КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.22.3138
УДК 336.71:004.056

Лаптєв Олександр Анатолійович
доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації Факультету інформаційних технологій
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID 000-0002-4149-402X
olaptiev@knu.ua

Зозуля Сергій Анатолійович
аспірант, старший викладач
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID 0000-0003-1733-1415
zozulya_sa@ukr.net

МЕТОД ВИКЛЮЧЕННЯ ВІДОМИХ СИГНАЛІВ ПРИ СКАНУВАННЯ ЗАДАНОГО РАДІОДІАПАЗОНУ

Анотація. Отримання доступу до інформації за допомогою засобів негласного отримання інформації залишається актуальним у теперішний час. Це обумовлено вагомими перевагами до яких відносяться неможливість виявлення фахівця, якій робить прослухування або відео контроль приміщення. Фахівець знаходиться на відстані від цього приміщення. Цілісністю інформації, тому що інформація надходить з першоджерела. Тому проблема виявлення радіосигналів засобів негласного отримання інформації є актуальним науковим завданням. Ця робота присвячена проблематики скорочення часу виявлення сигналів засобів негласного отримання інформації.

Виявлення радіосигналів засобів негласного отримання інформації обтяжується тим, що засоби негласного отримання інформації нового покоління працюють у цілком дозволеному радіодіапазоні і їх виявлення у приміщенні, яке межує з іншими, заповненими радіопристроями є проблематичним. Зараз вже практично увесь доступний радіочастотний спектр залучений під роботу різноманітних радіопередавачів. Це викликає ускладнення виявлення радіосигналів засобів негласного отримання інформації, особливо у великих містах.

У роботі здійснення розробка методу видалення відомих сигналів, якій дозволяє, на відміну від існуючих методів, враховувати відомі сигнали ще на етапі перетворення. Процес перетворення є необхідним процесом у роботі автоматизованих комплексів виявлення радіосигналів. Він застосовується на першому етапі, ще до процесу виявлення сигналів. Це надає велику перевагу , у часі, приблизно у два рази скорочує час пошуку випадкових радіосигналів. Це дозволяє виявляти імпульсні радіосигнали короткої тривалості, тобто виявляти радіосигнали імпульсних засобів негласного отримання інформації, та частково вирішити наукове завдання виявлення імпульсних засобів негласного отримання інформації, які працюють в приміщеннях, де обробляється інформація з обмеженим доступом.

Напрямком подальших досліджень є розробка або удосконалення методів та алгоритмів визначення автоматизованими комплексами сигналів засобів негласного отримання інформації, які працюють під прикриттям радіочастот маючих дозвіл на роботу у цьому радіодіапазоні.

Ключові слова: радіосигнал; спектр; експоційні компоненти; алгоритм, відомі сигнали.

ВСТУП

Сучасні засоби негласного отримання інформації, постійно удосконалюються, відрізняються високими технічними характеристиками та гарною якістю маскування. Виявлення таких систем стає дедалі складнішою задачею, оскільки методи та режими їх роботи також ускладняються. Ситуація обтяжується тим, що засоби негласного

отримання інформації нового покоління працюють у цілком дозволеному радіодіапазоні і їх виявлення у приміщенні, яке межує з іншими, заповненими радіопристроями є проблематичним. Зараз вже практично увесь доступний радіочастотний спектр залучений під роботу різноманітних радіопередавачів. Це викликає ускладнення виявлення радіосигналів засобів негласного отримання інформації, особливо у великих містах.

Можливо навести приклад типової установи, де проводиться перевірка. Десятки комп'ютерів, радіотелефонів DECT, мобільних телефонів різних стандартів (CDMA-2000, GSM-900/1800, 3G (UMTS), 4G (WiMax)), підсилювачів мобільного зв'язку (в деяких будівлях зустрічаються підсилювачі всіх стандартів), радіомікрофони, безпроводові гарнітури, пристрої Wi-Fi, різні електронні зчитувачі систем контролю та управління доступом, безпроводові та проводові охоронні пристрої (які часто мають рівні побічних випромінювань, сумірні з випромінюванням радіозакладок) та інше.

