



DOI 10.28925/2663-4023.2025.29.940

УДК 534.83:621.375

Романюк Валентин Сергійович

студент факультету інформаційних технологій та математики
Київського столичного університету імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0004-8965-3098
vsromaniuk.fitm24m@kubg.edu.ua

Платоненко Артем Вадимович

Кандидат технічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-2962-5667
a.platonenko@kubg.edu.ua

АНАЛІЗ ЯКОСТІ ГЕНЕРАТОРІВ РОЖЕВОГО ШУМУ

Анотація. У роботі було поставлено завдання комплексної оцінки якості генераторів рожевого шуму з використанням трьох різних аналітичних методів та критеріїв. Дослідження спрямоване на розв'язання актуальної проблеми забезпечення надійного захисту конфіденційної мовленнєвої інформації від несанкціонованого доступу через акустичні канали витоку в умовах зростаючих загроз інформаційній безпеці. Методологічна база дослідження включає три основні підходи до оцінки якості генераторів, а саме: визначення коефіцієнта якості шуму за допомогою коефіцієнтів асиметрії та ексцесу, що дозволяє оцінити відповідність розподілу значень сигналу нормальному закону; визначення коефіцієнту якості ентропії з використанням формули ентропії для нормального Гаусівського розподілу; визначення коефіцієнту ентропії якості розподілу обвідної шумового сигналу на основі розподілу Релея. Експериментальна частина дослідження базується на порівняльному аналізі двох типів генераторів рожевого шуму з обробкою 10-секундних вибірок по 441 000 відліків. За еталонну вибірку в ході дослідження було взято апаратний генератор акустичного шуму марки ST-NG1, який використовується для захисту акустичної інформації в офісних приміщеннях та має сертифіковані технічні характеристики. Для порівняння було досліджено програмний генератор, створений за допомогою мови програмування Python з використанням псевдовипадкової послідовності та застосування алгоритмів цифрової фільтрації. Результати експериментальних досліджень продемонстрували різну ефективність застосованих методів оцінки. Найбільш інформативним став метод визначення коефіцієнта ентропії якості розподілу обвідної сигналу, який забезпечив чітку диференціацію між генераторами, що використовувались. Практична значимість результатів дослідження полягає в можливості застосування отриманих підходів для сертифікації та контролю якості засобів захисту акустичної інформації. Визначено перспективні напрямки подальших досліджень на розширення експериментальної бази дослідження та залучення більшої кількості типів генераторів різних виробників та різних принципів дії для універсальності запропонованих методів.

Ключові слова: генератор шуму; коефіцієнт якості шуму; генератор псевдовипадкової послідовності; рожевий шум; коефіцієнт якості ентропії; огибающая шумового сигналу.

ВСТУП

Проблема захисту та обробки мовленнєвої інформації є однією з ключових проблем інформаційної безпеки сучасності. У сучасному світі, зі зростанням обсягів даних, що оброблюються, зростає також і кількість мовленнєвої інформації в установах та на підприємствах, в процесі проведення різних зустрічей, конференцій, переговорів та



інших заходів, де обговорюється конфіденційна інформація. Акустична, а тим більше мовленнєва інформація, може бути вловлена різними пристроями через канали витоку акустичної інформації та є основним джерелом витоку конфіденційних відомостей.

Канали витоку акустичної інформації характеризуються спільною рисою — впливом акустичних сигналів. Зловмисники можуть використовувати різноманітні методи для перехоплення мовленнєвої інформації: від простого прослуховування акустичних сигналів за допомогою закладних пристроїв до зняття коливань вікна з акустичного сигналу за допомогою датчиків вібрації. Це робить проблему захисту акустичної інформації особливо актуальною для організацій, що працюють з державною таємницею, комерційною таємницею та іншою конфіденційною інформацією.

Серед методів захисту від прослуховування, відповідно до загальних принципів інформаційної безпеки, виділяють структурний камуфляж та енергетичне приховування [1], [2]. Структурний камуфляж включає шифрування семантичної інформації, технічне екранування кабелів і обладнання, створення дезінформації. Енергетичне приховування реалізується через звукоізоляцію акустичного сигналу, поглинання звуку акустичних хвиль, зашумлення приміщення іншими звуками для маскування акустичних сигналів, а також виявлення та вилучення вбудованих закладних пристроїв.

