4-е изд., испр. и доп. – Москва: Интуит, 2020. – 536 с.
10. Лось, А. Б. Управление информационной безопасностью: учебник и практикум для вузов / А. Б. Лось, П. А. Лось, В. В. Мельников. – Москва: Юрайт, 2021. – 456 с.
11. Петраков, А. В. Основы практической защиты информации: учебное пособие / А. В. Петраков. – Москва: Радио и связь, 2020. – 368 с.
12. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. – Москва: ИД «Форум»: ИНФРА-М, 2019. – 416 с.
13. Расторгуев, С. П. Основы биометрической идентификации: учебное пособие для вузов / С. П. Расторгуев, А. В. Семкин. – Москва: Горячая линия – Телеком, 2018. – 280 с.
14. Чалгин, Н. Н. Речевые технологии: распознавание и синтез речи / Н. Н. Чалгин. – Санкт-Петербург: БХВ-Петербург, 2018. – 320 с.
15. Анисимов, А. В. Методы и средства защиты от атак на системы голосовой биометрии / А. В. Анисимов, Д. С. Козлов // Информационная безопасность. – 2022. – Т. 19, № 3. – С. 45-56.
16. Баранов, М. А. Анализ уязвимостей систем голосового управления в интернете вещей / М. А. Баранов, К. Л. Смирнов // Защита информации. Инсайд. – 2021. – № 4. – С. 32-41.
17. Васенин, В. А. Поведенческая биометрия: новые подходы к аутентификации пользователей / В. А. Васенин, Е. А. Калинина // Труды СПИИРАН. – 2020. – Т. 19, № 5. – С. 112-135.

18. Грибунин, В. Г. Моделирование угроз информационной безопасности: современные подходы и инструменты / В. Г. Грибунин, О. В. Максимов // Известия ЮФУ. Технические науки. – 2019. – № 10 (211). – С. 158-170.
19. Девянин, П. Н. Формальные модели политик безопасности при обработке биометрических данных / П. Н. Девянин // Прикладная дискретная математика. – 2021. – № 52. – С. 67-78.
20. Иванов, И. В. Адверсариальные атаки на системы распознавания речи: обзор и классификация / И. В. Иванов, С. К. Петров // Искусственный интеллект и принятие решений. – 2023. – № 1. – С. 22-35.
21. Коржов, А. Ю. Сравнительный анализ методов выделения просодических признаков для задач идентификации диктора / А. Ю. Коржов, М. П. Сергеева // Речевые технологии. – 2022. – № 2. – С. 15-28.
22. Крылов, В. В. Правовые аспекты использования биометрических персональных данных в Российской Федерации / В. В. Крылов // Закон. – 2020. – № 8. – С. 112-125.
23. Лебедев, А. Н. Архитектура системы защищенного голосового управления для объектов КИИ / А. Н. Лебедев, Т. А. Фролова // Вопросы кибербезопасности. – 2022. – № 5 (48). – С. 18-27.
24. Овчинский, А. С. Угрозы, связанные с использованием технологий глубоких фейков в аудиоданных / А. С. Овчинский, Е. В. Матвеев // Безопасность информационных технологий. – 2021. – Т. 28, № 4. – С. 77-89.
25. Прохоров, Д. А. Оценка устойчивости алгоритмов голосовой биометрии к спуфинг-атакам на основе синтеза речи / Д. А. Прохоров // Компьютерная оптика. – 2019. – Т. 43, № 6. – С. 1052-1060.
26. Семкин, А. В. Методы обнаружения аномалий в поведенческих профилях пользователей / А. В. Семкин, Н. Н. Чалгин // Системы высокой доступности. – 2020. – Т. 16, № 4. – С. 51-59.

27. Тихонов, А. И. Нейросетевые подходы к распознаванию русской речи в условиях шума / А. И. Тихонов, В. П. Яковлев // Информационно-управляющие системы. – 2021. – № 2. – С. 64-72.
28. Федотов, А. М. Применение отечественной речевой платформы Vosk для создания защищенных интерфейсов / А. М. Федотов // Открытые семантические технологии проектирования интеллектуальных систем (OSTIS-2023): материалы междунар. науч.-техн. конф., Минск, 16–18 февр. 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – С. 215-220.
29. Шестаков, В. И. Обеспечение безопасности в системах человеко-машинного взаимодействия: новые вызовы / В. И. Шестаков // Научно-технический вестник информационных технологий, механики и оптики. – 2020. – Т. 20, № 3. – С. 440-447.
30. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). – URL: https://www.fstec.ru/ (дата обращения: 15.04.2024).
31. Документация по открытой речевой платформе Vosk (поддержка русского языка). – URL: https://alphacephei.com/vosk/
32. Аналитический отчет «Угрозы голосовой биометрии – 2023». Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/
33. Соколов, Р. А. Разработка методов и средств повышения устойчивости систем голосовой биометрии к спуфинг-атакам: дис. … канд. техн. наук: 05.13.19 / Соколов Роман Андреевич. – М., 2021. – 178 с.
34. Филиппова, Е. Д. Модели и методы идентификации личности по динамическим признакам речи: автореф. дис. … д-ра техн. наук: 05.13.19 / Филиппова Елена Дмитриевна. – СПб., 2020. – 48 с.