СИНТЕЗ РЕЧЕОБРАЗНОГО ШУМА НА БАЗЕ МОДЕЛИ НЕЙРОННОЙ СЕТИ

Шуневич А.И., студент гр.362201, Макареня Е.А., студент гр.361401

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук, доцент

Аннотация. Проект «Синтез речеобразного шума на базе модели нейронной сети» посвящен разработке методов защиты речевой информации от утечек в условиях современного информационного общества. Основное внимание уделяется созданию акустических помеховых сигналов, адаптированных к конкретной речи с использованием машинного обучения. Исследуются существующие методы и устройства, а также разрабатываются алгоритмы для формирования речеподобных помех на русском языке. Работа направлена на повышение уровня безопасности конфиденциальных переговоров и может найти применение в бизнесе и государственных структурах.

Речевая информация, защита, помеховые сигналы, акустическая маскировка, нейронные сети, машинное обучение, конфиденциальность, алгоритмы, речеподобные помехи, информационная безопасность, анализ, синтез речи, технологии, сегментация, классификация, аудиосигнал, русский язык, фреймы, динамическое создание, системы защиты.

Речь является наиболее естественной формой человеческого взаимодействия и носителем множества конфиденциальной информации, включая личные данные, финансовые сведения и коммерческие тайны. Эта особенность делает речевую информацию уязвимой в контексте информационной безопасности, так как утечка таких данных может иметь серьезные последствия. В условиях стремительного развития технологий и нарастающей цифровизации угроза утечек данных становится все более актуальной, и защита речевой информации приобретает критическое значение. С каждым днем увеличивается количество устройств и платформ, на которых происходит обмен речевой информацией, что только усиливает необходимость в надежной защите.

Существующие методы защиты, такие как активная маскировка информации с помощью помехового сигнала, включают различные типы помех. К числу таких методов относятся белый шум, окрашенный шум и некоррелированная речеподобная помеха. Каждый из этих методов имеет свои преимущества и недостатки. Однако у всех них есть общая проблема: доступное в интернете программное обеспечение может эффективно компенсировать эти помехи, что ставит под угрозу безопасность речевой информации. Это создает необходимость в разработке более сложных алгоритмов и устройств, которые будут генерировать помеховой шум непосредственно из скрываемого речевого сигнала. Такой подход позволит создать уровень маскировки, при котором отделение информационного сигнала от помехового станет практически невозможным.

В частности, применение методов машинного обучения и искусственного интеллекта для динамического создания помехового сигнала, адаптированного к конкретной речи, может значительно повысить эффективность маскировки. Использование алгоритмов, которые учитывают интонации, паузы и другие особенности речи, может усложнить задачу для программного обеспечения, пытающегося распознать исходный сигнал. Это, в свою очередь, откроет новые горизонты в области защиты информации, так как позволит создать более совершенные системы, способные эффективно справляться с современными угрозами.

Таким образом, разработка новых методов защиты речевой информации становится не только желательной, но и необходимой в условиях постоянно меняющегося технологического ландшафта. Создание более надежных и адаптивных систем защиты позволит не только обеспечить безопасность конфиденциальных данных, но и повысить уровень доверия пользователей к технологиям, используемым для общения. Повышение уровня защиты речевой информации также может

способствовать развитию новых стандартов и практик в области информационной безопасности, что в конечном итоге принесет пользу обществу в целом.

Цель данной работы заключается в разработке метода формирования акустического помехового сигнала на основе речи дикторов, участвующих в конфиденциальных переговорах. Этот метод будет предназначен для использования в активных системах защиты информации и будет реализован в виде программно-аппаратного модуля, что позволит обеспечить высокую степень защиты.

Для достижения указанной цели сформулированы следующие задачи:

1. **Анализ существующих методов защиты речевой информации.** Необходимо изучить и оценить текущие технологии и подходы, используемые для защиты речевых данных, чтобы выявить их сильные и слабые стороны. Это позволит понять, какие элементы защиты работают эффективно, а какие требуют доработки.
2. **Обзор устройств формирования речеподобных помех.** Потребуется исследовать существующие устройства и технологии, которые могут генерировать помехи, имитирующие человеческую речь, и оценить их эффективность в контексте защиты информации. Это включает анализ того, как различные устройства справляются с задачами маскировки и какой уровень защиты они могут обеспечить.
3. **Создание речеподобных помех на русском языке.** Будет разработан алгоритм для формирования речеподобных помех с использованием компиляции фрагментов записи речи дикторов. При этом будет учитываться псевдотекст, который основывается на статистических особенностях русского языка. Это обеспечит более естественное звучание генерируемых помех, что важно для повышения их эффективности.
4. **Разработка программно-аппаратного средства.** На завершающем этапе работы будет создано программно-аппаратное средство, способное генерировать речеподобные помехи в реальном времени. Это устройство должно быть достаточно гибким, чтобы адаптироваться к различным условиям использования и обеспечивать высокий уровень защиты речевой информации.