Особливе місце серед методів енергетичного приховування займає використання генераторів маскуючого шуму. Ці пристрої створюють акустичні завади, що ускладнюють або унеможливають виділення корисної мовленнєвої інформації з загального акустичного фону. Однак зашумлений інформаційний сигнал може бути відфільтрований сучасними засобами цифрової обробки сигналів, і у разі неякісного маскування зловмисник може отримати доступ до захищеної інформації.

Вибір правильного типу шуму для маскування є критично важливим фактором ефективності захисту. Залежно від застосування та специфіки інформації що захищається, може використовуватися білий, рожевий або коричневий шум. Кожен тип шуму має свої спектральні характеристики та особливості впливу на сприйняття мовленнєвої інформації. Рожевий шум, що характеризується спадом потужності пропорційно частоті, особливо ефективний для маскування мовленнєвих сигналів завдяки своїм спектральним властивостям, які близькі до природного розподілу енергії в мовленні.

Тому існує гостра проблема, пов'язана з оцінкою якості шумового сигналу, що генерується засобами активного захисту, зокрема генераторами рожевого шуму. Необхідність забезпечення гарантованого захисту конфіденційної інформації вимагає розробки надійних методів оцінки ефективності маскуючих властивостей генераторів шуму та їх відповідності вимогам інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Велика кількість робіт присвячена розробці та дослідженню різних методів обробки та захисту мовленнєвої інформації, а також визначенню розбірливості мовленнєвих повідомлень як основного показника їхньої безпеки.

У [1], [4] описано розробку системи захисту акустичної інформації від прослуховування, яка використовує активне шумове маскування. Замість традиційного «білого» шуму пропонується Scrambler-тип генератора, що створює складні лінгвістично подібні завади, стійкі до сучасних методів цифрової обробки сигналів.

Методику оцінки статистичної надійності шумових завад, які використовують для запобігання витоку інформації технічними каналами розглянуто у [2]. Надійність визначають як імовірність того, що статистичні характеристики створеного шуму залишаться в допустимих межах, забезпечуючи потрібну спектральну щільність та

рівень помилок у каналі витоку. Оцінювання включає аналіз кореляційної функції шумового процесу, перевірку його нормального розподілу, після чого обчислюють ефективну спектральну щільність.

Вибірки шумових сигналів [3], згенеровані різними псевдовипадковими генераторами, відповідають рівномірному закону розподілу. Порівнювали генератори Martin, конгруентний та вбудований у Matlab, використовуючи багатокритеріальний аналіз і пошук оптимальних рішень.

Публікація [5] присвячена захисту інформації від витоку акустичними каналами із застосуванням пасивних і активних методів захисту. Пасивні методи мають на меті послаблення акустичних сигналів на межі контрольованої зони до рівня, при якому неможливе їх виділення засобами розвідки на фоні природних шумів. При розгляданні активних методів створюються маскуючі акустичні, вібраційні завади для зменшення співвідношення сигнал/шум на границі контрольованої зони для унеможливлення їх виділення.

Стаття [6] розглядає сучасні методи захисту інформації від витоку через канали високочастотного наведення. Проаналізовано їхні переваги та недоліки, типи сигналів і потенційні шляхи витоку через електроживлення, заземлення та повітряне середовище, а також приклади пасивних, активних і комбінованих заходів захисту.

Дослідження показують, що ефективний захист конфіденційної інформації за допомогою активних засобів захисту інформації від витоку акустичними каналами є важливим завданням установи де обробляється конфіденційна інформація.

Метою статті є дослідження та розробка методів аналізу якості генераторів рожевого шуму для забезпечення ефективного захисту мовленнєвої інформації від несанкціонованого доступу через акустичні канали витоку.

МЕТОДИКА ДОСЛІДЖЕННЯ

Перш ніж представити методи визначення коефіцієнтів якості шуму, необхідно проаналізувати інформацію про рожевий шум, який використовується в генераторах для маскування інформації.

Рожевий шум — це шум, спектральна щільність якого змінюється з частотою згідно із законом $\frac{1}{f}$. Це гарантує, що сигнал завад має однакову енергію на октаву. Іноді рожевим шумом називають будь-який шум, спектральна щільність якого зменшується зі зменшенням частоти (рис. 1).

