1. A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies / K. Bennouk et al. Journal of Cybersecurity and Privacy. 2024. Vol. 4, no. 4. P. 853–908. DOI: https://doi.org/10.3390/jcp4040040

Біометрична автентифікації для платформ дистанційного навчання на основі голосових відбитків

УДК 004.056

Олена Головачова[1], Лідія Тимошенко[2]

Національний університет «Одеська політехніка»,
4507629@stud.op.edu.ua[1], l.m.timoshenko@op.edu.ua[2]

Актуальність теми зумовлена стрімким переходом освіти у цифровий формат в умовах пандемії, вимушеної міграції або навчання із зон конфлікту та необхідністю гарантувати академічну доброчесність та безпеку даних. Дистанційне навчання створює значні виклики для контролю знань [1]. Традиційні методи не дають 100% впевненості, що виконує завдання або дає усну відповідь саме той учень. Голосова біометрія дозволяє підтвердити особу, що запобігає підміни особи. На відміну від паролів, які можна передати іншим, унікальні характеристики голосу (тембр, висота, ритм) підробити значно складніше.

Метою роботи є розробка захищеної архітектури системи голосової біометричної автентифікації для підвищення рівня безпеки та академічної доброчесності в дистанційній освіті.

Основною проблемою ідентифікації учнів при дистанційному навчанні є виявлення того, що відповідає саме учень, а не стороння особа, нейромережа, або використовується запис. При побудові архітектури для освітніх платформ безпека передачі даних є критично важливою. Оскільки будь-яке перехоплення даних може мати серйозні наслідки. Коли учень вимовляє фразу, дані проходять шлях від мікрофона до сервера. Аудіопотік має шифруватися, кожен пакет голосових даних має підписуватися унікальним токеном учня. Аудіопотік передається під час верифікації, його не можна зберігати довго, після виділення математичних ознак він має видалятися. Потім звук перетворюється у математичний вектор До голосового вектора додається «сіль» — випадкове унікальне число, прив'язане до унікального токену учня [2]. Додавання «солі» до біометричних даних робить систему стійкою до атак через витік бази даних. Навіть якщо зловмисник викрав голосові вектори, він не зможе порівняти їх між собою або використати в іншій системі, бо кожен вектор має унікальний ключ. «Сіль» завжди однакова для одного учня, це дозволяє проводити порівняння. Якщо учень видаляється із системи, сервер видаляє «сіль». Без цієї специфічної «солі» відновити оригінальний голосовий вектор із бази практично неможливо. Далі числовий код голосу (голосовий вектор) шифрується за допомогою алгоритму AES-256[2]. Події логуються, вони розділені на три типи: пройдена - успішна ідентифікація, попередження – низька схожість, критична – виявлена підробка або підозра на атаку. Для порівняння біометричних шаблонів використовується косинусна подібність[3].

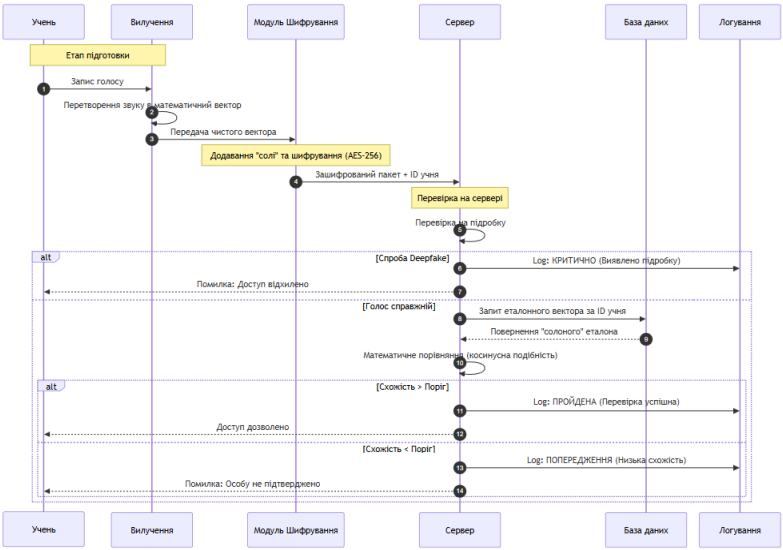

Рис. 1. Процес голосової верифікації

Архітектуру системи можна розподілити на чотири загальні рівні: збору даних, безпеки, серверної обробки, даних та аудиту. Така архітектура реалізує принцип конфіденційності, тому що, в системі ніде не зберігається запис оригінального голосу, через додавання «солі» дані є анонімними та кожен крок контролюється модулем безпеки. Процес голосової верифікації наведено на рис.1.

Ідентифікації за голосом сприяє самодисципліні. Учень розуміє, що система розпізнає особистість, це зменшує спокусу вдатися до допомоги сторонніх осіб або використанню синтезованого мовлення (deepfakes). Це, в свою чергу, сприяє вихованню академічної відповідальності. Використання сучасних біометричних методів захисту у повсякденному навчанні підвищує загальний рівень цифрової культури учнів. Це готує їх до життя у високотехнологічному суспільстві, де біометричні стандарти вже стають нормою безпеки.

1. Левченко Я.С., Семененко І.Є. Деякі особливості проблеми диференційованого оцінювання в системі дистанційного навчання, URL: https://www.innovpedagogy.od.ua/archives/2022/52/part_1/26.pdf.
2. Костюк Ю. В., Складанний П.М. Захист інформації в комп'ютерних системах та мережах. Частина І: підручник – Київ : Київський столичний університет імені Бориса Грінченка, 2026. – 401 с., URL: https://elibrary.kubg.edu.ua/id/eprint/56332/1/ZIKSM_part_1_2026_FITM.pdf
3. Cosine Similarity. URL: https://www.geeksforgeeks.org/cosine-similarity/