

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕОРІЯ КОДУВАННЯ

УДК 004.8 + 004.056

В. В. Лукічов, Ю. В. Баришев, Н. Р. Кондратенко, В. І. Маліновський
МЕТОД АДАПТИВНОГО БАГАТОШАРОВОГО ЗАХИСТУ
ІНФОРМАЦІЇ НА ОСНОВІ СТЕГАНОГРАФІЇ ТА
КРИПТОГРАФІЇ

Вінницький національний технічний університет, м. Вінниця

Анотація. Наведено аналіз відомих розв'язків задачі поєднання стеганографічних та криптографічних методів для досягнення багатoshарового захисту інформації. Результати аналізу дозволили виявити тенденції та перспективи розвитку цих методів. За результатами аналізу виконано постановку задачі дослідження щодо адаптації використовуваних криптографічних та стеганографічних методів для досягнення найкращого рівня захисту, який є необхідним в критичних системах. Визначено метрики на основі, яких можливо здійснювати вибір найкращого поєднання методів криптографічного та стеганографічного захисту. Представлено метод багатoshарового захисту інформації, який поєднує в собі криптографічний та стеганографічний підходи для забезпечення підвищеного рівня захисту конфіденційності та цілісності інформації. Запропоновано ввести критерії вибору криптографічних перетворень таким чином, щоб їх поєднання разом зі стеганографічними давала найкращий ефект. Наведено приклад реалізації методу для доведення концепції. Розроблено алгоритм, що реалізує запропонований метод адаптивного багатoshарового захисту інформації. Визначено перспективу подальших досліджень.

Ключові слова: стеганографія, криптографія, кібербезпека, критичні системи, метрики.

Abstract. An analysis of known solutions to the problem of steganographic and cryptographic methods combining to achieve multilayer information protection is presented. Results of the analysis allowed us to identify trends and prospects for the development of these kind of methods. Based on the results of the analysis, the research task was determined concerning the adaptation of the used cryptographic and steganographic methods in order to achieve the best level of protection, which is needed at critical systems. Metrics were defined, those allowed to choose the best combination of cryptographic and steganographic protection methods parameters. A method of multilayered information protection is presented, which combines cryptographic and steganographic approaches to ensure an increased level of information's confidentiality and integrity protection. It is proposed to introduce criteria for the selection of cryptographic transformations in such a way that their combination together with steganographic transformations gives the best impact. An instance of the proposed method implementation is given in order to prove the concept. An algorithm has been developed that implements the proposed method of adaptive multilayer information protection. The perspective of further research is determined.

Key words: steganography, cryptography, cyber security, critical systems, metrics.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-4-11>.

Вступ

Захист інформації є актуальною проблемою в сучасному світі, де цифрові зображення широко використовуються в різних галузях, включаючи критичні системи такі, як медицина, банкінг, правоохоронну діяльність та багато інших. Завдяки методам стеганографії є можливість приховувати факт передавання інформації. Таким чином, конфіденційність даних захищається завдяки тому, що зловмисникам складно її виявити. Водночас криптографічні методи дозволяють приховати зміст даних. Поєднання цих підходів дозволяє побудувати багатoshаровий захист даних. Так, спочатку зловмиснику потрібно виявити факт передавання даних, а потім розкрити їх зміст, шляхом розшифрування.

Актуальність

Підсилення захисту інформації, прихованої в зображення, застосуванням методів шифрування є природним. Більше того, завдяки властивості шифрування перетворювати вихідне повідомлення у шифротекст, статистичні властивості якого подібні до статистичних властивостей випадкових чисел, відрізнити видобуті внаслідок стегоаналізу дані від шумів становить складну задачу без знання використаного стеганографічного методу вбудовування даних. Таким чином такі методи можуть бути застосовані в задачах кібербезпеки критичних систем, де висувуються підвищені вимоги щодо захисту конфіденційності. Наразі відомі підходи до поєднання стеганографічних методів захисту з криптографічними. Однак попри те, що ці підходи передбачають використання різних контейнерів, різних алгоритмів вбудовування та різних криптографічних алгоритмів – вони залишаються поза увагою дослідження ступеня синергії цих складових. При цьому вибір певних алгоритмів може як покращувати показники якості захисту інформації, так їх й погіршувати. Внаслідок цього постає актуальна задача вимірювання та врахування явища синергії між ними та побудова методу захисту інформації на основі визначення найкращої комбінації.

Мета

Метою дослідження є покращення захисту конфіденційності даних при одночасному використанні методів стеганографічного та криптографічного захисту за рахунок врахування явища синергії між ними.

Задачі

1. Проаналізувати відомі підходи одночасного використання методів стеганографії та криптографії для захисту конфіденційності даних.
2. Виконати постановку задачі розробки адаптивного багатопланового захисту інформації.
3. Розробити метод такого захисту як доведення концепції можливості такої розробки.

Аналіз відомих досліджень

Аналіз джерел показав широке поширення поєднання методів стеганографії та криптографії. Зокрема в роботі [1] запропоновано зашифрування секретних даних за допомогою блокового симетричного шифру AES в режимі роботи OFB, доєднання ключа шифрування до зашифрованих даних та вбудовування в зображення методом кластеризації найближчого центроїда. Основним недоліком такого підходу є зберігання ключа шифрування разом з даними, які зашифровані цим ключем з їх подальшим передаванням в одному контейнері. Таким чином, шифрування дозволило авторам покращити статистичні властивості відкритої інформації для ускладнення виконання криптоаналізу. Однак при цьому застосування криптографії не утворило ще один шар захисту, оскільки при успішному стеганоаналізі розшифрувати дані не становитиме складності, оскільки зловмиснику буде доступним ключ шифрування.

В роботі [2] автори пропонують подвійне використання стеганографічного перетворення. Таким чином відкритий текст зашифровують, згодом вбудовують в один контейнер, який вбудовують в інший контейнер. Автори розраховують, що внаслідок успішного стеганоаналізу зловмисником буде виявлено дані, які насправді є контейнером для приховування справжнього секрету. Відповідно зловмисник зупинить подальший аналіз, отримавши контейнер. На жаль, автори не зазначають використовувані криптографічні перетворення та спосіб розв'язання задачі ключового транспорту. Більше того вони пропонують використання методу LSB для вбудовування даних в зображення, який ефективний для окремих контейнерів як-то файли формату *.bmp, які не відповідають сучасним форматам, а тому привертають увагу потенційного зловмисника. Крім того, загальним недоліком робіт [1, 2] є забезпечення стійкості за рахунок концепції security by obscurity, який суперечить принципам Керкгоффса [3], прийнятих за найкращу практику сучасних методів захисту інформації.

Відомий підхід [4] який передбачає поєднання шифру AES-128, методу гешування SHA-256 та методу вбудовування LSB, використовуючи відеопотік HEVC (high-efficiency video coding) як контейнер. Для цього методу автори передбачають використання єдиного ключа, який зазнає процедуру розгортання на основі SHA-256 і використовує отримані геш-значення як ключ для шифрування та визначення місць вбудовування. Подібний підхід запропонований авторами [5], але вони використовують сталий ключ, шифр DES та аудіо-файли як контейнер. Недоліком цих методів є те, що при передаванні аудіо- та відеопотоків забезпечення сталої швидкості є важливішим за коректність передавання даних, відповідно повторного пересилання кадрів, що надійшли з помилками не відбувається, щоб не втрачати темп відображення користувачеві. Таким чином, існує ймовірність, що дані будуть пошкоджені під час передавання, а через зашифрування стане неможливим відновлення всіх прихованих даних, що слідує за пошкодженням кадром. Крім того, аудіо-файли та відео HEVC використовують методи ущільнення даних, а тому LSB не дозволяє досягти мінімуму спотворень відеопотоку при сталому обсязі даних для вбудовування.

Детальний аналіз відомих поєднань стеганографічних та криптографічних методів, наведений в роботі [6], відзначає відсутність оцінок стійкості результату такого поєднання. Крім того, автори [6] наголошують на недостатності аналізу відомих методів, оскільки у відомих роботах навіть у тих випадках, коли відбувається аналіз отриманих результатів, то він виконується методами стеганоаналізу, ігноруючи криптографічні складові запропонованих методів.

Підхід, запропонований в роботі [7], передбачає спочатку застосування методів стеганографії з подальшим шифруванням контейнеру. Завдяки застосуванню швидкого методу шифрування автори досягають високої швидкості перетворення, але, на жаль, запропонований метод шифрування не досліджувався щодо показників стійкості та будується на основі записування бітів двовимірного зображення в масив з трьома вимірами та накладанні масок. Як видно із зовнішнього вигляду зашифрованого зображення, наведеного авторами роботи [7], попри зашумленість, отриману внаслідок такого перетворення, все одно видно основні риси оригінального зображення, що свідчить про недостатню стійкість шифрування. Крім того, застосування шифрування до контейнера привертає увагу зловмисників до контейнерів.

В роботі [8] автори розглядають поєднання LSB з DES, Blowfish та дискретним косинусним перетворенням (як криптографічним перетворенням). Сильною стороною роботи [8] є використання MSE (Mean Square Error), SNR (signal-to-noise ratio) та PSNR (peak signal-to-noise ratio) як метрик для до-

слідження ефективності цих комбінацій. На жаль, використання застарілих методів шифрування Blowfish, який має слабкі ключі [9], та DES, вразливості якого були виявлені ще у 1991 році в роботі [10], подальший розвиток якої дозволив виявити низку ефективних атак [11]. Відповідно здобуті в роботі [8] результати не дозволяють забезпечити достатню стійкість криптографічного шару захисту, а тому стійкість забезпечується лише методами стеганографії.

Автори роботи [12] демонструють можливість багатошарового захисту для застосування в контейнерах на основі ланцюгів протеїнів. Для цього в [12] використовують специфічні методи шифрування та стеганографії, які враховують специфіку контейнеру. Зокрема запропонований підхід дозволяє генерувати ключ на основі аналізу молекул ДНК. Однак, попри перспективність застосування підходу в майбутньому, використання цього підходу для найбільш поширених інформаційних технологій наразі потребує додаткових ресурсів для придбання аналізаторів ланцюгів протеїнів та їх інтеграції до інформаційних систем.

Постановка задачі

Результати аналізу досліджень показали перспективність застосування багатошарового захисту. Проте загальним недоліком робіт відсутність метрик вимірювання синергії використовуваних алгоритмів захисту та контейнерів. При цьому дослідження, представлені у [8], показали, що різні комбінації криптографічних алгоритмів при фіксованому типі контейнера та стеганографічного методу дозволяють досягти різного ступеня ефективності з точки зору метрик MSE, SNR та PSNR. Таким чином впливає, що існує актуальна задача вибору найкращих параметрів використання стеганографічних та криптографічних моделей та методів при багатошаровому захисті інформації.

Метод адаптивного багатошарового захисту інформації

В межах цього дослідження обрано найбільш поширений шлях поєднання стеганографічних та криптографічних методів – шифрування кроків:

Крок 1: Вибір криптографічного алгоритму.

Для прикладу обрано стійкий та глибоко досліджений алгоритм шифрування як-то AES для захисту та покращення статистичних показників інформації в зображеннях.

Крок 2: Вибір стеганографічного алгоритму.

З метою демонстрації можливості реалізації методу обрано алгоритм стеганографії Convolutional Neural Networks (CNN).

Крок 3: Визначення параметрів адаптації.

Попри те, що стійкі шифри мають формувати шифротекст, який за статистичними показниками аналогічний послідовності випадкових чисел, варто врахувати, що вбудовуються зазвичай невеликі за обсягом дані. Відповідно статистичні показники коротких повідомлень не завжди матимуть бажані статистичні показники (аналогічні послідовності випадкових чисел). Для таких випадків необхідно визначити ті показники шифрування, які можуть бути замінені для вибору найкращого варіанту. Наприклад, для наведеного прикладу з шифром AES таким показником є режим роботи блокового шифру (як-то CBC, OFB, CTR тощо).

Крок 4: Застосування адаптивної криптографії

Для прикладу, що розглядається цей крок реалізується шляхом шифрування повідомлення за допомогою AES в режимі роботи, визначеному на кроці 3.

Крок 5: Вбудовування зашифрованої інформації в контейнер.

Відповідно до наведеного прикладу цей крок передбачатиме використання методу CNN.

Внаслідок адаптації використовуюваного криптографічного методу захисту до потреб стеганографічного досягається покращення синергії між цими методами. Що дозволяє покращити показники якості вбудовування інформації в контейнер.

Для видобування інформації необхідно виконати обернений процес до зазначеного в методі: спочатку видобути з контейнера приховану інформацію, а згодом розшифрувати її. На рисунку 1 наведено алгоритм, що реалізує запропонований метод.

Для досягнення найкращих показників синергії пропонується використовувати комбінацію метрик SNR, PSNR та MSE. У випадку, коли показники якості, що відображаються цими метриками будуть суперечити одна одній, пропонується прийняття рішення за мажоритарним принципом.

Експериментальні дослідження застосування методу

Для доведення концепції розглянемо приклад застосування методу. Нехай секретним повідомленням є таке "The quick brown fox jumps over the lazy dog", подане у кодуванні UTF-8. Як метод шифрування оберемо AES-128. Для того, щоб секретне повідомлення було зручніше обробляти його необхідно представити у вигляді рядка байтів, доповненого нулями до довжини блоку шифра. Як параметри адаптації оберемо ключі шифрування та режим роботи блокового шифру {key, modeOfOperations}. Було роз-

роблено програмний засіб мовою Dart на основі реалізації AES в бібліотеці з відкритим кодом Pointy Castle. На вхід розробленої програми надходили повідомлення та параметри адаптивного шифрування представлені в таблиці 1.

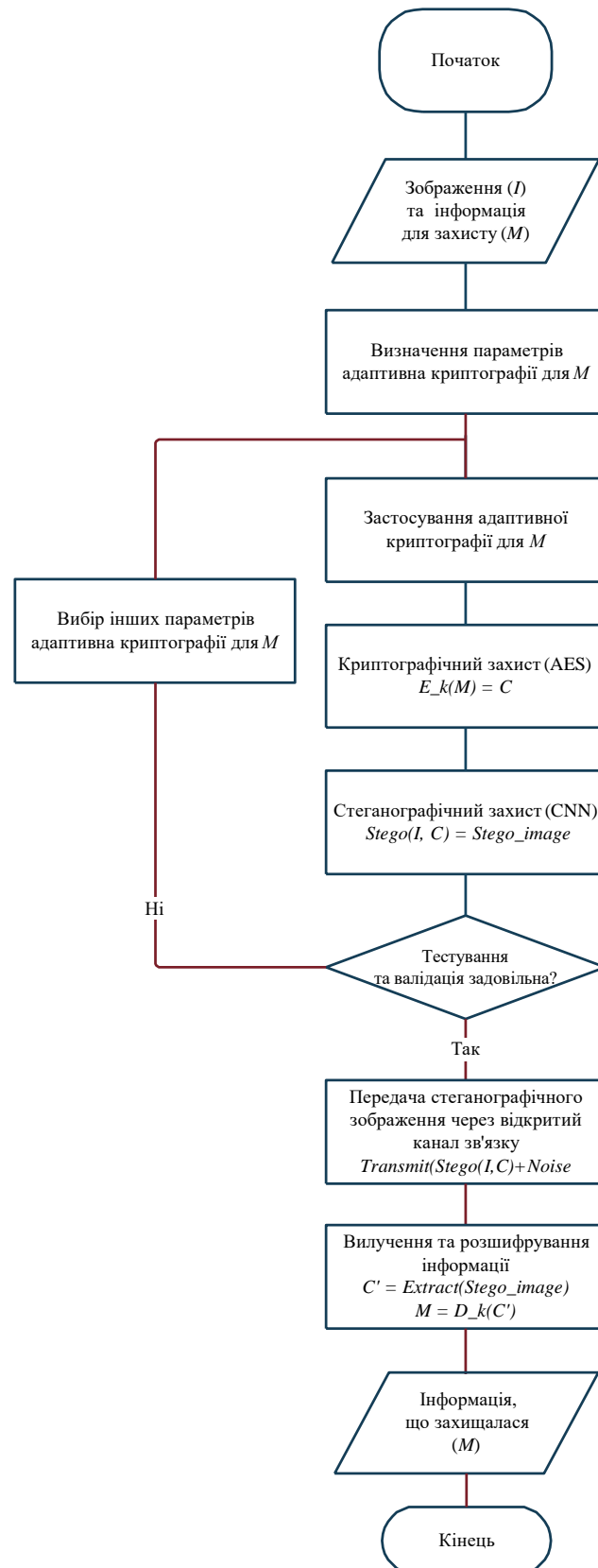


Рисунок 1 – Алгоритм багатoshарової системи захисту інформації в зображеннях

Таблиця 1 – Параметри адаптивного шифрування

Назва параметрів	Значення параметрів
Повідомлення	0x717569636b2062726f776e20666f78206a756d7073206f76657220746865206c617a7920646f670000000000000000
Ключ 1	0x010203040506070809000a0b0c0d0e0f
Ключ 2	0x0f0e0d0c0b0a00090807060504030201
Режим шифрування 1	CBC
Режим шифрування 2	CTR

Внаслідок зашифрування отримано варіанти потенційних шифротекстів для стеганографічного вбудовування в контейнер, наведені в таблиці 2.

Таблиця 2 – Отримані варіанти шифротекстів

Використані параметри шифрування	Значення шифротексту
{Ключ 1, CBC}	0xad3c3e6b346855b3cc4f1a62d9709004396d608c6cf0b85cd460d6381ad9c6ca96a2c5118564c24a9add945510fcb94f
{Ключ 1, CTR}	0x733243f172c2feffa5d75cdb4835d4325880fb2ece35303f53b77ef9c848f06ab83881c1deba35b145bec1608d9415a6
{Ключ 2, CBC}	0xffab26ecb4f3aa6e9d3abf3aa85cc35c1f1b430f121bb03bd711743cc383758dfdc86dd5545e6d9a97b7878ef948c58
{Ключ 2, CTR}	0xdd0869271f057b09f48cf74e9a6a1a2da497876bf79e2a4aacf5d30b07c978526585341d2715b429faf4332be7515474

Наступним кроком реалізації методу є вибір поміж отриманих шифротекстів того, який дозволить досягти найкращої синергії на основі значень метрик MSE, SNR та PSNR. Для дослідження синергії було використано три зображення як контейнери вбудовування інформації, наведені на рис. 2.

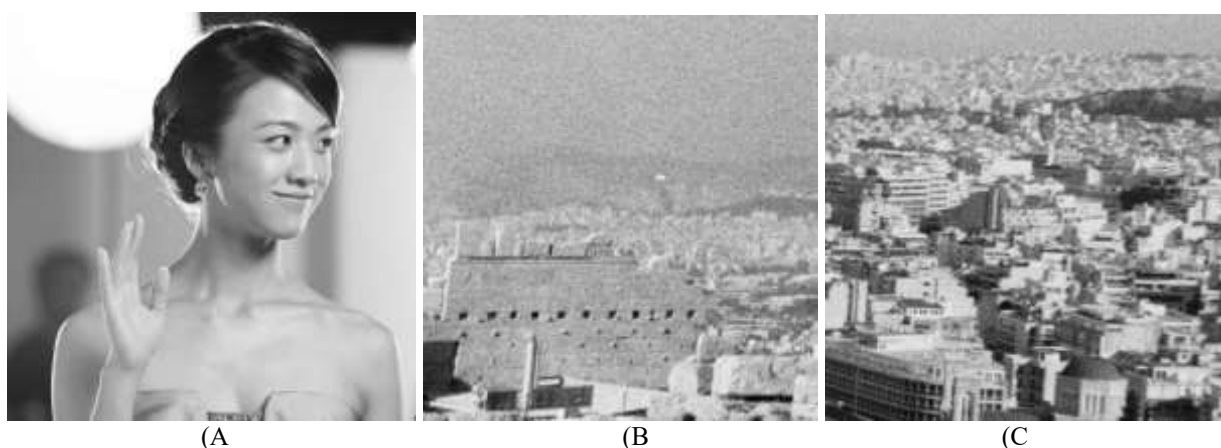


Рисунок 2 – Контейнери для вбудовування шифротекстів

За результатами вбудовування було проведено визначення обраних метрик. Результати наведено в таблиці 3.

Вищий показник метрик PSNR і SNR означає, що якість стегозображення подібна до зображення вхідного. У випадку метрики MSE – нижче значення свідчить, що якість стегозображення подібна до

зображення оригінального контейнера. Таким чином, з таблиці 3 видно, що для різних контейнерів найкращими виборами будуть різні шифротексти, тобто від вибору конкретних значень параметрів криптографічного та стеганографічного захисту залежить стійкість остаточного результату. Так для зображень А та В найкращі показники забезпечує варіант {Ключ 2, CBC}, а для зображення С – {Ключ 1, CBC}. Отже, експеримент дозволив довести, що при поєднанні криптографічного та стеганографічного методів захисту за рахунок адаптації досягаються кращі показники якості приховування інформації порівняно з відомими методами, які обирають ці показники незалежно один від одного.

Таблиця 3 – Значення метрик MSE, SNR та PSNR

Використані параметри шифрування	Зображення А			Зображення В			Зображення С		
	MSE	SNR	PSNR	MSE	SNR	PSNR	MSE	SNR	PSNR
{Ключ 1, CBC}	0.000828	386686	78.9517	0.00036	785984	82.5655	0.000936	25329494	78.4175
{Ключ 1, CTR}	0.000844	379054	78.8651	0.000373	758679	82.4120	0.000958	24742144	78.3156
{Ключ 2, CBC}	0.000803	398729	79.0849	0.00035	800386	82.6444	0.000967	24528849	78.2787
{Ключ 2, CTR}	0.000822	389298	78.9809	0.000377	751223	82.3691	0.000966	24599537	78.2905

Висновки

В межах цього дослідження були розроблено метод багат шарового захисту цифрових зображень, що базується на комбінації криптографічних та стеганографічних підходів. На відміну від відомих підходів цей метод передбачає оптимізацію під час вибору використовуваних методів стеганографічного та криптографічного перетворень, а також контейнера. Проведений аналіз дозволив підтвердити актуальність подальших досліджень в цій галузі. На основі виконаного аналізу здійснена постановка задачі дослідження. Для доведення концепції можливості розв'язання поставленої задачі, запропоновано метод, реалізація кожного кроку якого була проілюстрована прикладами реалізації відповідних кроків. Розроблене програмне забезпечення дозволило поставити експеримент, який довів можливість покращення багат шарового захисту за умов адаптації їх параметрів.

Запропонований метод доцільно використовувати в системах, де висуваються підвищені вимоги до захисту конфіденційності даних таких, як критичні системи. Перспектива подальших досліджень в цьому напрямі передбачається в ідентифікації параметрів адаптації та застосуванні методів математичного моделювання для апроксимації задачі оптимального вибору, яка розв'язується на етапі адаптації параметрів криптографічних перетворень. Це пов'язано з дискретною природою вхідних даних. Зокрема у наведеному прикладі такими параметрами було обрано режим роботи блокового шифру.