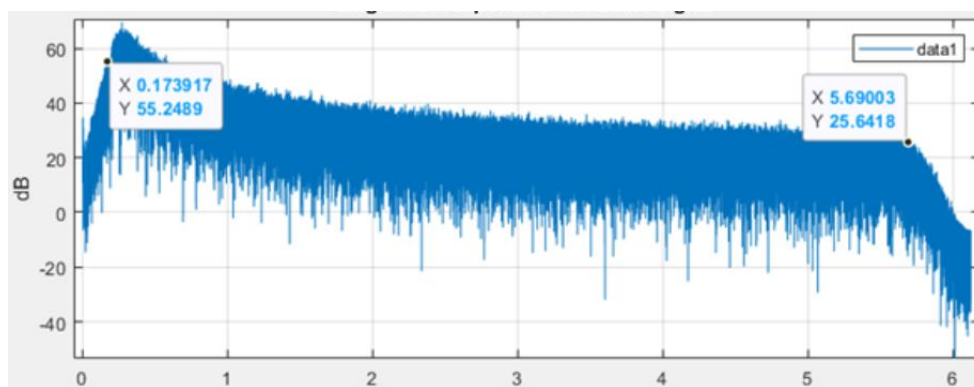


Рис. 1. Графік спектральної щільності шумового сигналу в діапазоні 180–5600 Гц



Отже, рожевий шум характеризується сталістю енергії в межах кожної октави зміни частоти. Це означає, що спектральна щільність зменшується зі збільшенням частоти відповідно до логарифмічного закону. Такий шум широко поширений у природі, і багато випадкових процесів йому підпорядковуються.

Нижче наведено різні методи, описані в літературі, для характеристики якості акустичного шуму, що випромінюється генераторами.

Метод визначення коефіцієнта якості шуму за допомогою коефіцієнтів асиметрії та ексцесу. Цей метод був розроблений для оцінки якості електромагнітного шумового поля, проте під час експерименту було зроблено спробу використати його для генератора рожевого шуму, який використовуються для активного маскування мовного сигналу. Методологія така [7]:

1. Отримання вибірки шумового сигналу в дискретній формі.
2. Визначення середніх значень m_1 отриманої вибірки.
3. Обчислення другого m_2 , третього m_3 та четвертого m_4 центральних моментів.
4. Визначення розрахункових значень асиметрії $\gamma_a = \frac{m_3}{\sqrt{m_2^3}}$ і коефіцієнт ексцесу

$$\gamma_e = \frac{m_4}{m_2^2} - 3 \text{ досліджуваної вибірки.}$$

5. Визначення коефіцієнта якості шуму за формулою

$$\theta = 1.06987 + 3\gamma_e - 1.56\ln(e^{2\gamma_e} + 0.037e^{0.23e^{3.43|\gamma_e|}}), \quad (1)$$

Наступні методи зводяться до серії обчислювальних операцій, що виконуються над квантованими вимірними значеннями електричного сигналу, в який перетворюється маскувальний шум. Основою цих методів є розрахунок ступеня невизначеності закону розподілу миттєвих значень маскувального шуму, а також ентропії закону розподілу значень огинаючої шумового сигналу.

У роботах [11]–[15] вводиться поняття коефіцієнта якості ентропійного шуму. Ці коефіцієнти розраховуються відповідно до певних еталонних законів розподілу. За обмежень, накладених на середню потужність, стандартний закон розподілу миттєвих значень маскувального шуму є нормальним. Водночас, для огинаючої нормально розподілених миттєвих значень маскувального шуму еталонним законом є розподіл Релея.

Метод визначення коефіцієнта якості ентропії. У низці робіт [12], [16]–[20], замість описаного вище коефіцієнта якості шуму пропонується знаходити коефіцієнт якості ентропійного шуму. Ентропія дозволяє оцінювати маскувальні властивості сигналів, що заважають, незалежно від конкретних методів їх прийому та обробки. Завдання вибору найефективнішої завади зводиться до визначення такого розподілу завад, при якому за заданих статистичних властивостей сигналу відтворена інформація засобами технічної розвідки була б мінімальною.