Перераховані вище фактори дозволяють зробити висновок, що на сучасному етапі розвитку суспільства процес пошуку сигналів засобів негласного отримання інформації виходить на якісно інший рівень, тому аналіз методів виявлення радіосигналів е дуже актуальним.

Постановка проблеми. Основне протиріччя, яке лежить в основі наукового дослідження полягає, в тому, що незважаючи на велику кількість публікацій, встановлено, що на сьогодні існує об'єктивне протиріччя між існуючими математичними моделями та методами виявлення радіосигналів та необхідністю ефективного та надійного виявлення сигналів засобів негласного отримання інформації. Тому розробка та удосконалення методів виявлення радіосигналів негласного отримання інформації є актуальним науковим завданням.

Аналіз останніх досліджень і публікацій. Процесу виявлення засобів негласного отримання інформації присвячено багато наукових робіт. Так в роботі [1] наведена розроблена модель оптимального підходу до побудові математичної моделі безпеки, досліджені формальні математичні моделі для забезпечення безпеки інформації, але виявлення радіосигналів вона не чіпає. В роботі [2] проведено аналіз вимірювальних пристроїв радіосигналів. З метою удосконалення методики виявлення цифрових засобів негласного отримання інформації запропоновано векторний аналізатор. Вибір обґрунтовується на основі детального аналізу технічних характеристик і принципів роботи сучасних вимірювальних пристроїв але питання виявлення радіосигналів іншими пристроями не розглядається. В роботі [3] розглядаються та аналізуються методи та принципи перетворення радіосигналів різними методами перетворення (частково — на базі перетворень Фур'є), але подальшого розвідку методи не набрали. В [3] роботі розглянуто нові засоби негласного отримання інформації, що передають інформацію за допомогою Wi-Fi технологій, розроблена часткова методика виявлення таких засобів, але інші частотні діапазони, залишились поза межами запропонованих методик. В роботах [4], [5] проведено аналіз та розроблена комплексна методика виявлення та розпізнавання засобів негласного отримання інформації, що працюють у цифровому радіодіапазоні, але виявленні аналогових радіосигналів не розглядається. В роботах [9], [10] проведено аналіз існуючих на сьогоднішній день автоматизованих програмних комплексів та апаратури пошуку засобів негласного отримання інформації, але тільки у оглядовому ракурсі. В роботі [11] розглянута технологія розпізнавання засобів негласного отримання інформації за методом мультиагентної кластерізації з прямим зв'язком між агентами інші варіанти розпізнавання радіосигналів не розглядались. В роботах [12] – [15] розглядаються тенденції розвитку цифрових засобів негласного отримання інформації, що працюють під прикриттям радіосигналів діапазонна Wi-Fi; в

[13] представлено результати математичного моделювання випадкових сигналів у стаціонарній гіпермережі, питання інших радіосигналів цього радіодиапазону залишились поза розгляду у цей роботі. В роботі [15] розглядається розробка методики та математичної моделі розпізнавання засобів негласного отримання інформації на основі кластерного аналізу, аналіз аналогових радіосигналів зачеплено частково, повністю не розкрито. В роботах [16] – [18] запропоновано методику визначення спектральної щільності сигналу у процесі пошуку засобів негласного отримання інформації, яка базується на методі диференційних перетворень з урахуванням швидкості зміни щільності спектру, що дозволяє виявляти та аналізувати імпульсні сигнали у режимі «спектрального аналізу з часовою селекцією». В роботі [19] розроблено методику та математичну модель розпізнавання сигналів на основі диференційних перетворень, але застосування цей моделі в автоматизованому пошуковому комплексі не розглядається.

Таким чином, у результаті вивчення наукових публікацій за темою дослідження, монографій та практичних доробок виявились невирішними завдання ефективного виявлення радіосигналів засобів негласного отримання інформації.

