АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

Голобородько Д.В., Олейніков А.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист мовної інформації є актуальною проблемою сучасних телекомунікаційних систем, оскільки мовні канали зв'язку залишаються вразливими до різноманітних загроз інформаційній безпеці. Розвиток цифрових технологій обробки мовних сигналів створює нові виклики для забезпечення конфіденційності та автентичності голосових даних, особливо в контексті критичної інфраструктури [1, 2]. Метою роботи є аналіз сучасних методів захисту мовної інформації в телекомунікаційних системах та розробка рекомендацій щодо побудови багаторівневих систем захисту голосових комунікацій з урахуванням вимог до якості передачі мовлення в реальному часі. Основні загрози включають пасивне прослуховування каналів, активні атаки з модифікацією голосових даних, підміну голосу користувача та несанкціонований аналіз мовних записів із застосуванням методів машинного навчання. Зростання обчислювальних потужностей дозволяє атакуючим застосовувати складні алгоритми розпізнавання мовлення, що підвищує ризики витоку конфіденційної інформації [3].

У роботі розглядаються криптографічні методи, що базуються на математичних перетвореннях мовних потоків з використанням симетричних та асиметричних алгоритмів шифрування. Симетричні алгоритми забезпечують високу швидкість обробки та низькі затримки, що критично важливо для голосових комунікацій. Критичною особливістю є дотримання обмежень на затримки обробки, оскільки затримки понад 150 мілісекунд призводять до помітного погіршення якості інтерактивного спілкування.

Стеганографічні методи дозволяють вбудовувати додаткові дані в мовний сигнал через модифікацію його параметрів з мінімальним впливом на сприйняття

якості мовлення. Це досягається використанням психоакустичних моделей людського слуху. Стеганографічні підходи ефективно застосовуються для передачі службової інформації про стан захищеності каналу або додаткових ключових даних [4]. Методи скремблювання забезпечують захист через трансформацію часової або частотної структури сигналу. Часове скремблювання здійснює перестановку коротких сегментів мовного сигналу, тоді як частотне скремблювання інвертує спектральні компоненти. Проте ці методи забезпечують обмежений рівень захисту і використовуються як додатковий рівень безпеки. У доповіді також розглядаються методи запобігання несанкціонованому документуванню мови з використанням акустичного ультразвукового та електромагнітних методів подавлення. Біометричні методи верифікації базуються на аналізі унікальних характеристик голосу диктора з використанням статистичних моделей на основі мел-частотних кепстральних коефіцієнтів. Ці методи дозволяють аутентифікувати користувача та здійснювати періодичну верифікацію протягом розмови. Розвиток технологій синтезу мовлення вимагає вдосконалення методів виявлення спуфінгу та атак з використанням штучно згенерованого голосу [4]. Найбільш ефективним є побудова багаторівневої системи безпеки, що включає криптографічне шифрування каналу, біометричну аутентифікацію учасників та стеганографічне приховування службової інформації. Важливою є реалізація механізмів адаптивного управління рівнем захисту залежно від поточної оцінки загроз та доступних обчислювальних ресурсів [5]. Перспективні напрямки досліджень пов'язані з використанням квантових технологій для генерації криптографічних ключів, застосуванням методів глибокого навчання для виявлення аномалій у голосовому трафіку та розробкою захисту від атак з використанням синтезованого голосу та дипфейків. Забезпечення надійного захисту мовної інформації вимагає комплексного застосування методів різної природи. Вибір засобів має базуватися на аналізі специфічних загроз та врахуванні вимог до якості передачі мовлення. Подальший розвиток систем захисту має спрямовуватися на створення адаптивних рішень з автоматичним підбором конфігурації захисту.

Список літератури

1. Засоби та системи технічного захисту інформації: Навчальний посібник для студентів ЗВО / І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов, В. Д. Кукуш, І. О. Милютченко. 2-е вид., перероб. і доп. Харків: ХНУРЕ, 2024. 266 с.

2. Рубан І. В., Міхаль О. П. Методи захисту інформації в телекомунікаційних мережах критичного застосування. *Системи обробки інформації*. 2024. № 3. С. 45-52.

3. Сєвєрінов О. В., Ляшенко О. С. Біометричні методи ідентифікації в системах захисту інформації. *Радіоелектронні і комп'ютерні системи*. 2024. № 2. С. 118-125.

4. Kuchuk N., Kovalenko A. Approaches to synthesis of informational and technical structures of critical application object's control system. *Advanced Information Systems*. 2024. Vol. 8, No. 3. P. 34-40.

5. Ruban I., Sievierinov O. Method of voice information protection in telecommunication systems. *Telecommunications and Radio Engineering*. 2024. Vol. 83, No. 2. P. 15-24.