Розрахунок ентропії зводиться до побудови гістограми розподілу щільності ймовірності $p(x_i)$, після чого необхідно скористатися формулою

$$H(x) = -\sum_{i=1}^n p(x_i)\log(p(x_i)) \quad (2)$$

де $p(x_i)$ — ймовірність потрапляння елемента вибірки в i -й діапазон гістограми, n — кількість діапазонів гістограми.

Коефіцієнт якості ентропійного шуму знаходиться за формулою:

$$\gamma = \frac{e^{2H(x)}}{2\pi e} \quad (3)$$



Метод визначення коефіцієнта ентропії якості розподілу огинаючої шумового сигналу. Цей метод подібний до попереднього, але ентропія знаходиться не для вибірки генератора шуму, а для вибірки огинаючої генератора шуму, яка повинна підлягати розподілу Релея. Алгоритм визначення коефіцієнта якості такий [4]:

1. Знаходження огинаючої шумового сигналу за формулою

$$A(t) = \sqrt{x(t)^2 + H(x(t))^2} \quad (4)$$

де $H(x(t))$ Гільбертове перетворення $(x(t))$.

2. Побудова гістограми закону розподілу огинаючої шумового сигналу.
3. Знаходження ентропії закону розподілу огинаючої за формулою (2).
4. Знаходження параметра стандартного розподілу Релея r за формулою

$$\frac{\mu_2^0}{2r^2} + \ln r = M[\ln x] + 1 + \frac{\gamma}{2} - \ln\sqrt{2} \quad (5)$$

де μ_2^0 — другий момент закону розподілу огинаючої шумового сигналу;
 $M[\ln x]$ — середнє значення натурального логарифма значень огинаючої шумового сигналу, γ — стала Ейлера.

5. Знаходження ентропії стандартного розподілу Релея за формулою

$$H = 1 + \frac{\gamma}{2} + \ln\left(\frac{r}{\sqrt{2}}\right) \quad (6)$$

6. Знаходження коефіцієнта якості ентропії розподілу огинаючої шумового сигналу за формулою

$$n = e^{H_0 - H} \quad (7)$$

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Результати також наведено окремо для кожного розглянутого методу.

Метод визначення коефіцієнта якості шуму за допомогою коефіцієнтів асиметрії та ексцесу. Згідно з цією методикою, коефіцієнт якості шуму повинен бути в діапазоні від 0,8 до 1,0. Було проведено експериментальні дослідження з генератором рожевого шуму марки ST-NG1, а також експеримент на генераторах, побудованих з використанням псевдовипадкової послідовності чисел, реалізованої в програмному середовищі Python. Результати для всіх 10-секундних вибірок (441 000 вибірок) дали результати коефіцієнта якості шуму, наведені в табл. 1.

Таблиця 1

**Оцінені показники коефіцієнта якості шуму
за допомогою коефіцієнтів асиметрії та ексцесу**

Генератор шуму	Коефіцієнт асиметрії	Коефіцієнт ексцесу	Коефіцієнт якості шуму
Генератор ST-NG1	0.0119	- 0.1219	0.9936
Створено з псевдовипадкової послідовності	- 0.0089	- 0.6998	0.8823

Як видно з табл. 1, ця методика показала, що на практиці можна використовувати як генератор марки ST-NG1, так і шумовий сигнал, отриманий з псевдовипадкової послідовності чисел.

Метод визначення коефіцієнта якості ентропії. Коефіцієнт якості ентропійного шуму не повинен перевищувати 1. Однак, у процесі досліджень з генератором рожевого шуму, виявилось, що, використовуючи формулу (2) для знаходження ентропії,

коефіцієнт якості ентропії перевищує одиницю в сотні разів, що унеможливило використання цієї формули. Тому було вирішено використовувати іншу формулу для знаходження ентропії.

Враховуючи, що в дослідженні використовується генератор рожевого шуму, слід зазначити, що рожевий шум підпорядковується нормальному закону розподілу. Це було підтверджено шляхом знаходження гістограми для генератора шуму (рис. 2).

