КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.778
УДК 004.056:519.61

Карпович Іван Миколайович
к.ф.-м.н, доцент,
доцент кафедри комп'ютерних технологій та економічної кібернетики
Національний університет водного господарства та природокористування,
Рівне, Україна
ORCID ID: 0000-0002-4601-0541
i.m.karpovich@nuwm.edu.ua

Гладка Олена Миколаївна
к.т.н, доцент,
доцент кафедри комп'ютерних технологій та економічної кібернетики
Національний університет водного господарства та природокористування,
Рівне, Україна
ORCID ID: 0000-0003-4728-0663
o.m.hladka@nuwm.edu.ua

Паламарчук Андрій Сергійович
здобувач вищої освіти
Навчально-науковий інститут кібернетики, інформаційних технологій та інженерії
Національний університет водного господарства та природокористування,
Рівне, Україна
palamarchuk_ak24@nuwm.edu.ua

ВИКОРИСТАННЯ МЕТОДІВ МАТЕМАТИЧНОЇ ОПТИМІЗАЦІЇ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. Забезпечення захищеності інформації є актуальним завданням сучасності, оскільки проблема інформаційних ризиків та пошуку шляхів зменшення шкоди від кібератак стає дедалі гострішою. В роботі проведено аналіз методів забезпечення інформаційної безпеки. Серед економічних методів захисту інформації важливе місце займає страхування інформаційних ризиків. Проте, таке страхування продовжує залишатися поодиноким явищем через побоювання страхових компаній щодо необхідності виплати страхувальникам значних сум компенсацій збитків у випадку масового настання страхових випадків. Використання методів математичного моделювання дозволяє аргументовано довести менеджерам, що вкладення коштів у систему інформаційної безпеки сприяє збільшенню прибутків компанії, а також, в умовах обмеженості ресурсів, відведених на розробку і функціонування системи кіберзахисту, вибрати оптимальний набір засобів захисту і на основі математичної моделі переконливо довести, наскільки створена система інформаційної безпеки ефективна в боротьбі проти найпоширеніших загроз. Мета роботи — математичне моделювання максимізації ефективності засобів захисту інформації від несанкціонованого доступу при обмеженнях на обсяг витрат. Застосування методів оптимізації до математичного моделювання кількісних оцінок якості функціонування системи кібербезпеки дозволяє оцінити економічну ефективність застосування засобів захисту інформації з метою підвищення рівня надійності системи інформаційної безпеки. Запропоновано математичну модель максимізації ефективності засобів захисту інформації при обмеженнях на обсяг витрат, використання якої може бути аргументуючим фактором для мотивації андеррайтерів. Перспективи подальших досліджень можуть полягати у деталізації критеріїв оптимальності створення системи інформаційної безпеки підприємства для захисту від можливих інформаційних загроз, а також у дослідженні більш складних випадків комбінованих інформаційних загроз, що пов'язані між собою.

Ключові слова: інформаційна безпека; інформаційні ризики; математична модель; методи оптимізації; інформаційна загроза.

ВСТУП

Інформація стала важливим стратегічним ресурсом, який сприяє підвищенню ефективності практичної діяльності у всіх сферах життя. Масове застосування інформаційних технологій, з одного боку, веде до значних переваг у діяльності підприємств та організацій, а з іншого — потенційно створює передумови для витоку, розкрадання, втрати, спотворення, підробки, знищення, копіювання та блокування інформації і, як наслідок, завдання економічної, соціальної або інших видів шкоди. Згідно ISO/IEC 27000:2009 інформаційна безпека (ІБ) — це збереження конфіденційності, цілісності і доступності інформації.

Особливого значення захист інформаційної безпеки набув в умовах гібридної війни, важливим елементом якої є інформаційне протистояння за вплив на різні аспекти суспільних відносин та встановлення контролю над стратегічними ресурсами [1].

Постановка проблеми. Забезпечення захищеності інформації є актуальним завданням сучасності, оскільки проблема інформаційних ризиків та пошуку шляхів зменшення шкоди стає дедалі гострішою. Під ризиком для інформаційної безпеки [2] розуміють імовірність того, що дана загроза, відшукавши вразливість активу або групи активів, завдасть шкоду організації.

