

ОТЗЫВ

официального оппонента

доктора технических наук, профессора Дворянкина Сергея Владимировича на диссертационную работу Волкова Никиты Андреевича на тему «Методика оценки защищенности акустической речевой информации от утечки по техническим каналам с применением сверточных нейронных сетей», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертации

Актуальность диссертационного исследования, проведенного Волковым Никитой Андреевичем, заключается в решении одной из приоритетных задач в области обеспечения информационной безопасности — защите акустической речевой информации от утечки по техническим каналам в помещениях, предназначенных для проведения закрытых переговоров. Для оценки защищенности информации в таких условиях применяется общепринятая инструментально-расчётная методика, основанная на результатах формантного метода Н.Б. Покровского.

Однако данная методика, будучи частным случаем более общего подхода, имеет ряд ограничений: не рассматривались условия с высоким уровнем маскирующих помех; не учитывались различия в спектрах речи дикторов; маскировка речи учитывалась только с помощью помех на основе белого шума, исключая возможность оценки защищенности с помощью помех типа «речевой хор». Эти особенности приводят к тому, что возможности применения методики в современных условиях оказываются ограниченными.

В контексте перечисленных ограничений исследование Волкова Никиты Андреевича приобретает особую значимость. Работа направлена на разработку методики оценки защищенности акустической речевой информации с использованием многоканальной системы сверточных нейронных сетей, анализирующей спектрограммы и графики мел-частотных кепстральных коэффициентов. Предложенная методика обеспечивает возможность оценки защищенности в условиях, недоступных для общепринятой методики, и позволяет формировать выводы, отражающие фактический уровень защищенности акустической речевой информации в помещениях.

Оценка структуры и содержания работы

Работа состоит из введения, шести глав, заключения, списка сокращений, списка литературы и приложений. Общее количество страниц — 172, включая 27 рисунков, 21 таблицу и 5 приложений. Список использованных источников состоит из 123 наименований.

Во введении сформулированы цель и задачи диссертационного исследования, обоснована его актуальность, а также выделены компоненты научной новизны работы и практическая значимость полученных результатов.

Первая глава посвящена анализу современного состояния исследований в области оценки защищенности акустической речевой информации. Рассматриваются основные технические каналы её утечки и существующие методы оценки разборчивости речи, включая общепринятую инструментально-расчётную методику, основанную на формантном методе Н.Б. Покровского. Показано влияние различных типов акустических помех на разборчивость речи и обозначены ограничения традиционных методов в условиях маскирующих воздействий. На основании проведённого анализа обосновывается необходимость разработки новой методики на основе сверточных нейронных сетей, определяются требования к представлению данных (спектрограммы, графики MFCC) и выбирается архитектура сверточной нейронной сети как наиболее подходящая для решения задачи.

Во второй главе рассмотрена методика предобработки данных, необходимой для обучения многоканальной системы сверточных нейронных сетей, применяемой для

оценки разборчивости акустической речевой информации. Представлен процесс формирования обучающих выборок: запись речевых сигналов дикторов с различными тембрами, наложение четырёх типов маскирующих помех в различных отношениях сигнал/шум, последующая классификация полученных аудиозаписей по уровню разборчивости и генерация спектрограмм и графиков MFCC. Приведены параметры, влияющие на формирование обучающих данных, включая длительность записей, размеры изображений и параметры спектрального анализа, а также выполнено обоснование выбора архитектуры сверточной нейронной сети и проведено обучение моделей на сформированных наборах данных.

В третьей главе представлена модель оценки разборчивости акустической речевой информации на основе многоканальной системы сверточных нейронных сетей. В главе описывается принцип работы модели - каждая нейронная сеть выполняет классификацию аудиозаписей по уровням разборчивости речи, после чего итоговое значение определяется с использованием мажорантной оценки, при которой выбирается максимальный индекс разборчивости из полученных результатов. Такой механизм согласуется с концепцией оценки защищённости через наихудший сценарий и позволяет получать достоверную оценку уровня разборчивости акустической речевой информации.

В четвёртой главе предложена методика оценки защищённости акустической речевой информации, основанная на анализе распределения энергии речевого и маскирующего сигналов в акустическом спектре. В отличие от общепринятой инструментально-расчётной методики, в предлагаемом подходе используется тестовый сигнал в виде последовательности аудиозаписей речи нескольких дикторов, что позволяет учитывать спектральные особенности реальной речи при различных типах помех. На основе определённого уровня разборчивости формируется показатель защищённости и вводится пороговый критерий, позволяющий определить, обеспечивает ли объект требуемый уровень защищённости. В главе также рассматриваются отличия предлагаемой методики от общепринятого подхода и возможность её практической реализации.

