

6. Hosnieh Sattar, Mario Fritz, and Andreas Bulling. Deep gaze pooling: Inferring and visually decoding search intents from human gaze fixations. *Neurocomputing*, 387:369–382, 2020. doi: <https://doi.org/10.1016/j.neucom.2020.01.028>.
7. Florian Strohm, Ekta Sood, Sven Mayer, Philipp M^uller, Mihai B[^]ace, and Andreas Bulling. Neural photofit: Gaze-based mental image reconstruction. In *Proc. IEEE International Conference on Computer Vision (ICCV)*, pages 1–10, 2021.

Малярєнко Д. С.

курсант факультету № 4 Харківського національного університету внутрішніх справ

Рвачов О. М.

старший викладач кафедри кібербезпеки та DATA-технологій факультету № 6 Харківського національного університету внутрішніх справ

СИНТЕЗ МОВЛЕННЯ: ВІД ІННОВАЦІЙ ДО КІБЕРЗЛОЧИННОСТІ

Сінтез мовлення (СМ) – це перетворення друкованого тексту на мовний сигнал. Система, яка може виконувати конвертування нормального друкованого тексту на аудіо в реальному часі називається text-to-speech (TTS) [1].

Основним завданням СМ є перетворення будь-якої текстової інформації в акустичний сигнал. З розвитком технологій цифрової обробки сигналів мета дослідження синтезу мовлення еволюціонувала від зрозумілості та чіткості до природності та виразності [2].

Розвиток синтезу голосу – це динамічний процес, що відзначився важливими науковими та технологічними досягненнями протягом останніх десятиліть. Історія цієї галузі охоплює ряд ключових подій і кроків, які допомогли сформувати сучасний синтез голосу [3]. Рішення для синтезу мовлення пропонують полегшений спосіб читання текстових документів зі смартфонів та комп'ютерів.

Технологія СМ допомагає в автоматизації різних процесів, таких як:

- увімкнення мовлення під час передпродажної та післяпродажної роботи, що мінімізує робоче навантаження на людей, скорочує операційні витрати та прискорює пропускну здатність;
- допомога людям, які мають обмежені можливості (особливо людям із вадами зору) та проблеми в навчанні, читанні, включно з порушенням навчання мови.

Прослуховування інформації з використанням функції СМ дає можливість:

- одночасно виконувати різні фізичні завдання, як-от приготування їжі, прибирання, фізичні вправи тощо;
- слухати матеріали під час подорожі та здійснювати переміщення за допомогою голосових підказок від навігатора [4].

Попри чималу користь технології TTS, є негативний аспект – стрімке зростання шахрайських схем зі застосуванням нейромережевого синтезу мови. Зловмисники здійснюють фішингові дзвінки під час яких, наприклад, імітують розмову з родичем, який, нібито, попав у надзвичайну ситуацію та негайно потребує фінансової допомоги.

Шахраї можуть використовувати синтезовані записи голоів керівників та працівників компаній, щоб отримати корпоративну інформацію, яку можна продати конкурентам чи отримати фінансову винагороду за її нерозповсюдження [5; 6].

На теперішній час технології синтезу голосу можуть імітувати тембр та інтонації голосу політиків та інших знаменитостей. Сторонні особи можуть озвучити чужим

голосом що завгодно, будь-який текст, у тому числі те, що власники голосів ні за яких обставин вимовляти не хотіли б – це може спричинити масове невдоволення, конфлікти, тощо [7].

Також зловмисники можуть синтезувати голоси співробітників банків або служб підтримки, щоб обманним шляхом примусити клієнтів таких установ надати доступ до своїх рахунків або іншої конфіденційної інформації [8]. Під час розмови для більшої переконливості шахраї можуть підмінити свій номер телефону на телефонні номери банків, різних державних організацій та великих відомих компаній, використавши можливості сучасної технології телефонії – Session Initiation Protocol (SIP) і Primary Rate Interface (PRI) [9].

Крім того, чимало кіберзлочинців продають послуги віртуальних дикторів. «Комп'ютерні крадії» пропонують потенційним покупцям несанкціоновано, оминаючи норми законодавства про авторські права, скористатись згенерованими за допомогою штучного інтелекту голосами відомих артистів для озвучування текстів.

Висновок: синтез мовлення є важливим для сьогодення, який постійно розвивається і з часом ставатиме лише кращим. Технологія TTS відкриває широкі можливості для доступу до інформації, покращення комунікації, допомозі людям з обмеженими можливостями та в багатьох інших сферах.

Проте на фоні позитивних аспектів використання СМ необхідно враховувати ризики та використання цієї технології для злочинних цілей. Зловмисники активно використовують синтетичні голоси для отримання конфіденційної інформації та неправомірного збагачення.