Список літератури

- [1] Shifa, A., Afgan, M. S., Asghar, M. N., Fleury, M., Memon, I., Abdullah, S., Rasheed, N. "Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering" IEEE Access, vol. 6, 2018. pp. 16189-16206, 2018, doi: 10.1109/ACCESS.2018.2815037.
- [2] Bandela, H. B., Babu, M. G., Venkata, D., Deepthi, V. "Crypto-Stego Technique for Secure Data Transmission." Journal of Physics: Conference Series. 1228, 012012, 2019. 11 p. doi:10.1088/1742-6596/1228/1/012012.
- [3] Kerckhoffs, A. "La cryptographie militaire" Journal des sciences militaires IX: 5–38, 1883. pp. 161–191. <http://www.petitcolas.net/fabien/kerckhoffs/>
- [4] Almomani, I., Alkhayer, A., El-Shafai, W. A. "Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices." Sensors, 22(6), 2281. 2022. <https://doi.org/10.3390/s22062281>
- [5] Abikoye, O. C., Adewole, K. S., Oladipupo, A. J. "Efficient Data Hiding System using Cryptography and Steganography." International Journal of Applied Information Systems. Volume 4– No.11. 2012. pp. 6-11. doi: 10.5120/ijais12-450763.
- [6] Jan, A., Parah, S.A., Hussan, M., Malik, B. A. "Double layer security using crypto-stego techniques: a comprehensive review." Health and Technology. 12, 2022. pp. 9–31. <https://doi.org/10.1007/s12553-021-00602-1>

- [7] Rasras, R. J., AlQadi, Z. A., Sara, M. R. A. A "Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages." *Engineering, Technology & Applied Science Research*, 9(1), 2019. pp. 3681–3684. <https://doi.org/10.48084/etasr.2380>
- [8] Singhal, V., Singh, D., & Gupta S. K. "Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms." *Journal of Algebraic Statistics*. Volume 13, No. 3, 2022. p. 1162-117. <https://www.publishoa.com/index.php/journal/article/view/734/624>
- [9] Kara, O., Manap, C. "A New Class of Weak Keys for Blowfish. In: Biryukov, A. (eds) *Fast Software Encryption*." *Lecture Notes in Computer Science*, vol 4593. 2007. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_11
- [10] Biham, E., Shamir, A. "Differential cryptanalysis of DES-like cryptosystems." *Journal of Cryptology* 4, 1991. pp. 3–72. <https://doi.org/10.1007/BF00630563>
- [11] Biham, E., Perle, S. "Conditional Linear Cryptanalysis - Cryptanalysis of DES with Less Than 242 Complexity" *IACR Trans. Symmetric Cryptol.*, 2018, pp. 215-264.
- [12] Mawla, N. A., Khafaji, H. K. "Enhancing Data Security: A Cutting-Edge Approach Utilizing Protein Chains in Cryptography and Steganography" *Computers*, 12(8), 166. 2023. <https://doi.org/10.3390/computers12080166>
- [13] Pointy Castle. URL: <https://github.com/bcg/pc-dart>

Стаття надійшла: 12.12.2023

References

- [1] Shifa, A., Afgan, M. S., Asghar, M. N., Fleury, M., Memon, I., Abdullah, S., & Rasheed, N. (2018). Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering, *IEEE Access*, vol. 6, pp. 16189-16206, 2018, doi: 10.1109/ACCESS.2018.2815037.
- [2] Bandela, H. B., Babu, M. G., Venkata, D., Deepthi, V. (2019) Crypto-Stego Technique for Secure Data Transmission. *Journal of Physics: Conference Series*. 1228, 012012. 11 p. doi:10.1088/1742-6596/1228/1/012012.
- [3] Kerckhoffs, A. (1883). *La cryptographie militaire*. *Journal des sciences militaires IX*: 5–38, 161–191. <http://www.petitcolas.net/fabien/kerckhoffs/> [in French]
- [4] Almomani, I.; Alkhayer, A.; El-Shafai, W. A. (2022). Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices. *Sensors*, 22(6), 2281. <https://doi.org/10.3390/s22062281>
- [5] Abikoye, O. C., Adewole, K. S., Oladipupo, A. J. (2012). Efficient Data Hiding System using Cryptography and Steganography. *International Journal of Applied Information Systems*. Volume 4–No.11. pp. 6-11. doi: 10.5120/ijais12-450763.
- [6] Jan, A., Parah, S.A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto-stego techniques: a comprehensive review. *Health and Technology*. 12, pp. 9–31. <https://doi.org/10.1007/s12553-021-00602-1>
- [7] Rasras, R. J., AlQadi, Z. A., & Sara, M. R. A. (2019). A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages. *Engineering, Technology & Applied Science Research*, 9(1), pp. 3681–3684. <https://doi.org/10.48084/etasr.2380>
- [8] Singhal, V., Singh, D., & Gupta S. K., (2022). Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms. *Journal of Algebraic Statistics*. Volume 13, No. 3, p. 1162-117. <https://www.publishoa.com/index.php/journal/article/view/734/624>
- [9] Kara, O., Manap, C. (2007). A New Class of Weak Keys for Blowfish. In: Biryukov, A. (eds) *Fast Software Encryption*. FSE 2007. *Lecture Notes in Computer Science*, vol 4593. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_11
- [10] Biham, E., Shamir, A. (1991) Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology* 4, pp. 3–72. <https://doi.org/10.1007/BF00630563>
- [11] Biham, E., & Perle, S. (2018). Conditional Linear Cryptanalysis - Cryptanalysis of DES with Less Than 242 Complexity. *IACR Trans. Symmetric Cryptol.*, 2018, pp. 215-264.
- [12] Mawla, N. A., Khafaji, H. K (2023). Enhancing Data Security: A Cutting-Edge Approach Utilizing Protein Chains in Cryptography and Steganography. *Computers*, 12(8), 166. <https://doi.org/10.3390/computers12080166>
- [13] Pointy Castle. URL: <https://github.com/bcg/pc-dart>

Відомості про авторів

Лукічов Віталій Володимирович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

Баришев Юрій Володимирович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

Кондратенко Наталія Романівна – к. т. н., професор кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

Маліновський Вадим Ігорович – к. т. н., доцент кафедри захисту інформації Вінницького національного технічного університету, м. Вінниця.

V. Lukichov, Y. Baryshev, N. Kondratenko, V. Malinovskyi

METHOD OF THE ADAPTIVE MULTILAYER INFORMATION PROTECTION ON THE BASIS OF STEGANOGRAPHY AND CRYPTOGRAPHY

Vinnitsia National Technical University, Vinnitsia

УДК 004:78.08

О.В. Сілагін, Є.О. Сілагін, В.О. Денисюк, А.В. Денисюк

РОЗРОБКА ОНТОЛОГІЧНОЇ МОДЕЛІ БАЗИ ЗНАНЬ «БІБЛІОТЕКА» НА БАЗІ СЕРЕДОВИЩА PROTÉGÉ

Вінницький національний технічний університет, Вінниця

Анотація. Сучасний розвиток суспільства, підвищення ступеня і темпів інтеграції досягнень інформаційних технологій у сферу життєдіяльності людини традиційні підходи до побудови інформаційних систем перестають бути ефективними або стають надто громіздкими. Розробка та використання систем, заснованих на знаннях є одним із шляхів вирішення цієї проблеми. Матеріал роботи присвячено онтологічному моделюванню нової предметної галузі «Бібліотека». Онтологія розглядається в контексті обміну знаннями. Створена онтологічна модель бази знань «Бібліотека» є досить сучасною та актуальною на сьогодні. Розроблена онтологічна модель бази знань у цій галузі може бути реалізована на тематичних веб-ресурсах і значно полегшить семантичний пошук інформації в межах предметної області у порівнянні з існуючими. Термінологічний словник із цієї предметної галузі визначається за допомогою поняття терміносистеми. Здійснено аналіз можливостей середовища розробки онтології Protégé для моделювання конкретної предметної області «Бібліотека». Обрано базовий принцип моделювання онтології у вигляді семантичної мережі. Запропонована мережа має можливість розширити та поглибити знання про предметну сферу «Бібліотека». Використання середовища Protégé для реалізації онтологічної моделі бази знань дозволило використати переваги та особливості створеної моделі «Бібліотека», як: структурованість, повнота, рефлексивність, функціональність, транзитивність, достовірність та узгодженість інформації. Обрано та використано критерій оцінки коректності онтологічної моделі бази знань. Проведено тестування розробленої онтологічної моделі бази знань і підтверджено досить високий рівень її коректності в процесі інформаційного пошуку. Середній показник (Average) за метрикою SUM, визначений для всіх користувачів, дорівнює 83,25%, що є прийнятним показником онтологічної бази знань. При використанні класичної реляційної моделі організації бази даних для реалізації бази даних «Бібліотека», середня метрика SUM для 10 користувачів становить 75,26%. Розглянуто приклад розробленої онтології в Protégé, наведено графічне зображення базового графу онтологічної моделі бази знань «Бібліотека», модель включає 10 класів і підкласів, для кожного класу і підкласу визначено 2 властивості-відносини та до 10 властивостей-даних, наведено приклад класів онтологічної моделі «Бібліотека», наведено приклад «властивості-відносини» онтологічної моделі «Бібліотека», наведено приклад «властивості-дані» онтологічної моделі «Бібліотека». Визначено можливі напрямки подальшого розвитку онтологічної моделі «Бібліотека».

Ключові слова: онтологічна модель, бібліотека, семантичний пошук, база даних, Protégé.

Abstract. Modern development of society, increasing the degree and pace of integration of information technology achievements into the sphere of human life, traditional approaches to the construction of information systems cease to be effective or become too cumbersome. The development and use of knowledge-based systems is one way to solve this problem. The material of the work is devoted to the ontological modeling of the new subject area «Library». Ontology is considered in the context of knowledge sharing. The created ontological model of the «Library» knowledge base is quite modern and relevant today. The developed ontological model of the knowledge base in this field can be implemented on thematic web resources and will significantly facilitate the semantic search of information within the subject area in comparison with the existing ones. The terminological dictionary of this subject area is defined using the term system. An analysis of the capabilities of the Protégé ontology development environment for modeling the specific subject area «Library» was carried out. The basic principle of ontology modeling in the form of a semantic network was chosen. The proposed network has the opportunity to expand and deepen knowledge about the subject area «Library». Using the Protégé environment for the implementation of the ontological model of the knowledge base made it possible to use the advantages and features of the created «Library» model, such as: structuredness, completeness, reflexivity, functionality, transitivity, reliability and consistency of information. The criterion for assessing the correctness of the ontological model of the knowledge base was selected and used. Testing of the developed ontological knowledge base was conducted and a fairly high level of its correctness in the process of information search was confirmed. The average indicator (Average) according to the SUM metric, determined for all users, is equal to 83.25%, which is an acceptable indicator of the ontological knowledge base. When using the classic relational model of database organization to implement the «Library» database, the average SUM metric for 10 users is 75.26%. An example of the developed ontology in Protégé is considered, a graphical representation of the basic graph of the ontological model of the «Library» knowledge base is given, the model includes 10 classes and subclasses, 2 properties-relations and up to 10 properties-data are defined for each class and subclass, an example of the classes of the ontological model is given «Library», an example of the "property-relations" of the ontological model «Library» is given, an example of the "property-data" of the ontological model «Library» is given. Possible directions of further development of the ontological model «Library» have been determined.

Keywords: ontological model, library, semantic search, database, Protégé.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-12-21>.

Вступ

Розвиток сучасних інформаційних систем, що засновані на знаннях, зумовлюють та підтримуються сучасним науково-технічним процесом. Отже, важливим чинником стає підвищення продуктивності інформаційних систем. Одним із перспективним та актуальним напрямків розв'язку цієї задачі є розробка онтологічних інформаційних систем на основі баз знань. Об'єктом дослідження є розробка онтологічної системи, що базуються на знаннях.

Актуальність

Тематика статті присвячена створенню онтологічної моделі бази знань «Бібліотека», яка є доволі актуальною на сьогоднішній день. Розроблена онтологічна модель бази знань цього напрямку має та може бути впроваджена на тематичних веб-ресурсах і значно полегшувати семантичний пошук інформації в межах предметної області. Дана тематика також чудово використовується для проведення дослідження можливостей редактору онтологій Protégé. Розробка онтологічної моделі бази знань

«Бібліотека» на базі середовища Protégé дозволяє провести дослідження можливостей редактору онтологій, зробити висновки про доцільність розширення функціональності середовища проектування або встановлення додаткових плагінів у майбутньому в разі необхідності

Мета дослідження

Метою дослідження є збільшення повноти та коректності семантичного пошуку інформації користувачами за рахунок створення нової онтологічної моделі бази знань "бібліотека" на базі середовища Protégé. Зазначена мета досягається створенням нової онтологічної моделі бази знань з виконанням таких основних завдань дослідження: дослідити предметну область для створення онтологічної моделі бази знань; створити базову графічну модель семантичної мережі; реалізувати онтологічну модель бази знань сучасними програмними засобами; провести тестування коректності пошуку інформації в реалізованій онтологічній базі знань; розглянути можливості розширення та перспективи розвитку онтологічної моделі бази знань.

Матеріали та методи дослідження. На початку розробки онтологічної моделі бази знань «Бібліотека» на базі середовища Protégé необхідно побудувати термінологічний словник для предметної області «Бібліотека». Наступним етапом створення онтологічної моделі бази знань «Бібліотека» є створення базової графічної моделі семантичної мережі у вигляді фрагменту семантичної мережі. Необхідним етапом побудови онтологічної моделі «Бібліотека» є наступний крок, а саме її реалізація засобами сучасного програмного забезпечення - засобами Protégé (вільний, відкритий редактор онтологій і фреймворк для побудови бази знань); також на цьому етапі треба зафіксувати ключові концепти і терми, закодувати їх. Завершальний етап присвячено проведенню тестування коректності пошуку інформації в реалізованій засобами Protégé онтологічній базі знань та оцінці коректності пошуку за допомогою метрики Single Usability Metrics (єдиний юзабіліті-показник, який об'єднує стандартизовані показники продуктивності, ефективності та відповідної задовільності використання в єдину оцінку).

Аналіз останніх досліджень та публікацій

Онтологія у комп'ютерній лінгвістиці визначається як «специфікація концептуалізації» (Том Грубер, 1992р.) [1, 2]. Розглядається онтологія у контексті обміну знаннями. Таким чином, можна визначити онтологію як опис (формальна специфікація програми) відносин і концепцій, які можуть існувати для агента або множини (спільноти) агентів. Таке поняття відповідає використанню онтології як набору визначень концепцій та є більш загальним. Завдання онтології полягає у забезпеченні обміну знаннями та їх повторного використання. Отже онтологія - це специфікація, яка використовується для прийняття онтологічних зобов'язань, набір визначень формальної лексики. Це не єдиний спосіб задати концептуалізацію, він має деякі позитивні властивості для обміну знаннями між програмним забезпеченням (наприклад, семантика, незалежна від читача та контексту). Практично, онтологічне зобов'язання - це угода використовувати словниковий запас (тобто ставити запити та робити твердження) у спосіб, який є послідовним (але не повним) щодо теорії онтології.

Множина формально представлених знань базується на концептуалізації: об'єкти, концепції та інші сутності, які, як передбачається, існують у певній області інтересу, і відносини, які існують між ними. Концептуалізація становить собою спрощений, абстрактний погляд на реальний об'єкт, який представляється з метою використання. Кожній системі, заснованій на знаннях, базі знань або агенту на рівні знань властива відповідна явна чи неявна концептуалізація.

Під поняттям «онтологія» розуміють явну специфікацію концептуалізації. Для систем штучного інтелекту «існує те, що можна представити». Коли знання про предметну область представлено в декларативному формалізмі, набір об'єктів, які можуть бути представлені, називається всесвітом дискурсу. Саме такий набір об'єктів і зв'язки між ними, які можна описати, відображаються в репрезентативному словнику, за допомогою якого програма, заснована на знаннях, представляє знання. Отже, у контексті штучного інтелекту можливо описати онтологію програми, визначивши набір репрезентативних термінів. У такій онтології визначення пов'язують назви сутностей у всесвіті дискурсу (наприклад, класи, відносини, функції чи інші об'єкти) із зрозумілим для людини текстом, який описує, що означають назви, та формальними аксіомами, які обмежують інтерпретацію та добре сформоване використання цих термінів. Формально онтологія - це твердження логічної теорії.[1]. Загальні онтології використовуються для опису онтологічних зобов'язань для набору агентів, щоб вони могли спілкуватися про область дискурсу, причому, не обов'язково оперуючи глобальною теорією. Якщо спостережувані дії агента узгоджуються з визначеннями в онтології, тоді агент може використовувати онтологію. Ідея онтологічних зобов'язань заснована на знаннях перспективних рівнів. Цілком слушно визначити рівень знань рівнем опису знань агента, який не залежить від представлення на рівні символів, який використовується всередині агента. Знання приписують агентам шляхом спостереження за їхніми діями; агент щось «знає», якщо він діє так, ніби володіє інформацією, і діє раціонально для досягнення своїх

цілей. Такі «дії» агентів (також сервери баз знань і системи, засновані на знаннях) можна побачити через функціональний інтерфейс «скажи та запитай», яким клієнт взаємодіє з агентом, подає запити (запитує) та формулює логічні твердження (розповідає).

Загальна онтологія визначає словниковий запас, за допомогою якого агенти обмінюються запитам та твердженнями. Онтологічні зобов'язання - це домовленості щодо використання спільного словникового запасу узгодженим і послідовним чином. Агенти, які мають спільний словниковий запас, не повинні спільно використовувати базу знань; кожен знає те, чого не знає інший, і агент, який займається онтологією, не зобов'язаний відповідати на всі запити, які можуть бути сформульовані в спільному словнику. Прихильність до загальної онтології є гарантією узгодженості, але не повноти щодо запитів і тверджень, що використовують словниковий запас, який визначений в онтології. Онтології часто ототожнюють з таксономічними ієрархіями класів, але визначенням класів і відношенням підрахунку, але онтології не обов'язково обмежуються цими формами. Онтології також не обмежуються консервативними визначеннями, тобто визначеннями в традиційному логічному розумінні, які лише вводять термінологію і не додають жодних знань про світ. Щоб визначити концептуалізацію, необхідно сформулювати аксіоми, які обмежують можливі інтерпретації визначених термінів.

Відомі такі розширені визначення онтології за Губертом: експліцитна специфікація концептуалізації, де як концептуалізація виступає опис безлічі об'єктів предметної області та зв'язків між ними; формальна специфікація концептуалізації, що розділяється, яка має місце в деякому контексті предметної області; база знань, що описує факти, які передбачаються завжди істинними в рамках певного суспільства на основі загальноприйнятого сенсу словника, що використовується; знання, формально представлені на основі концептуалізації (формально онтологія складається з термінів, організованих у таксономію, їх визначень та атрибутів, а також пов'язаних з ними аксіом та правил виведення).

Поняття онтології знань набуло важливого практичного значення останнім часом у сферах штучного інтелекту, управління знаннями та розробки складних спеціалізованих інформаційних ресурсів. Для спеціалістів з різних сфер є необхідним структурування знань у межах предметної області їх дослідження. Детальна формалізація знань має на меті побудову концептуальної схеми предметної області. Така схема будується на основі двох базових термінів, а саме набору понять та інформації про дані поняття [1,2]. Більшість сучасних автоматизованих систем успішно реалізується побудовою детальних карт набору понять. Більш складним завданням є правильна подача усієї можливої інформації про поняття. Властивості об'єктів, відношення між ними, обмеження усіх відомих видів (з урахуванням типу даних та обмежень на взаємодію певних об'єктів між собою), аксіоми – це значимі блоки інформації. Protégé – це редактор онтологій [3]. Представляє собою один із найпотужніших засобів формалізації знань, який може реалізовувати більшість взаємодій об'єктів. Крім того, Protégé є системою з можливістю розширення функціональності, що дозволяє доповнюватися та розвиватися.

Виклад основного матеріалу

Відправним кроком при створенні онтологічної моделі бази знань «Бібліотека» є побудова термінологічного словника для предметної області «Бібліотека». Терміносистема представляє собою систематизовану сукупність термінів певної предметної області, яка створюється експертами на основі теорії та має такі властивості: відкритість, системність, повнота, динамічність, несуперечливість та відносна стабільність [4]. При наявності декількох теорій в одній предметній області можуть існувати множина терміносистем. У процесі розвитку онтології необхідно розвивати кожен з них окремо, але основа повинна бути єдиною (спільною). Змістом першого кроку є створення структурованої мінімальної таблиці з основними дефініціями майбутньої онтології. Для цього необхідно врахувати основні поняття, відокремити їх від другорядних та обрати найбільш яскраві приклади певних термінів у вигляді класів і створити їх ієрархію. Ієрархія доповнюється по мірі поглиблення і розширення онтології. Базис ієрархії повинен дати достатнє уявлення про структуру предметної області користувачеві або розробнику, яким би нескінченно малим не був його набір знань у даному напрямку. Особливість обраної предметної області полягає у тому, що вона торкається як внутрішніх до країни так і зовнішніх видань, як використання у читальному залі бібліотеки так і користування абонементом.

Статус бібліотек, правові та організаційні засади діяльності бібліотек і бібліотечної справи в Україні, доступ до інформації, знань, залучення до цінностей національної та світової культури, науки та освіти, що зберігаються в бібліотеках гарантується законодавством України [5]. Стандарти з інформації, бібліографії, бібліотечної та видавничої справи відображені у відповідних документах [6].

Крім того, з урахуванням міжнародних, національних стандартів та видавничої практики можна виокремити деякі основні види видавничої продукції за такими узагальненими ознаками [7].

1. Періодичність випуску в світ тих чи інших видів видань. Одні з них виходять одноразово (книги, брошури), інші мають заздалегідь визначену кількість назв протягом певного проміжку часу — року, кварталу, місяця чи тижня (альманахи, журнали, газети).
2. Характер інформації. Йдеться про ряд ознак, за якими визначаються стилеві й лексичні особливості творення текстів залежно від функціонального призначення — наукові, офіційні, виробничі, навчальні, довідкові, літературно-художні.
3. Форма знаків, якими фіксується та передається інформація. Це можуть бути текстові (буквені), нотні чи картографічні знаки.
4. Матеріальна конструкція, або зовнішня будова видань. Скажімо, книга, брошура, журнал, газета, незважаючи на свої, відмінні від інших, розміри, обсяги, мають немало спільних ознак у побудові: відповідно задруковані і скріплені або вставлені у певному порядку шпальти, які можна гортати, складати, певні захисні чи розпізнавальні елементи цих шпальт тощо. Зовсім інша конструкція в електронного видання, де інформація фіксується на електронних носіях.
5. Мовна ознака. Видання може бути оригінальним, випущеним державною або іншою мовою; у перекладі з будь-якої іноземної мови; з паралельним текстом двома або кількома мовами.
6. Повторність випуску. За цими ознаками можна визначити видання, які випускаються вперше, або різні варіанти перевидань (доповнених, виправлених і перероблених тощо).
7. Формат. Важливо розрізнити малоформатні, мініатюрні видання стандартних форматів. Кількість сторінок нерідко є принциповою у віднесенні того чи іншого видання до певного виду. Так, видання обсягом від 1 до 4 сторінок — це листівка, обсягом від 4 до 48 сторінок — брошура, а обсягом понад 48 сторінок — книга.

У таблиці 1 надано базовий набір знань та уявлень для подальшого розуміння предметної області «Бібліотека».

Важливим наступним кроком створення онтологічної системи «Бібліотека» є створення базової графічної моделі семантичної мережі. Розглянемо цей крок створення на фрагменті семантичної мережі. Після виявлення ключових концептів доцільним є побудувати ієрархії предметної області, в корені якої буде знаходитись терміносистема, а у вузлах – номенклатура. За модель представлення знань номенклатури використовуємо семантичну мережу знаків-фреймів.

Семантичну мережу побудуємо з використанням об'єднання знаків-фреймів Φ_i (1):

$$S = U_i \Phi_j, \quad (1)$$

де S - семантична мережа.

Вважаємо, що загалом сформовано множину термінів $Term$. Також вважаємо, що потужність множини $\Phi = \{\Phi_j\}$ більша потужності множини $Term$. На рисунку 1 надане графічне зображення фрагменту семантичної мережі S для побудови онтології «Бібліотека». У семантичній мережі дугам відповідає значення «це-є» («is-a»).

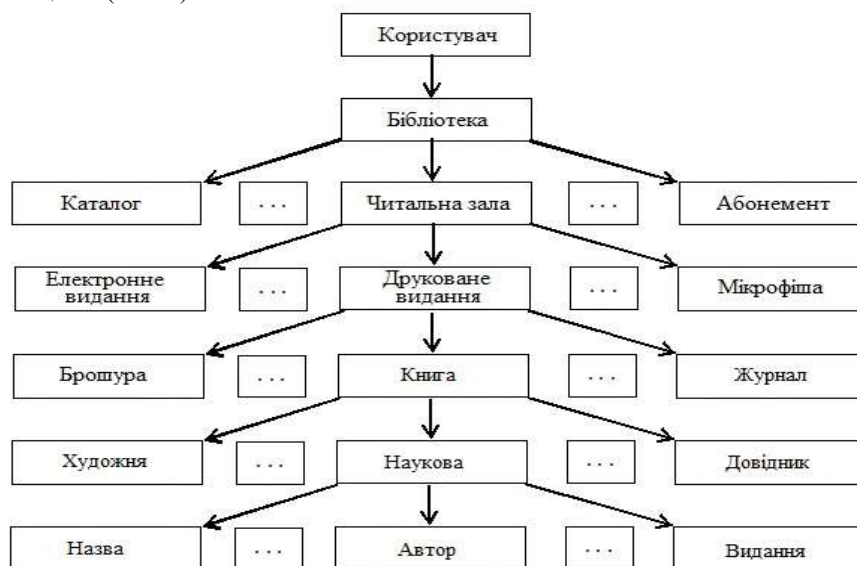


Рисунок 1- Фрагмент семантичної мережі для побудови онтології «Бібліотека»

Наступним кроком проведемо кодування базису онтології «Бібліотека». Починати треба із налаштування ієрархії класів та підкласів, потім надати їм властивості відношень та властивості даних

(визначити усі необхідні типи даних зі списку, а також за потреби створити нові), потім переходимо до створення окремих індивідів у межах кожного класу.