Практика функціонування інформаційних систем показує, що досягнення стовідсоткового рівня безпеки — справа дорога і не завжди доцільна, оскільки навіть найдосконаліша на сьогодні система інформаційного захисту не може протидіяти загрозам, які можуть виникнути в майбутньому. Крім того, вартість комплексного захисту може виявитися значно вищою, ніж вартість інформаційних ресурсів, що захищаються. Тому правомірно можна ставити питання про впровадження засобів мінімізації загроз.

Аналіз останніх досліджень і публікацій. Страхування ризиків інформаційної безпеки є одним із варіантів опрацювання цих ризиків та економічно вигідним методом захисту інформації, заснованим на видачі страховими компаніями гарантій суб’єктам інформаційних відносин щодо відшкодування їх матеріального збитку у разі реалізації загроз інформаційної безпеки [3] – [5]. На жаль, страхування інформаційних ризиків продовжує залишатися поки-що ексклюзивним видом страхування [6]. Однією із причин цього є побоювання страхових компаній щодо необхідності здійснення значних компенсацій збитків страхувальників у випадку масового настання страхових випадків.

Побудова ефективної системи інформаційної безпеки неможлива без використання методів математичного моделювання [7] – [9]. Хоча, на перший погляд, система кібербезпеки прямого впливу на зростання прибутків не має, однак існує чимало інформаційних систем, у яких правильно побудована система захисту інформації позначається на зростанні доходів компанії. Наприклад, згідно з дослідженнями компанії PricewaterhouseCoopers [10], недостатньо забезпечена безпека електронних платежів стала основним бар’єром для користувачів, тобто, створення надійної інформаційної безпеки у таких системах обумовлює довіру клієнтів, а це, в свою чергу, сприяє збільшенню прибутків.

Психологічний чинник, пов’язаний з усвідомленням загрози потенційного шахрайства, залишається основною перешкодою для використання мережі Інтернет як засобу проведення комерційних операцій, оскільки користувачі і фахівці досі не розглядають Інтернет як безпечне середовище. Опитування показують, що найбільшою потенційною загрозою є несанкціоноване отримання персональних даних під час використання відкритих каналів зв’язку Інтернет. За даними розробників платіжної

системи VISA близько 23% транзакцій електронної комерції не проводиться через острах клієнта ввести персональну інформацію при роботі, наприклад, з електронним магазином [11].

Впровадження заходів системи інформаційної безпеки зазвичай призводить до продуктивнішого використання робочого часу співробітниками. Це пов'язано, зокрема, з обмеженням доступу до інформації, яка не використовується для роботи, в результаті виключається доступ до розважальних сайтів, а також зменшується обсяг неслужбового листування.

Лише за наявності системи математичних моделей захисту інформації можна стверджувати, що робота компанії із забезпечення ІБ здійснюється на належному рівні. В роботі [12] виконано моделювання, аналіз і оцінювання ризиків інформаційної безпеки на основі прикладних аспектів теорії графів у поєднанні з експертними методами оцінювання. Проаналізовано сучасні підходи до моделювання заходів та методики оцінки ризиків в інформаційній безпеці. Сформульовано рекомендації щодо підвищення ефективності системи захисту інформації. Запропонована модель може бути застосована на етапі аудиту безпеки організації для виявлення слабких місць системи захисту, а також для удосконалення діючої системи кіберзахисту.