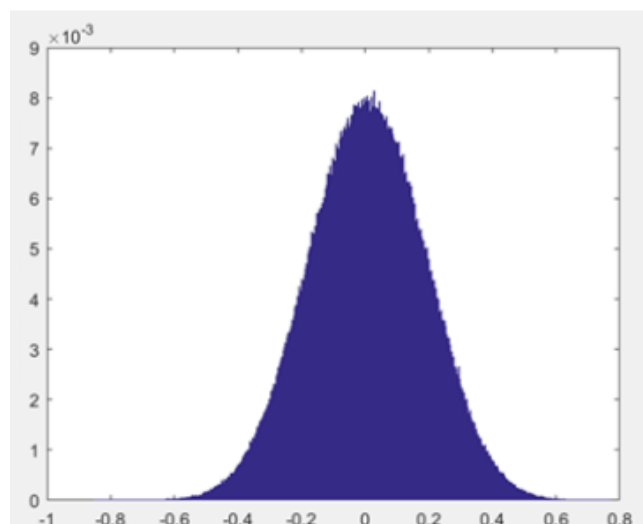


Рис. 2. Гістограма генератора шуму

У зв'язку з цим було вирішено замінити ентропію за формулою (2) знаходженням ентропії для нормального Гаусівського розподілу, який має вигляд:

$$H(x) = \ln(\sqrt{2\pi e\sigma^2}) \quad (8)$$

де σ^2 — дисперсія вибірки.

Використовуючи формулу (8) для знаходження коефіцієнта ентропійного шуму, отримано результати, наведені в табл. 2.

Таблиця 2

Результати визначення коефіцієнта якості ентропійного шуму

Генератор шуму	Коефіцієнт ентропії	Середня потужність сигналу	Коефіцієнт якості сигналу
Генератор ST-NG1	0.0534	0.0533	1.0
Створено з псевдовипадкової послідовності	0.2118	0.2118	1.0

Як видно з табл. 2, коефіцієнт ентропії дорівнює 1 для всіх типів генераторів, що використовувалися в експерименті. Слід зазначити, що при експерименті змінювалась довжина вибірки (тривалість сигналу), рівень шуму та рівні квантування, але результати знаходження коефіцієнта ентропії якості сигналу завжди були в діапазоні 0,99-1,0.

Таким чином, можна зробити висновок про неефективність використання методики визначення коефіцієнта якості ентропійного шуму на практиці.



Метод визначення коефіцієнта ентропії якості розподілу огинаючої шумового сигналу. Слід зазначити, що при використанні формули (2) для знаходження коефіцієнта ентропії даним методом коефіцієнт ентропії знаходився в діапазоні 0,01-0,02. Однак ці результати не відповідають дійсності.

Тому було вирішено замість використання формули (2) використовувати формулу для знаходження ентропії розподілу Релея:

$$H = 1 + \ln\left(\frac{\sigma}{\sqrt{2}}\right) + \frac{\gamma}{2} \quad (9)$$

де σ — стандартне відхилення, $\gamma \approx 0,57721566490153286060$ — стала Ейлера.

Після серії експериментів з використанням цього методу отримано результати, наведені в табл. 3.

Таблиця 3

Результати знаходження коефіцієнта якості ентропії розподілу огинаючої сигналу генератора шуму

Генератор шуму	Ентропія оболонки	Ентропія опорного розподілу Релея	Коефіцієнт якості ентропії
Генератор ST-NG1	1.0059	0.8661	1.15
Створено з псевдовипадкової послідовності	0.3124	0.8661	0.5748

Як видно з отриманих результатів, метод оцінки коефіцієнта якості ентропії розподілу огинаючої шумового сигналу є єдиним методом, який дає різні результати для різних типів генераторів шуму та потребує подальшої статистичної розробки для визначення інтервалу, відповідального за адекватну роботу генераторів шуму.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження було здійснено комплексний аналіз якості генераторів рожевого шуму з використанням трьох різних методик оцінки. Експериментальні дослідження проводились на апаратному генераторі рожевого шуму марки ST-NG1 та програмному генераторі, створеному з використанням псевдовипадкової послідовності чисел у середовищі Python.