Мета статті. Провести аналіз існуючих моделей та методів виявлення радіосигналів. Розробити метод виключення відомих сигналів при скануванні заданого радіодіапазону, що дозволить скоротити час сканування, чим збільшить ефективність виявлення імпульсних радіосигналів, які можуть бути сигналами засобів негласного отримання інформації

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Характерною особливістю пошуку засобів негласного отримання інформації є те, що для скорочення часу обробки потрібно видалити з радіоефіру дані відомих сигналів таких як сигнали телевізійних каналів, радіотрансляції та інших. Потрібно позбавиться цих сигналів з моделі пошуку засобів негласного отримання інформації.

Тоді ми можемо ще модифікувати запропонований метод з метою обліку відомих частот сигналів.

Для цього припустимо що q експоційних компонент $z_{1...}z_q$ відомі.

Тоді характеристичний поліном буде мати вигляд:

$$\prod_{k=1}^{q}(z\ -z_k)=\sum_{k=0}^{q}c_k\ z^k\ , \tag{1}$$

де $c(q)=1$.

Тоді характеристичний поліном для усіх компонент q, можливо розкласти на складові та записати у наступному вигляді:

$$\sum_{m=0}^{p}a_m z^m=\left(\sum_{k=0}^{q}c_k z^k\right)\left(\sum_{i=0}^{p-q}\alpha_i z^i\right), \tag{2}$$

де $\alpha_{p-q}=1$, якщо прирівняти члени с однаковими степенями компонент z, отримаємо:

$$a_m=\sum_{k=0}^{q}c_k\alpha_{m-k}\,, \tag{3}$$

ISSN 2663 - 4023

де $\alpha_i = 0, p-q+1 < i < 0$, Зробимо підстановку виразу (3) у вираз (2) і отримаємо:

$$\sum_{m=1}^{p} a_m x_{n-m} = \sum_{m=1}^{p} \left(\sum_{k=0}^{q} c_k \alpha_{m-k} \right) \cdot x_{n-m} = 0, \quad (4)$$

де $p+1 \le n \le 2p$.

Нова послідовність y_n, буде визначатися виразом:

$$y_n = \sum_{k=0}^{q} c_k x_{n-k} \cdot \quad (5)$$

Цей вираз є операцією згортання, через яку здійснюється фільтрація початкової часової послідовності x_n з метою отримання нової послідовності y_n. Далі початкова послідовність фільтрує за допомогою фільтра з коефіцієнтами, визначеними відомими полюсами вираз (2). Потім відфільтровані дані проходять увесь алгоритм лінійного передбачення на основі найменших квадратів і ми отримуємо оцінки параметрів α_m. Корні полінома зниженого порядку і дають оцінку невідомих полюсів:

$$\sum_{i=0}^{p-q} \alpha_i z^i \cdot \quad (6)$$

Ці $p-q$ полюсів та q відомих полюсів далі об'єднуються з метою виконання операції мінімізації за методом найменших квадратів. Результатом буде визначені параметри сигналів-амплітуди, фази усіх компонент q. Потім визначаються спектри цих сигналів. Алгоритм отримання характеристик сигналу, амплітуди, частоти, фази та спектра сигналу з урахуванням відомих сигналів приведено на рис.1.