У роботі [13] запропоновано методику графічного моделювання процесу оцінки ризиків кількісним та якісним методом з використанням діаграм діяльності та обчислення ймовірних втрат від реалізації загрози із врахуванням коефіцієнта руйнування. Для проведення аналізу визначено список і цінність активів (ресурсів), що підлягають захисту; ідентифіковано список загроз інформаційній безпеці, актуальних для даної інформаційної системи; оцінено ймовірність реалізації загроз; визначено вразливість активів та розмір потенційних збитків; виконано оцінку ризиків; запропоновано рішення, яке забезпечує необхідний рівень інформаційної безпеки, забезпечує реалізацію і тестування обраних способів захисту та проведення оцінки залишкового ризику. Детально проаналізовано особливості зовнішніх і внутрішніх загроз та вразливостей об'єктів ІТ-інфраструктури в енергетичному секторі. Основними загрозами для інформаційних систем автоматизації та управління вважаються: несанкціоноване використання точок доступу до дистанційного технічного обслуговування; мережеві атаки через корпоративну мережу; атаки на стандартні компоненти, що використовуються в мережі ICS; DDoS-атаки; людська помилка або саботаж; проникнення вірусу через знімний носій чи зовнішні пристрої; несанкціонований доступ до ресурсів; атаки на компоненти мережі; технічні збої або форс-мажор. Узагальнено перелік заходів щодо управління ІТ-ризиками та способи планування, здійснення і контролю контрзаходів, спрямованих на захист інформаційних систем.

Проведений аналіз показав різнорідність існуючих загроз і необхідність комплексного підходу до їх нейтралізації з урахуванням уразливостей, які можуть експлуатуватися порушником у процесі атаки та виявлятися на різних рівнях діяльності інформаційної системи.

Метою статті є висвітлення підходу до математичного моделювання максимізації ефективності засобів захисту інформації від несанкціонованого доступу при обмеженнях на обсяг витрат. Застосування методів оптимізації до математичного моделювання кількісних оцінок якості функціонування системи кібербезпеки дозволяє оцінити економічну ефективність застосування засобів захисту інформації з метою підвищення рівня надійності системи інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Методи забезпечення інформаційної безпеки, як відомо, поділяються на правові, організаційно-технічні та економічні. До економічних методів підтримки ІБ відносять: розробку і впровадження програм забезпечення інформаційної безпеки та визначення порядку їх фінансування, удосконалення системи фінансування робіт, пов'язаних з реалізацією правових та організаційно-технічних методів захисту інформації, створення системи страхування інформаційних ризиків фізичних та юридичних осіб. Поєднання класичних (програмних і технічних) методів захисту інформації та механізму страхування можуть допомогти компанії створити надійну систему інформаційної безпеки.

Страхування інформаційних ризиків — відносно новий вид страхування. Відсутність досвіду і напрацьованих стандартів роботи змушує страховиків застосовувати індивідуальний підхід до потенційних клієнтів. Тому страхувальник може ставити і обговорювати питання щодо вартості страхового захисту. Страхувальник повинен чітко уявляти, що чим більше він витратив на безпеку своєї інформаційної системи, чим надійніша в нього система інформаційної безпеки, тим нижчою є ймовірність того, що зловмиснику вдасться проникнути і порушити цілісність інформації, що зберігається, і тим менше йому доведеться заплатити страховій компанії за поліс страхування.

Основою будь-якої насправді ефективної системи інформаційної безпеки є використання методів математичного моделювання. По-перше, саме з їх допомогою можна переконливо довести менеджерам, що вкладення коштів у систему інформаційної безпеки в ряді випадків сприяє збільшенню прибутків компанії, а, по-друге, в умовах обмеженості ресурсів, відведених на розробку і функціонування системи кіберзахисту, за допомогою цих методів можна вибрати оптимальний набір засобів захисту і на основі математичної моделі аргументовано довести, наскільки створена система інформаційної безпеки ефективна в боротьбі проти найпоширеніших загроз.

Вирішення першої задачі можна здійснити за допомогою показника змін R, що визначається за формулою:

$$R = \frac{\Delta P}{I},$$

де ΔP — зміна прибутків, обумовлена інвестиціями I, здійсненими в інформаційну безпеку.

Побудова математичної моделі

Передбачається, що для успішного функціонування системи інформаційної безпеки підприємства, вона оснащена комплексом апаратних та програмних засобів захисту від можливих інформаційних загроз таким чином, щоб можна було встановити певний критерій оптимальності створення такої системи ІБ. При цьому припускаємо, що інформаційні загрози між собою не пов'язані. На основі аналізу ризиків, уразливостей, зловмисників та загроз виконується планування, здійснення та контроль контрзаходів, спрямованих на захист інформаційної системи, зокрема, з використанням сучасних методів цифрового обміну даними в умовах сильних перешкод [14].

