УДК 004.056

А. О. Лівандовська
В. С. Катаєв

МОЖЛИВОСТІ НЕСАНКЦІОНОВАНОГО ОТРИМАННЯ МОВНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ ОПТИЧНИЙ КАНАЛ ВИТОКУ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

Проведено дослідження можливостей несанкціонованого доступу до мовної інформації через оптичні канали витоку. Окрему увагу можливості відновлення змісту розмови за допомогою технологій відеоаналізу рухів губ (ліпсингу). Наведено приклад системи штучного інтелекту LipNet, яка демонструє високу точність розпізнавання мовлення за відеозаписом.

Ключові слова: витік інформації, несанкціонований доступ, оптичний канал, ліпсинг

Abstract

The study investigates the possibilities of unauthorized access to speech information through optical information leakage channels. Special attention is given to the potential reconstruction of conversation content using video-based lip movement analysis technologies (lipreading). An example of the artificial intelligence system LipNet is presented, which demonstrates high accuracy in speech recognition based on video recordings.

Keywords: information leak, unauthorized access, optical channel, lipsing

Вступ

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням обсягів обміну даними, зокрема мовною інформацією, яка є, мабуть, головною формою комунікації між людьми. Особливої актуальності проблема захисту даної інформації набуває в умовах підвищених вимог до інформаційної безпеки, що обумовлено як розвитком технічних засобів розвідки, так і зростанням кіберзагроз. Розмови можуть містити конфіденційну, комерційну, службову або навіть таємну інформацію, витік якої здатен призвести до значних матеріальних, репутаційних і навіть національних безпекових втрат. Крім того, сучасні технології обробки сигналів і штучного інтелекту значно спрощують завдання аналізу та відновлення мовних сигналів навіть за умов їх часткового спотворення або перешкод, а в деяких випадках зміст розмови можна отримати навіть не прямим методами без перехоплення самих акустичних сигналів, зокрема через оптичні канали витоку інформації із застосуванням технології ліпсингу, тощо. У зв'язку з цим аналіз загроз для мовної інформації є важливим науково-практичним завданням, що потребує дослідження навіть тих сценаріїв, які на перший погляд можуть здаватись малоймовірними.

Результати дослідження

Мовна інформація — це сукупність відомостей, що передаються за допомогою усного мовлення у вигляді акустичних сигналів. Вона формується внаслідок роботи мовного апарату людини та являє собою звукові хвилі, які поширюються в повітряному середовищі приміщення або відкритого простору. Такі сигнали характеризуються певними фізичними параметрами, зокрема частотою, амплітудою та спектральним складом, що дозволяє ідентифікувати зміст повідомлення та особливості мовця. У межах приміщення мовна інформація може поширюватися не лише безпосередньо через повітря, а й частково передаватися через конструкції будівель, інженерні комунікації та інші середовища, що створює додаткові ризики її несанкціонованого перехоплення.

Враховуючи фізичну природу мовної інформації як акустичних коливань, більшість технічних каналів витоку інформації (ТКВІ) так чи інакше пов'язані з їх перетворенням, передаванням або побічним відтворенням. Незалежно від конкретного способу перехоплення — через повітряне середовище, вібрації конструкцій, електроакустичні перетворення чи побічні електромагнітні випромінювання — першоджерелом інформації в таких каналах залишається саме акустичний

сигнал, що виникає під час мовлення. Переважна більшість таких каналів витоку є загальновідомими, достатньо добре дослідженими та описаними в науково-технічній літературі, що створює основу для розробки ефективних заходів їх виявлення та нейтралізації [1]. Однак, існують і загрози, які на перший погляд, можуть здатися абсолютно безпечними саме для мовної інформації, оскільки в першу чергу вони використовуються для отриманні інших видів інформації, до таких загроз відносяться оптичні ТКВІ. Оптичний канал витоку інформації – це шлях, через який конфіденційні дані стають відомими зловмиснику у вигляді зображення, відео та фотокопій. Тобто, головним чином, даний канал направлений на отримання інформації з друкованих документів, екранів пристроїв, проєкторів і т. д. Способи отримання інформації даним каналом можна поділити на два основних види – це спостереження за об'єктом та зйомка об'єкта розвідки. Спостереження за об'єктом відбувається при безпосередній присутності зловмисника та триває протягом певного періоду. Зйомка об'єкта не вимагає постійної присутності зловмисника, проводиться для документування результатів спостереження і більш докладного вивчення об'єктів з часом [2]. Обидва способи не вимагають фізичного проникнення зловмисника в середину об'єкту і можуть реалізовуватись, наприклад, через вікна приміщення.