Таблиця 1 - Мінімальний термінологічний словник для уявлення про наповнення онтології «Бібліотека»

Термін	Дефініція	Приклади властивостей відношення	Приклади властивостей даних	Тип даних	Приклади індивідів
Користувач бібліотеки	тематика ресурсу або необхідної інформації	визначає, отримує, користується, надає, платить, повертає	ім'я (прізвище, по батькові), вік, паспорт (номер, серія), пільги	String (можливо Real)	гість, звичайний користувач, науковець, студент
Працівник бібліотеки	визначає та забезпечує доступ до наявних ресурсів бібліотеки	надає читальний зал до кінця дня, надає доступ до використання комп'ютера	посада, повноваження, пріоритет доступу	String	асистент, бібліотекар, оператор, керівник секції
Ресурс бібліотеки	тематика, область знань, спеціалізація, носій ресурсу, місце публікації, автор	мати відповідну тематику або їх набір, мати місце видання, мати основи для формування особливостей та зручностей користування	періодичність випуску в світ тих чи інших видів видань; характер інформації; форма знаків, якими фіксується та передається інформація; матеріальна конструкція, або зовнішня будова видань; мовна ознака; повторність випуску; формат.	String	газета, журнал, книга, діафільм, диск, комп'ютер, флешносій
Сервіс бібліотеки	обирається вперше, повторно, постійно	мати властивість бути невідомим, мати властивість бути відомим, мати властивість бути широковідомим	не обирати, можливо обрати, обрати ресурс	String (можливо Boolean)	консультація, алфавітний показчик, предметний показчик, читальна зала, використання ресурсів
Тематика ресурсу (бібліотеки)	відношення до різних галузей знання, мистецтва тощо	мати відповідний рейтинг серед групи користувачів	не цікаво, цікаво	String	художня, наукова, науково-популярна, образотворча, музична, комбінована
Популярність ресурсу	як часто такими ресурсами цікавляться та користуються	мати відповідний рейтинг серед користувачів	не цікаво, цікаво	Boolean (можливо String)	видання «мертвою» мовою, видання з великою кількістю неточностей та помилок
Вік користувача	фізичний вік користувача бібліотекою	мати відповідну кількість років за віком	немовля (з дорослим), діти, підлітки, середній вік, зрілий вік	integer (можливо Real, String)	до 10 років, 10-20 років, 20-40 років, більше 40 років, конкретне значення віку

Продовження таблиці 1

Спеціалізація ресурсу	додатковий час на підготовку користувача (може бути пов'язаним із фізичною, психологічною та інтелектуальною підготовками користувача, оволодінням ним специфічними навичками та знаннями)	мати спеціальну підготовку за окремими видами інформаційних технологій, мати спеціальну підготовку за декількома мовами спілкування, мати підготовку на рівні початківця у галузях знань, мати наукову ступінь, мати відповідну кваліфікацію за областями знань	користувач спроможний, неспроможний до користування ресурсом бібліотеки	String (можливо Boolean)	школярі, абітурієнти, студенти, викладачі, науковці
Спеціальне обладнання для використання ресурсу	обладнання, спорядження	мати специфічні параметри для виконання особливих дій	засоби зчитування інформації	String (можливо Boolean)	комп'ютер, офісне обладнання, зчитувач діафільмів
Об'єми матеріалу ресурсу	параметри ресурсу, які визначають можливість або зручність користувачеві узяти із собою до читального залу чи на винос (у фізичних параметрах, параметрах об'єму для електронних носіїв)	мати фізичні розміри та параметри, мати кількість обумовлених екземплярів	великий дозволений розмір або вага, недостатній об'єм носіїв	integer (можливо Real)	один чи декілька екземплярів носія, об'єм у розмірах пам'яті електронних носіїв, вага у 10 кг
Строки використання ресурсом	часові параметри використання ресурсу	мати обмежені часові рамки	достатній час, лімітований час, можливий часовий діапазон, частина доби для використання	integer (можливо Real)	хвилини, години, тиждень, 12 діб, місяць, рік або з початкової дати до наступної дати за календарем
Вартість використання ресурсу	орієнтовна чи точна вартість, безоплатно	мати обмежені вартісні рамки	дешево, дорого	Real	100 умовних грошових одиниць за певний строк, 100 умовних грошових одиниць за день використання
Способи оплати за використання ресурсу	повна, по частинам, часткова оплата, пільги, знижки, безоплатно	мати прийнятні для користувача умови оплати	накопичувальна система знижок та пільг, знижка для постійних клієнтів	String (можливо Boolean)	оплата карткою, оплата кешем,

Надалі проведемо *побудову онтологічної моделі бази знань «Бібліотека» засобами Protégé*. Під час розробки онтології «Бібліотека» необхідно врахувати реалізацію пошуку індивідів за певними критеріями. Для цього зручно використовувати Class Expression Editor, як інструмент для написання виразів у межах певного класу.

Protégé має потужний засіб для створення запитів на пошук інформації, а саме - вбудований конструктор мови запитів SPARQL [8]. Основними видами таких запитів є: SELECT, CONSTRUCT, ASK, та DESCRIBE. SELECT запит – це найбільш поширений із даних різновидів запитів. Результати виведення запиту подаються у зручному для користувача табличному вигляді. є однією з ознак правильності побудови онтології. Однією із ознак правильності побудови онтології є коректність

виведення запитів. Інструмент Ontograf у Protégé дає можливість вивести онтологію у найбільш зрозумілому, наочному та простому вигляді графічного відображення семантику предметної області.

Побудовано онтологічну модель «Бібліотека» у середовищі Protégé. Модель включає 10 класів і підкласів. Для кожного класу і підкласу визначено 2 властивості-відносини та від 2-х до 10-и властивостей-даних. Приклад класів онтологічної моделі «Бібліотека» приведено на рисунку 2. Приклад «властивості-відносини» онтологічної моделі «Бібліотека» приведено на рисунку 3. Приклад «властивості-дані» онтологічної моделі «Бібліотека» приведено на рисунку 4. Детальний граф онтологічної моделі «Бібліотека» приведено на рисунку 5.

Оцінювання коректності семантичного пошуку інформації в онтологічній базі знань «Бібліотека». Існує визначення оцінки онтології у контексті технологій сумісного використання знань [9], згідно якого критеріями можуть виступати вимоги до специфікації, питання компетенції, і / або реальний світ. За для більш повного охоплення оцінки онтології обрано метрику Single Usability Metrics (SUM) [10] (2):

$$S = \frac{SM_{completion} + SM_{satisfaction} + SM_{times} + SM_{errors}}{4}, \quad (2)$$

де *Completion* - булеве значення і позначає досягнення мети здобуття інформації користувачем, *Satisfaction* - рівень задоволення від структуризації інформації у даній онтології, *Errors* - показує виникнення певних суперечливостей або інших помилок при отриманні інформації, *Times* - показує середню кількість запитів для отримання тієї чи іншої інформації. Для визначення коректності пошуку інформації онтологічна база знань була надана 10 користувачам, кожен з яких реалізував 10 запитів у реалізованій онтологічній базі знань. У таблиці 2 наведено результати опитування за даною метрикою.

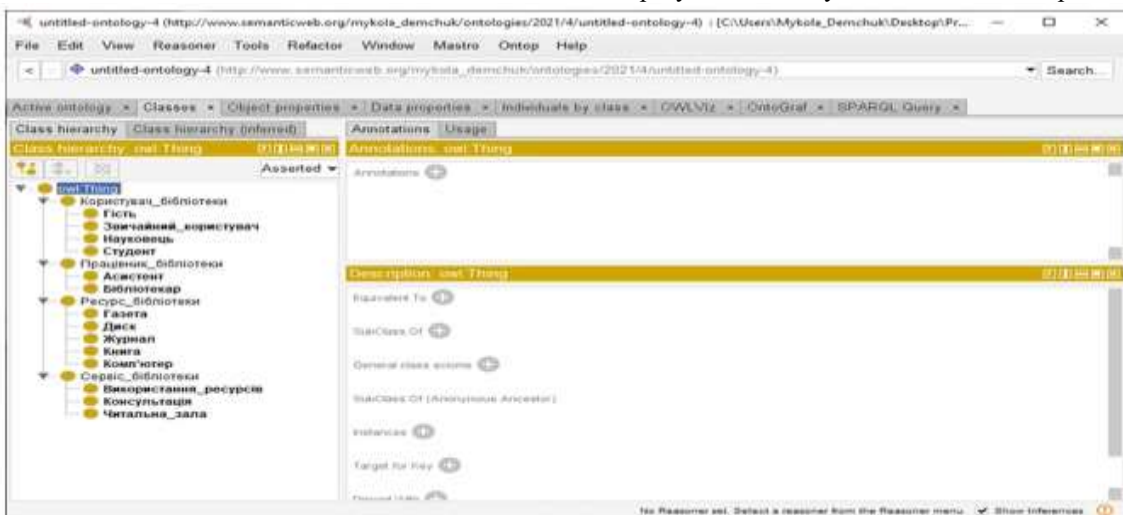


Рисунок 2 - Класи онтологічної моделі «Бібліотека»

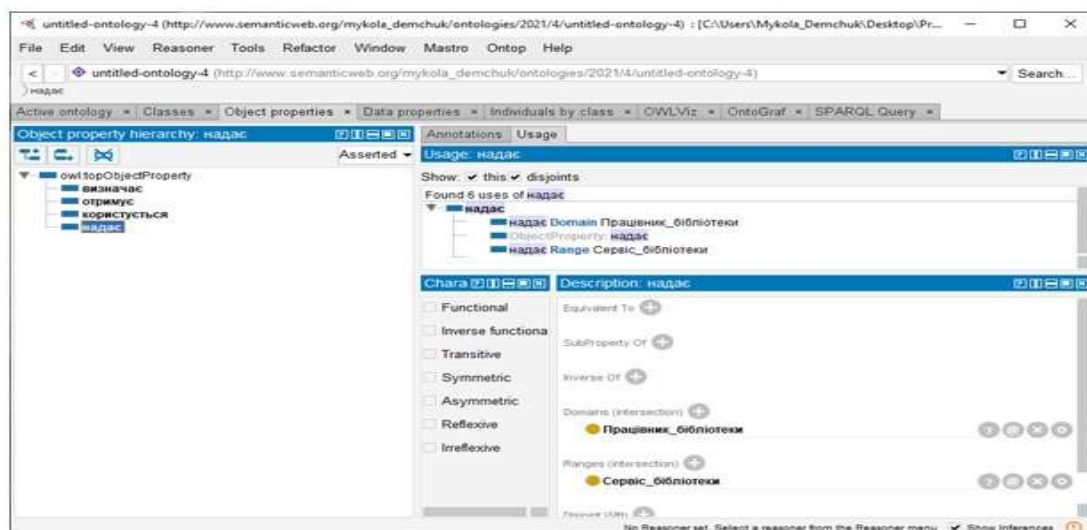


Рисунок 3 - Властивості-відносини онтологічної моделі «Бібліотека»

Середній показник (Average) по всім користувачам, визначений за метрикою SUM, дорівнює значенню 83,25%. Таке значення становить прийнятний показник для онтологічної бази знань. Якщо реалізувати класичну реляційну модель організації баз даних для реалізації бази даних «Бібліотека», середній показник за метрикою SUM по 10 користувачам дорівнює значенню 75,26%.

Обговорення результатів дослідження. Для прикладу розробки онтологічної моделі бази знань «Бібліотека» на базі середовища Protégé, у отриманій онтологічній моделі «Бібліотека» було визначено для кожного класу 2-5 індивідів, для кожного індивіда задано 2-5 властивості-відносини/властивості-данні.

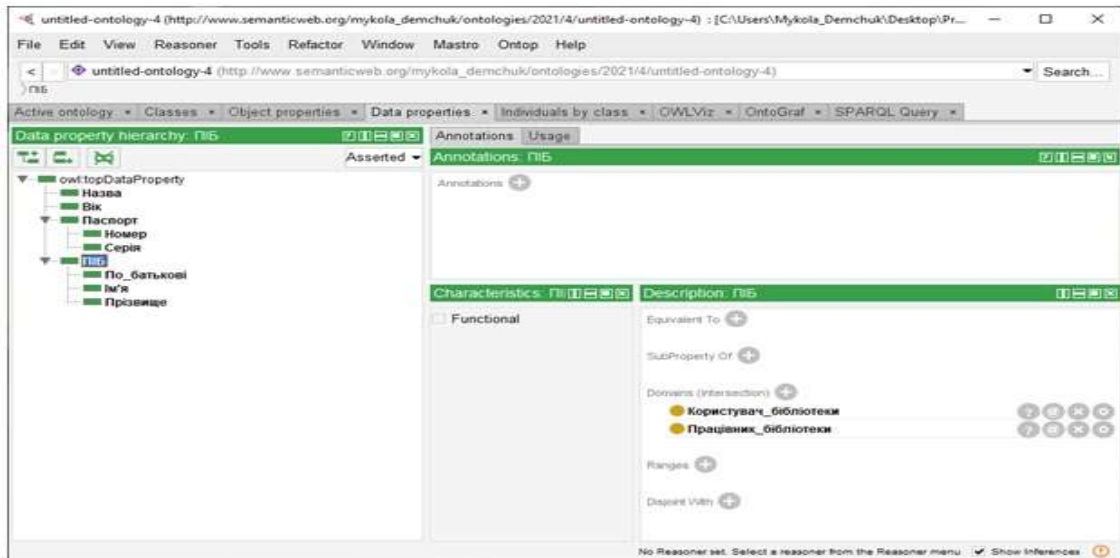


Рисунок 4 - Приклад «властивості-дані» онтологічної моделі «Бібліотека»

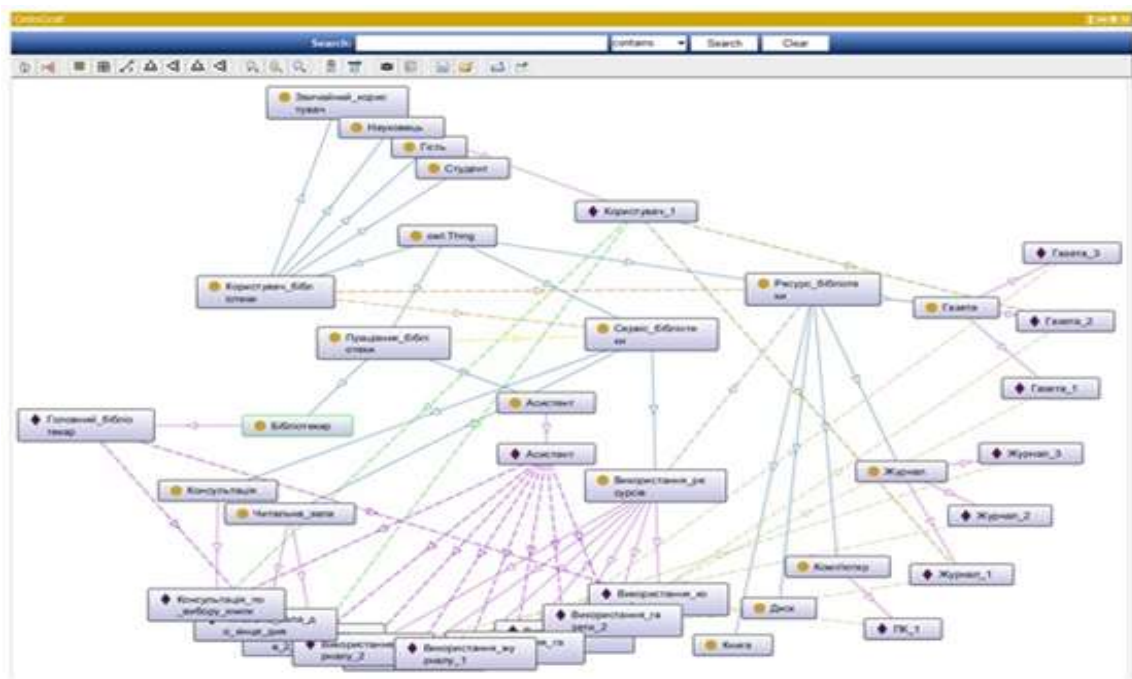


Рисунок 5 - Детальний граф онтологічної моделі «Бібліотека»

Створено 7 SPARQL-запитів та проведено тестування онтологічної моделі в Protégé за допомогою SPARQL-запитів. Наукова новизна отриманих результатів дослідження полягає у тому, що вперше розроблено онтологічну модель бази знань «Бібліотека»; розроблена онтологія предметної області «Бібліотека», яка реалізована у вигляді бази знань; отримано прийнятний результат тестування реалізованої бази знань та виконана метрична оцінка коректності семантичного пошуку. Практична

значущість результатів дослідження підтверджена більшою прийнятністю запропонованої онтологічної моделі у порівнянні з традиційною. Для перспективних досліджень є цікавим та новим розглянути інші сфери використання онтологій для збільшення достовірності та прийнятності моделей баз знань.

Таблиця 2 - Результати опитування щодо коректності розробленої онтології «Бібліотека»

User	Completion	Satisfaction	Times	Errors	Average
1	0	4	4	2	68,25%
2	1	5	4	2	79,25%
3	1	4	3	0	93,25%
4	1	5	3	0	87,50%
5	1	5	4	0	96,25%
6	1	5	11	1	70,25%
7	1	5	5	0	90,25%
8	1	5	3	0	100,00%
9	0	4	7	2	63,25%
10	1	5	4	0	84,25%

Висновки

Досягнута мета дослідження, підвищення коректності семантичного пошуку інформації, за рахунок застосування в реалізації бази знань нової онтологічної моделі «Бібліотека». У порівнянні з реляційною моделлю організації баз даних використання нової онтології дозволяє підняти коректність пошуку на 8%.

Список літератури

1. Gruber T. R. (1993). A translation approach to portable ontologies. Knowledge Acquisition. № 5(2). 199-220. <https://doi.org/10.1006/knac.1993.1008>
2. Tom Gruber. (2008). Ontology. Entry in the Encyclopedia of Database Systems. Springer-Verlag. <https://tomgruber.org/writing/definition-of-ontology>
3. Protégé. <https://protege.stanford.edu/>
4. Pryntsyryu pobudovy bankiv danykh. https://web.posibnyky.vntu.edu.ua/fitki/10savchuk_organizaciya_bazdanih_znan/gl_14.html.
5. Закон України «Про бібліотеки і бібліотечну справу». <http://ru.osvita.ua/legislation/law/3198/>
6. Стандарти з інформації, бібліографії, бібліотечної та видавничої справи. <http://www.library.univ.kiev.ua/ukr/about/dstu.html>
7. Видавнича продукція. https://uk.wikipedia.org/wiki/Видавнича_продукція.
8. SPARQL Query Language for RDF. <https://www.w3.org/TR/rdf-sparql-query/>
9. Gomez-Perez, N. Juristo, J. Pazos. (1995). Evaluation and assessment of knowledge sharing technology. Towards Very Large Knowledge Bases. 289- 296.
10. Raschet SUM. Podkhod ot Dzhefa Soro. <https://v-shliachkov.medium.com/расчет-сум-подход-от-джефа-соро-c1ecf796f1b2>

Стаття надійшла: 10.09.2023 р.

References

1. Gruber T. R. (1993). A translation approach to portable ontologies. Knowledge Acquisition. № 5(2). 199-220. <https://doi.org/10.1006/knac.1993.1008>
2. Tom Gruber. (2008). Ontology. Entry in the Encyclopedia of Database Systems. Springer-Verlag. <https://tomgruber.org/writing/definition-of-ontology>
3. Protégé. <https://protege.stanford.edu/>
4. Pryntsyryu pobudovy bankiv danykh. https://web.posibnyky.vntu.edu.ua/fitki/10savchuk_organizaciya_bazdanih_znan/gl_14.html.
5. The Law of Ukraine "On Libraries and Library Matters". <http://ru.osvita.ua/legislation/law/3198/>
6. Information, bibliography, library and publishing standards. <http://www.library.univ.kiev.ua/ukr/about/dstu.html>
7. Publishing products. https://uk.wikipedia.org/wiki/Publishing_products.
8. SPARQL Query Language for RDF. <https://www.w3.org/TR/rdf-sparql-query/>
9. Gomez-Perez, N. Juristo, J. Pazos. (1995). Evaluation and assessment of knowledge sharing technology. Towards Very Large Knowledge Bases. 289- 296.

10. Raschet SUM. Podkhod ot Dzhefa Soro. <https://v-shliachkov.medium.com/расчет-sum-подход-от-джефа-соро-c1ecf796f1b2>

Відомості про авторів

Сілагін Олексій Віталійович - к.т.н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця, Україна

Silagin Olexiy Vitaliyovich - Ph.D., associate professor of the Department of Computer Sciences, Vinnytsia National Technical University, Vinnytsia, Ukraine

Сілагін Єгор Олексійович - асистент кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця, Україна

Silagin Yehor Olexiyovych - assistant of the Department of Computer Sciences, Vinnytsia National Technical University, Vinnytsia, Ukraine

Денисюк Валерій Олександрович - к.т.н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, Вінниця, Україна

Denysiuk Valerii Olexandrovich - Ph.D., associate professor of the Department of Computer Sciences, Vinnytsia National Technical University, Vinnytsia, Ukraine

Денисюк Алла Василівна - асистент кафедри програмного забезпечення, Вінницький національний технічний університет, Вінниця, Україна

Denysiuk Alla Vasylivna - assistant of the Department of Software, Vinnytsia National Technical University, Vinnytsia, Ukraine

Silagin O. V., Y. Silagin, V. Denysiuk, A. Denysiuk

DEVELOPMENT OF THE ONTOLOGICAL MODEL OF THE KNOWLEDGE BASE "LIBRARY" BASED ON THE PROTÉGÉ ENVIRONMENT

Vinnytsia National Technical University, Vinnytsia, Ukraine

УДК 004.7

Л.А. Савицька¹, Т.І. Коробейнікова², О.П. Волос¹, М. Г. Тарновський¹

МЕТОД ТА ЗАСІБ МОНІТОРИНГУ БЕЗПЕКИ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ЗАСОБАМИ SIEM

¹Вінницький національний технічний університет, Вінниця²Національний університет «Львівська політехніка»

Анотація. Дана робота присвячена дослідженню, аналізу та вдосконаленню методів та засобів моніторингу безпеки в комп'ютерних мережах. У цій роботі засоби і методи моніторингу безпеки мережі розробляються на основі агентів системи SIEM (система управління інформацією про моніторинг мережі) з удосконаленням процесу нормування даних від журналів безпеки. Причому, для прискорення процесів реагування на загрози мережевої безпеки комп'ютерної мережі досліджується робота SIEM з точки зору триади SIEM-EDR-NDR. Дослідження ґрунтуються на досвіді роботи іноземних компаній та вітчизняних банківських мереж.

У дослідженні розглядається взаємодія компонентів SIEM-EDR-NDR, утворюючи SOC-тріаду. SIEM використовується для централізованого аналізу даних, включаючи EDR і NDR, надаючи повну картину безпеки. EDR виявляє та реагує на загрози на кінцевих точках, а NDR доповнює його, розширюючи аналіз SIEM. Така комбінація забезпечує ефективне реагування на кібератаки, зменшуючи "час перебування" до виявлення.