У загальному випадку вважаємо, що задано множину T інформаційних загроз, які можуть виникнути в інформаційній системі підприємства, та множину S апаратних і програмних засобів захисту, за допомогою яких ці загрози можуть бути нейтралізовані. Для кожного поєднання «інформаційна загроза — засіб захисту» визначено число $r(i, j)$ — ефективність нейтралізації i-м засобом захисту j-ї інформаційної загрози.

ISSN 2663 - 4023

Для побудови математичної моделі введемо змінну $y(i, j)$:

$$y(i, j) = \begin{cases} 1, & \textit{якщо } j-\textit{а загроза нейтралізується за допомогою } i-\textit{го засобу захисту} \\ 0, & \textit{в інших випадках} \end{cases}.$$

Тоді завдання вибору оптимальної системи інформаційної безпеки полягатиме в максимізації ефективності нейтралізації наявних інформаційних загроз різними засобами захисту при обмеженнях на обсяг витрат Q.

Математична модель задачі має вигляд:

$$\sum_{j=1}^{m}\sum_{i=1}^{n} r(i, j)y(i, j) \to \max$$

за обмежень

$$\sum_{i=1}^{n} q(i)\sum_{x_j \in T} y(i, j) \le Q;$$

$$\{y(i, j)\} = \{0; 1\},$$

де $q(i)$ — витрати на розробку чи придбання i-го засобу захисту.

За аналогічною схемою може бути розглянута задача мінімізації витрат на забезпечення захисту інформаційної системи від інформаційних загроз з обмеженням на заданий рівень ефективності E засобів захисту:

$$\sum_{i=1}^{n} q(i)\sum_{j=1}^{m} y(i, j) \to \min$$

за обмежень

$$\frac{\sum_{j=1}^{m}\sum_{i=1}^{n} r(i, j)y(i, j)}{\sum_{i=1}^{n} \max\left(r(i, j)\right)} \le E;$$

$$\{y(i, j)\} = \{0; 1\}.$$

Дослідження моделі

Проведені розрахунки дозволяють виконати кількісну оцінку якості функціонування системи інформаційної безпеки, а також оцінити економічну ефективність застосування засобів захисту інформації. У наведеній моделі передбачається, що найвищий рівень ефективності системи інформаційної безпеки буде тоді, коли для нейтралізації кожної загрози буде обрано засіб захисту з максимальною ефективністю. Найвищий рівень ефективності системи інформаційної безпеки дорівнює сумі максимальних елементів у кожному стовпці матриці $r(i, j)$. Відмітимо, що вибір найбільш оптимального набору класичних засобів захисту буде ефективним для протидії інформаційним ризикам в умовах виділеного обсягу фінансових ресурсів. Разом з тим, слід враховувати, що створення ефективної системи інформаційної безпеки на такому рівні, на якому ймовірність настання ризику заподіяння шкоди інформаційній системі компанії стане низькою, буде вагомою підставою для практичного застосування механізму страхування.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Створення надійної системи інформаційної безпеки компанії вимагає активного поєднання класичних (програмних та технічних) та економічних методів захисту інформації. Ефективне ж залучення економічних механізмів, що дозволяють компенсувати збитки компанії, пов'язані із заподіянням шкоди інформаційній системі, можливе лише у разі наявності системи інформаційної безпеки, що з великою ймовірністю гарантує збереження інформації. Запропонований комплекс моделей може надати істотну допомогу для розробки найефективнішої щодо протидії інформаційним ризикам системи кібербезпеки в умовах обмежень на ресурси, що виділяються на неї, а також при визначенні допустимих ймовірностей заподіяння шкоди інформаційній системі основними інформаційними загрозами (як зовнішніми, так і внутрішніми).