Пятая глава посвящена реализации разработанной методики оценки защищённости акустической речевой информации в виде программно-аппаратного комплекса. В ней показана структура комплекса, включающей модули подготовки аудиоданных, формирования спектрограмм и графиков MFCC, определения уровня разборчивости речи и последующего определения показателя защищённости. Представлены основные этапы обработки и взаимодействие программных компонентов, а также принципы построения интерфейса и структуры комплекса, обеспечивающие возможность практического применения предложенной методики.

В шестой главе представлена апробация разработанной методики в реальных условиях и сравнению её результатов с субъективной оценкой и общепринятой инструментально-расчётной методикой. Представлены данные измерений при различных типах помех, выполнена статистическая обработка результатов и рассчитаны показатели погрешности и достоверности. Анализ показывает, что общепринятая методика во многих случаях существенно расходится с субъективными оценками, тогда как разработанная методика демонстрирует высокую согласованность с ними и обеспечивает отклонение показателя защищённости от субъективных данных не более 4% в наиболее значимом диапазоне. Полученные результаты подтверждают адекватность методики и её практическую применимость.

В заключении приведены основные результаты диссертационного исследования.

Приложения содержат программные коды обучения сверточной нейронной сети на наборах данных, статистическая обработка результатов измерений разборчивости речи, а также акты о внедрении результатов работы.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Представленные в диссертации научные положения, выводы и рекомендации являются обоснованными и подтверждаются корректным выбором и применением методов исследования, а также ясной постановкой целей и задач работы. Диссертация выстроена логично и последовательно, её материалы сопровождаются достаточным набором иллюстраций и таблиц, которые наглядно отражают полученные результаты. Содержание автореферата адекватно передаёт основные идеи и положения диссертационной работы. Отмеченные результаты соответствуют пунктам паспорта научной специальности 2.3.6 «Методы и системы защиты информации; информационная безопасность».

Достоверность полученных результатов подтверждается проведённым сравнительным анализом значений разборчивости и показателей защищённости, измеренных при помощи разработанной методики, с данными субъективных испытаний и результатами общепринятой инструментально-расчётной методики. Установленная высокая степень согласованности, а также отклонение не более 4 % в наиболее значимом диапазоне демонстрируют корректность предложенного подхода. Все положения, выносимые на защиту, логически вытекают из теоретических обоснований и подтверждаются экспериментальными данными, не противоречащими известным принципам оценки защищённости акустической речевой информации. Дополнительным подтверждением достоверности служит практическая апробация методики при различных типах маскирующих помех и наличие публикаций автора по теме исследования.

Научная новизна полученных результатов

Наиболее существенные новые научные результаты, полученные в диссертационной работе, отражают авторский вклад в развитие методик оценки защищённости акустической речевой информации от утечки по техническим каналам. К новым научным результатам, полученным в диссертационном исследовании, относятся следующие:

1. Методика предобработки данных для оценки разборчивости акустической речевой информации, отличающаяся созданием зашумлённых аудиозаписей речи со множеством незначительных стохастических вариаций амплитуды шумового сигнала, а также классификацией аудиозаписей по уровням разборчивости речи на основе анализа распределения энергии речевого и маскирующего сигнала в акустическом спектре, что позволяет формировать обучающие наборы данных для многоканальной системы сверточных нейронных сетей при оценке защищённости акустической речевой информации от утечки по техническим каналам.

2. Модель оценки разборчивости акустической речевой информации на основе многоканальной системы сверточных нейронных сетей, отличающаяся использованием отдельных каналов обработки спектрограмм и графиков мел-частотных кепстральных коэффициентов и обеспечивающая учёт высокого уровня маскирующих помех, различных спектров помех на основе белого шума, помех типа «речевой хор», а также различий в спектрах речи дикторов при определении уровня разборчивости речи на основе мажорантной оценки.

3. Методика оценки защищённости акустической речевой информации, отличающаяся от общепринятой инструментально-расчётной методики переходом от измерения интегральных уровней сигналов в октавных полосах частот к анализу распределения энергии речевого и маскирующего сигнала в акустическом спектре, а также наличием тестового сигнала в виде последовательности аудиозаписей речи дикторов, что обеспечивает повышение достоверности оценки защищённости акустической речевой информации в наиболее значимом диапазоне значений показателя защищённости.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость результатов диссертационной работы заключается в разработке методики предобработки данных, модели оценки разборчивости акустической речевой информации на основе многоканальной системы сверточных нейронных сетей, а также методики оценки защищенности акустической речевой информации. Полученные результаты развивают существующие подходы к оценке защищенности акустической речевой информации от утечки по техническим каналам.