Розглянуто формування завдань компонентів EDR у триаді SIEM-EDR-NDR. Звернуто увагу на важливість захисту кінцевих пристроїв від всіх етапів атаки та визначено ефективні стратегії, такі як аналіз трафіку, контроль додатків та централізоване управління кібербезпекою. Наголошено на інтеграції EDR з існуючими засобами безпеки для створення комплексної системи.

У контексті SIEM висвітлено етапи обробки даних, починаючи від збору журналів і нормалізації до класифікації подій і кореляції. Підкреслено роль кореляції у формуванні інцидентів та проведенні розслідувань. Запропоновано удосконалену схему нормалізації з розширеною розгорткою агентів та ключовими етапами обробки даних в межах SIEM-системи.

Робота розглядає вдосконалення обробки журналів подій у SIEM для ефективного моніторингу мережевої безпеки та оперативного усунення загроз. Досягнута мета сприяє прискоренню процесів реагування на загрози завдяки інтеграції агентів SIEM в середовище, що дозволяє упорядковувати та класифікувати потоки інформації для оперативного усунення загроз.

Ключові слова: моніторинг, SIEM, EDR, NDR, триаді SIEM-EDR-NDR, процес нормалізації журналів.

Abstract. This work focuses on researching, analyzing, and enhancing methods and tools for security monitoring in computer networks. The study develops security monitoring tools and methods based on SIEM agents, improving the data normalization process from security logs. The research explores SIEM's role in the SIEM-EDR-NDR triad perspective to accelerate responses to network security threats. The investigation is grounded in the experiences of foreign companies and domestic banking networks.

The interaction of SIEM-EDR-NDR components, forming a SOC triad, is examined. SIEM is utilized for centralized data analysis, including EDR and NDR, providing a comprehensive security overview. EDR detects and responds to threats on endpoints, complemented by NDR, extending SIEM analysis. This combination ensures effective response to cyberattacks, reducing "dwell time" until detection.

The formulation of tasks for EDR components in the SIEM-EDR-NDR triad is discussed. Emphasis is placed on the importance of protecting endpoints at all stages of an attack, and effective strategies, such as traffic analysis, application control, and centralized cybersecurity management, are identified. Integration of EDR with existing security tools to create a comprehensive system is highlighted.

Within the SIEM context, data processing stages, from log collection and normalization to event classification and correlation, are illuminated. The role of correlation in incident formation and investigation is underscored. An enhanced normalization scheme with an expanded agent deployment and key data processing stages within the SIEM system is proposed.

The work addresses the improvement of event log processing in SIEM for effective network security monitoring and timely threat mitigation. The achieved goal accelerates threat response processes through SIEM agent integration, facilitating the organization and classification of information flows for prompt threat mitigation.

Key words: testing, monitoring, SIEM, EDR, NDR, SIEM-EDR-NDR triad, log normalization process.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-22-32>.

Вступ

Питання моніторингу безпеки в комп'ютерній мережі (КМ) стає все більш актуальним і важливим у всьому світі. Протягом лише 2021 року світова економіка зазнала значних втрат через кібератаки на загальну суму 6 трлн. доларів [1]. Україна не вийшла з-під цієї загрози, ба навіть зазнала її ще більше. За даними аналізу, проведеного компанією Microsoft у 2021 році, майже 20% світових кібератак спрямовані на Україну, що робить нашу країну другою за кількістю кібератак у світі, випереджаючи багатонаціональні корпорації [2]. Це великий виклик, оскільки з 2014 року Україна веде гібридну війну, включаючи і кібернетичний фронт.

З початком відкритої війни росії проти України в лютому 2022 року атаки ще більш загострилися. Лише впродовж перших 400 днів війни на Україну було скоєно понад 3000 потужних кібератак: DDoS атаки, атаки шкідливим програмним забезпеченням (ПЗ), ботнети, фішингові розсилки тощо [3].

Ураховуючи значні втрати моніторинг безпеки в КМ є одним із головних пріоритетів у системі національної безпеки. Отже, для відповіді на ці зростаючі загрози Україна вживає такі контрзаходи:

1) Працює Національний координаційний центр з безпеки [4], який курує заходи щодо кібербезпеки на національному рівні.

2) Працюють державний центр CERT-UA (Computer Emergency Response Team) та регіональні центри CSIRT (Computer Security Incident Response Team), які відповідають за забезпечення захисту інформації та комп'ютерних мереж від несанкціонованих доступів та кібератак [5].

3) Активно ведуть дії кібервійська [6], яка містять спецпідрозділи і фахівців для ведення операцій з кібербезпеки.

4) З метою нормативно-правового регулювання, у 2021 році прийнята нова Стратегія кібербезпеки України, яка має на меті створення безпечного кіберпростору та забезпечення безпеки в цьому важливому сегменті [7].

Актуальність

Всі ці заходи мають на меті забезпечити постійний моніторинг безпеки в КМ, аналіз вторгнень у мережу та виявлення атак в режимі real_time. Враховуючи нові виклики, що виникають у зв'язку з повною цифровою трансформацією країни, створюються можливості для досягнення цих завдань:

1) Розвиток новітніх організаційно-технічних моделей, що сприяють ефективному захисту комп'ютерних мереж та даних.

2) Впровадження інноваційних інструментів для оперативного виявлення та запобігання атак, і це допомагає реагувати на загрози вчасно та ефективно.

3) Підтримка досліджень і розробок у галузі кібербезпеки, спрямованих на розвиток новітніх ІТ-технологій та штучного інтелекту (ШІ).

Отже, тематика дослідження є актуальною, водночас існує реальна потреба у подальшому вдосконаленні методів і засобів для постійного і надійного моніторингу безпеки в комп'ютерних мережах.

Мета

Метою статті є прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовище. Запропонований підхід має потенціал упорядковувати і систематизувати хаотичні та розкидані дані про події у комп'ютерній мережі. Це дозволить конвертувати цю інформацію в зручний та легко зрозумілий формат, представленням у вигляді діаграм і графіків. Такий підхід сприяє оперативному виявленню можливих загроз та надає адміністраторам системи інструменти для їх швидкого усунення.

Задачі

1. дослідити новітній підхід щодо моніторингу безпеки в комп'ютерних мережах, зокрема, в парадигмі тріади SIEM-EDR-NDR;
2. дослідити новітній підхід щодо розробки неперервного ефективного моніторингу безпеки в комп'ютерних мережах у центрах SOC;
3. запропонувати альтернативний процесу обробки журналів подій.

Моніторинг безпеки в комп'ютерних мережах

Відповідно до стандарту ISO/IEC 27005 [8-9], рекомендується виконувати підготовку моніторингу безпеки в КМ за таким планом (рис. 1).



Рисунок 1 – Узагальнений план моніторингу безпеки в КМ

Дослідження потенційних загроз, дослідження можливих вразливостей активів та формування політик безпеки – це ті пункти плану, що становлять інтерес дослідження і де присутній моніторинг безпеки в КМ. За визначенням, активами вважаються всі ресурси, які мають цінність для компанії і вимагають захисту [9] (рис. 2). Серед таких активів можна відзначити: приміщення, в якому розміщена КМ; інформація, яку тут обробляють і зберігають; засоби комп'ютерних мереж: програмне, технічне обладнання (сервери, мережеві та кінцеві пристрої, засоби зв'язку і т. д.) [10].

Усі ці активи повинні бути ідентифіковані і обліковані. Фахівці проводять експертну оцінку відносної цінності цих активів (низька, середня, висока) з урахуванням можливих втрат або пошкоджень. На рисунку 2 показана схема дослідження активів під час моніторингу безпеки в інформаційній КМ.



Рисунок 2 – Узагальнена схема дослідження активів під час моніторингу безпеки в КМ

Кіберзагроза є потенційно небезпечним явищем чи фактором, що становить ризик для активів мережі та загалом для інформаційної безпеки (ІБ) компанії [9-14]. ІБ містить заходи, спрямовані на забезпечення захищеності від потенційних загроз. Загроза може завдати шкоди активам. Важливо ідентифікувати і випадкові, і навмисні загрози та визначити їх джерела. Типові загрози ІБ можуть бути класифіковані за різними ознаками: за аспектом, який вони спрямовані порушити; за місцем походження загроз; за рівнем впливу на КМ; за природою виникнення. За відношенням до аспектів, який можна порушити, загрози такі: загрози конфіденційності, цілісності, доступності. За локалізацією джерела загроз, їх можна поділити на: внутрішні та зовнішні. За розмірами завданої шкоди, загрози поділяються на: загальні, локальні загрози та приватні загрози. За ступенем впливу на КМ, загрози поділяються на: пасивні загрози та активні загрози. За природою виникнення загрози, загрози можна розмежувати на природні (об'єктивні) та штучні (суб'єктивні) загрози. Джерелами загроз можуть бути суб'єкти (особи), об'єктивні прояви (конкуренти або злочинці).

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В ПРОЦЕСАХ МОНІТОРИНГУ КМ

ЗА АСПЕКТОМ	ЗА РОЗМІЩЕННЯМ ДЖЕРЕЛА ЗАГРОЗ	ЗА СТУПЕНЕМ ВПЛИВУ НА КМ	ЗА ПРИРОДОЮ ВИНИКНЕННЯ
Загроза конфіденційності	Внутрішні	Активні	Природні (об'єктивні)
Загроза цілісності	Зовнішні	Пасивні	Штучні (суб'єктивні)
Загроза доступності	За розміром шкоди, що завдається		
	Загальні		
	Локальні		
	Приватні		

Рисунок 3 – Схема загальної класифікації загроз під час моніторингу КМ

Джерела загроз призначені для отримання доступу до даних, їх модифікації і завдання прямої матеріальної шкоди. Необхідно позначити кожний актив у відповідності до видів загроз. Результатом аналітичної обробки цієї інформації є схема загальної класифікації загроз під час моніторингу інформаційної КМ (див. рис. 3).

Дослідження вразливостей активів є важливою частиною процесу моніторингу безпеки КМ. Уразливість в цьому контексті означає недолік або слабкість в активі або засобах захисту, яка може бути використана загрозами [112]. Різноманітність вразливостей покладає особливі вимоги на системи моніторингу безпеки в КМ. Поняття політики безпеки є ключовим в під час моніторингу безпеки КМ.

Після аналізу активів, потенційних загроз і вразливостей активів, формулюються політики інформаційної безпеки (ІБ).

Згідно зі стандартом ISO/IEC 27002 [5], політика ІБ є комплексом нормативних, організаційних та експлуатаційних документів, які охоплюють всі аспекти організації, керування та контролю ІБ та експлуатації засобів захисту. Отже, основною метою забезпечення ІБ є захист інформації від випадкових або навмисних втручань. Водночас ІБ також спрямована на забезпечення неперервності бізнес-процесів.

В таблиці 1 наведено принципи побудови системи ІБ.

Таблиця 1.1 – Принципи побудови системи інформаційної безпеки

Генеральний підхід	СЗ інформації повинна бути комплексною, охоплювати організаційні заходи, технічні та програмні засоби.
Системний підхід	Всі заходи і засоби захисту повинні бути пов'язані, узгоджені і забезпечувати цілісність системи.
Структурна ієрархія	Згідно із завданням тут повинен бути реалізований принцип поглибленого багаторівневого захисту.
Усеосяжність	Система захисту повинна охоплювати всі активи, всі вузли та кінцеві пристрої КМ, у тому числі BYOD.
Забезпечення надійності	Повинні бути створені такі механізми захисту, щоб вартість зламу її була дорожчою за інформацію, яку зловмисник прагне поцупити.
Контроль на всіх рівнях	Контроль повноважень будь-якого звернення до інформації повинен охоплювати всі рівні контролю: інформацію, ПЗ, апаратуру, персонал.
Цикл «PDCA» Демінга	Цикл моделі «PDCA» передбачає обов'язкові етапи: 1) Встановлення цілей та політик СЗ (Plan); 2) Реалізацію і впровадження СЗ (Do); 3) Оцінку, контроль, моніторинг і аналіз (Check); 4) Покращення (удосконалення і розвиток) СЗ (Act).

У таблиці 1 вказані основні загальноприйняті принципи побудови системи ІБ та використані такі скорочення: СЗ – система захисту; BYOD – Bring Your Own Device, особисті мобільні пристрої, яким дозволений доступ до КМ; PDCA – Plan-Do-Check-Act, модель безперервного поліпшення процесів.

Для виконання політик інформаційної безпеки на підприємстві реалізується відповідна низка заходів. Ці заходи включають в себе розробку і впровадження правил і процедур для забезпечення конфіденційності, цілісності і доступності інформації, встановлення відповідних технічних засобів захисту, навчання персоналу з питань інформаційної безпеки, а також постійний моніторинг і аналіз з метою виявлення і вирішення потенційних загроз

Моніторинг безпеки в комп'ютерних мережах в парадигмі тріади SIEM-EDR-NDR

Компоненти SIEM-EDR-NDR взаємодіють та вирішують завдання спільно, формуючи єдиний функціональний блок (SOC-тріаду) [15-19]. SIEM створює централізоване інформаційне вікно для аналітиків, щоб корелювати зібрані дані в середовищі, в т.ч. від EDR і NDR, та дозволяє командам забезпечення безпеки відокремлювати системні попередження та проводити аналіз потенційних загроз. SIEM забезпечує всебічний погляд на безпеку і використовує механізми з різних джерел, включаючи кінцеві точки, спеціальні програми, хмарні служби та інші джерела даних. Ці журнали збираються у різних форматах і піддаються аналізу для забезпечення їх кореляції та ефективного аналізу, що вказує на покращені можливості раннього виявлення і, отже, на досягнення головної мети SIEM – скорочення «часу перебування» до моменту виявлення.

EDR надає інформацію про зловмисну активність на кінцевих точках організації в рамках SOC-тріади. Виявляє, реагує на різні типи зловмисного ПЗ, а також забезпечує докладний огляд та повну видимість пристроїв у мережі. Можливості NDR доповнюють засоби EDR, усуваючи прогалини агентів EDR, і розширюють аналіз журналу SIEM, асоціюючи виявлені загрози з мережевою активністю та надаючи їм необхідний контекст.

Отже, комбінація цих рішень у складі SOC-тріади забезпечує неперевершену видимість та автоматичність реагування в умовах кібератаки.



Рисунок 4 – SOC-тріада

Тобто разом всі ці рішення, які схематично зображенні на рис. 4, забезпечують повну видимість та безпеку системи.

Новітній підхід щодо розробки неперервного ефективного моніторингу безпеки в комп'ютерних мережах у центрах SOC

Формування задач складових EDR у тріаді SIEM-EDR-NDR. Кожен кінцевий пристрій, який підключений до мережі, є «входом» до конфіденційної інформації. Тому важливо враховувати основні принципи розробки ефективної стратегії кіберзахисту кінцевих пристроїв у мережі:

Захист повинен виявляти і ліквідувати всі етапи атаки. А саме, ефективний захист від вторгнень містить: засоби перевірки поштових додатків (електронна пошта залишається основним «засобом поширення зловмисних кодів» на пристроях користувачів); засоби захисту від завантаження небажаних. Тут працює технологія, яка аналізує весь вхідний та вихідний трафік і надає захист браузера, щоб блокувати такі загрози перед їх запуском на кінцевому пристрої; потужний захист самого кінцевого пристрою, із службами контролю та додатків, а також сам пристрій.

Механізм реагування та розслідування інцидентів має демонструвати конкретні результати, має мати можливість ізолювати кінцевий пристрій для ефективного вивчення інциденту, зупинити поширення вірусів та відновлювати пристрій за допомогою його незараженої копії.

Система не повинна впливати на бізнес-процеси, тобто заходи безпеки не повинні заважати нормальному функціонуванню бізнес-процесів та швидкому обміну даними в мережі.

Централізоване управління кібербезпекою. Отже, політики адміністрування та сам протокол безпеки повинні включати заходи забезпечення безпеки всіх компонентів мережі підприємства, об'єднуючи всі кінцеві пристрої (BYOD). Кожен такий пристрій повинен відповідати вимогам доступу до мережі, що передбачає автоматизацію їхнього кіберзахисту.

Загалом, для дотримання політик безпеки кінцевих пристроїв урахувавши зростання загроз, необхідно застосовувати: мережеві екрани для різних типів пристроїв; антивіруси для електронної пошти; моніторинг, фільтрацію та захист web-трафіку; управління безпекою та захисні рішення для MDM; контроль роботи додатків; шифрування; виявлення вторгнень.

EDR є інтегрованою системою безпеки кінцевої точки, об'єднує постійний моніторинг у реальному часі та збір даних із функціями автоматизованого реагування та аналізу на основі правил. Важливо відзначити, що EDR доповнюють, а не замінюють попередні засоби безпеки, інтегруються з ними для створення більш ефективної та комплексної системи захисту.

Інструментарій EDR складається із трьох основних компонентів:

1. Агенти збору даних. Моніторинг кінцевих точок та збір даних (процеси, підключення, обсяг активності та передача даних) і передавання цієї інформації у центральну БД.
2. Автоматизована відповідь. Заздалегідь налаштовані правила в рішенні EDR спроможні виявляти вхідні дані, що вказують на відомий тип порушення безпеки, та запускати автоматизовану реакцію, наприклад, вихід із системи кінцевого користувача чи висилання сповіщення співробітнику.
3. Аналіз та криміналістика. Аналіз в реальному часі та швидка діагностики загроз, застосування інструментів криміналістики для виявлення загроз чи проведення пост-аналізу атаки.

Безпека системи EDR забезпечує інтегроване централізоване середовище для збору, кореляції та аналізу даних кінцевих точок, а також для координації сповіщень і реагування на активні загрози (рис. 5). EDR операційно взаємодіють за допомогою агентів, які встановлюються на локальних пристроях. З метою полегшення управління ними вони централізовано об'єднуються через центральний хаб. Кілька

агентів приєднуються до цього централізованого хабу, і кожен постійно моніторить пристрій та надає інформацію для подальшого аналізу.

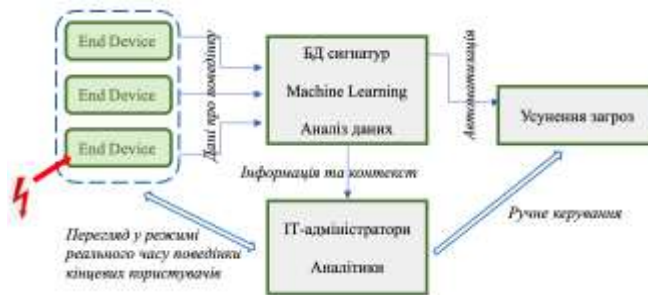


Рисунок 5 – Відома схема роботи EDR-систем

Дані, отримані з різних кінцевих точок, транслюються до централізованого хабу для проведення обробки та аналізу, часто використовуючи машинне навчання. Розроблені під час цього процесу статистичні моделі використовуються для часу аналізу вхідних даних з кінцевих точок та виявлення потенційних загроз.

У випадку виявлення загрози система EDR генерує сповіщення та надсилає його IT-адміністраторам чи команді кібербезпеки через інтерфейс користувача, які, здійснюють ізоляцію (переміщення в пісочницю) або вилучення шкідливих файлів, і так усувають потенційну загрозу. Саме так і пропонується вдосконалити схему відомого принципу функціонування EDR-системи (рис. 6).

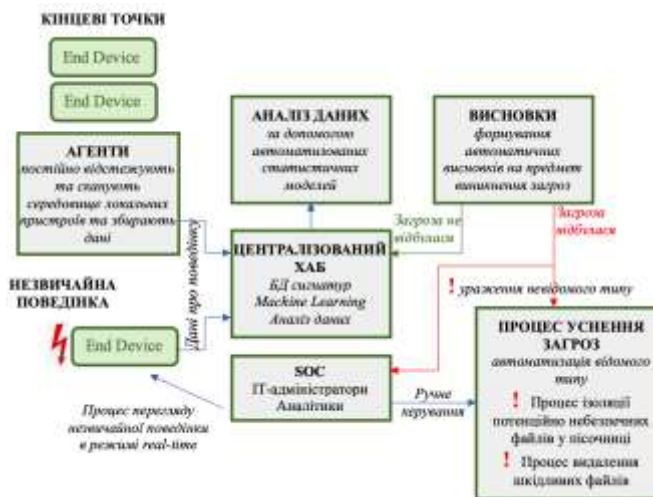


Рисунок 6 – Вдосконалений принцип роботи EDR-системи

Методи виявлення потенційних загроз в EDR:

- аналіз сигнатур – порівняння сигнатур мережевого трафіку із базою даних відомих сигнатур зловмисного програмного забезпечення;
- аналіз поведінки – поріг прийняття поведінки кінцевої точки порівнюється для виявлення випадків аномальної активності;
- аналіз пісочниці – потенційно небезпечні файли ізолюються в безпечному середовищі (пісочниці), і їхнє взаємодію спостерігається, уникаючи можливих негативних впливів на кінцеву точку;
- відповідність білого/чорного списків – дії кінцевих точок порівнюються із наперед визначеним списком IP-адрес у білому та чорному списках для контролю дозволеного/забороненого мережевого трафіку.

Формування задач складових NDR у тріаді SIEM-EDR-NDR. Як важливий елемент мережевої безпеки, система NDR (мережеве виявлення та реагування) містить технології мережевої безпеки для автоматизованого контролю, виявлення, аналізу та реагування на кіберзагрози.

Засоби NDR, які реалізовані для аналізу мережевого трафіку, включають IDS/IPS і розширений аналіз загроз, що надає змогу командам забезпечення безпеки спостерігати за мережевим трафіком в реальному часі та швидко реагувати на потенційні загрози.

У зв'язку з розширенням розподілених мереж, інструменти безпеки на основі сигнатур, такі як IDS/IPS, стають недостатніми для ефективного забезпечення безпеки підприємств. Рішення NDR використовують розширену поведінкову аналітику, машинне навчання та штучний інтелект для забезпечення додаткового рівня захисту в локальних і хмарних середовищах. Важливо відзначити, що рішення NDR не замінюють, а доповнюють попередні засоби моніторингу та аналізу мережі, утворюючи єдину повноцінну систему.

Рішення NDR можуть відстежувати транспортні потоки в обох напрямках (північ-південь та схід-захід, як внутрішні, так і зовнішні) за допомогою стратегічно розташованих датчиків.

Ефективні рішення NDR демонструють ряд переваг:

1. Розширена видимість загроз: групи безпеки можуть відслідковувати загрози, в т.ч. вторгнення та сторонні активності в мережі на локальному рівні та у хмарному середовищі.
2. Зменшення помилкових спрацьовувань: акцентування уваги на реальних вторгненнях.
3. Швидше запобігання або зупинка вторгнення: NDR використовує штучний інтелект і машинне навчання для роботи в режимі реального часу, розпізнавання та зупинки загроз зі швидкістю мережевого зв'язку.
4. Повна візуалізація атак: завдяки інформації про план вторгнень та детальному графіку загроз у мережі, служби безпеки можуть оперативно зрозуміти масштаб атаки та визначити пріоритетність ресурсів.

Рішення NDR постійно аналізують та корелюють значні обсяги мережевого трафіку та подій безпеки (Sec_Event_Logs) між різними активами та переходами. Інструменти NDR засновано на штучному інтелекті, який постійно самонавчається та адаптується для автоматичного виявлення еволюціонуючих та складних загроз. У випадку виявлення атаки рішення NDR забезпечують всебічний криміналістичний аналіз хронології атаки, починаючи від ініціювання проникнення та стороннім переміщеннями в мережі, а також автоматично запускають процеси для запобігання майбутнім атакам.

Альтернативний процес обробки журналів подій

Відомий процес нормалізації журналів подій. Процес нормалізації журналів подій відомий та продемонстрований на рисунку 7.



Рисунок 7 – Відомий процес нормалізації журналів подій

Система SIEM має здатність виконувати різноманітні функції: проводити таксономію (класифікацію отриманих даних за типами та категоріями) і здійснювати кореляцію (пов'язувати здавалося б розрізнені події між собою). Крім того, вона може надсилати повідомлення відповідальним особам про виявлені підозрілі події в журналах.