Перспективи подальших досліджень полягають у деталізації критеріїв оптимальності створення системи інформаційної безпеки підприємства для захисту від можливих інформаційних загроз, а також у дослідженні більш складних випадків комбінованих інформаційних загроз, що пов'язані між собою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press.
2. *Information technology. Security techniques. Information security risk management*: BS ISO/IEC 27005:2008.
3. Kopytin, Yu.V. (2010). Information security risk insurance model. *Digital technologies, (8),* 97–109.
4. Ksyonzhyk, I., Zhovta, N., & Pavlina, A. (2021). Insurance of cybersecurity risks of business entities in the modern information space. *Economy and Society, (34).* https://doi.org/10.32782/2524-0072/2021-34-90
5. Goodman, M., & Brenner, S. (2012). The Emerging Consensus on Criminal Conduct in Cyberspace. *UCLA J.L. & Tech., 3.*
6. Zamulyanets, K.V. (2012). Insurance of information security risks. *In VIII International Scientific and Practical Conference "Socio-economic Reforms in the Context of Ukraine's Integration Choice"*. http://www.confcontact.com/2012_11_29/6_zamulyanets.htm
7. Hu, Z., Khokhlachova, Y., Sydorenk, V., & Opirskyy, I. (2017). Method for Optimization of Information Security Systems Behavior under Conditions of Influences. *International Journal of Intelligent Systems and Applications, 9(12),* 46–58. https://doi.org/10.5815/ijisa.2017.12.05
8. Barrett, C., Eubank, S., & Marathe, M. (2006). Modeling and simulation of large biological, information and socio-technical systems: An interaction based approach. *In Interactive Computation,* 353–392. Springer Berlin Heidelberg.
9. Maevsky, D. A., Maevskaya, E. J., Jekov, O. P., & Shapa, L. N. (2014). Verification of the software reliability models. *Reliability: Theory & Applications, 9(3(34)),* 14–23.
10. *Global PwC.* (n. d.) https://www.pwc.com/gx/en.html
11. Hladka, O., Karpovich, I., & Buryan, D. (2022). Modeling technologies for assessment of information security risks in e-commerce. *In International Conference on Innovative Solutions in Software Engineering (ICISSE),* 78–82.
12. Karpovich, I., Hladka, O., & Bukhalo, Y. (2021). Technologies of modeling and assessment of the information security risk. *Technical Sciences and Technologies, (1(23)),* 62–68. https://doi.org/10.25140/2411-5363-2021-1(23)-62-68
13. Karpovich, I. M., Hladka, O. M., & Kalashnikov, V. I. (2022). Modeling of information security risk analysis processes as a way of cost optimization. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences, (5),* 93–99. https://doi.org/10.32782/2663-5941/2022.5/13
14. Lazarovych, I., Kozlenko, M., Kuz, M., Tkachuk, V., Dutchak, M., Savka, I., & Pikuliak, M. (2021). Software implemented enhanced efficiency BPSK demodulator based on perceptron model with randomization. *In 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON).* IEEE. https://doi.org/10.1109/ukrcon53503.2021.9575458

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Ivan Karpovich
PhD on Physics and Mathematics Science, Associate Professor,
Associate Professor at the Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering, Rivne, Ukraine
ORCID ID: 0000-0002-4601-0541
i.m.karpovich@nuwm.edu.ua

Olena Hladka
PhD on Engineering Science, Associate Professor,
Associate Professor at the Department of Computer Technology and Economic Cybernetics
National University of Water and Environmental Engineering, Rivne, Ukraine
ORCID ID: 0000-0003-4728-0663
o.m.hladka@nuwm.edu.ua

Andrii Palamarchuk
Student at the Institute of Cybernetics, Information Technologies and Engineering
National University of Water and Environmental Engineering, Rivne, Ukraine
palamarchuk_ak24@nuwm.edu.ua