Объектом исследования являются системы активной защиты информации, предназначенные для защиты речевых данных в различных сферах, включая бизнес и личные коммуникации. Это подчеркивает важность разработки универсальных решений, которые могут быть адаптированы к различным условиям и требованиям пользователей.

Предметом исследования являются алгоритмы анализа и синтеза речи, которые обеспечивают формирование речеподобных помех, способствующих повышению уровня безопасности информации. Эти алгоритмы должны быть достаточно мощными и гибкими, чтобы справляться с разнообразными задачами, возникающими в процессе защиты речевой информации.

Гипотеза: Современные системы активной защиты речевой информации используют помеховые сигналы, которые не обеспечивают необходимого уровня защиты. Эти сигналы могут быть эффективно компенсированы с помощью доступного программного обеспечения, что ставит под угрозу конфиденциальность передаваемой информации. В связи с этим предлагается новый подход, заключающийся в формировании маскирующего акустического сигнала непосредственно из скрываемого речевого сигнала. Этот метод позволит создать помехи, которые будут значительно сложнее для идентификации и компенсации, что повысит уровень защиты конфиденциальных переговоров.

В процессе исследования применялись различные методы и подходы, включая теоретические (анализ), эмпирические (эксперимент), общенаучные (синтез) и количественные (сбор и классификация данных). Эти методы обеспечили углубленное понимание проблематики защиты речевой информации и способствовали разработке эффективных стратегий.

Блоки установки:

1. **Блок загрузки сигнала.** В ходе цифровой обработки речевой сигнал представляется как последовательность отдельных стационарных фрагментов, известных как фреймы. На вход блока поступают отсчёты аудиосигнала, которые могут быть получены из файла или с микрофона. Затем сигнал разбивается на несколько фреймов (анализируемых окон) продолжительностью 0,07 секунды. Фреймы накладываются с частичным перекрытием, что позволяет избежать потерь информации на границах.

Далее полученная последовательность в каждом фрейме умножается на весовую функцию окна Хемминга. Эта функция акцентирует внимание на центральных данных и минимизирует затухание на краях. Формула для расчёта функции Хемминга представлена ниже.

2. **Блок детектирования речи.** Принцип функционирования блока обнаружения речи основывается на сравнении параметров сигнала с заранее установленными порогами. В качестве таких параметров используются среднеквадратичное значение сигнала, количество нулевых переходов и спектральная характеристика.

Среднеквадратичное значение (Root Mean Square) позволяет вычислить среднюю мощность сигнала в анализируемом окне и затем сравнить её с установленным пороговым значением. Формула для расчета среднеквадратичного значения сигнала:

$$RMS = \sqrt{\frac{1}{N}\sum_{i=1}^{N} x_i^2}$$

Среднее количество нулевых переходов сигнала может быть вычислено по формуле:

$$Z = \frac{1}{T}\sum_{t=1}^{T} |s(t)| \cdot \delta(s(t))$$

где δ — функция, указывающая на переход через ноль.

3. **Блок сегментации речи.** На вход блок сегментации получает массив речевых фрагментов, представляющих собой последовательность временных фреймов. Сегментация осуществляется путём вычисления расстояний между значениями классификационных параметров соседних фреймов. Для этой задачи было выбрано расстояние Минковского, так как оно обеспечивает наилучшее соотношение между количеством неверно определённых и пропущенных границ.

4. **Блок классификации речи.** Блок классификации речи принимает на вход сегментированный речевой сигнал и создает массив фонетических единиц, организованных по классам и дикторам. Эти данные затем сохраняются в базе аллофонов для каждого диктора. В основе процесса классификации лежит модель нейронной сети Salute Speech, которая обеспечивает высокую точность классификации фонетических единиц.

5. **База аллофонов дикторов.** База данных аллофонов предназначена для хранения и быстрого извлечения аллофонов, принадлежащих различным дикторам. Данные каждого диктора организованы отдельно, что позволяет эффективно управлять информацией. Это обеспечивает возможность предварительно загрузить уже сформированную базу данных для конкретного диктора или сохранить новосозданную базу для последующего использования.

6. **Блок формирования фонемного псевдотекста.** Для создания фонемного псевдотекста были проанализированы статистические характеристики русского языка с

испоыльзованием специального программного инструмента. В исследовании рассматривались тексты различных стилей с объемом более 80 тысяч символов каждый. Это обеспечило репрезентативность данных и позволило получить надежные статистические результаты преимуществ и недостатков представленных в таблице 1.