Функціонал SIEM на прикладі компанії середнього розміру (близько 1000 співробітників, їх робочі ПК, інформація та бізнес-системи зберігаються та працюють на серверах):

1. Антивірусні рішення, які призначені для уникнення активності шкідливого коду зловмисного ПЗ на кінцевих точках, у локальному та web-трафіку, а також в електронній пошті.
2. Засоби захисту від експлойтів, які здатні виявляти та запобігати негативному впливу встановленого прикладного чи системного ПЗ.
3. Системи управління та контролю обліковими записами, які реалізують централізоване керування обліковими записами користувачів та адміністраторів ІТ-систем.
4. Засоби захисту від витоку даних, які спрямовані на запобігання несанкціонованій передачі цінної інформації з порушенням установлених у компанії.
5. Мережеві брандмауери, які регулюють вхідний та вихідний мережевий трафік як в локальній, так і в інтернет-мережі.

6. Системи виявлення та/або запобігання мережевим вторгненням призначені для аналізу мережевого трафіку з метою виявлення ознак атаки на пристрої через мережу за допомогою експлойтів.
7. «Пісочниці» (засоби ізолюваного виконання програм) дозволяють запускати сумнівний файл в ізолюваному віртуальному середовищі, призначеному для виявлення аномалій.
8. Сканери вразливостей застосовуються для аналізу різних ІТ-систем, отримуючи дані про використовувані версії ПЗ для застосування відомих вразливостей, що застосовуються до зазначених версій.
9. Системи ресурсів-приманок для зловмисників (honeypots і honeynets) створюються як імітаційні системи інформаційних ресурсів, аналогічні реальним системам компанії, але не містять жодної цінної інформації. Атакуючі, потрапивши в таку пастку, намагаються використовувати свій інструментарій для атаки, і їхні дії ретельно журналюються та аналізуються фахівцями з безпеки інформації.
10. Засоби управління портативними пристроями (MDM – Mobile Device Management) – це програми контролю та захисту портативних пристроїв співробітників (BYOD). Встановивши такий інструмент, співробітник отримує можливість контрольованого та безпечного віддаленого доступу до ІТ-ресурсів організації, наприклад, підключивши робочу пошту на свій смартфон.

Вдосконалений процес нормалізації журналів подій. Розглянемо, як функціонує система SIEM, яка користь від її впровадження та які завдання вона виконує (рисунок 8).

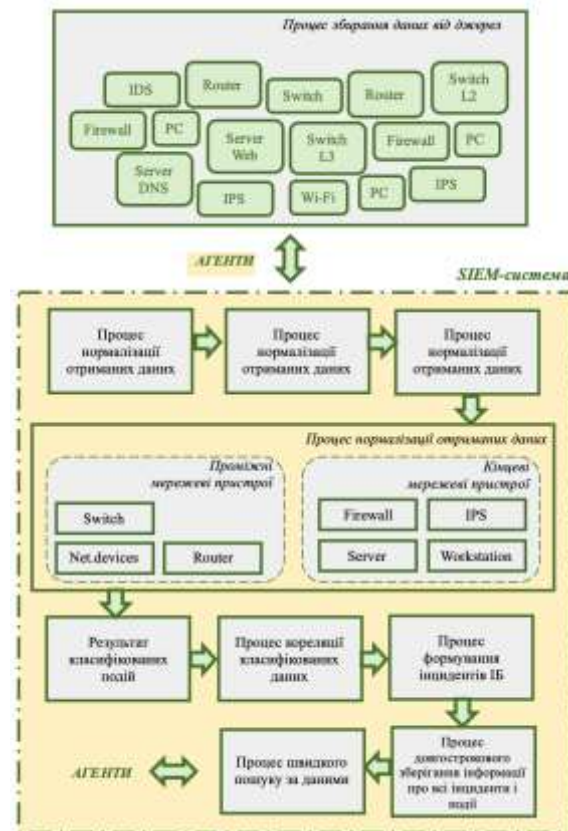


Рисунок 8 – Вдосконалений процес нормалізації журналів подій

Перше завдання SIEM – отримати дані від джерела. Це може бути як «активне» джерело, здатне передавати дані у SIEM, достатньо вказати мережеву адресу приймача (так званий менеджер), або «пасивне», до якого SIEM-система повинна самостійно звертатися (так званий агент). Отримавши дані від джерела, SIEM-система перетворює їх у єдиний, придатний для подальшого використання формат – це процес нормалізації. Далі SIEM-система виконує таксономію, класифікуючи вже нормалізовані повідомлення відповідно до їхнього змісту: яка подія вказує на успішну мережеву комунікацію, яка – на вхід користувача на ПК, а яка – на спрацювання антивіруса. Таким чином, отримуємо не лише набір записів, а послідовність подій (Sec_Event_Logs) із конкретним змістом та часом виникнення. Тепер ми

можемо зрозуміти, як взаємодіяли події та встановити можливий зв'язок між ними. В цьому контексті важливу роль відіграє основний механізм SIEM-системи – кореляція. Кореляція в SIEM – це встановлення взаємозв'язку між подіями, які відповідають конкретним умовам (правилам кореляції).

За результатами застосування правил кореляції у SIEM формується інцидент ІБ. В такому випадку фахівець, що працює в SIEM, має ефективно знаходити серед попередніх інцидентів та подій, що зберігаються в системі SIEM. Отже, ключові завдання системи SIEM такі: 1. Збір журналів з усіх наявних засобів захисту; 2. Нормалізація отриманих даних; 3. Таксономія нормалізованих даних; 4. Кореляція класифікованих подій (Sec_Event_Logs); 5. Створення інциденту та забезпечення інструментів для проведення розслідування; 6. Збереження інформації про події та інциденти протягом значного періоду (принаймні 6 місяців); 7. Швидкий пошук за даними, які зберігаються в SIEM. Враховуючи ці аспекти, пропонується удосконалити схему відомого процесу нормалізації журналів подій.

Нова концепція схеми відрізняється від існуючих за такими параметрами: 1) вона була ретельно розглянута та уточнена, з докладно визначеними складовими процесу нормалізації журналів подій; 2) в ній визначено роль агентів між джерелом даних та SIEM-системою; 3) тут представлені ключові етапи обробки даних в межах SIEM-системи.

Висновки

Потреба у аналізі та удосконаленні методів та засобів неперервного моніторингу безпеки в комп'ютерних мережах засобами SIEM стала підставою для дослідження.

У даній роботі досягнута поставлена мета, яка дозволяє прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовищі. У підсумку це дозволяє упорядковувати та класифікувати хаотичні неосяжні потоки інформації про події в мережі та перетворити у зручну візуально прийнятну інформацію для оперативного усунення загроз адміністратором системи.

Список літератури

- [1] Кібербезпека бізнесу в умовах нестабільності [Електронний ресурс] // PwC Україна. – 2022. – Режим доступу до ресурсу: <https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html>
- [2] Про Національний координаційний центр кібербезпеки [Електронний ресурс] // Верховна Рада України. – 2016. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/242/2016#Text>
- [3] Про CERT-UA [Електронний ресурс] // Державна служба спеціального зв'язку та захисту інформації України. – 2023. – Режим доступу до ресурсу: <https://cert.gov.ua>
- [4] Військова кібербезпека [Електронний ресурс] // Міністерство оборони України. – 2023. – Режим доступу до ресурсу: <https://www.mil.gov.ua/ukbs>
- [5] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 [Електронний ресурс] // Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". – 2021. – Режим доступу до ресурсу: <https://www.president.gov.ua/documents/4472021-40013>
- [6] What is the SOC visibility triad? [Електронний ресурс] // SOC visibility triad Режим доступу до ресурсу: <https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/>
- [7] Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
- [8] Miller D. Security Information and Event Management (SIEM) - Implementation Guide / David R. Miller. CRC Press, 2020.
- [9] Гребенюк А. М. Основи управління інформаційною безпекою [Ел. ресурс] / А. М. Гребенюк, Л. В. Рибальченко. – 2020. – Режим доступу: <https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3%D0%91%20.pdf>
- [10] Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.
- [11] Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices [Електронний ресурс] // DNSstuff. – 2020. – Режим доступу до ресурсу: <https://www.dnsstuff.com/common-siem-alerts>.
- [12] Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020 – 242p.
- [13] Коробейнікова Т.І. Системний моніторинг мережевої безпеки в тріаді SIEM-EDR-NDR / Коробейнікова Т.І., Федорченко В. В. // International scientific journal «Grail of Science» – 2023. – №

27 (May, 2023). – С. 354–360. ISSN: 2710–3056. ISBN 979-8-88955-792-0.

- [14] Коробейнікова Т.І. Системний моніторинг мережевої безпеки в триаді SIEM-EDR-NDR / Коробейнікова Т.І., Федорченко В. В. // International periodical scientific journal «SWorldJournal» – 2023. – № 19 (part 1) (May, 2023). – С. 33–39. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-19-01-029.
- [15] Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп'ютерна інженерія 2021: - №1 (50). - С. 31–35
- [16] Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // Інформаційні технології та комп'ютерна інженерія. – 2023. – № 1. – С. 66-74.

Стаття надійшла: 20.11.2023 р.

References

- [1] Kiberbezpeka biznesu v umovakh nestabil'nosti [Elektronnyy resurs] // PwC Ukrayina. – 2022. – Rezhym dostupu do resursu: <https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html>
- [2] Pro Natsional'nyy koordynatsiynyy tsentr kiberbezpeky [Elektronnyy resurs] // Verkhovna Rada Ukrayiny. – 2016. – Rezhym dostupu do resursu: <https://zakon.rada.gov.ua/laws/show/242/2016#Text>
- [3] Pro CERT-UA [Elektronnyy resurs] // Derzhavna sluzhba spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrayiny. – 2023. – Rezhym dostupu do resursu: <https://cert.gov.ua>
- [4] Viys'kova kiberbezpeka [Elektronnyy resurs] // Ministerstvo oborony Ukrayiny. – 2023. – Rezhym dostupu do resursu: <https://www.mil.gov.ua/ukbs>
- [5] UKAZ PREZYDENTA UKRAYINY №447/2021 [Elektronnyy resurs] // Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku "Pro Stratehiyu kiberbezpeky Ukrayiny". – 2021. – Rezhym dostupu do resursu: <https://www.president.gov.ua/documents/4472021-40013>
- [6] What is the SOC visibility triad? [Elektronnyy resurs] // SOC visibility triad Rezhym dostupu do resursu: <https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/>
- [7] Pobudova zakhyshchenykh merezh na bazi obladnannya kompaniyi Cisco. // Zakharchenko S.M., Troyanovs'ka T. I., Boyko O.V. Navchal'nyy posibnyk. Vinnytsya : VNTU, 2017. – 133 s.
- [8] Miller D. Security Information and Event Management (SIEM) - Implementation Guide / David R. Miller. CRC Press, 2020.
- [9] Hrebenyuk A. M. Osnovy upravlinnya informatsiynoy bezpekoyu [El. resurs] / A. M. Hrebenyuk, L. V. Rybal'chenko. – 2020. – Rezhym dostupu do resursu: <https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1%D0%91%D0%9D%D0%98%D0%9A%D0%9E%D0%A3%D0%91%20.pdf>
- [10] Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.
- [11] Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices [Elektronnyy resurs] // DNSstuff. – 2020. – Rezhym dostupu do resursu: <https://www.dnsstuff.com/common-siem-alerts>.
- [12] Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020 – 242p.
- [13] Korobeynikova T.I. Systemnyy monitorynh merezhevoyi bezpeky v triadi SIEM-EDR-NDR / Korobeynikova T.I., Fedorchenko V. V. // International scientific journal «Grail of Science» – 2023. – № 27 (May, 2023). – С. 354–360. ISSN: 2710–3056. ISBN 979-8-88955-792-0.
- [14] Korobeynikova T.I. Cystemnyy monitorynh merezhevoyi bezpeky v triadi SIEM-EDR-NDR / Korobeynikova T.I., Fedorchenko V. V. // International periodical scientific journal «SWorldJournal» – 2023. – № 19 (part 1) (May, 2023). – С. 33–39. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-19-01-029.
- [15] Savyts'ka L.A., Korobeynikova T.I. Udoskonalenny metod rozrobky ARI pidvyshchenoyi shvydkodiyi Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya 2021: - №1 (50). - С. 31–35
- [16] Savyts'ka L. A. Prohrannyi modul' poperedn'oho diahnostuvannya patsiyentiv na osnovi neyronnoyi merezhi Kokhonena [Tekst] / L. A. Savyts'ka, N. V. Dobvol's'ka, V. O. Kondratyuk // Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya. – 2023. – № 1. – С. 66-74.

Відомості про авторів

Савицька Людмила Анатоліївна – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Savytska Liudmyla, PhD – associate professor of computing engineering department, Vinnytsya national technical university

Коробейнікова Тетяна Іванівна – к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana – PhD, associate professor of information technology security department, National university "Lvivska Politechnika"

Волос Олександр Павлович – магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Volos Oleksandr Pavlovych – magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering

Тарновський Микола Геннадійович – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Tarnovskyi Mykola, PhD, associate professor of computing engineering department, Vinnytsya national technical university

L. Savytska¹, T. Korobeinikova², O. Volos¹, M. Tarnovskyi¹

METHOD AND MEANS OF SECURITY MONITORING IN A COMPUTER NETWORK BY SIEM MEANS

¹Vinnytsya national technical university, Vinnytsya

²National university "Lvivska Politechnika"

КОМП'ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 004.358

Б. В. Блощинський, Я. М. Клятченко

**ЕФЕКТИВНІСТЬ КОМП'ЮТЕРНИХ ЗАСОБІВ
КЕРУВАННЯ АВТОМАТИЧНИМ НАПРАВЛЕННЯМ
АНТЕН У БЕЗДРОТОВИХ СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ

Анотація. Сучасні телекомунікаційні системи набули значної популярності завдяки, в першу чергу, ефективним засобам передачі інформації. Однак, незалежно від способу передачі інформації, ефективність будь-якої системи може бути обмежена максимальною швидкістю та дальністю цієї передачі. Також, ефективність та доцільність використання, наприклад, бездротових систем передачі даних залежить від рельєфу, швидкості розгортання, економічних показників та тривалості використання. В системах бездротової передачі даних в приймачах (передавачах) використовуються антени спрямованої дії, які мають бути розгорнуті для встановлення каналу зв'язку шляхом направлення на джерело (приймач) сигналу. Але значний вплив на швидкість розгортання таких бездротових систем передачі даних із спрямованими антенами чинить процес автоматичного направлення антени. Підвищення ефективності засобів автопозиціонування антен досягається за рахунок нової запропонованої їхньої структурної організації, вдосконалених алгоритмів керування направленням антени та застосування сучасної елементно-компонентної бази. Проведено аналіз та порівняння експериментальних результатів роботи запропонованого рішення для бездротових систем передачі даних. Також, запропоновано структури системи автоматичного направлення антени, реалізовано діючий прототип, створено керуюче програмне забезпечення та проведено тестування його функціонування згідно розроблених алгоритмів. Продемонстровано широкі можливості сучасної елементно-компонентної бази для реалізації апаратури засобів автоматичного направлення антен. При аналізі отриманих результатів тестування створеного прототипу було показано ефективність запропонованих алгоритмів, яка досягається за рахунок їхнього комбінування для отримання гарантованого результату. Запропоновано схему застосування цих алгоритмів, суть якої полягає в тому, що один алгоритм має керувати направленням антени, яке буде приблизним, а інший алгоритм буде виконувати точне позиціонування, тобто коригувати та завершувати направлення антени.

Ключові слова: бездротові системи передачі даних, мікроконтролер, автопозиціонування, направлення антени, бездротовий зв'язок.

Abstract. Modern telecommunication systems have gained considerable popularity thanks, first of all, to effective means of information transmission. However, regardless of the method of information transmission, the effectiveness of any system can be limited by the maximum speed and range of this transmission. Also, the effectiveness and feasibility of using, for example, wireless data transmission systems depends on the terrain, speed of deployment, economic indicators and duration of use. In wireless data transmission systems, directional antennas are used in receivers (transmitters), which must be deployed to establish a communication channel by directing the signal to the source (receiver). But the automatic antenna pointing process has a significant impact on the speed of deployment of such wireless data transmission systems with directional antennas. Increasing the efficiency of the means of auto-positioning of antennas is achieved due to the newly proposed structural organization of them, improved algorithms for controlling the direction of the antenna and the use of a modern element-component base. An analysis and comparison of the experimental results of the proposed solution for wireless data transmission systems was carried out.

Also, the structure of the automatic antenna direction system was proposed, a working prototype was implemented, the control software was created and its functioning was tested according to the developed algorithms. The broad capabilities of the modern element-component base for the implementation of equipment for automatic antenna pointing are demonstrated. The analysis of the test results of the created prototype showed the effectiveness of the proposed algorithms, which is achieved by combining them to obtain a guaranteed result. A scheme of application of these algorithms is proposed, the essence of which is that one algorithm should control the direction of the antenna, which will be approximate, and the other algorithm will perform exact positioning, that is, correct and complete the direction of the antenna.

Key words: wireless data transmission systems, microcontroller, auto positioning, antenna pointing, wireless.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-33-40>.

Вступ

В сучасних телекомунікаційних системах вплив засобів для організації бездротового зв'язку стає все більш помітним та відіграє ключову роль завдяки підключенню віддалених об'єктів до спільної мережі. Наприклад, ці засоби є незамінними при створенні магістрального каналу мережі операторів зв'язку коли неможливо підключитись до віддаленої комп'ютерної мережі або у випадку, коли економічно недоцільно прокладати волоконно-оптичну магістраль. Основними перевагами сучасних бездротових ліній зв'язку є: швидке розгортання ліній зв'язку при відносно низьких грошових витратах; можливість безперешкодного проходження мережі через транспортні магістралі та по водній поверхні; висока рентабельність роботи бездротового ретранслятора; мінімальна вартість експлуатації мережі; ефективна організація якісного зв'язку в складних географічних і кліматичних умовах; багатофункціональне викорис-

тання каналів для забезпечення доступу до засобів Інтернету для передачі електронних документів, головної та відеоінформації. [1].

Актуальність

Для того щоб встановити бездротовий канал зв'язку, необхідно встановити приймач або передавач і розгорнути антену. Але проблемним питанням використання спрямованої антени є її направлення на джерело або приймач сигналу. Зазвичай кінцеві станції передають або приймають сигнали з одного напрямку зв'язку, а проміжні станції і приймають, і передають сигнали в обох напрямках. Для забезпечення стабільності, антени сусідніх станцій розташовують на природних височинах, щоглових пристроях або баштах з дотриманням умови, що на шляху сигналу немає жодних перешкод. До однієї із функцій проміжних станцій можна віднести ретрансляцію, яка буває т. з. чиста (наскрізна) та вузлова. Чиста ретрансляція використовується у випадках, коли необхідно прийняти, перетворити, посилити і передати наступній станції отриманий сигнал повністю. Вузлова ретрансляція використовується, коли потрібно оперативно відокремити частину отриманої на станції інформації і замінити її на нову, наприклад, отриману з інших джерел. Отже, постає задача розробки, реалізації та підвищення ефективності засобів автоматичного направлення антен для систем бездротового зв'язку.

Мета

Метою роботи є підвищення ефективності засобів направлення антен шляхом відображення завдань і алгоритмів на структуру, склад та функціональні можливості цих засобів.

Задачі

1. Аналіз можливостей та особливостей застосування сучасної елементно-компонентної бази для апаратних структур засобів автоматичного направлення антен.
2. Дослідження і реалізація алгоритмів керування направленням антени, а також аналіз їхньої ефективності.
3. Оцінка результатів роботи створеного прототипу реалізованої системи.

Розв'язання задач

Організація бездротового зв'язку зводиться до побудови лінії зв'язку, що у свою чергу залежить від засобів для точного та швидкого направлення антен, які характеризуються наявністю в своєму складі системи команд управління, ручним/автоматичним позиціонуванням, наявністю складових для контролю і аналізу вхідних даних та організацією обміну даними через послідовний інтерфейс. Також сюди можна включити програмне забезпечення, яке має керувати орієнтацією антени по азимуту і куту місця. Цей пристрій за допомогою спеціальних алгоритмів має забезпечувати направлення антени на джерело сигналу з певною точністю. Оскільки пристрій встановлюється у комплекси зв'язку для керування іншими системами цього комплексу, то необхідно забезпечити можливості для розширення кількості одиниць периферійного обладнання, що могло б підключатися до розробленого пристрою. Для реалізації пристрою [2] вибрано одноплатний мінікомп'ютер – RaspberryPi 3B+ [3]. На цій платформі система побудована на базі комплекту розробника – Arduino UNO, виконаного на базі 8-бітного мікроконтролера ATmega 328P [4].

Пропонується наведена нижче структура системи автоматичного направлення антени (рис.1).

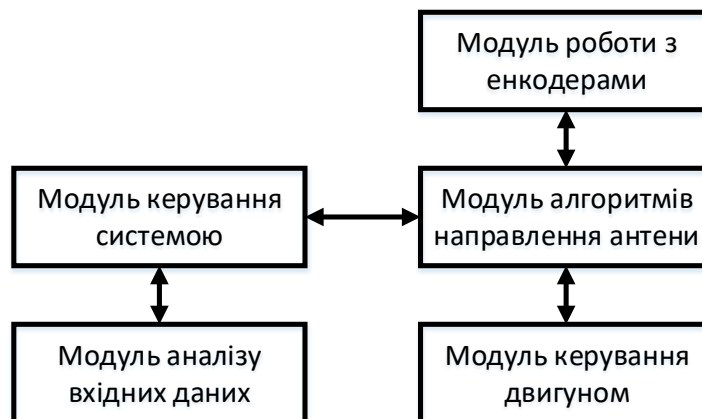


Рисунок 1 – Структура системи автоматичного направлення антени

Модуль керування системою призначено для отримання та виконання команд, які надходять від оператора системи. До таких команд можна віднести, наприклад, команду повернути приймач на певний кут в одній із площин або ініціювати процедуру направлення на сигнал за одним із алгоритмів.

До функцій модуля аналізу вхідних даних входять: зчитування показників від приймача, їхній аналіз та перетворення у цифровий вигляд для подальшого використання. У модулі алгоритмів направлення реалізовано декілька алгоритмів направлення приймаючого пристрою на джерело сигналу. Цей модуль пов'язаний з модулем керування двигунами і модулем роботи з енкодерами. Цей модуль, аналізуючи дані, отримані від енкодера, керує двигунами.

Для того, щоб визначитись із способом орієнтації у просторі, тобто як програмне забезпечення системи має визначити місце розташування антени у конкретний момент часу, оптимальним рішенням є застосування крокового двигуна [5] з енкодером [6]. Модуль роботи з енкодерами збирає інформацію від енкодерів і передає її до модуля алгоритмів направлення.

Модуль керування двигунами відповідає за надсилання керуючих сигналів на мікросхему-драйвер керування кроковими двигунами (базі мікросхеми A4988) [7]. Крокові двигуни використовуються для керування позицією об'єкта або для обертання певного вузла з фіксованою швидкістю на заданий кут. Перед використанням двигуна необхідно провести налаштування драйвера, а саме обмежити максимальний струм, що протікає через обмотки двигуна. Після конфігурування виконується цикл, під час якого на вивід драйвера посилюються імпульси для обертання двигуна.

Для оцінки запропонованих рішень створено прототип (макет) для тестування роботи системи автоматичного направлення антен [2]. Корпус пристрою виконано із пластмаси, він представляє собою короб, до якого кріпляться усі необхідні для його роботи компоненти, а саме: два енкодера, два крокових двигуна, плата Arduino UNO, два драйвери крокових двигунів, фоторезистор (див. рис.2).

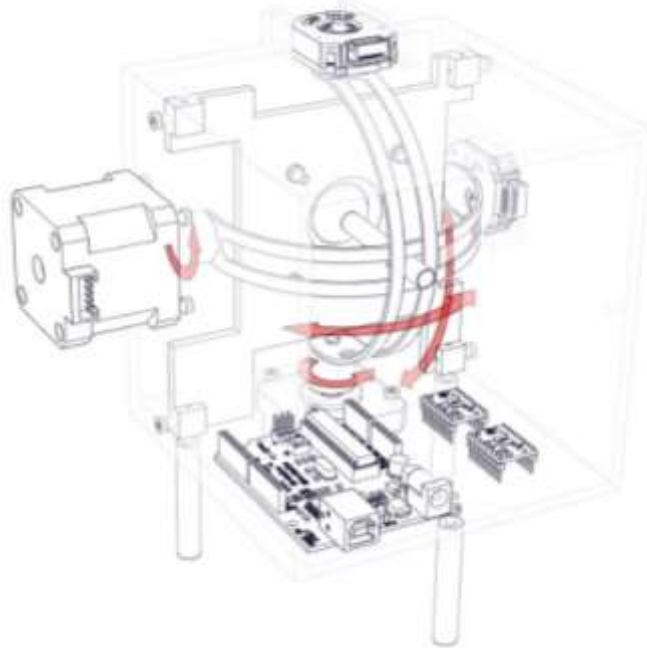


Рисунок 2 – Вигляд прототипу системи автоматичного направлення антен

У розробленому прототипі системи автоматичного направлення антени для проведення тестування у ролі приймаючого пристрою використовується фоторезистор. Як вхідні дані використовується значення напруги, яка знімається між двома резисторами, один з яких є фоточутливим. Коли світло потрапляє на поверхню фоторезистора, його опір зменшується, і таким чином, знаходиться напрямок джерела світла.