USE OF MATHEMATICAL OPTIMIZATION METHODS TO INCREASE THE EFFICIENCY OF INFORMATION SECURITY SYSTEMS

Abstract. Ensuring information security is a pressing task of our time, as the problem of information risks and finding ways to reduce damage from cyberattacks is becoming increasingly acute. In this paper, we analyzed methods for ensuring information security. Among the economic methods of information protection, information risk insurance occupies an important place. However, such insurance continues to remain a rare occurrence due to insurance companies' concerns about the need to pay policyholders significant amounts of compensation for losses in the event of a mass occurrence of insured events. The use of mathematical modeling methods allows to convincingly prove managers that investing in an information security system contributes to increasing the company's profits, and also, in conditions of limited resources allocated to the development and operation of a cyber defense system, to choose the optimal set of protection tools and, based on a mathematical model, convincingly prove how effective the created information security system is in the fight against the most common threats. The purpose of the work is mathematical modeling of maximizing the effectiveness of information protection tools against unauthorized access with restrictions on the amount of costs. The application of optimization methods to mathematical modeling of quantitative assessments of the quality of functioning of a cybersecurity system allows us to assess the cost-effectiveness of using information protection tools to increase the level of reliability of the information security system. We proposed a mathematical model for maximizing the effectiveness of information protection tools under cost constraints, the use of which can be an argumentative factor for motivating underwriters. Prospects for further research may consist in detailing the criteria for the optimality of creating an enterprise information security system to protect against possible information threats, as well as in studying more complex cases of combined information threats that are interconnected.

Keywords: information security; information risks; mathematical model; optimization methods; information threat.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press.
2. *Information technology. Security techniques. Information security risk management*: BS ISO/IEC 27005:2008.
3. Kopytin, Yu.V. (2010). Information security risk insurance model. *Digital technologies, (8),* 97–109.
4. Ksyonzhyk, I., Zhovta, N., & Pavlina, A. (2021). Insurance of cybersecurity risks of business entities in the modern information space. *Economy and Society, (34).* https://doi.org/10.32782/2524-0072/2021-34-90

5. Goodman, M., & Brenner, S. (2012). The Emerging Consensus on Criminal Conduct in Cyberspace. *UCLA J.L. & Tech., 3.*
6. Zamulyanets, K.V. (2012). Insurance of information security risks. *In VIII International Scientific and Practical Conference "Socio-economic Reforms in the Context of Ukraine's Integration Choice"*. http://www.confcontact.com/2012_11_29/6_zamulyanets.htm
7. Hu, Z., Khokhlachova, Y., Sydorenk, V., & Opirskyy, I. (2017). Method for Optimization of Information Security Systems Behavior under Conditions of Influences. *International Journal of Intelligent Systems and Applications, 9(12),* 46–58. https://doi.org/10.5815/ijisa.2017.12.05
8. Barrett, C., Eubank, S., & Marathe, M. (2006). Modeling and simulation of large biological, information and socio-technical systems: An interaction based approach. *In Interactive Computation,* 353–392. Springer Berlin Heidelberg.
9. Maevsky, D. A., Maevskaya, E. J., Jekov, O. P., & Shapa, L. N. (2014). Verification of the software reliability models. *Reliability: Theory & Applications, 9(3(34)),* 14–23.
10. *Global PwC.* (n. d.) https://www.pwc.com/gx/en.html
11. Hladka, O., Karpovich, I., & Buryan, D. (2022). Modeling technologies for assessment of information security risks in e-commerce. *In International Conference on Innovative Solutions in Software Engineering (ICISSE),* 78–82.
12. Karpovich, I., Hladka, O., & Bukhalo, Y. (2021). Technologies of modeling and assessment of the information security risk. *Technical Sciences and Technologies, (1(23)),* 62–68. https://doi.org/10.25140/2411-5363-2021-1(23)-62-68
13. Karpovich, I. M., Hladka, O. M., & Kalashnikov, V. I. (2022). Modeling of information security risk analysis processes as a way of cost optimization. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences, (5),* 93–99. https://doi.org/10.32782/2663-5941/2022.5/13
14. Lazarovych, I., Kozlenko, M., Kuz, M., Tkachuk, V., Dutchak, M., Savka, I., & Pikuliak, M. (2021). Software implemented enhanced efficiency BPSK demodulator based on perceptron model with randomization. *In 2021 IEEE 3rd Ukraine Conference on Electrical and Computer Engineering (UKRCON).* IEEE. https://doi.org/10.1109/ukrcon53503.2021.9575458