Аналіз результатів показав різну ефективність застосованих методів оцінки якості генераторів шуму. Найбільш інформативним виявився метод визначення коефіцієнта ентропії якості розподілу огинаючої шумового сигналу. Цей метод забезпечив чітку диференціацію між різними типами генераторів: апаратний генератор ST-NG1 показав коефіцієнт 1,15, тоді як програмний генератор — 0,5748. Така значна різниця в результатах свідчить про високу чутливість методу до характеристик генераторів та його потенціал для практичного застосування.

Проведене дослідження підтвердило, що рожевий шум підпорядковується нормальному закону розподілу, що було експериментально підтверджено побудовою гістограм розподілу. Це спостереження має важливе значення для подальшої оптимізації методів оцінки якості генераторів [21], [22].

Практична значущість отриманих результатів полягає в можливості використання розроблених підходів для сертифікації та контролю якості засобів захисту акустичної інформації. Особливо перспективним є метод аналізу розподілу огинаючої сигналу, який



може стати основою для розробки стандартизованих процедур оцінки ефективності генераторів маскуючого шуму.

Результати проведеного дослідження показують, що майбутні зусилля мають бути спрямовані на розширення експериментальної бази дослідження та залучення більшої кількості типів генераторів різних виробників та різних принципів дії для універсальності запропонованих методик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Blintsov, V., Nuzhniy, S., Kasianov, Y., & Korytskyi, V. (2020). MATHEMATICAL MODEL OF THE SYSTEM OF ACTIVE PROTECTION AGAINST EAVESDROPPING OF SPEECH INFORMATION ON THE SCRAMBLER GENERATOR. *EUREKA: Physics and Engineering*, 3, 11–22. <https://journal.eu-jr.eu/engineering/article/view/1315>
2. Ivanchenko, S., Bezshanko, V., & Havrylenko, O. (2016). Statistical reliability of noise hindrance for ensuring protection against leakage of information through technical channels. *Collection "Information technology and security"*, 4(2), 207–215. <https://doi.org/10.20535/2411-1031.2016.4.2.109981>
3. Мартинюк, Г. В., Оникієнко, Ю. Ю., Щербак, Л. М. (2016). Analysis of the pseudorandom number generators by the metrological characteristics. *Eastern-European Journal of Enterprise Technologies*, 1(9(79)), 25. <https://doi.org/10.15587/1729-4061.2016.60608>
4. Blintsov, V., Nuzhniy, S., Parkhuts, L., & Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. *Eastern-European Journal of Enterprise Technologies*, 5(9 (95)), 26–34. <https://doi.org/10.15587/1729-4061.2018.144146>
5. Давлет'янц, О. І., & Бурзаковський, Р. В. (2010). ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ АКУСТИЧНИМ КАНАЛОМ. *Ukrainian Information Security Research Journal*, 12(4 (49)). <https://doi.org/10.18372/2410-7840.12.1977>
6. Larysa Kriuchkova & Ivan Tsmokanych. (2021). ОГЛЯД МЕТОДІВ ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ, СФОРМОВАНИМИ ВИСОКОЧАСТОТНИМИ НАВ'ЯЗУВАННЯМИ. *International Journal of Innovative Technologies in Social Science*, (3(31)). https://doi.org/10.31435/rsglobal_ijitss/30092021/7685
7. Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. (2016) ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ. ПОРЯДОК СТВОРЕННЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, Навчальний посібник НТУУ “Київський політехнічний інститут”.
8. Siniuhin, V. V., Kataiev, V. S., & Hrytsak, A. V. (2021). Modular Noise Generator for Blocking Acoustic Information Leaks. *Visnyk of Vinnytsia Politechnical Institute*, 159(6), 158–164. <https://doi.org/10.31649/1997-9266-2021-159-6-158-164>
9. S.V Lenkov, D.A. Peregudov and V.A. Khoroshko, Methods and Means of Information Protection. Volume I. Unauthorized Receiving the Information. Kyiv, Ukraine: Aarii, 2008.
10. С.О Іванченко, В.О. Хорошко, О.В. Гавриленко, та О.М. Кулініч, “Метод діагностування шумових завад для забезпечення захищеності інформації від витоку технічними каналами”, *Захист інформації*. 22, с. 74-86, 2015.
11. Yudin, O., Ziubina, R., Buchyk, S., Bohuslavska, O., & Teliushchenko, V. (2019). Speaker's Voice Recognition Methods in High-Level Interference Conditions. *У 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*. IEEE. <https://doi.org/10.1109/ukrcon.2019.8879937>
12. Purwins, H., Li, B., Virtanen, T., Schluter, J., Chang, S.-Y., & Sainath, T. (2019). Deep Learning for Audio Signal Processing. *IEEE Journal of Selected Topics in Signal Processing*, 13(2), 206–219. <https://doi.org/10.1109/jstsp.2019.2908700>
13. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
14. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
15. Hulak, H. M., Zhylysov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.