Таким чином, через оптичний канал може бути здійснено відеозапис процесу розмови людини: навіть за відсутності можливості чути звук, на записі добре фіксуються міміка, рухи губ та артикуляційні особливості оратора. Отримані візуальні дані можуть бути використані для подальшого аналізу та часткового відновлення змісту розмови із застосуванням сучасних методів обробки зображень та алгоритмів розпізнавання мовлення за відеосигналом, що підкреслює актуальність захисту не лише акустичних, а й візуальних каналів витоку інформації, така технологія називається ліпсинг. Ліпсинг – це метод читання по губах, саме ця технологія поєднує в собі як оптичний канал, так і акустичний, оскільки первинним джерелом є мовлення людини.

На сьогодні існують засоби та програмне забезпечення, розроблені спеціально для збору інформації за технологією ліпсингу. Наприклад, учені з Оксфордського університету описали систему штучного інтелекту, яка називається LipNet, вона може точно читати по губах [3]. Особливістю LipNet є здатність обробляти цілі речення, а не окремі слова, що підвищує імовірність правильної інтерпретації. Модель реалізує підхід «end-to-end» і поєднує просторово-часові згорткові нейронні мережі з рекурентними структурами та методом Connectionist Temporal Classification (CTC), що дозволяє безпосередньо перетворювати послідовність відеокадрів на текстовий результат на рівні повних речень. За результатами експериментальних досліджень на стандартному наборі даних GRID **corpus** система продемонструвала точність розпізнавання на рівні понад 95%**,** що суттєво перевищує показники попередніх методів і підтверджує високу ефективність використання візуальної інформації для відновлення змісту мовлення.

Саме такі новітні технології створюють небезпеку несанкціонованого доступу. Для того, щоб забезпечити конфіденційність даних необхідно:

- використовувати щільні світлонепроникні штори або вертикальні жалюзі;
- застосовувати правило «чистого столу»;
- звертати увагу на розташування моніторів у кімнаті щодо вікон та дзеркальних поверхонь;
- контролювати відвідувачів приміщень.

Такі способи, які на перший погляд можуть виглядати занадто простими, є найбільш дієвими для захисту себе від оптичного каналу витоку інформації.

Висновок

У підсумку, можна стверджувати, що оптичні канали витоку інформації створюють суттєву загрозу для забезпечення захисту конфіденційних даних, а новітні технології забезпечують миттєве читання по губах, що порушує таємність розмов навіть за умови повної звукоізоляції приміщення. Це підкреслює необхідність комплексного підходу до захисту інформації, що включає не лише традиційні методи контролю доступу, а й організаційні та фізичні заходи захисту від оптичного спостереження. Використання простих, але ефективних заходів такі як штори чи жалюзі дозволяє суттєво знизити ризик несанкціонованого перехоплення мовної інформації, забезпечуючи конфіденційність і безпеку комунікацій у сучасному інформаційному середовищі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аль-Амморі А., Іщенко Р., Дяченко П., Німич І. Фізичні механізми утворення технічних каналів витоку акустичної інформації // Системи управління, навігації та зв'язку. – 2025. – Том. 3, №81. – С. 189–200.
2. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов. – К.: ІС33І НТУУ «КПІ», 2016. – 104 с.
3. Оксфордські вчені мають штучний інтелект, який може читати по ваших губах // ФУТУРО. URL: https://futuro.in.ua/news/243-oksfordcski-vcheni-mayut-shi-mozhe-chytaty-hubam.html (дата звернення: 16.03.2026).

Лівандовська Анастасія Олегівна – студентка групи 1БКС-23Б, кафедри захисту інформації факультету інформаційних технологій комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: anastasialivandovska@gmail.com

Катаєв Віталій Сергійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, kataev@vntu.net

Livandovska Anastasiia Olehivna – student of group 1BKS-23B, Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: anastasialivandovska@gmail.com

Vitaliy Kataiev Serhiyevich – assistant of the Department of Management and Security of Information Systems; Vinny-tsia National Technical University , Vinnytsia, kataev@vntu.net