Практическая значимость результатов, представленных автором диссертации, определяется разработкой программно-аппаратного комплекса для оценки защищенности помещений при проведении закрытых переговоров в условиях высокого уровня маскирующих помех, включая различные спектры помех на основе белого шума и помехи типа «речевой хор», с учётом различий в спектрах речи дикторов. Результаты испытаний подтверждают высокую точность оценки словесной разборчивости речи (более 90 %) и возможность практического применения разработанной методики.

Замечания по работе

1. В диссертационной работе не представлены модель угроз и модель нарушителя. Отсутствие формализованного описания возможностей и ограничений нарушителя затрудняет интерпретацию условий, в рамках которых проводится оценка защищенности акустической речевой информации. В частности, в работе не рассматриваются потенциальные действия нарушителя, направленные на повышение разборчивости акустических речевых сигналов за счёт применения методов шумопонижения, фильтрации или иной постобработки сигналов, полученных за пределами защищаемого помещения. Учет подобных сценариев позволил бы более полно охарактеризовать область применимости предложенной методики и повысить строгость анализа условий утечки акустической речевой информации по техническим каналам.

2. В представленной работе выбор типов маскирующих помех, использованных при формировании экспериментальных данных и проверке методики, в целом выглядит обоснованным, однако в диссертации не приведены критерии, по которым именно эти группы помех были выделены в качестве базовых. Поскольку в реальных условиях могут применяться и другие виды маскирующих воздействий (тональные, импульсные, комбинированные и др.), полезно было бы обсудить, как предложенная методика будет вести себя при таких воздействиях, либо явно указать, что рассмотренные типы помех задают область применения и условия корректности оценки.

3. В работе в качестве входных данных для нейросетевых моделей используются как спектрограммы (для одного канала), так и графики мел-частотных кепстральных коэффициентов (для остальных каналов). При этом, поскольку мел-частотные кепстральные коэффициенты формируются на основе спектрального представления сигнала и по информативности близки к спектрограмме, возникает вопрос о целесообразности одновременного использования обоих представлений в разных каналах. Представляется целесообразным более явно пояснить, почему в составе методики сохранены именно спектрограммы, связав их применение с фонетической функцией Пирогова, согласно которой разборчивость речи в значительной степени определяется изменениями амплитудного спектра во времени. Такое пояснение сделало бы выбор признаков представлений более прозрачным.

4. Автором, при анализе воздействия речеподобных маскирующих помех, рассмотрена только помеха типа «речевой хор», тогда как в целом класс речеподобных помех является существенно более широким и активно исследуется в работах ряда отечественных и зарубежных авторов. При этом иные разновидности речеподобных маскирующих воздействий в рамках исследования не рассматриваются. Более детальное обсуждение существующих подходов к формированию и применению речеподобных помех, а также обоснование выбора помехи типа «речевой хор» в качестве представителя данного класса позволили бы более полно охарактеризовать область применимости предложенной методики оценки защищенности акустической речевой информации.

5. При построении спектрограмм в диссертационной работе используется окно Хэмминга, однако в тексте не обсуждаются причины выбора именно данного оконного преобразования. Между тем в ряде исследований показано, что окно Гаусса может обладать лучшими свойствами при анализе временно-спектральных характеристик сигналов. Представляется целесообразным либо обосновать использование окна Хэмминга в контексте решаемой задачи оценки разборчивости акустической речевой информации, либо сопоставить его с окном Гаусса с точки зрения влияния на формирование спектрограмм и последующую нейросетевую обработку.

Необходимо отметить, что вышеуказанные замечания не влияют на общую положительную оценку научных результатов выполненного соискателем диссертационного исследования и не снижают ценности полученных результатов.

Заключение

Диссертационная работа Волкова Никиты Андреевича по своей новизне и практической значимости является законченной научно-квалификационной работой, решающей актуальную задачу повышения достоверности оценки защищенности акустической речевой информации за счет учета реальных условий с использованием методики, основанной на многоканальной системе сверточных нейронных сетей.

Диссертационная работа соответствует требованиям п. 9 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842 (с изменениями и дополнениями), а ее автор, Волков Никита Андреевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:

Доктор технических наук, профессор,
профессор кафедры стратегии и
технологии кибербезопасности (№43)
Института интеллектуальных
кибернетических систем,
ФГАОУ ВО «Национальный
исследовательский ядерный
университет «МИФИ»

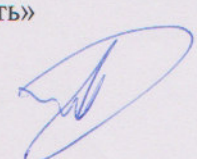


Дворянкин Сергей Владимирович

« 12 » 02 2026 г.

Докторская диссертация защищена по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»

Даю согласие на обработку персональных данных.



Адрес места основной работы:
115409, г. Москва, Каширское шоссе, дом 31
Рабочий телефон: +7 (495) 788-56-99
Адрес эл. почты: svdvoryankin@mephi.ru



Сергеев
НАЧАЛЬНИК ОТДЕЛА
АУП и УВП
МИКИРОВА Н.О.
и
Дата