Таблица 1 – Преимущества и недостатки методов защиты

Метод	Преимущества	Недостатки
Белый шум	Простота реализации	Легко компенсируется
Окрашенный шум	Более естественное звучание	Уязвимость к специальным алгоритмам
Некоррелированная помеха	Сложнее для распознавания	Ограниченная эффективность
Речеподобные помехи	Высокая степень маскировки	Сложная реализация

В ходе выполнения работы была обоснована необходимость защиты речевой информации от утечек через акустические и вибрационные каналы. Современное общество сталкивается с множеством угроз, связанных с конфиденциальностью данных, особенно в условиях цифровой трансформации. Увеличение объема передаваемой информации, включая личные данные и коммерческие тайны, делает защиту речевой информации актуальной. Эта ситуация обостряется ростом числа кибератак и утечек данных, что подчеркивает важность разработки эффективных методов защиты.

Показано, что активные средства акустической маскировки представляют собой более эффективное решение для защиты речевой информации. Эти методы позволяют снижать отношение сигнал/шум в контролируемой зоне путем увеличения уровня шума, что делает распознавание и анализ речевого сигнала значительно более сложными. Использование новых технологий и алгоритмов, основанных на искусственном интеллекте и машинном обучении, позволяет динамически адаптировать помеховые сигналы к особенностям передаваемой информации и окружающей акустической среды. Разработанный модуль синтеза речеподобных сигналов включает в себя ключевые этапы, такие как обнаружение речи, её сегментацию, классификацию на аллофоны, формирование фонемного псевдотекста и компиляцию аллофонов. Каждый из этих этапов играет важную роль в создании эффективной системы защиты. Например, сегментация речи позволяет выделить ключевые моменты, которые должны быть замаскированы, а классификация на аллофоны обеспечивает более высокую точность и качество синтезируемых сигналов.

Актуальность данного проекта обусловлена растущей угрозой утечки конфиденциальной информации в условиях современного информационного общества. Технологический прогресс, связанный с развитием систем обработки речи и анализа данных, открывает новые возможности для злоумышленников, что делает защиту речевой информации необходимой. В условиях, когда утечки конфиденциальной информации могут привести к значительным финансовым и репутационным потерям, использование активных средств акустической маскировки становится важным. Современные системы защиты должны быть способны адаптироваться к меняющимся условиям и угрозам, что подразумевает не только использование статических методов, но и внедрение динамических алгоритмов, которые могут эффективно реагировать на новые вызовы.

Разработанные технологии и методы могут значительно повысить уровень защиты речевой информации, что делает проект вкладом в область информационной безопасности. Эта работа продвигает научные исследования в области обработки речи и имеет практическое значение для защиты конфиденциальной информации в различных сферах, таких как бизнес, государственные структуры и личные коммуникации. Применение полученных результатов может привести к созданию более безопасных систем передачи данных. В бизнесе это может обеспечить защиту переговоров, в государственных структурах — конфиденциальность государственных тайных данных, а в личной жизни — защиту от утечек личной информации. Использование новых технологий и методов может способствовать повышению доверия пользователей к современным средствам связи и улучшению

общей ситуации в области информационной безопасности.

Работа по разработке методов защиты речевой информации является шагом к созданию более безопасной среды для коммуникаций. Учитывая текущие тенденции в области информационных технологий, реализация предложенных решений может снизить риск утечек и повысить уровень защиты данных. Это позволит обеспечить безопасность не только личных, но и коммерческих интересов в условиях глобализированного мира. Успешная реализация данного проекта может стать основой для дальнейших исследований и разработок в области защиты информации, открывая новые горизонты для применения активных средств акустической маскировки и других инновационных технологий.

Список использованных источников:

1. Зайцев, А. П., Шелупанов, А. А., Мещеряков, Р. В., Голубятников, И. В., Солдатов, А. А., Скрыль, С. В. Технические средства и методы защиты информации - *горячая линия-Телеком, 2012.Россия.*

*2. Калинин, С. В., Кондратьев, А. В..*Защита информации: Учебное пособие - *инфра-М, 2015. Россия - М.: Книжный дом "ЛИБРОКОМ", 2014.*

*3. Кузнецов, А. В..*Методы защиты информации в компьютерных системах - *БХВ-Петербург, 2014.*

4. Смирнов, И. А. Информационная безопасность: Теория и практика - *Юрайт, 2016.*

SYNTHESIS OF SPEECH-LIKE NOISE BASED ON NEURAL NETWORK MODEL

Shunevich A.I., student of group 362201, Makarenya E.A., student of group 361401

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Zelmanovsky O.B. – Candidate of Technical Sciences, Associate Professor

Annotation. The project "Synthesis of Speech-Like Noise Based on Neural Network Model" is dedicated to developing methods for protecting speech information from leaks in the context of modern information society. The main focus is on creating acoustic noise signals adapted to specific speech using machine learning. Existing methods and devices are studied, and algorithms for generating speech-like noise in the Russian language are developed. The work aims to enhance the security of confidential negotiations and can be applied in business and government structures.

Keywords: speech information, protection, noise signals, acoustic masking, neural networks, machine learning, confidentiality, algorithms, speech-like noise, information security, analysis, speech synthesis, technologies, segmentation, classification, audio signal, Russian language, frames, dynamic creation, protection systems.