

ОТЗЫВ

на автореферат диссертации Волкова Никиты Андреевича «Методика оценки защищенности акустической речевой информации от утечки по техническим каналам с применением сверточных нейронных сетей», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Современное развитие информационно-телекоммуникационных технологий и расширение сферы применения аудиокommunikаций в условиях обработки конфиденциальных данных определяют научную значимость исследования Волкова Н.А. Акустическая составляющая речевого сигнала сохраняет статус критически уязвимого информационного ресурса вследствие риска несанкционированного перехвата через технические каналы утечки информации (ТКУИ). Постоянное совершенствование аппаратуры разведывательного перехвата объективно обуславливает необходимость разработки и применения формализованных методологий количественной оценки защищенности речевых каналов, обеспечивающих верифицируемые гарантии конфиденциальности передаваемых сообщений.

В условиях совместного влияния активных маскирующих воздействий и интериндивидуальной вариативности акустико-фонетических параметров речевого сигнала количественная оценка уровня конфиденциальности акустической речевой информации приобретает характер некорректно поставленной обратной задачи. Данная некорректность проявляется в неустойчивости решений относительно возмущений входных данных и требует применения регуляризирующих методологий. Вследствие этого традиционные методики оценки защищенности, базирующиеся на упрощенных модельных предположениях, теряют прогностическую состоятельность, что объективно обуславливает необходимость разработки адаптивных вычислительных подходов, ориентированных на прямую обработку эмпирических акустических реализаций с учетом реальных

условий распространения звуковых волн в неконтролируемых акустических средах.

Предложенная автором методология количественной оценки защищенности акустической речевой информации реализована в виде многоканальной архитектуры глубокого обучения, построенной на ансамбле специализированных сверточных нейронных сетей (CNN). Архитектура обеспечивает нелинейное отображение из пространства спектрограммных представлений в пространство метрик разборчивости речи, при этом весовые коэффициенты сверточных фильтров адаптивно настраиваются на выделение дифференциальных признаков, чувствительных к степени маскирования информативных формантных областей. В результате формируется классификационная оценка уровня конфиденциальности акустического канала, обоснованная эмпирическими закономерностями восприятия речи человеком и инвариантная к интериндивидуальной вариативности дикторов и акустическим искажениям среды распространения.

Предложенный подход позволяет формализовать задачу оценки защищенности акустического канала как проблему статистического обнаружения сигнала на фоне аддитивных и нестационарных помех в спектрально-временной области. Анализ распределения энергии речевого и маскирующего сигналов в базисе, адаптированном к локальным особенностям речевого потока, обеспечивает выделение информативных признаков, инвариантных к вариативности диктора и условиям распространения звука. Такая методология повышает аргументированность решений о наличии технического канала утечки информации (ТКУИ).

Автореферат отражает концептуальные основы, целеполагание и содержательную структуру диссертационного исследования, а также корректно фиксирует научную новизну и теоретико-практическую значимость полученных результатов.

К числу фундаментальных научных результатов, составляющих основной вклад работы, относятся:

- разработанная методика предварительной обработки акустических данных, включающая формирование спектральных представлений речевых сигналов и маскирующих помех и подготовку данных для последующей

нейросетевой обработки, что обеспечивает корректность оценки разборчивости речи в условиях воздействия маскирующих помех и различий параметров речи дикторов;

– оригинальная вычислительная модель оценки разборчивости речи на основе многоканальной системы сверточных нейронных сетей, использующей спектрограммы и графики MFCC в качестве входных данных и реализующей определение итогового значения показателя на основе мажорантной оценки по наихудшему сценарию среди рассматриваемых вариантов представления сигнала;

– разработанная методика оценки защищенности акустической речевой информации, основанная на анализе распределения энергии речевого и маскирующего сигналов в акустическом спектре, а также с использованием тестового сигнала в виде набора аудиозаписей речи дикторов, что обеспечивает повышение достоверности оценки в наиболее значимом диапазоне значений показателя защищенности.

Результаты диссертационного исследования опубликованы в 4 статьях из Перечня ВАК и в двух изданиях, индексируемых Scopus, апробированы на всероссийских и международных научных конференциях.

Замечания по тексту автореферата:

1. В автореферате не рассмотрена возможность дообучения моделей сверточных нейронных сетей многоканальной системы после ее развертывания. Не ясно, можно ли и каким образом добавлять в систему данные о новых типах помех или дикторов для повышения ее точности и адаптивности без замены всего программного обеспечения.

2. Не описана форма итогового документа (протокола измерений), который должен формироваться по результатам работы комплекса. Не указано, какие именно данные (например, значения разборчивости по каждому диктору, рассчитанный показатель защищенности, использованный порог) автоматически вносятся в этот отчет для его полноты и соответствия стандартам отчетности в области оценки защищенности.

Сформулированные замечания носят уточняющий и редакционный характер, не затрагивают фундаментальных положений исследования и не влияют на научную состоятельность полученных результатов.

Диссертация «Методика оценки защищенности акустической речевой информации от утечки по техническим каналам с применением сверточных нейронных сетей» является законченной научно-исследовательской работой, обладающей научной новизной и практической значимостью. Работа соответствует требованиям п. 9 «Положения о присуждении ученых степеней», предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, 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.

Заведующий кафедрой управления
информационной безопасностью
федерального государственного
бюджетного образовательного
учреждения высшего образования
«Уфимский университет науки и
технологий», доктор физико-
математических наук, доцент

И.С.И.

Исмагилова
Альбина Сабирьяновна
«9» февраля 2026 г.

Докторская диссертация защищена по специальности 02.00.04 – Физическая химия (физико-математические науки).

Даю согласие на обработку персональных данных.

Адрес места основной работы:

450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, дом 32/1

Рабочий телефон: +7 (347) 273 66 92

Адрес эл. почты: ismagilovaas@yandex.ru

