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

робота ботнетів та командно-контрольних каналів [2]. Система використовує наступні парадигми аналізу:

1. Профілювання тривалих з'єднань та виявлення періодичних сигналів дозволяє системі Slips ідентифікувати приховані канали керування C&C, оскільки вона фокусується не на аналізі окремих пакетів, а на тривалих поведінкових патернах мережевих пристроїв. Використовуючи потужності фреймворку Zeek, Slips відстежує часові інтервали активності та накопичує докази шкідливої поведінки, що дає змогу виявляти шкідливе ПЗ, яке підтримує зв'язок із сервером зловмисника через характерні низькочастотні «маяки».

2. Аналіз за допомогою нейронних мереж та машинного навчання у реальному часі є фундаментом Slips як першої вільної системи IDS/IPS, що базується на методах машинного навчання для детекції шкідливих дій [3]. Система застосовує адаптивні моделі для класифікації трафіку, зокрема аномалій у HTTPS-з'єднаннях, із підтримкою механізмів обробки дрейфу даних, а через субмодуль реалізує концепцію федеративного навчання для підвищення точності прогнозів без передачі конфіденційних даних

3. Інтеграція з Threat Intelligence та автоматизована перевірка загроз забезпечується шляхом постійного оновлення даних із понад 40 спеціалізованих джерел розвідки та можливості перевірки IP-адрес на зовнішніх платформах, таких як VirusTotal або RiskIQ. Особливої ефективності цьому підходу додає наявність P2P-модуля, який дозволяє вузлам Slips автоматично та безпечно обмінюватися індикаторами компрометації з іншими довіреними вузлами в мережі, формуючи спільну систему протидії кіберзагрозам [1].

Система поєднує декілька підходів, що дозволяє досягти високої точності при мінімізації помилкових спрацювань. Гібридні моделі, що поєднують глибоке навчання DL та класичне машинне навчання ML, демонструють найкращі результати в сучасних мережевих середовищах [4].

Порівняльну характеристику модулів SLIPS представлено у таблиці 1.

Таблиця 1

Характеристика модулів аналізу Stratosphere Linux IPS

Модуль аналізу	Тип виявлення	Перевага	Складність
Behavioral Module	Поведінковий	Виявляє невідомі C&C канали	Середня
Machine Learning	Алгоритмічний	Адаптація до нових типів трафіку	Висока
TI Module	Репутаційний	Миттєве виявлення відомих загроз	Низька
Ensemble Logic	Гібридний	Найнижчий рівень false positives	Висока

Ключовою особливістю SLIPS є використання алгоритмів машинного навчання для аналізу мережевих подій. Система перетворює мережеві потоки у текстове представлення, що дозволяє застосовувати методи обробки природної мови для пошуку аномалій. Для IoT-мереж, інтегрованих у Linux-інфраструктуру, особливо ефективним є поєднання методів Deep Learning, що забезпечує точну класифікацію підозрілих патернів. Це дозволяє виявляти активність шкідливого ПЗ навіть у зашифрованому трафіку без його дешифрації.

Сучасний стек технологій для аналізу трафіку за допомогою SLIPS включає інструменти захоплення Zeek і Suricata та обробки даних у реальному часі. Використання алгоритмів типу Isolation Forest підтвердило свою ефективність для швидкого виявлення аномалій у вебтрафіку. Платформа SLIPS використовує Redis для швидкого обміну даними між модулями та пропонує інструменти візуалізації інцидентів, такі як Kalipso.

Особливе значення має відкритість датасетів, на яких тренується SLIPS, наприклад, Stratosphere IoT Dataset, що дозволяє дослідникам адаптувати систему під специфічні потреби Linux-серверів або IoT-інфраструктур.

Stratosphere Linux IPS представляє собою сучасний приклад інтелектуальної системи захисту, яка успішно поєднує статистичний аналіз з методами глибокого навчання. Застосування SLIPS дозволяє значно підвищити рівень виявлення складних кіберзагроз за рахунок аналізу довгострокової поведінки вузлів мережі. Перспективами подальшого розвитку є вдосконалення модулів аналізу зашифрованого трафіку та автоматизація реагування на інциденти IPS mode в хмарних середовищах.

1. IBM Security. Cost of a Data Breach Report 2025. IBM Corporation, 2025.
2. Alsoufi M. A., et al. Anomaly-based intrusion detection model using deep learning for IoT networks. Computer Modeling in Engineering & Sciences. – 2024. – Vol. 141, №1. – P. 823–845.
3. Chua W., et al. Web traffic anomaly detection using Isolation Forest. Informatics. – 2024. – Vol. 11, №4. – P. 83.
4. Garcia S. Stratosphere Linux IPS: Behavioral-based Intrusion Detection System. Stratosphere Laboratory, 2025. URL: https://github.com/stratosphereips/StratosphereLinuxIPS

Cybersecurity for small and medium-sized businesses: a practical framework for organizations with limited resources

UDK 004.056.53

Iurii Zhurov

SMB Cybersecurity Advisors LLC, iurii.zhurov@smbsecurityadvisors.com

Over the past decade, the number of cyber incidents targeting small and medium-sized businesses (SMBs) has grown at an accelerating rate. According to the Verizon Data Breach Investigations Report (2024), 46% of cyberattacks in the United States are directed at SMBs, while 60% of businesses that suffer a significant cyber incident cease operations within six months [1]. At the same time, the SMB segment — over 33 million enterprises accounting for 44% of U.S. GDP [2] — remains critically underprotected. The root cause lies not in the absence of standards, but in their inapplicability under conditions of limited resources.

Existing information security frameworks — NIST Cybersecurity Framework 2.0, ISO/IEC 27001:2022, and CIS Controls v8 — were designed primarily for large organizations with dedicated security departments, certified personnel, and substantial implementation budgets. For SMBs that typically lack any dedicated cybersecurity specialist, full implementation of these standards is practically unfeasible.