16. V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.
17. V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.
18. V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.
19. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421.
20. V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi: 10.1109/AICT61584.2023.10452687.
21. L. Kriuchkova, et al., Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 261–268.
22. L. Kriuchkova, et al., Influence of protective signals on dangerous signals of high-frequency imposition, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 419–425.

**Valentyn Romaniuk**

Student of Faculty of Information Technologies and Mathematics
of Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0004-8965-3098
vsromaniuk.ftm24m@kubg.edu.ua

Artem Platonenko

PhD, Associate Professor,
Docent of the Department of Information and Cyber Security
named after Professor Volodymyr Buryachok,
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-2962-5667
a.platonenko@kubg.edu.ua

QUALITY ANALYSIS OF PINK NOISE GENERATORS

Abstract. The article set the task of comprehensively assessing the quality of pink noise generators using three different analytical methods and criteria. The study is aimed at solving the current problem of ensuring reliable protection of confidential speech information from unauthorized access through acoustic leakage channels in the face of growing threats to information security. The methodological basis of the study includes three main approaches to assessing the quality of generators: determining the noise quality coefficient using the asymmetry and kurtosis coefficients, which allows assessing the compliance of the distribution of signal values with the normal law; determining the entropy quality coefficient using the entropy formula for the normal Gaussian distribution; determining the entropy coefficient of the quality of the distribution of the noise signal envelope based on the Rayleigh distribution. The experimental part of the study is based on a comparative analysis of two types of pink noise generators with processing of 10-second samples of 441,000 samples. The reference sample was taken as a hardware acoustic noise generator of the ST-NG1 brand, which is used to protect acoustic information in office premises and has certified characteristics. For comparison, a software generator created using the Python programming language using a pseudo-random sequence and digital filtering algorithms was studied. The results of experimental studies demonstrated the different effectiveness of the applied evaluation methods. The most informative was the method of determining the quality entropy coefficient of the envelope signal distribution, which provided a clear differentiation between the generators used. The practical significance of the research results lies in the possibility of applying the obtained approaches for certification and quality control of acoustic information protection means. Promising directions for further research were identified to expand the experimental base of the study and involve a larger number of types of generators from different manufacturers and different principles of operation for the universality of the proposed methods.

Keywords: noise generator; noise quality coefficient; pseudo-random sequence generator; pink noise; quality entropy coefficient; noise signal envelope.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Blintsov, V., Nuzhniy, S., Kasianov, Y., & Korytskyi, V. (2020). MATHEMATICAL MODEL OF THE SYSTEM OF ACTIVE PROTECTION AGAINST EAVESDROPPING OF SPEECH INFORMATION ON THE SCRAMBLER GENERATOR. *EUREKA: Physics and Engineering*, 3, 11–22. <https://journal.eu-jr.eu/engineering/article/view/1315>
2. Ivanchenko, S., Bezshanko, V., & Havrylenko, O. (2016). Statistical reliability of noise hindrance for ensuring protection against leakage of information through technical channels. *Collection "Information technology and security"*, 4(2), 207–215. <https://doi.org/10.20535/2411-1031.2016.4.2.109981>
3. Martyniuk, H. V., Onykienko, Yu. Yu., Shcherbak, L. M. (2016). Analysis of the pseudorandom number generators by the metrological characteristics. *Eastern-European Journal of Enterprise Technologies*, 1(9(79)), 25. <https://doi.org/10.15587/1729-4061.2016.60608>
4. Blintsov, V., Nuzhniy, S., Parkhuts, L., & Kasianov, Y. (2018). The objectified procedure and a technology for assessing the state of complex noise speech information protection. *Eastern-European Journal of Enterprise Technologies*, 5(9 (95)), 26–34. <https://doi.org/10.15587/1729-4061.2018.144146>