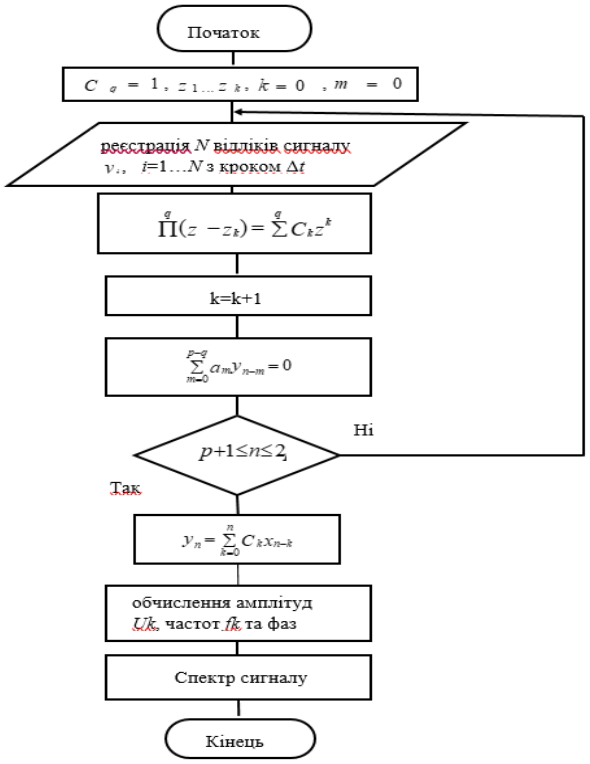

Рис. 1. Алгоритм знаходження спектру з урахуванням відомих сигналів

Алгоритм приведений на рис. 1 дозволяє отримати характеристики сигналу, амплітуди, частоти, фази та енергетичного спектра сигналу з урахуванням відомих сигналів q експоційних компонент $z_{1...}z_q$. Виключення цих сигналів з аналізу дозволяє, за сформований системою діагностичних ознак цифрових радіосигналів, за час-частотними властивостями цих сигналів проводити експрес ідентифікацію сигналів і здійснювати прийняття рішення.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розроблено метод видалення відомих сигналів, який дозволяє, на відміну від існуючих методик, враховувати відомі сигнали ще на етапі перетворення, до процесу виявлення сигналів, що приблизно у 2 рази скорочує час пошуку випадкових сигналів. Це дозволяє виявляти імпульсні радіосигнали короткої тривалості, тобто виявляти радіосигнали імпульсних засобів негласного отримання інформації, та частково вирішити наукове завдання виявлення імпульсних засобів негласного отримання інформації, які працюють в приміщеннях, де обробляється інформація з обмеженим доступом.

Напрямком подальших досліджень є розробка або удосконалення методів та алгоритмів визначення автоматизованими комплексами сигналів засобів негласного отримання інформації, які працюють під прикриттям радіочастот маючих дозвіл на роботу у цьому радіодіапазоні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лаптєв, О., Барабаш, О., & Зозуля, С. (2019). Векторні аналізатори сигналів для удосконалення методики пошуку засобів негласного отримання інформації. *Телекомунікаційні та інформаційні технології, (1)*, 55–61. https://doi.org/10.31673/2412-4338.2019.015561
2. Zamrii, I., et al. (2022). Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences, 17(4), 424–435.
3. Лаптєв, О., Федоренко, Р., & Берестов, Д. (2019). Удосконалення методики пошуку цифрових радіозакладок в діапазоні Wi-Fi. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, 2(66)*, С102 – 109
4. Laptev, A., et al. (2019). Analysis of Existing Signal Detection Methods, Development of a Technique for Calculating the Probability of Secret Information Capture. *International Journal of Science and Engineering Investigations (IJSEI) Denmark, 8(92)*, 99–103.
5. Кікоть, О., Лаптєв, О., & Бурдело, Є. (2020). Аналіз проблеми виявлення засобів негласного отримання інформаціїу автоматизованих пошукових комплексів радіозакладних пристроїв. *Інтернет конференція «Актуальні проблеми кібербезпеки»*, 148–151
6. Лаптєва, Т., Лукова-Чуйко, Н., & Собчук, А. (2022) Дослідження основних загроз і оцінка безпеки інформаційних систем. Математика. Інформаційні технології. Освіта, 101–103.
7. Рябий, М., Хатян, О., & Багацький, С. (2015). Модель виявлення PR-впливу через публікації в інтернет ЗМІ. *Інформаційна безпека, 21(2)*, 131–139.
8. Theocharis, V., et al. (2015). Using Twitter to mobilize protest action: Online mobilization patterns and action repertoires in the Occupy Wall Street, Indignados, and Aganaktismenoi movements. *Information, Communication & Society, 18*, 202–220.
9. Savchenko, V., et al. (2020). Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 246 –251.
10. Butko, T., Prokhorchenko, A., & Muzykin, M. (2016). An improved method of determining the schemes of locomotive circulation with regard to the technological peculiarities of railcar traffic. *Eastern-European Journal of Enterprise Technologies. 5(3(83))*, 47–55. https://doi.org/10.15587/1729-4061.2016.80471.

