Forbidden and restricted access zones were defined for the objects in area B.

Analysis of Results. Statistical data processing demonstrated that as the number of iterations increases, the distribution of results converges to a normal distribution.

The findings indicate that utilizing the dual-level model allows for an average flight time gain of 19% compared to the maximum bypass trajectory. Such an indicator is critically important for the operational planning of UAV missions, particularly in electronic warfare, reconnaissance, and monitoring tasks under time-sensitive conditions.

Conclusions.

1. The application of an adaptive trajectory model instead of rigid "No-Fly Zones" significantly increases the efficiency of UAV utilization.

2. The dual-level access model ensures reliable protection of confidential information regarding critical objects even during the physical transit of the vehicle through their location zone.

3. The results confirm the algorithm's stability under the random distribution of objects, allowing for its recommended integration into the intelligent control systems of autonomous unmanned complexes.

1. Zhou, Y., Ma, L., & Wen, M. (2015). Task-Constrained RBAC Model and Its Privilege Redundancy Analysis. 2nd ISCE, pp. 489–492.
2. Ren, M., et al. (2024). Conception of Foreign Heterogeneous EW UAV Cross Domain Cooperative Operations. ICAUS 2023, vol 1171.
3. Zhang, Y., et al. (2023). Modeling and simulation of UAVs swarm electromagnetic operation. Systems Engineering and Electronics, Vol. 45(7).

Кібербезпека систем розпізнавання мовлення в реальному часі

УДК 004.056

Олег Єгоров[1], Тарас Кравченко[2]

Український державний університет науки і технологій,
[1]egoroffoleg@ukr.net, [2]t.o.kravchenko@ust.edu.ua

Розвиток технологій синтезу мовлення та deepfake-голосу створює нові кіберзагрози для систем розпізнавання мовлення. Синтетичний голос може використовуватися для підміни особи, обходу голосової автентифікації і несанкціонованого доступу до інформаційних ресурсів. За таких умов традиційні підходи до розпізнавання мовлення, орієнтовані переважно на точність і швидкодію, не забезпечують достатнього рівня захисту даних.

Актуальність дослідження зумовлена поширенням голосових сервісів і одночасним зростанням доступності засобів генерації синтетичного мовлення. Для систем реального часу особливо важливим є своєчасне виявлення deepfake-голосу без істотного збільшення затримки обробки, оскільки від цього залежить безпека доступу до даних і надійність роботи мовних сервісів.

Метою роботи є підвищення рівня захисту даних у системах розпізнавання мовлення реального часу шляхом виявлення deepfake-голосу та синтетичного мовлення на основі інтелектуального аналізу аудіопотоку.

Ефективне виявлення deepfake-голосу та синтетичного мовлення доцільно розглядати як окремий функціональний модуль, інтегрований у загальну систему розпізнавання мовлення. Такий модуль має працювати паралельно з основними етапами обробки аудіосигналу та виконувати попередню оцінку його автентичності ще до завершення процедури розпізнавання. Це дає змогу не лише підвищити надійність інтерпретації мовних команд, а й своєчасно запобігти обробці потенційно небезпечного вхідного сигналу.

Для виявлення синтетичного мовлення можуть використовуватися ознаки різної природи: спектральні характеристики сигналу, особливості часової структури, неприродна стабільність тембру, атипові переходи між фонемами, а також відхилення в ритміко-інтонаційній організації мовлення. У поєднанні з інтелектуальними методами аналізу такі параметри дозволяють формувати оцінку ймовірності штучного походження голосу. У межах захищеної архітектури системи розпізнавання мовлення результати такого аналізу можуть використовуватися для адаптивного керування подальшими діями системи. При підвищеному рівні ризику доцільно ініціювати додаткову перевірку користувача, блокувати доступ до окремих функцій або переводити обробку в режим підвищеного контролю. Цей підхід дозволяє поєднати вимоги до швидкодії з вимогами до безпеки без погіршення користувацького досвіду.

Отже, виявлення deepfake-голосу та синтетичного мовлення є важливою складовою підвищення кіберзахищеності систем розпізнавання мовлення в реальному часі. Інтеграція інтелектуальних механізмів аналізу аудіосигналу в архітектуру таких систем дозволяє своєчасно виявляти ознаки підробленого голосу, зменшувати ризик несанкціонованого доступу та підвищувати рівень захисту даних. Практичне значення цього підходу полягає у можливості створення адаптивних мовних сервісів, у яких забезпечуються не лише точність і швидкодія, а й стійкість до актуальних кіберзагроз.

Аналіз та виявлення аномалій у мережевому трафіку з використанням SLIPS

УДК 004.056.53 (004.75)

Анатолій Жуков[1], Сергій Чернишук[2]

Житомирський військовий інститут імені С.П. Корольова,
[1]anzhukov@ukr.net, [2]sergiy.chernyshuk@ukr.net

В умовах еволюції цілеспрямованих атак (APT) та поширення складного шкідливого програмного забезпечення, традиційні методи захисту, що базуються виключно на сигнатурах, стають недостатніми. За даними звіту IBM Cost of a Data Breach 2025, середня вартість витоку даних у світі сягнула рекордних показників, що підкреслює необхідність впровадження про активних засобів захисту [1]. Одним із найбільш перспективних інструментів для вирішення цієї проблеми є поведінковий аналіз трафіку, реалізований у відкритих проектах, таких як Stratosphere Linux IPS (SLIPS) [4].

Stratosphere Linux IPS - це модульна система виявлення вторгнень IDS/IPS, що базується на аналізі поведінки мережевих потоків. На відміну від класичних IDS, SLIPS орієнтована на виявлення патернів шкідливої активності, таких як