При роботі система може наводитись на джерело сигналу, працюючи за двома алгоритмами. Перший алгоритм – це алгоритм прямокутних спіралей, який працює за таким принципом: починаючи процес пошуку у центрі, “око” переміщується у заданому напрямку, доки покази напруги з фоторезистора не почнуть зменшуватись. Після цього “око” повернеться у останню точку по заданій координаті, де напруга не зменшувалася, і почне рухатися у перпендикулярному напрямку, також аналізуючи значення напруги. Результат роботи алгоритму зображено на рис.3. Зірка показує місце розташування джерела сиг-

налу. Пунктирна лінія зображує приблизний шлях, який проходить "око" для направлення на джерело сигналу.



Рисунок 3 – Схематичне зображення роботи алгоритму прямокутних спіралей

Спрощену блок-схему алгоритма представлено на рис.4.

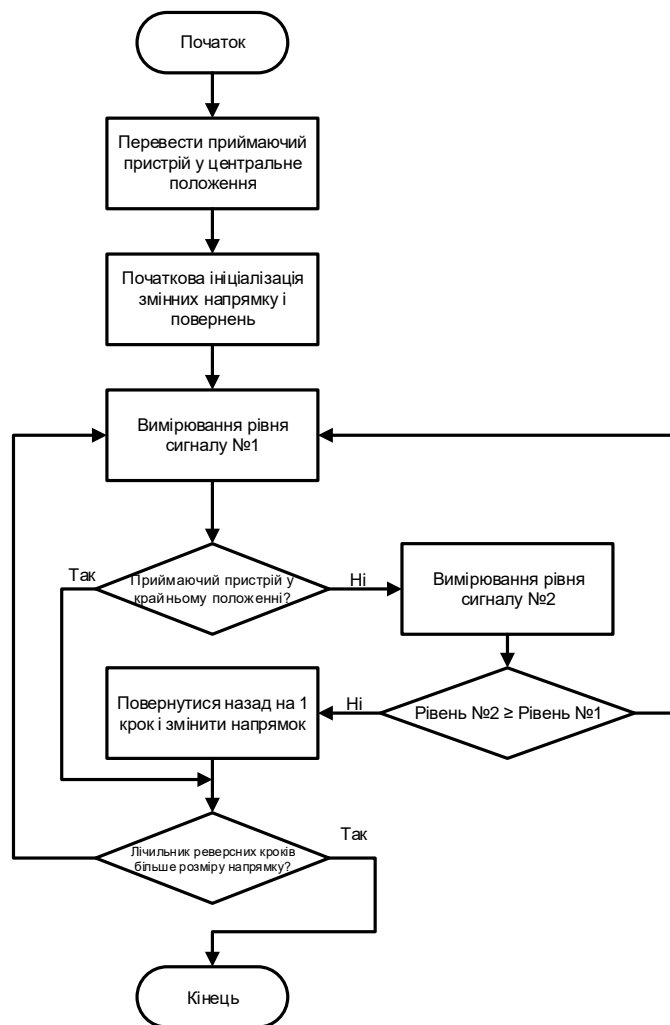


Рисунок 4 – Спрощена схема алгоритма прямокутної спіралі

Другий алгоритм – алгоритм простого сканування (рис.5). "Око" сприймає видиму йому область як матрицю, і сканує її, порівнюючи значення напруги у кожній її клітинці. Після знаходження найбільшого значення напруги, алгоритм запам'ятовує декілька параметрів, таких як значення напруги, координату X, координату Y. Після проходження по всій області, "око" повертається у точку з координатами X і Y, у якій значення напруги найбільше з усієї області, що доступна для "ока".

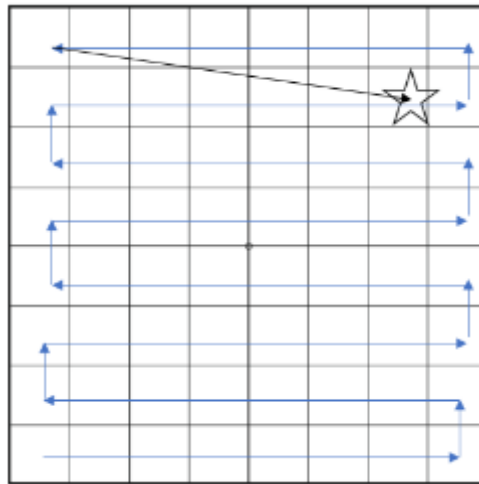


Рисунок 5 – Схематичне зображення роботи алгоритму простого сканування

Крокові двигуни керуються через драйвери сигналами з плати Arduino UNO. До валу кожного двигуна прикріплено кулісу, яка вигнута у формі півкола (див. рис. 6). Дві куліси закріплені під прямим кутом. У область, що утворюється при перетині куліс, вставляється палець з вмонтованим на протилежній стороні фоторезистором. З іншої сторони палець вставляється у сферу, яка затискається між двома пластинами, і тим самим утворюється шаровий механізм. Таким чином, при обертанні валу двигуна куліса, що закріплена на ньому, теж обертається. При обертанні куліса рухає палець з фоторезистором у площині другої куліси. Кут повороту контролюється енкодерами.

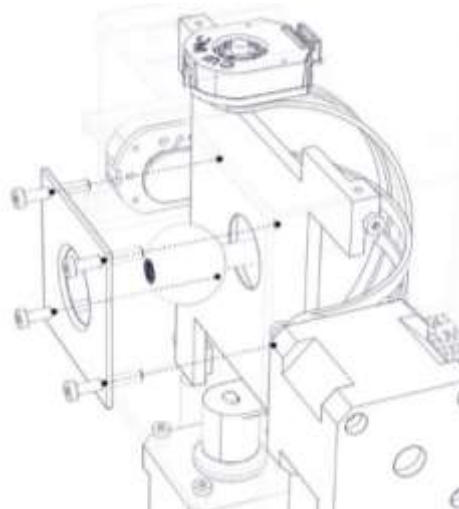


Рисунок 6 – Рухома частина прототипу

Аналіз результатів роботи створеного прототипу реалізованої системи направлення антени показав наступне. Тестування складалося із чотирьох частин:

- незалежне тестування кожного алгоритму з одним джерелом світла;
- незалежне тестування кожного алгоритму з двома джерелами світла;
- тестування комбінації алгоритмів з одним джерелом світла;
- тестування комбінації алгоритмів з двома джерелами світла.

При тестуванні алгоритму простого сканування з одним джерелом світла процес направлення тривав 37,3 секунди. У результаті приймаючий пристрій було повернуто у сторону передавача у горизонтальній площині, але у вертикальній площині приймаючий пристрій було піднято надто високо. Також на основі отриманих даних було побудовано дві діаграми (див. рис. 7). З їх допомогою можна оцінити характер розповсюдження світла по області видимості.

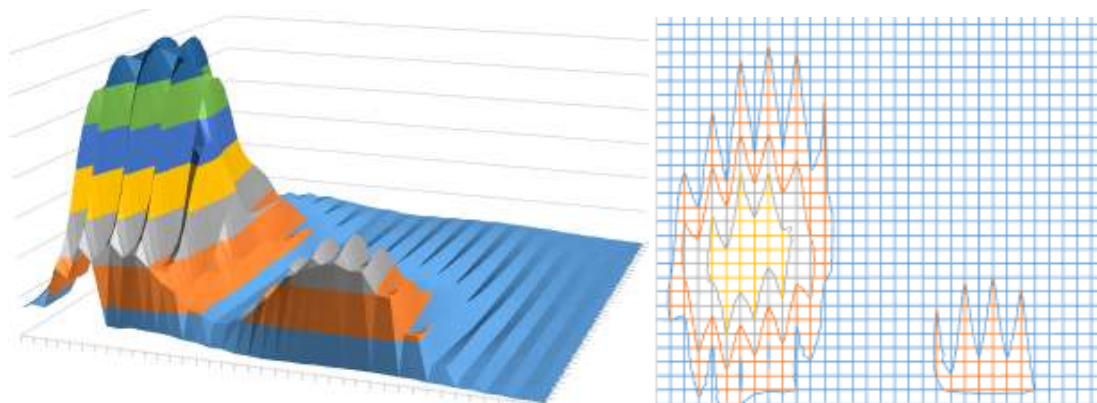


Рисунок 7 – Об'ємна та плоска діаграми, що ілюструють розповсюдження сигналу по області сканування із одним джерелом світла

На цих графіках можна виділити дві групи сигналів, один з яких більше за інший. Оскільки використовувалось світло у ролі сигналу, то можна стверджувати, що через неідеальність зовнішніх умов проведення випробувань світло може відбиватися від предметів, що знаходяться поруч із стендом для випробувань.

При тестуванні алгоритму прямокутної спіралі з одним джерелом світла направлення куліси із фоточутливим елементом тривало 3,3 секунди. Як результат, приймаючий пристрій було повернуто у сторону передавача. При використанні цього алгоритму з одним джерелом сигналу було встановлено, що точність направлення виявилася краще, ніж при використанні першого алгоритму.

При тестуванні пристрою за алгоритмом простого сканування з двома джерелами світла для випробувань було взято два джерела світла, одне з яких більш потужне за інше. Процес направлення тривав 37,3 секунди. У результаті приймаючий пристрій було повернуто у сторону більш потужного передавача з невеликим зсувом по вертикалі. На основі отриманих даних також було побудовано два графіка.

При цьому тестуванні на графіках (рис.8) чітко видно дві окремі групи сигналів, що відображають окремі джерела сигналів, де група вищих піків – це потужне джерело світла, а група менших – це слабше.

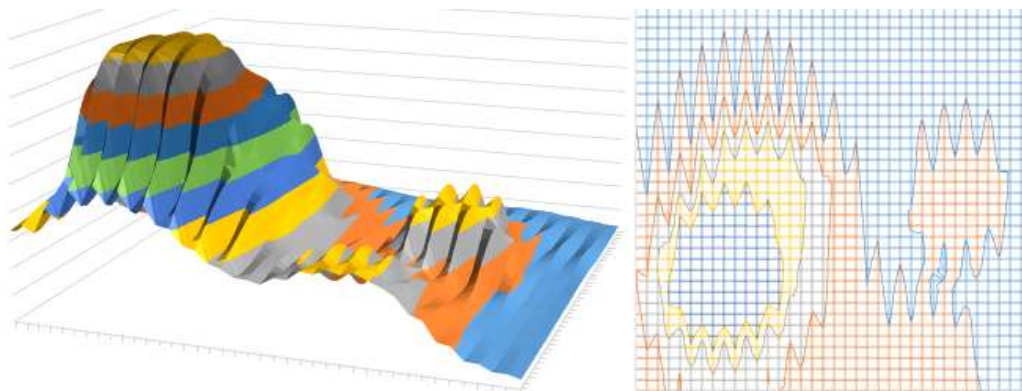


Рисунок 8 – Об'ємна та плоска діаграми, що ілюструють розповсюдження сигналу по області сканування з двома джерелами світла

Направлення куліси із фоточутливим елементом за алгоритмом прямокутної спіралі з двома джерелами світла тривало 3,1 секунди. В результаті роботи приймаючий пристрій було направлено у сторону слабшого джерела світла, що обумовлено особливістю реалізації алгоритму, оскільки менш потужне джерело на маршруті обходу знаходиться першим, і тому алгоритм вважає його єдиним, і виконує направлення антени лише на нього.

Під час тестування роботи системи, що працює за комбінацією алгоритмів з одним і двома джерелами світла процес направлення антени тривав 40,2 секунди. В обох випадках приймаючий пристрій було повернуто у напрямку джерела світла, точніше ніж при використанні алгоритмів окремо один від одного (у випадку з двома джерелами сигналу, приймаючий пристрій виконав направлення антени на потужне джерело сигналу).

Керування направленням антени в реалізованому прототипі здійснюється в ручному та автоматичному (програмне керування) режимах. Для ручного керування використовується система команд та про-

грамне забезпечення, що уможливило зв'язок через послідовний інтерфейс. Керування за допомогою програмного забезпечення відбувається через програму Guidance Control (рис. 9).

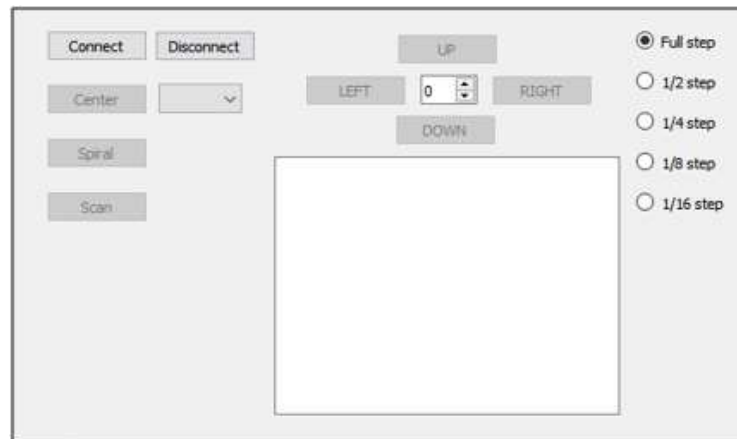


Рисунок 9 – Інтерфейс програми Guidance Control

До основних функцій цього програмного засобу можна віднести: підключення пристрою, який з'єднано з обраним портом (кнопка "Connect"), надсилання команди для виконання центрування приймаючого пристрою (кнопка "Center"), надсилання команди для виконання направлення приймаючого пристрою за алгоритмом прямокутної спіралі (кнопка "Spiral"), виконання направлення приймаючого пристрою за алгоритмом простого сканування (кнопка "Scan"), відключення пристрою (кнопка "Disconnect"), керування поворотом приймаючого пристрою у відповідному напрямку, на кількість кроків задану у полі з стрілками (кнопки "UP", "DOWN", "LEFT", "RIGHT"), налаштування дільника кроків крокових двигунів ("Full Step", "1/2 step ... 1/16 step").

Висновки

1. Можливості сучасної елементно-компонентної бази для реалізації апаратури засобів автоматичного направлення антен дозволяють ефективно вирішити широкий спектр завдань.
2. В результаті аналізу отриманих результатів тестування створеного прототипу було виявлено, що запропоновані алгоритми виконують поставлену їм задачу, але для досягнення гарантованого результату необхідно їх комбінувати. В розрізі цього запропоновано схему застосування цих алгоритмів, де один із них має керувати направленням антени, яке буде приблизним, а інший алгоритм буде виконувати точне позиціонування. В результаті проведених з прототипом експериментів з'ясовано, що алгоритм простого сканування виконує приблизне позиціонування, а алгоритм прямокутної спіралі є коригуючим і має завершувати направлення антени.

Список літератури

- [1] Янко А.С. Основні тенденції та перспективи розвитку радіорелейного зв'язку [Електронний ресурс] / А.С. Янко, В.В. Авдєєв // Новітні інформаційні системи та технології – Modern information system and technologies. – Полтава : ПолтНТУ, 2018. – № 9.
- [2] Блощинський, Б. В. Система керування автопозиціонуванням антен радіорелейного зв'язку : дипломний проект ... бакалавра : 123 Комп'ютерна інженерія / Блощинський Богдан Вікторович. – Київ, 2020. – 66 с.
- [3] «Raspberry Pi 3 Model B+»/ Посилання: <https://arduino.ua/prod2590-raspberry-pi-3-b-plus>
- [4] «ATMEGA328P Datasheet (PDF) - ATMEL Corporation» / Посилання: <https://www.alldatasheet.com/datasheet-pdf/pdf/1425641/ATMEL/ATMEGA328P.html>
- [5] 17HD4401 2 Phase Hybrid Stepper Motor/ Посилання: <https://datasheetspdf.com/pdf-file/928661/MotionKing/17HS4401/1>
- [6] AMT20 MODULAR ABSOLUTE ENCODER/ Посилання: <https://www.cuidevices.com/product/resource/amt20-v.pdf>
- [7] Драйвер крокового двигуна A4988/ Посилання: <https://www.mini-tech.com.ua/ua/drayver-shagovogo-dvigatelya-a4988>

References

- [1] Yanko A.S. The main trends and prospects for the development of radio relay communication [Electronic resource] / A.S. Yanko, V.V. Avdeev // Modern information system and technologies. – Poltava: PoltNTU, 2018. – No. 9.
- [2] Bloschynskyi, B.V. System for controlling the auto-positioning of radio relay antennas: diploma project ... bachelor's degree: 123 Computer engineering / Bohdan Viktorovich Bloschynskyi. - Kyiv, 2020. - 66 p.
- [3] «Raspberry Pi 3 Model B+»/ Посилання: <https://arduino.ua/prod2590-raspberry-pi-3-b-plus>
- [4] «ATMEGA328P Datasheet (PDF) - ATMEL Corporation» / Link: <https://www.alldatasheet.com/datasheet-pdf/pdf/1425641/ATMEL/ATMEGA328P.html>
- [5] 17HD4401 2 Phase Hybrid Stepper Motor/ Link: <https://datasheetspdf.com/pdf-file/928661/MotionKing/17HS4401/1>
- [6] AMT20 MODULAR ABSOLUTE ENCODER/ Link: <https://www.cuidevices.com/product/resource/amt20-v.pdf>
- [7] Stepper motor driver A4988/ Link: <https://www.mini-tech.com.ua/ua/drayer-shagovogo-dvigatelya-a4988>

Стаття надійшла: 15.11.2023 р.

Відомості про авторів

Блощинський Богдан Вікторович – провідний інженер ТОВ Науково-впроваджувальної фірми «Криптон», Київ.

Bloschynskyi Bohdan Viktorovich – Senior Engineer of Crypton LTD company.

Клятченко Ярослав Михайлович – кандидат технічних наук, доцент кафедри системного програмування і спеціалізованих комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Klyatchenko Yaroslav Mikhailovich – PhD, associate professor of Department of System Programming and Specialized Computer Systems of Igor Sikorsky Kyiv Polytechnic Institute.

B.V. Bloschynskyi, Y.M. Klyatchenko

EFFICIENCY OF COMPUTER MEANS FOR AUTOMATIC ANTENNAS DIRECTION IN WIRELESS DATA TRANSMISSION SYSTEMS

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv

УДК 004.7

Л.А. Савицька¹, Т.І. Коробейнікова², І. В. Леонтєв¹, С. В. Богомолів¹

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ РЕСУРСІВ В КОМП'ЮТЕРНІЙ SDN-МЕРЕЖІ

¹Вінницький національний технічний університет, Вінниця²Національний університет «Львівська політехніка»

Анотація. Робота присвячена аналізу та вдосконаленню методів та засобів побудови архітектури програмно-керованих мереж. Важливим аспектом є порівняння відмінностей між керуванням мережі за допомогою традиційних методів та з використання SDN контролера. Основна увага приділяється розробці моделей безпеки на базі програмно-керованих мереж.

Дослідження ґрунтуються на аналізі конкретних випадків використання таких мереж, включаючи збір думок та експертних оцінок від професіоналів у галузі та використовують загальнодоступну інформацію про методи та засоби безпеки архітектури програмно-керованих мереж. Технологія SDN надає більше гнучкості та швидкості впровадження заходів безпеки, що дозволяє реагувати на загрози в реальному часі. У сучасних умовах, коли кіберзагрози стають складнішими та виразнішими, SDN-мережі дозволяють виявляти атаки, блокувати шкідливі дії та застосовувати політики безпеки в реальному часі. Проте, зростаюча складність кіберзагроз та постійні зміни технологій вимагають подальшого розвитку і вдосконалення інформаційної безпеки ресурсів SDN-мережі компанії. Існує необхідність у подальшому аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерних SDN-мережах. Потреба у подальшому аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерних SDN-мережах стала фундаментом для проведення цього дослідження. У результаті досягнуто підвищення рівня інформаційної безпеки ресурсів SDN-мережі шляхом: 1) скорочення часу втручання у мережу; 2) застосування вдосконаленого методу оброблення трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажаним мережевими додаткам ефективно керувати пересиланням.

Ключові слова: SDN-мережа, Семантична модель SDN, модель взаємодії мережевої операційної системи та SDN, модель мережі із гнучкими ресурсами.

Abstract. The work is dedicated to the analysis and improvement of methods and tools for building the architecture of software-defined networks (SDNs). A crucial aspect involves comparing the differences between network management using traditional methods and utilizing an SDN controller. Primary attention is given to the development of security models based on software-defined networks.

The research is grounded in the analysis of specific cases involving the use of such networks, including gathering opinions and expert assessments from professionals in the field. It leverages publicly available information on methods and tools for securing the architecture of software-defined networks. SDN technology provides greater flexibility and speed in implementing security measures, allowing real-time responses to threats. In contemporary conditions, where cyber threats are becoming more complex and pronounced, SDN networks enable the detection of attacks, blocking malicious actions, and applying security policies in real-time. However, the increasing complexity of cyber threats and constant technological changes necessitate further development and enhancement of the information security of SDN network resources for companies. There is a need for further analysis and improvement of methods and tools for protecting information and other resources in computer-based SDN networks. The necessity for further analysis and improvement of methods and tools for protecting information and other resources in computer-based SDN networks serves as the foundation for this research. As a result, an enhancement in the level of information security for SDN network resources has been achieved by: 1) reducing the intervention time in the network; 2) applying an improved method of traffic processing based on network security of packet flows, allowing desired network applications to efficiently manage forwarding.

Key words: SDN network, SDN Semantic Model, network operating system interaction model and SDN, network model with flexible resources.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-41-52>.

Вступ

Кожна компанія, незалежно від свого розміру або галузі, має важливі ресурси, такі як конфіденційні дані клієнтів, комерційна інформація, інтелектуальна власність, фінансові дані тощо. Збереження цих ресурсів від несанкціонованого доступу, витоку інформації та зловживань є критично важливим завданням для забезпечення успіху компанії і захисту її репутації. Основними викликами, з якими може зіткнутися мережа компанії, може бути мережеві атаки на активи та ресурси (real time) внаслідок недосконалості або навіть відсутності політик доступу, складністю їх налаштувань, підтримки та оновлення; недостатній рівень керування мережевими трафіком; відсутність адекватного контролю, що призводить до зменшення гнучкості мережі; відсутність автоматизації базових мережевих функцій тощо [1-4].

Комп'ютерні SDN-мережі надають нові можливості для забезпечення безпеки мережевих ресурсів. Ця технологія дозволяє централізовано керувати мережевими пристроями і програмно налаштувати правила безпеки [5-6].

Актуальність

Технологія SDN забезпечує більшу гнучкість та швидкість впровадження заходів безпеки,

дозволяючи реагувати на загрози в реальному часі [8-10]. На сьогоднішній день, коли кіберзагрози стають все більш складними і виразними, SDN-мережі дозволяють виявляти атаки, блокувати шкідливі дії та застосовувати політики безпеки в реальному часі. Проте, зростаюча складність кіберзагроз та постійні зміни технологій вимагають подальшого розвитку і вдосконалення інформаційної безпеки ресурсів SDN-мережі компанії [7-10]. Тому тема дослідження є актуальною. Таким чином, існує потреба у аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерній SDN- мережі.

Мета

Метою дослідження є підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок застосування вдосконаленої безпекової моделі SDN-мережі.

Задачі

1. Виконати аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами;
2. Запропонувати семантичну модель SDN та схему розподілу потоків трафіку в SDN;
3. Запропонувати спосіб розрахунку надійності мережі;
4. Запропонувати модель взаємодії мережевої операційної системи із комп'ютерною SDN-мережею та спосіб оброблення трафіку;
5. Запропонувати безпекову модель та описати прототип комп'ютерної SDN-мережі.