11. Молодецька, К. (2016). Підхід до виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах. Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. *Застосування підрозділів, комплексів, засобів зв'язку та автоматизації в АТО: збірн. матер.*, 130–131.
12. Faraz, A. (2016). A comparison of text Categorization methods. *International Journal on Natural Language Computing, 5(1)*, 31–44.
13. Лаптєв, О., Бабенко, Р., Правдивий, А., Зозуля, С., & Стефурак, О. (2020). Удосконалена методика вибору послідовності пріоритетів обслуговання потоків інформації. *Науково-практичний журнал «Зв'язок»*., *4*(146), 27–31.
14. Svynchuk, O., et al. (2021). Image compression using fractal functions. *Fractal and Fractional, 5(2)*, 1–14. https://doi.org/10.3390/fractalfract5020031
15. Zamrii, I., et al. (2022). Fractal Functions and Their Application to Source Data Coding. *ARPN Journal of Engineering and Applied Sciences, 17(4)*, 424–435.
16. Yevseiev, S., et al. (2021). Synergy of building cybersecurity systems. *Publisher PC TECHNOLOGY CENTER*. https://doi.org/10.15587/978-617-7319-31-2
17. Svynchuk, O., et al. (2021). Image compression using fractal functions. *Fractal and Fractional, 5(2)*, 1–14. https://doi.org/10.3390/fractalfract5020031
18. Kyrychok, R., et al. (2022). Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. *Eastern-European journal of enterprise technologies, 9(115)*, 93–101.
19. Лаптєв, О., Кузавков, В., & Хорошко, В. (2023). Системи пошуку засобів негласного здобуття акустичної інформації. *Міленіум.*

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (22), 2023
ISSN 2663 - 4023

Oleksandr Laptiev
Doctor of Sciences, senior researcher, associate professor of the Department of Cyber Security and Information Protection of the Faculty of Information Technologies
Taras Shevchenko National University, Kyiv, Ukraine
ORCID 0000-0002-4194-402X
olaptiev@knu.ua

Serhii Zozulia
Postgraduate student, Senior lecturer
State University of information and communication technologies, Kyiv, Ukraine
ORCID 0000-0003-1733-1415
zozulya_sa@ukr.net

THE METHOD OF EXCLUSION OF KNOWN SIGNALS WHEN SCANNING A SPECIFIED RADIO RANGE

Abstract. Obtaining access to information using the means of obtaining information secretly remains relevant at the present time. This is due to significant advantages, which include the impossibility of identifying a specialist who is doing listening or video monitoring of the premises. The specialist is located at a distance from this room. The integrity of the information, because the information comes from the original source. Therefore, the problem of detecting radio signals of means of covertly obtaining information is an urgent scientific task. This work is devoted to the problem of reducing the time of detection of signals of means of covertly obtaining information.
The detection of radio signals of the means of covert information acquisition is burdened by the fact that the means of covert information acquisition of the new generation work in a fully permitted radio range and their detection in a room bordering on other, filled radio devices is problematic. Now almost the entire available radio frequency spectrum is involved in the work of various radio transmitters. This complicates the detection of radio signals of means of covertly obtaining information, especially in large cities.
We are working on the development of a method for removing known signals, which allows, unlike existing methods, to take into account known signals even at the conversion stage. The conversion process is a necessary process in the operation of automated radio signal detection complexes. It is applied at the first stage, even before the signal detection process. This gives a great advantage, in terms of time, by about two times reducing the time of searching for random radio signals. This makes it possible to detect pulsed radio signals of short duration, that is, to detect radio signals of pulsed means of covertly obtaining information, and to partially solve the scientific task of detecting pulsed means of covertly obtaining information that work in rooms where information with limited access is processed.
The direction of further research is the development or improvement of methods and algorithms for determining by automated complexes the signals of means of covertly obtaining information, which work under the cover of radio frequencies authorized to work in this radio range.