У майбутньому використання нейромережевого СМ без створення нормативної бази щодо їх використання назавжди може позбавити роботи дикторів та ставить під загрозу безпеку користувачів інтернет-сервісів.

Безсумнівно, сама технологія синтезу голосу важлива і корисна, але її використання необхідно врегулювати на державному рівні.

З огляду на ці виклики, важливо розробляти та впроваджувати ефективні методи захисту від синтетичних голосових атак, регулювати використання технології для запобігання її незаконному використанню та забезпечити дотримання авторських прав та етичних стандартів. Таким чином, розвиток синтезу мовлення повинен іти пліч-о-пліч із заходами щодо забезпечення безпеки, щоб забезпечити користь використання цієї інновації для суспільства.

Література

1. Учасники проєктів Вікімедіа. Синтез мовлення // Вікіпедія : вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Синтез_мовлення
2. Deep Learning Based Speech Synthesis / Y. Ning et al. // Encyclopedia MDPI | Scholarly Community. URL: <https://encyclopedia.pub/2975>
3. How speech synthesis works // Explain that Stuff : вебсайт. URL: <https://www.explainthatstuff.com/how-speech-synthesis-works.html>
4. 11 найкращих рішень синтезу мовлення для бізнесу та особистого використання // techukraine.net : вебсайт. URL: <https://techukraine.net/11-найкращих-рішень-синтезу-мовлення-дл/>
5. Українцям розповіли чому шахраї записують їх голос по телефону // GSMinfo : вебсайт. URL: <https://gsminfo.com.ua/32512-ukrayinczyam-rozpovily-chomu-shahrayi-zapysuyut-yih-golos-po-telefonu.html>

6. Кушнерик Т. Курйозний злочин. В ОАЕ шахраї пограбували банк, клонувавши голос директора // Главком | Glavcom: вебсайт URL: <https://glavcom.ua/economics/finances/kuryozniy-zlochin-v-oae-shahraji-pograbuvali-bank-klonuvavshi-golos-direktora-791319.html>
7. Нейромережу навчили говорити голосом Путіна, Познера і Собчак. Відео // Волинські новини : вебсайт. URL: <https://www.volynnews.com/news/all/neyromerezhunavchyly-hovoryty-holosom-putina-poznera-i-sobchak-video/>
8. Шахраї актуалізували схему «дзвінок із банку». Як вберегти свої кошти? // Hromadske | Громадське : вебсайт URL: <https://hromadske.ua/posts/nova-shema-obmanu-vid-shahrayiv-u-policiyi-rozpovili-detali>
9. Стало відомо, як шахраї роблять підміну телефонного номера // GSMinfo: вебсайт. URL: <https://gsminfo.com.ua/31827-stalo-vidomo-yak-shahrayi-robyat-pidminu-telefonnogo-numera.html>

Мейдич Р. О.

курсант факультету №4 Харківського національного університету внутрішніх справ

Лучик В. Є.

професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, доктор економічних наук

КІБЕРБЕЗПЕКА В СФЕРІ ІНТЕРНЕТ-ОСВІТИ

Через широкомасштабне вторгнення російської федерації на територію суверенної України, заклади до шкільної та середньої освіти були вимушені перейти на дистанційне навчання. Як показує статистика, близько 800 тисяч учнів перейшли з очної форми навчання на дистанційну[1]. Найбільше всього, це торкнулося південних та східних регіонів таких як: Харків, Луганськ, Запорізька та інші прифронтові регіони України [2]. Інші освітні заклади, перейшли або на змішану форму або на очну (звичайну) форму навчання. Але дистанційне навчання може бути і небезпечним. Наприклад, під час дистанційних занять, здобувач освіти, може зайти не на той сайт, або випадково вибрати не справжній сайт (наприклад систему Moodle чи Google Classroom або систему Google meet) та зайти на фішинговий сайт, що може призвести до того, що введені учнем його конфіденційні дані можуть потрапити у мережу або до злоумисників.

Фішинг – це вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані – наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів [3].

Крім ризику потрапити на фішинговий сайт, під час дистанційного навчання були виявлені такі проблеми як:

1. Обмежений доступ учнів до інтернету. У деяких регіонах України, особливо в прифронтових, доступ до інтернету є обмеженим або відсутнім. Це може ускладнювати участь учнів у дистанційних заняттях.
2. Відсутність у них цифрових пристроїв. У деяких сім'ях не вистачає коштів на придбання цифрових пристроїв, необхідних для дистанційного навчання. Це може ускладнювати або унеможливлювати участь таких учнів у дистанційних заняттях.