5. Davletiants, O. I., Burzakovskyi, R. V. (2010). HARDWARE AND SOFTWARE COMPLEX FOR PROTECTING INFORMATION FROM LEAKAGE THROUGH AN ACOUSTIC CHANNEL. *Ukrainian Information Security Research Journal*, 12(4 (49)). <https://doi.org/10.18372/2410-7840.12.1977>
6. Larysa Kriuchkova & Ivan Tsmokanych. (2021). OVERVIEW OF METHODS FOR PROTECTING ACOUSTIC INFORMATION FROM LEAKAGE THROUGH CHANNELS FORMED BY HIGH-FREQUENCY INTERFERENCES. *International Journal of Innovative Technologies in Social Science*, (3(31)). https://doi.org/10.31435/rsglobal_ijitss/30092021/7685
7. Ivanchenko S.O., Havrylenko O.V., Lypskyi O.A., Shevtsov A.S. (2016) TECHNICAL CHANNELS OF INFORMATION OUTPUT. PROCEDURE FOR CREATING TECHNICAL INFORMATION PROTECTION, Textbook of NTUU "Kyiv Polytechnic Institute".
8. Siniuhin, V. V., Kataiev, V. S., & Hrytsak, A. V. (2021). Modular Noise Generator for Blocking Acoustic Information Leaks. *Visnyk of Vinnytsia Politechnical Institute*, 159(6), 158–164. <https://doi.org/10.31649/1997-9266-2021-159-6-158-164>
9. S.V Lenkov, D.A. Peregudov and V.A. Khoroshko, Methods and Means of Information Protection. Volume I. Unauthorized Receiving the Information. Kyiv, Ukraine: Arii, 2008.
10. S.O Ivanchenko, V.O. Khoroshko, O.V. Havrylenko ta O.M. Kulinich, "A method for diagnosing noise interference to ensure information security from leakage through technical channels", Information protection.. 22, c. 74-86, 2015.
11. Yudin, O., Ziubina, R., Buchyk, S., Bohuslavska, O., & Teliushchenko, V. (2019). Speaker's Voice Recognition Methods in High-Level Interference Conditions. *Y 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON)*. IEEE. <https://doi.org/10.1109/ukrcon.2019.8879937>
12. Purwins, H., Li, B., Virtanen, T., Schluter, J., Chang, S.-Y., & Sainath, T. (2019). Deep Learning for Audio Signal Processing. *IEEE Journal of Selected Topics in Signal Processing*, 13(2), 206–219. <https://doi.org/10.1109/jstsp.2019.2908700>
13. Kostiuk, Yu. V., Skladannyi, P. M., Bebashko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
14. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebashko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
15. Hulak, H. M., Zhylytsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
16. V. Sokolov, P. Skladannyi, A. Platonenko, Jump-Stay Jamming Attack on Wi-Fi Systems, in: IEEE 18th International Conference on Computer Science and Information Technologies (2023) 1–5. doi: 10.1109/CSIT61576.2023.10324031.
17. V. Sokolov, P. Skladannyi, N. Korshun, ZigBee Network Resistance to Jamming Attacks, in: IEEE 6th International Conference on Information and Telecommunication Technologies and Radio Electronics (2023) 161–165. doi: 10.1109/UkrMiCo61577.2023.10380360.
18. V. Sokolov, P. Skladannyi, V. Astapenya, Bluetooth Low-Energy Beacon Resistance to Jamming Attack, in: IEEE 13th International Conference on Electronics and Information Technologies (2023) 270–274. doi: 10.1109/ELIT61488.2023.10310815.
19. V. Sokolov, P. Skladannyi, N. Mazur, Wi-Fi Repeater Influence on Wireless Access, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 33–36. doi: 10.1109/AICT61584.2023.10452421.
20. V. Sokolov, P. Skladannyi, V. Astapenya, Wi-Fi Interference Resistance to Jamming Attack, in: IEEE 5th International Conference on Advanced Information and Communication Technologies (2023) 1–4. doi: 10.1109/AICT61584.2023.10452687.
21. L. Kriuchkova, et al., Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 261-268.
22. L. Kriuchkova, et al., Influence of protective signals on dangerous signals of high-frequency imposition, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654, 2024, 419–425.