Keywords: radio signal; spectrum; exposure components; algorithm, known signals.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Laptiev, O., Barabash, O., & Zozulya, S. (2019). Vector signal analyzers for improving the method of finding means of obtaining information secretly. *Telecommunications and information technologies: a scientific journal, (1)*, 55–61. https://doi.org/10.31673/2412-4338.2019.015561
2. Zamrii, I., et al. (2022). Fractal Functions and Their Application to Source Data Coding. ARPN Journal of Engineering and Applied Sciences, 17(4), 424–435.
3. Laptiev, O., Fedorenko, R., & Berestov, D. (2019). Improvement of the method of searching for digital radio bookmarks in the Wi-Fi range. *Collection of scientific works of the Center for Military and Strategic Studies of the Ivan Chernyakhovsky National University, 2(66)*, 102–109

4. Laptev, A., et al. (2019). Analysis of Existing Signal Detection Methods, Development of a Technique for Calculating the Probability of Secret Information Capture. *International Journal of Science and Engineering Investigations (IJSEI) Denmark, 8(92)*, 99–103.
5. Kikot, O., Laptiev, O., & Burdelo, E. (2020). Analysis of the problem of detecting means of covertly obtaining information in automated search complexes of radio-trading devices. *Internet conference "Actual problems of cyber security"*, 148–151.
6. Laptieva, T., Lukova-Chuiko, & N., Sobchuk, A. (2022). Study of the main threats and assessment of the security of information systems. Math. Information Technology. Education, 101–103.
7. Ryabiy, M., Khatyan, O., & Bagatskyi, C. (2015). A model for detecting PR influence through publications on the Internet mass media. *Informational security, 21(2)*, 131–139.
8. Theocharis, V., et al. (2015). Using Twitter to mobilize protest action: Online mobilization patterns and action repertoires in the Occupy Wall Street, Indignados, and Aganaktismenoi movements. *Information, Communication & Society, 18*, 202–220.
9. Savchenko, V., et al. (2020). Hidden Transmitter Localization Accuracy Model Based on Multi-Position Range Measurement. *2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020)*, 246–251.
10. Butko, T., Prokhorchenko, A., & Muzykin, M. (2016). An improved method of determining the schemes of locomotive circulation with regard to the technological peculiarities of railcar traffic. *Eastern-European Journal of Enterprise Technologies. 5(3(83))*, 47–55. https://doi.org/10.15587/1729-4061.2016.80471.
11. Molodetska, K. (2016). An approach to identifying organizational features of information operations in social Internet services. Priority areas of development of telecommunication systems and special purpose networks. *Application of divisions, complexes, means of communication and automation in ATO: collection*, 130–131.
12. Faraz, A. (2016). A comparison of text Categorization methods. *International Journal on Natural Language Computing, 5(1)*, 31–44.
13. Laptiev, O., et al. (2020). An improved technique for choosing the sequence of priorities for servicing information flows. *Scientific and practical magazine "Zvyazok", 4(146)*, 27–31.
14. Svynchuk, O., et al. (2021). Image compression using fractal functions. *Fractal and Fractional, 5(2)*, 1–14. https://doi.org/10.3390/fractalfract5020031
15. Zamrii, I., et al. (2022). Fractal Functions and Their Application to Source Data Coding. *ARPN Journal of Engineering and Applied Sciences, 17(4)*, 424–435.
16. Yevseiev, S., et al. (2021). Synergy of building cybersecurity systems. *Publisher PC TECHNOLOGY CENTER*. https://doi.org/10.15587/978-617-7319-31-2
17. Svynchuk, O., et al. (2021). Image compression using fractal functions. *Fractal and Fractional, 5(2)*, 1–14. https://doi.org/10.3390/fractalfract5020031
18. Kyrychok, R., et al. (2022). Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. *Eastern-European journal of enterprise technologies, 9(115)*, 93–101.
19. Laptiev, O., Kuzavkov, V, & Khoroshko, V. (2023). Systems for finding means of tacit acquisition of acoustic information. *Millennium*.