Аналіз архітектур SD-WAN та SD-LAN на предмет організації у порівнянні із класичними архітектурними підходами

Комп'ютерна SDN-мережа (ПКМ, англ. Software-defined Networking, SDN) – це архітектура, яка розділяє функції управління мережею та пересилання даних, що дозволяє безпосередньо програмувати управління мережею, а базову інфраструктуру абстрагувати для програм і мережевих служб.

Ресурси SDN включають можливість більш ефективно та динамічно керувати мережевим трафіком, забезпечуючи підвищений рівень контролю та гнучкості в мережі. SDN дозволяє створювати кілька логічних мереж на основі однієї фізичної інфраструктури, що дозволяє віртуалізувати мережу. Крім того, SDN допомагає автоматизувати багато мережевих функцій, що може зменшити фізичне використання пристроїв та дозволити швидше розгортання та ефективне використання ресурсів мережі. Окрім цього, SDN надає централізований огляд всієї мережі, що забезпечує кращий рівень видимості та контролю.

Популярна архітектура комп'ютерної SDN-мережі складається з трьох рівнів (див. рис. 1, а):

- 1) Рівень інфраструктури містить набір мережевого обладнання.
- 2) Рівень керування містить мережеву операційну систему (MOC). MOC надає мережеві сервіси та програмний інтерфейс для управління мережевими пристроями.
- 3) Рівень мережевих додатків, який надає можливість гнучкого та ефективного керування мережею через різноманітні застосунки. Сюди входять програмні рішення щодо забезпечення безпеки, балансування навантаження (load balancing), виявлення вторгнень (IDS), адміністрування (IPS), а також функції управління потоками даних, мобільністю та доступом, які сприяють ефективній роботі мережі та багатьом іншим функціям.

Для налаштування комп'ютерної SDN-мережі достатньо просто додати програмний контролер, замість того, щоб редагувати великі обсяги коду в численних мережевих пристроях. Поведінкою комп'ютерної SDN-мережі можна керувати в реальному часі, а нові рішення можна впроваджувати значно швидше, ніж у традиційній архітектурі. Централізація стану мережі в єдиній точці керування дозволяє конфігурувати SDN-мережі за допомогою програмних інструментів. Мережеві контролери також включають набір програмних інтерфейсів, які реалізують стандартні завдання у сфері маршрутизації, такі як багатоканальність, безпека, контроль доступу, управління пропускнуою здатністю, забезпечення якості обслуговування, при цьому вони можуть бути спеціалізовані та налаштовані під конкретні потреби користувача.

Розширена схема архітектури комп'ютерної SDN-мережі забезпечує повну гнучкість у керуванні потоками передавання, що проявляється в простому балансуванні потоку без необхідності залучення окремого пристрою. (рис. 1, б).

Архітектура SD-LAN та традиційний підхід до організації локальної мережі

Локальна мережа (Local Area Network, LAN) є сукупністю комп'ютерів, які з'єднані між собою за допомогою провідного або безпроводного зв'язку, користуються спільним мережевим обладнанням та програмним забезпеченням, і підпорядковані єдиному адміністративному контролю. LAN забезпечують можливість спільної оброблення даних користувачами, підключеними до мережі комп'ютерами, обміну інформацією між користувачами та спільного використання програм та обладнання [11-14].

Важливо відзначити, що багато офісів дозволяють користувачам підключати свої власні пристрої до локальної мережі, що відомо як «BYOD» (Bring your own device, принеси свій власний пристрій). Це створює питання щодо безпеки, які системні адміністратори повинні враховувати.

Для забезпечення ефективної роботи LAN часто використовують один або кілька комп'ютерів у ролі серверів. На серверах зберігаються програми та бази даних (БД), які можуть бути використані спільно. Комп'ютери, які підключені до мережі, і які використовуються для роботи з цими ресурсами, називаються робочими станціями. У деяких випадках на робочих станціях, які працюють із даними на сервері (наприклад, використовують БД), можуть не встановлювати жорстких дисків з метою економії або з міркувань безпеки.

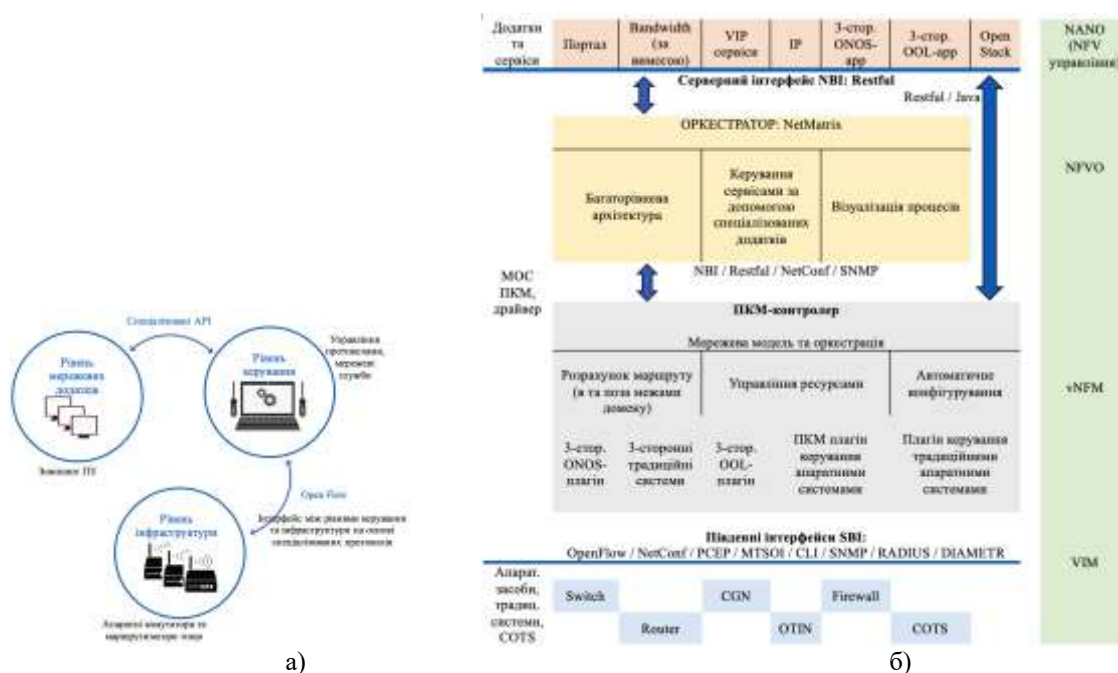


Рисунок 1 – Базова схема (а) та розширена (б) архітектури комп'ютерної SDN-мережі

Архітектура SD-LAN ґрунтується на принципах SDN і SD-WAN, що дозволяє мережевим адміністраторам керувати та налаштовувати мережу через програмне забезпечення, використовуючи централізований підхід та розділяючи мережу на потоки, щоб керувати розподілом ресурсів. Це забезпечує особливі переваги, такі як адаптивність, гнучкість, економічність та можливість масштабування для дротових та бездротових мереж доступу.

Адаптивність в мережі – це її здатність автоматично адаптуватися, налаштовуючи параметри, щоб забезпечити оптимальну роботу підключених пристроїв. В SD-LAN ця адаптивність досягається завдяки таким технологіям, як автоматична діагностика пристроїв, системи прикладних протоколів для налаштування хмарної мережі, автоматизація мережевих завдань та віртуалізація. Ці технології дозволяють мережі SD-LAN налаштовуватися автоматично відповідно до потреб підключених пристроїв, забезпечуючи оптимальну продуктивність і правильну роботу.

Гнучкість мережі – це її здатність змінювати параметри, щоб задовольняти потреби користувачів. Ця гнучкість досягається за допомогою маршрутизації, віртуалізації, контролю доступу та забезпечення безпеки. Це дозволяє мережі автоматично адаптуватися до змін у потребах користувачів.

Економічність – це принцип досягнення максимальної ефективності при найменших витратах. У SD-LAN ця економічність досягається завдяки технологіям, таким як розподіл обчислювальної потужності, використання програмно-апаратних архітектур, протоколи масштабного управління та мережеві інструменти для управління ресурсами. Це дозволяє використовувати бюджетні і легко адмініструвані програмно-апаратні рішення, що сприяють зниженню витрат на розвиток і експлуатацію мережі.

Розширення масштабу дротових і бездротових мереж доступу в SD-LAN включає в себе збільшення кількості користувачів, які можуть отримати доступ до мережі через одну точку входу, а також збільшення масштабу мережі, що дозволяє передавати дані від користувача до користувача безпосередньо.

Для досягнення розширення масштабу таких мереж використовуються наступні технології, підходи і протоколи:

- Технології віртуалізації: вони включають віртуалізацію мережі, віртуальні локальні мережі (VLAN) та віртуальні приватні мережі (VPN).
- Quality of Service (QoS): цей механізм дозволяє управляти пропускну здатністю мережі.
- Безпека мережі: забезпечення безпеки мережі за допомогою захисту мережі, такого як фільтрація пакетів, шифрування даних і ідентифікація користувачів.
- Протоколи: включають Ipv4, Ipv6, TCP/IP, UDP, які дозволяють мережі обмінюватися даними.
- Бездротові технології: такі як Wi-Fi, Bluetooth та інші бездротові технології, які надають користувачам можливість отримувати доступ до мережі.

Все це реалізується з урахуванням важливої безперервності бізнесу на рівні доступу до мережі.

Для розуміння вкладення цієї концепції: SD-LAN представляє собою систему, яка контролюється програмами та правилами, і вона відрізняє апаратний та програмний рівні, створюючи мережі, які автоматично організуються та централізовано управляються. Ці мережі прості у використанні, інтеграції та масштабуванні [11].

Використання SD-LAN надає більший контроль над комп'ютерною SDN-мережі аж до рівня застосунків та дозволяє отримати глибше розуміння продуктивності та використання мережі.

Завдяки архітектурі SD-LAN можна значно легше налаштувати комутатори для керування локальними мережами, впровадити віртуалізацію локальної мережі та застосовувати політику безпеки. Ця автоматизована функція спрощує операції, зменшує витрати та використовує мережу WAN і LAN для забезпечення безпечного підключення.

Архітектура SD-WAN та традиційний підхід до організації міжмережевої взаємодії

Зазвичай, під глобальною мережею (Wide Area Network, WAN) розуміють телекомунікаційну структуру, яка з'єднує різні локальні комп'ютерні мережі. Ця структура використовує загальний протокол зв'язку і методи обміну даними [15].

На відміну від локальних мереж, глобальні мережі мають більш складну топологію та структуру. Основою для передавання даних у WAN є комутаційні вузли, які сполучені між собою каналами передавального середовища. Місце та кількість таких вузлів обирається так, щоб забезпечити необхідну пропускну здатність для передавання даних з мінімальними витратами. Канали передавання даних призначені для передавання дискретної інформації у вигляді даних. Для надійної передавання інформації ставляться високі вимоги до якості передавання даних.

У WAN всю роботу виконує комунікаційний сервер, і зазвичай використовується декілька таких виділених серверів. У великих мережах може бути кілька файл-серверів, які виступають як сховище для даних, оскільки у таких мережах потрібно зберігати великі обсяги інформації та забезпечувати ефективний доступ до неї з боку робочих станцій. У WAN зазвичай підключено велику кількість робочих станцій. Для цього часто використовуються спеціальні сервери доступу, які дозволяють ефективно підключати багато робочих станцій до комп'ютерної мережі. Важливо також забезпечити потрібну пропускну спроможність для передавання даних в мережі, при цьому заощаджуючи ресурси. Таким чином, кількість і розташування вузлів комутації обираються так, щоб відповідати цим вимогам [14].

Для підключення віддалених комп'ютерів до WAN використовуються різні засоби зв'язку, такі як оптичні волоконні кабелі, телефонні лінії, супутниковий та радіозв'язок. Спосіб приєднання конкретного комп'ютера до WAN впливає на швидкість та безпеку передавання даних до цього комп'ютера в глобальній мережі.

У WAN можуть бути об'єднані локальні мережі, які працюють за різними протоколами. Для забезпечення взаємодії протоколів у таких випадках використовують спеціальні засоби, які називаються шлюзами. Шлюзи можуть бути апаратними або програмними.

Існують кілька основних способів підключення до WAN:

1) Комутоване з'єднання: використовуємо телефонні лінії для передавання даних. Для організації зв'язку необхідно мати модем, який перетворює цифровий комп'ютерний сигнал на формат, придатний для передавання через телефонну лінію і навпаки. Підключення до глобальної мережі за допомогою комутованого з'єднання є епізодичним, тобто користувач приєднується до мережі лише тоді, коли це необхідно. Нині цей спосіб комутації застосовується досить рідко.

2) Безперервне з'єднання: використовуємо окремий кабель або виділену лінію для зв'язку з провайдером. Цей метод зазвичай є безпечним і швидким, але він може бути вартісним, особливо якщо провайдер розташований на великій відстані від користувача.

3) З'єднання за допомогою супутникового та радіо-зв'язку: використання супутникового або радіо-зв'язку для підключення до глобальної мережі. Він може бути дуже швидким, але є дорогим і вимагає спеціального обладнання, наприклад, супутникової антени. Крім того, він може бути вразливим до атмосферних і природних впливів.

Ці різні способи підключення мають свої переваги і недоліки, і вибір залежить від конкретних

потреб та умов користувача.

SDN-мережірована глобальна мережа (SD-WAN) забезпечує контроль за фізичними та віртуальними компонентами глобальної мережі. Важливо відзначити, що багато з технологій, що складають SD-WAN, не є новими, але представляють собою комбінацію методів агрегації, централізованого управління та динамічного розподілу пропускної здатності мережі між точками підключення.

За словами аналітика Gartner Ендрю Лернера, який вивчає ринок SD-WAN, привабливими перевагами цієї технології є простота впровадження, централізована керуваність та економія витрат. За його оцінками, впровадження SD-WAN може коштувати приблизно в два з половиною рази менше, ніж традиційна архітектура глобальної мережі [16].

З іншого боку, SD-LAN використовує складні технології, такі як мережевий аналіз, маршрутизація, кількісний аналіз, аутентифікація та захист від зовнішнього втручання, для вирішення складних завдань. Однак це надає IT-відділам можливість працювати швидше та більш прогресивно.

SD-WAN також надає можливість гнучко керувати мережею, одночасно зберігаючи централізовані задалегідь визначені корпоративні політики, які контролюють маршрутизацію додатків. Це дає можливість визначити, які програми працюють через WAN, і встановлювати політики щодо їх пріоритету та використання.

Крім того, SD-WAN використовує динамічний вибір WAN для оптимальної маршрутизації цих додатків через шляхи з найвищою продуктивністю. Також, за допомогою SD-WAN можна використовувати кілька доступних каналів у конфігурації «active/active» для балансування навантаження та автоматичного відновлення після невеликого або повного відмови. Весь трафік між різними місцями проходить через динамічні, повністю зашифровані тунелі та може бути сегментованим, що забезпечує високий рівень безпеки.

Семантична модель SDN та схему розподілу потоків трафіку в SDN

Комп'ютерній SDN-мережі нині є надважливим інструментом управління великих обсягів даних із централізованим управлінням. Технологія SDN дозволяє ефективно керувати значним трафіком в мережах, що відповідають стандартам.

Завдяки ПЗ, яке можна використовувати на рівні застосунків SDN-мереж, вирішується багато задач та проблем. Воно надає можливість управляти та автоматизувати процеси та інтегрувати додаткові моделі та функції, що можуть сприяти зниженню витрат та покращенню характеристик мережі SDN.

Такий підхід має свої обмеження, включаючи недостатню надійність та високу ціну, що впливає з архітектури «клієнт-сервер» або її централізованого характеру. Деякі мережі є гетерогенними, і SDN може допомогти покращити керування цими мережами та прискорити впровадження обладнання різних виробників. Однак це може ускладнювати роботу персоналу та робити обслуговування мережі складним та дорогим завданням.

Архітектура SDN-мереж базується на ієрархічній системі передавання трафіку, де процеси управління контролером SDN керують комутаторами Open vSwitch (OvS) та таблицею переадресації. В даній архітектурі виникає залежність рівнів одного від одного, що може призводити до нестабільності в з'єднанні між цими рівнями. Однак варто зауважити, що така архітектура демонструє покращену ефективність, і головне завдання полягає в забезпеченні надійності та розробці моделі для резервування та розподілу слабких частин системи.

У мобільній мережі зі структурою, побудованою на класичній IP-адресації, кожен елемент функціонує самостійно, що призводить до децентралізованої структури і, більшої надійності. Однак IP-мережа має свої обмеження, такі як менша ефективність та менш динамічна система управління, що робить її менш підходящою для майбутніх мереж 5G.

Слід зауважити, що розробка SDN-мережі «з нуля» може бути дорогою і непрактичною, оскільки зупинка роботи існуючої інфраструктури надто складна. У такому контексті мережа OpenFlow набула популярності, оскільки можна розгорнути її поверх вже існуючої інфраструктури та розвивати її як окремий «налаштований шар» (Overlay).

На моделі SDN (рис. 2) можна побачити, що взаємодія структурована таким чином, що контролер, з'єднаний з кожним блоком, може керувати кожним блоком окремо та безпосередньо отримувати показники напружаму.

Інформаційні процеси інфраструктури сучасної SDN мережі

Процеси передавання даних в централізованих мережах відрізняються від процесів передавання трафіку в децентралізованих мережах, а саме основна взаємодія централізованих процесів проходить за допомогою сервера або групи серверів, відповідаючи кожен за свої задачі. В централізованій мережі або, якщо мова йде про мережу SDN, взаємодія керується сервером. Простий приклад даної системи – клієнт-серверна архітектура мережі. На рисунку 2, б зображена схема розподілу потоків трафіку в комп'ютерній мережі.

Треба зауважити, що SDN відокремлює сервісний трафік від трафіку користувачів, тому обчислювальної потужності треба набагато менше ніж для роботи з величезними масивами, в яких капсульовано користувацький і сервісний трафік. Варто також додати, що смуга передавання для кожного користувача в системі SDN на одного клієнта рівна тому, скільки цьому користувачеві потрібно, що цим самим робить роботу мережі більш оптимальною.

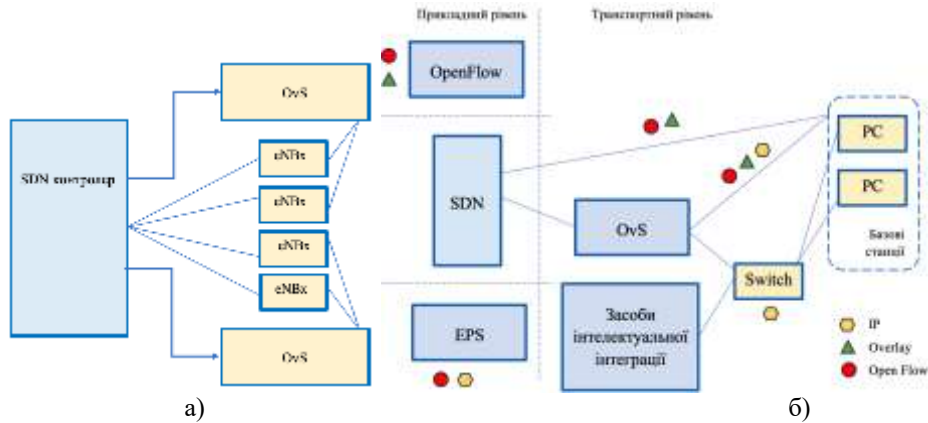


Рисунок 2 – Семантична модель SDN (а) та схема розподілу потоків трафіку (б)

Запропонувати спосіб розрахунку надійності мережі

Для розрахунку показників надійності спочатку треба абстрагувати архітектуру до блочного рівня, як показано на рисунку 3, де а) це децентралізована мережа (класична IP-мережа), б) це централізована мережа (схема SDN), P – довільний показник надійності.

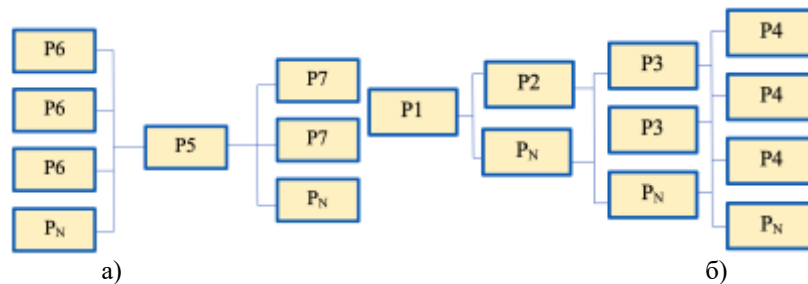


Рисунок 3 – Блоки архітектури під час розрахунку надійності мережі, де а) – централізована мережа SDN, б) – децентралізована мережа IP

Ідея способу розрахунку надійності – можливість прорахувати вразливості аналітичними виразами та застосувати відомі підходи для підвищення потрібних показників (наприклад, методика резервування або дублювання) даної системи (1).

$$P\{\sum_{i=1}^n A_i\} = 1 - P\{\prod_{i=1}^n \bar{A}_i\} \quad (1)$$

Ймовірність події A – P{A} визначається частотою її появи в серії випробувань і описується (2):

$$F_A = \frac{n_A}{N} \xrightarrow{N \rightarrow \infty} P\{A\}, \quad (2)$$

де: \bar{A} – деяка подія; N – загальне число дослідів; n_A – число появи події \bar{A} ; P{A} – ймовірність події \bar{A} .

Ймовірність достовірної події: $P\{A_{\partial}\} = \frac{n_a}{N} = \frac{N}{N} = 1$. Ймовірність неможливої події: $P\{A_i\} = \frac{i_i}{N} = \frac{0}{N} = 0$. Ймовірність випадкової події може змінюватись в межах $0 \leq P\{A\} \leq 1$, але ніколи $P\{A\} > 1$. Для повної групи подій: $P\{A\} + P\{\bar{A}\} = 1$. Ймовірність складної події може бути представлена через суму і добуток простих подій. Добутком подій $A_1 \cdot A_2 \cdot A_3 \cdot \dots \cdot A_n$ називається складна подія, яка складається з того, що відбувається і подія $A_1, A_2, A_3, \dots, A_n$, тобто відбуваються всі події. Така подія позначається так (3-4):

$$A_1 \cdot A_2 \cdot A_3 \cdot \dots \cdot A_n = \prod_{i=1}^n A_i; \quad (3)$$

$$P\{\prod_{i=1}^n A_i\} = \prod_{i=1}^n P\{A_i\} \quad (4)$$

Сумою подій $A_1 + A_2 + A_3 + \dots + A_n$ називається складна подія, яка має на увазі те, що відбудеться, або подія $A_1, A_2, A_3, \dots, A_n$, тобто виконуватиметься хоча б одна з подій. Сума подій позначається $A_1 + A_2 + A_3 + \dots + A_n = \sum_{i=1}^n A_i$ таким виразом.

Модель взаємодії мережевої ОС із комп'ютерною SDN-мережею та спосіб оброблення трафіку

Модель взаємодії мережевої операційної системи та SDN. На прикладному рівні можна розглядати операційні системи (ОС) хостів (комп'ютерів) на трьох рівнях (див. рис. 3, а). Перший рівень – це сама ОС, яка є посередником, контролюючи доступ додатків до базового апаратного забезпечення (АЗ). ОС також надає основні служби, які сприяють цьому процесу і відповідає за низькорівневе управління АЗ [17].

Модель SDN-мереж має схожість з моделлю операційної системи (див. рис. 3, б). Основна відмінність полягає в тому, що на середньому рівні розташована мережева операційна система (МОС), іншими словами, SDN-контролер. МОС зазвичай надає базові служби, які допомагають у взаємодії з хостами мережі та забезпечують програмований інтерфейс для мережевих додатків [16-17]. Мережеві пристрої тут розташовані замість АЗ і виконують оброблення мережевого трафіку. Ці пристрої отримують пакети та виконують різні операції, такі як відкидання пакету, зміна заголовків, відправка пакетів через один чи декілька інтерфейсів та оновлення лічильників.

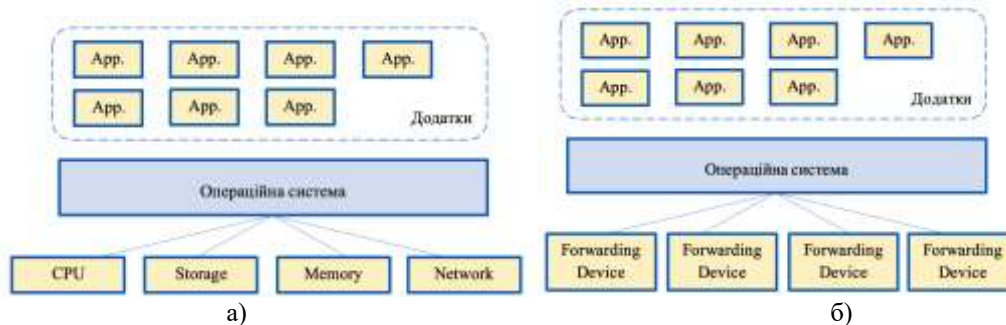


Рисунок 3 – Модель операційної системи з та без взаємодії з SDN

Інструкції для оброблення пакетів надходять від SDN-контролера. На вищому рівні розташовані мережеві додатки, які спеціалізуються на мережевій функціональності та виконують різноманітні завдання для оптимізації мережі. Мережеві додатки грають ключову роль у реалізації SDN та можуть виконувати різні функції для покращення продуктивності та управління мережею. Застосування переваг такої комбінації моделей, дозволяє відстежувати рух трафіку в мережах і значно полегшує перехід від традиційної архітектури до SDN.

Спосіб оброблення трафіку в SDN

Безпека потоків пакетів у SDN-мережі. Аналіз заголовків пакетів визначає подальші дії для оброблення пакетів при їх надходженні на мережевий пристрій, що під контролем SDN. Мережевий пристрій може відразу мати дані про етапи та спосіб оброблення пакета, або, у випадку необхідності, звернутися до SDN-контролера для отримання таких інструкцій. Мережеві додатки на SDN-контролері будуть інструктувати, які дії слід виконувати з конкретним пакетом і передають цю інформацію з інструкціями мережевим пристроям пересилання (див. рис. 4, а).

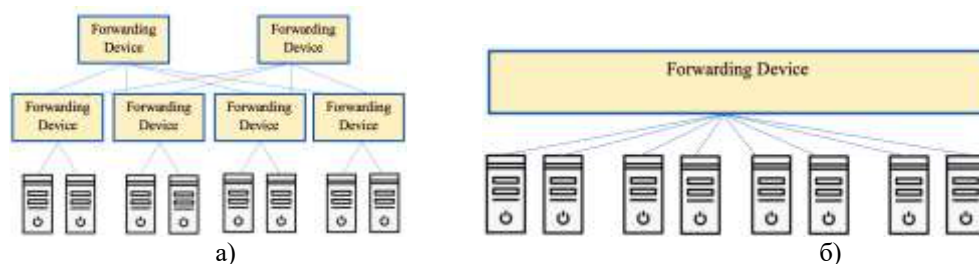


Рисунок 4 – Оброблення трафіку на рівні абстрактної мережі (а) на рівні додатків (б)

Пристрої пересилання, в свою чергу, діють відповідно до отриманих вказівок. Важливою є можливість кешування інструкцій пристроєм пересилання, що дозволяє зменшити навантаження на

SDN-контролер і прискорити оброблення мережевого трафіку. Аналогічний процес розгортається по маршруту від одного мережевого пристрою до іншого, доки пакет не досягне свого пункту призначення. Надалі, новосформовані пакети можуть проходити через мережу без звернення до SDN-контролера. Контролер SDN здатний створити абстрактну або спрощену модель мережі для мережевих додатків, які використовують цю інформацію для прийняття важливих рішень щодо впровадження мережевих політик.

Безпека мережевих додатків. Мережевий додаток може бути осторонь деталей щодо різних маршрутів, які пакети подолали б у мережі. SDN-контролер може створити абстракцію всієї мережі, розглядаючи її як великий комутатор (рис. 4, б). Ідеальною абстракцією пересилання була б така, яка дозволяла б мережевим додаткам (керуючим програмам) визначати бажану поведінку пересилання, не вдаючись до деталей, пов'язаних з конкретним обладнанням. Один із шляхів до реалізації цієї ідеї – це OpenFlow, який можна порівняти з «драйвером пристрою» у мережевій операційній системі.

Безпекова модель та прототип комп'ютерної SDN-мережі.

Компоненти безпекової моделі SDN. Безпекові складові в моделі SDN) можна уявити як композицію різних рівнів, кожен з яких виконує свої специфічні функції. Більшість з цих складових завжди присутні в будь-якій реалізації SDN, включно з: мережевими додатками; інтерфейсами додатків, таких як Java API і NorthBound (REST Conf); SDN-контролером, який містить служби топології, інвентаризації, статистики та хост-трекери; SouthBound інтерфейсами, які можуть містити протоколи, такі як OpenFlow, OVSDDB, NETCONF і SNMP; комутаційними пристроями.

Модель мережі із гнучкими ресурсами. Гнучкий підхід до створення мережі фокусується на швидких та адаптивних змінах. Ці невеликі та регулярні зміни сприяють підвищенню продуктивності додатків, збільшенню безпеки даних і сприяють швидкому розгортанню додатків та сервісів.

Мережа SDN дозволяє ефективно розділяти мережу для різних видів робочих завдань (див. рис. 3.6). Цей розподіл може бути реалізований на різних рівнях. Наприклад, на рівні SouthBound інтерфейсу трафік може бути спрямований до повністю окремих SDN-контролерів.

На рівні NorthBound інтерфейсу різні види трафіку можуть бути оброблені різними мережевими додатками або різними способами цими ж додатками. Це можливість розглядати мережу як ресурс, що використовується різними клієнтами або завданнями і дозволяє кожному клієнту або завданню використовувати мережу відповідно потребам.

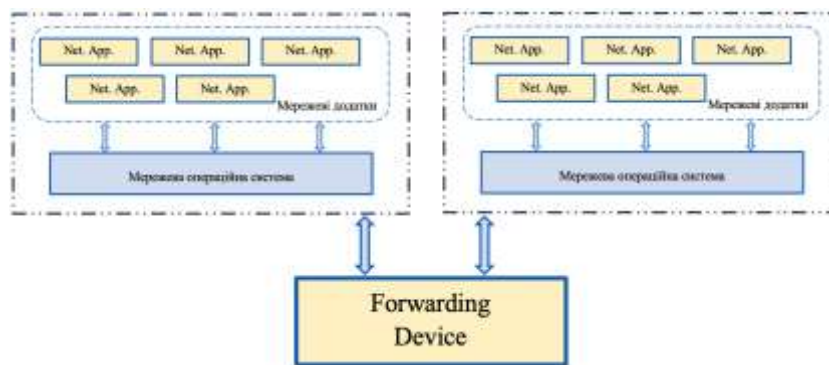


Рисунок 5 – Розподіл мережі для різних робочих навантажень

Модель відмовостійкості мережі. Висока надійність SDN-мережі досягається завдяки швидкому виявленню і усуненню відмов, причому це відбувається протягом короткого періоду. Є два основних підходи до забезпечення надійності в SDN-мережах: 1) захисне перемикання (резервування) та 2) відновлення (ремаршрутизація).

Зазвичай SDN-контролери вважаються централізованими. У реальних мережах користувачі не повинні залежати від конкретного фізичного контролера SDN, що створює єдину точку відмови для всієї мережі. Крім того, існують питання масштабування. Існують різні методи забезпечення високої доступності та масштабованості в SDN-мережах.

Один з таких методів – це кластеризація або групування (див. рис. 6). Цей підхід добре відомий в області серверів баз даних. Основна ідея полягає в тому, щоб мати кластер систем, які можуть розподіляти обчислювальні завдання балансовано, замість єдиної системи. Це забезпечує високу доступність, оскільки можуть бути відмови в окремих системах, але інші все ще можуть виконувати завдання. Крім того, цей метод забезпечує масштабованість, оскільки декілька систем можуть обробляти запити.

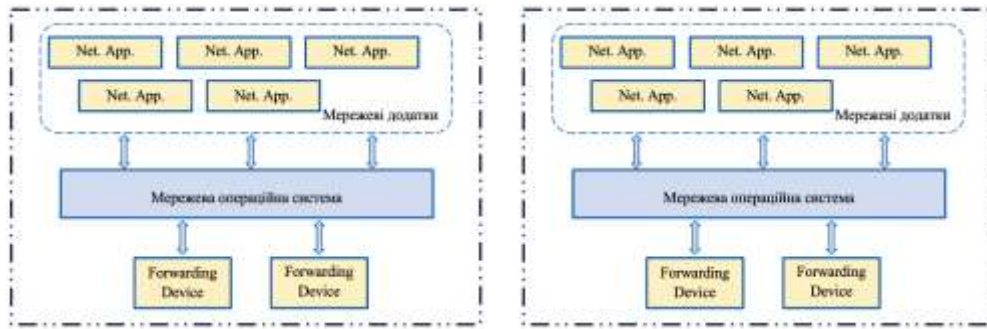


Рисунок 6 – Кластеризація мережі

Додатково є можливість поділити якусь спеціалізовану частину мережі можна на різні регіони, де кожен регіон управляється власним контролером SDN (див. рис. 7). Різні регіони можуть взаємодіяти між собою, обмінюючи інформацію за потреби через протокол East-West.



Рисунок 7 – Ієрархічна кластеризація мережі

Отож, контролери SDN можуть бути організовані в ієрархічній структурі. Таким чином, з'являються контролери вищого рівня із спрощеною абстракцією мережі та контролери нижчого рівня, що розташовані ближче до мережевих пристроїв пересилання.

В розробленій мережі (рис. 8) для 9 пристроїв мережі, поділених на групи, виконані часові заміри (рис. 9,а) і середнє значення зменшення часу налаштування зменшилося приблизно у 10 разів (рис. 9,б).

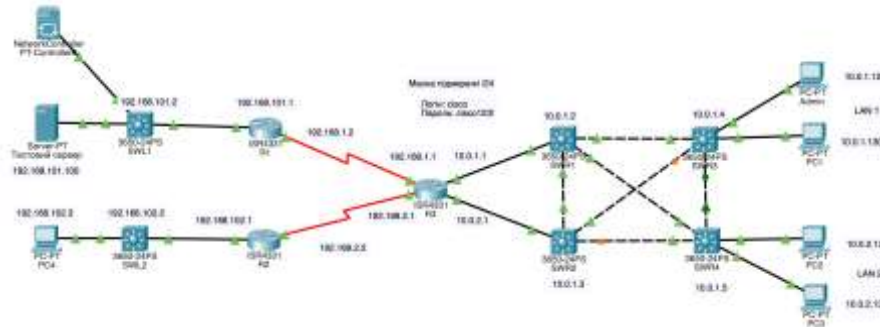


Рисунок 8 – Мережева конфігурація

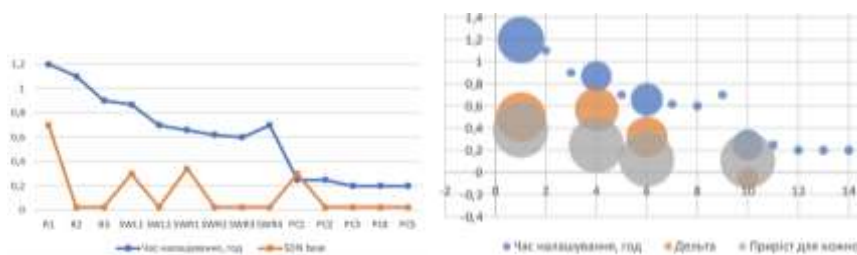


Рисунок 9 – Значення часу налаштування пристроїв у кожній з груп без (а) та з SND (б)

Очевидно, що застосування контролерів для програмного керування мережами є доцільним та прогресивним в умовах постійного розширення мережі, зміни кількості мережевих пристроїв чи хостів.

Висновки

Потреба у аналізі та вдосконаленні методів та засобів захисту інформаційних та інших ресурсів в комп'ютерній SDN- мережі стала основою для даного дослідження. У роботі досягнуто підвищення рівня інформаційної безпеки ресурсів SDN-мережі за рахунок: 1) зменшення часу втручання у мережу; 2) та із одночасним застосування вдосконаленого способу оброблення трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання.

Загалом результати полягають у такому:

- Вдосконалено модель взаємодії мережевої операційної системи та програмно-керованої мережі, що дає можливість відстежувати процеси, що відбуваються в мережах з ресурсами компанії, та забезпечує ефективний контроль і безпеку цих ресурсів;
- Вдосконалено спосіб передавання трафіку на основі мережевої безпеки потоку пакетів, що дозволяє бажану мережевим додатком поведінку пересилання;
- Вдосконалено модель відмовостійкості мережі за рахунок висхідного представлення компонентів безпеки моделі SDN.

Список літератури

- [1] Todd M. S., Rahman S. M. Complete Network Security Protection for Sme's Within Limited Resources. *International Journal of Network Security & Its Applications (IJNSA)*. 2013. Vol. 5, no. 6.
- [2] Alqahtani H. S. Latest Trends and Future Directions of Cyber Security Information Systems. *Journal of Information Engineering and Applications*. 2016. Vol. 6, no. 11.
- [3] Троян С. О. Захист інформаційних ресурсів. Умань, 2012. 120 с.
- [4] Медяник А. Інформаційна безпека та методи захисту інформації. 2020.
- [5] Simmons A. Software-Defined Networking (SDN) Explained. *Dgtl Infra*. URL: <https://dgtlinfra.com/software-defined-networking-sdn/>.
- [6] Ot A. The Software-Defined Networking (SDN) Market in 2022 | Enterprise Storage Forum. *Enterprise Storage Forum*. URL: <https://www.enterprisestorageforum.com/networking/software-defined-networking-market/>.
- [7] Software-Defined Networking: Challenges and research opportunities for Future Internet / A. Hakiri et al. *Computer Networks*. 2014. Vol. 75. P. 453–471. URL: <https://doi.org/10.1016/j.comnet.2014.10.015>.
- [8] Ashton, Metzler. The Business Case for Deploying SDN in Enterprise Networks. *Leverage technology & talent for success*.
- [9] Gray K., Nadeau T. D. *SDN: Software Defined Networks*. Sebastopol : O'Reilly Media, Inc, 2013.
- [10] Brief About What does The Future hold for Software Defined Networking (SDN). *YourTechDiet*. URL: <https://yourtechdiet.com/blogs/sdn-future/>.
- [11] SD-LAN vs LAN – What Are The Key Differences?. *Extreme Marketing Team*. URL: <https://www.extremenetworks.com/extreme-networks-blog/sd-lan-vs-lan-what-are-the-key-differences/>.
- [12] Селюков О. В. Забезпечення стандартизації параметрів управління для SDN архітектури при надійній передаванні інформації / О. В. Селюков, Ю. В. Хмельницький, В.М. Лоза, Р.В. Бойко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса. – 2018. – С. 134–145.
- [13] Управління телекомунікаціями із застосуванням новітніх технологій / Кривуца, Стеклов, Беркман та ін.], 2007. – 384 с. – (Підручник для ВНЗ).
- [14] Комп'ютерні мережі: навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2022. – 228 с.
- [15] Комп'ютерні мережі:[навчальний посібник] / А. Г.Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів: Магнолія 2006, 2013. – 256 с.
- [16] Коробейнікова Т.І. Розгляд архітектури програмно-керованих мереж / Коробейнікова Т.І., Калько Т.С., Лужецька Н. М. // *International scientific journal «Grail of Science»* – 2023. – № 23 (May, 2023). – С. 228–237. ISSN: 2710–3056. ISBN 979-8-88955-791-3. <https://doi.org/10.36074/grail-of-science.09.06.2023.36>
- [17] Кононенко А. В. Концепція software-defined-networking та основні принципи openflow / А. В. Кононенко, І. М. Кучма, М. В. Перетяцько, В. О. Кацалап, Д. О. Размислов // *Наукові записки Українського науково-дослідного інституту зв'язку*. – 2018. - № 3. – С. 51-58.
- [18] Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп'ютерна інженерія 2021: - №1 (50). – С. 31–35
- [19] Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // *Інформаційні технології та комп'ютерна інженерія*. – 2023. – № 1. – С. 66-74.

References

- [1] Todd M. S., Rahman S. M. Complete Network Security Protection for Sme's Within Limited Resources. International Journal of Network Security & Its Applications (IJNSA). 2013. Vol. 5, no. 6.
- [2] Alqahtani H. S. Latest Trends and Future Directions of Cyber Security Information Systems. Journal of Information Engineering and Applications. 2016. Vol. 6, no. 11.
- [3] Troyan S. O. Zakhyst informatsiynykh resursiv. Uman', 2012. 120 s.
- [4] Medyanyk A. Informatsiyna bezpeka ta metody zakhystu informatsiyi. 2020.
- [5] Simmons A. Software-Defined Networking (SDN) Explained. Dgtl Infra. URL: <https://dgtlinfra.com/software-defined-networking-sdn/>.
- [6] Ot A. The Software-Defined Networking (SDN) Market in 2022 | Enterprise Storage Forum. Enterprise Storage Forum. URL: <https://www.enterprisestorageforum.com/networking/software-defined-networking-market/>.
- [7] Software-Defined Networking: Challenges and research opportunities for Future Internet / A. Hakiri et al. Computer Networks. 2014. Vol. 75. P. 453–471. URL: <https://doi.org/10.1016/j.comnet.2014.10.015>.
- [8] Ashton, Metzler. The Business Case for Deploying SDN in Enterprise Networks. Leverage technology & talent for success.
- [9] Gray K., Nadeau T. D. SDN: Software Defined Networks. Sebastopol : O'Reilly Media, Inc, 2013.
- [10] Brief About What does The Future hold for Software Defined Networking (SDN). YourTechDiet. URL: <https://yourtechdiet.com/blogs/sdn-future/>.
- [11] SD-LAN vs LAN – What Are The Key Differences?. Extreme Marketing Team. URL: <https://www.extremenetworks.com/extreme-networks-blog/sd-lan-vs-lan-what-are-the-key-differences/>.
- [12] Selyukov O. V. Zabezpechennya standartyzatsiyi parametriv upravlinnya dlya SDN arkhitektury pry nadiyniyi peredavannya informatsiyi / O. V. Selyukov, YU. V. Khmel'nyts'kyy, V.M. Loza, R.V. Boyko // Zbirnyk naukovykh prats' Viys'kovoho instytutu Kyiv's'koho natsional'noho universytetu imeni Tarasa. – 2018. – S. 134–145.
- [13] Upravlinnya telekomunikatsiyamy iz zastosuvannam novitnikh tekhnolohiy / Kryvutsa, Steklov, Berkman ta in.], 2007. – 384 s. – (Pidruchnyk dlya VNZ).
- [14] Komp'yuterni merezhi: navch. posibnyk / T. I. Korobeŭnikova, S. M. Zakharchenko. – L'viv: Vydavnytstvo L'viv's'koi politekhniki, 2022. – 228 s.
- [15] Komp'yuterni merezhi:[navchal'nyy posibnyk] / A. H.Myktyshyn, M. M. Mytnyk, P. D. Stukhlyak, V. V. Pasichnyk. – L'viv: Mahnoliya 2006, 2013. – 256 s.
- [16] Korobeynikova T.I. Roz'hlyad arkhitektury prohramno-kerovanykh merezh / Korobeynikova T.I., Kal'ko T.S., Luzhets'ka N. M. // International scientific journal «Grail of Science» – 2023. – № 23 (May, 2023). – S. 228–237. ISSN: 2710–3056. ISBN 979-8-88955-791-3. <https://doi.org/10.36074/grail-of-science.09.06.2023.36>
- [17] Kononenko A. V. Kontsepsiya software-defined-networking ta osnovni pryntsypy openflow / A. V. Kononenko, I. M. Kuchma, M. V. Peretyat'ko, V. O. Katsalap, D. O. Razmyslov // Naukovi zapysky Ukrayins'koho naukovo-doslidnoho instytutu zv'yazku. - 2018. - № 3. - S. 51-58.
- [18] Savyts'ka L.A., Korobeynikova T.I. Udoskonalenny metod rozrobky ARI pidvyshchenoyi shvydkodiyi Informatsiyini tekhnolohiyi ta komp'yuterna inzheneriya 2021: - №1 (50). - S. 31–35
- [19] Savyts'ka L. A. Prohramnyy modul' poperedn'oho diahnostuvannya patsiyentiv na osnovi neyronnoyi merezhi Kokhonena [Tekst] / L. A. Savyts'ka, N. V. Dobovol's'ka, V. O. Kondratyuk // Informatsiyini tekhnolohiyi ta komp'yuterna inzheneriya. – 2023. – № 1. – S. 66-74.

Стаття надійшла: 20.11.2023 р.

Відомості про авторів

Савицька Людмила Анатоліївна – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця

Savytska Liudmyla – PhD, associate professor of computing engineering department, Vinnytsya national technical university, Vinnytsya

Коробейнікова Тетяна Іванівна – к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana – PhD, associate professor of information technology security department, National university "Lvivska Politechnika"

Леонт'єв Ігор Віталійович – магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця

Leontiev Ihor Vitaliyovych – magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering, Vinnytsy

Богомолів Сергій Віталійович – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, Вінниця

Bohomolov Serhii – PhD, associate professor of computing engineering department, Vinnytsya national technical university, Vinnytsya

L. Savytska, T. Korobeinikova, I. Leontiev, S. Bohomolov

METHODS AND MEANS OF PROTECTING RESOURCES IN COMPUTER SDN NETWORK

Vinnytsya national technical university, Vinnytsya

УДК 681.3:621.74:004.8

В. С. Дорошенко¹, О. Б. Янченко²

ЗАСТОСУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ДЛЯ ПРОЕКТУВАННЯ ТА 3D-ДРУКУ ЛИВАРНОЇ МОДЕЛІ З ВЕНТИЛЯЦІЙНИМИ КАНАЛАМИ В ЇЇ СТІНКАХ

¹Фізико-технологічний інститут металів та сплавів НАН України, Київ²Вінницький національний технічний університет, Вінниця

Анотація. В контексті впровадження концепції «Індустрія 4.0» цифровізація та автоматизація сьогодні стали вже не просто основою конкурентної переваги при виробництві товарів (робіт, послуг), у багатьох сферах вони сприймаються як необхідна умова організації виробничих процесів. Зокрема, завдяки цифровізації та автоматизації ливарного виробництва в Україні є можливість створення потужного потенціалу, що сприятиме відновленню країни. За рахунок розширення застосування комп'ютерних систем для проектування та 3D-друку полімерних ливарних моделей з вентиляційними каналами стала можливою розробка одного із способів лиття металу за моделями, що газифікуються (ЛГМ), з застосуванням друкованих моделей, що відповідає зростаючому тренду цифровізації та автоматизації ливарних процесів. Це стало можливим завдяки підвищенню інтенсивності евакуації продуктів газифікації друкованих моделей у ливарній формі з використанням вакууму цієї форми. Розроблений спосіб дозволяє отримати сумарну вигоду як від достатньо швидкоплинних комп'ютерно-орієнтованих 3D-процесів проектування і друку ливарної моделі, так і від короткотривалих процесів формовки та вибивки виливків завдяки використанню при ЛГМ ливарних форм з сухого піску. При цьому цифрова трансформація ЛГМ поєднується з ресурсоефективністю оборотного застосування формувальних матеріалів без зміни діючих стандартів контролю металопродукції ливарних цехів, а адаптація виробництва до адитивних технологій дозволяє за допомогою мережі Інтернет пряму взаємодію з покупцем товару, який проектується за його індивідуальним цифровим проектом. Останнє відповідає концепції «виробництво як послуга» (Маас). Також таке впровадження застосування комп'ютерних систем і нових цифрових процесів в традиційні ливарні процеси скорочує часовий розрив від створення прототипів і інструментів до масового виробництва металопродукції.

Ключові слова: комп'ютерні системи, 3D-технології, 3D-друк, разова ливарна модель, газифікація моделі, ливарне виробництво.

Abstract. In the context of the implementation of the "Industry 4.0" concept, digitalization and automation today have become not just the basis of competitive advantage in the production of goods (works, services), in many areas they are perceived as a necessary condition for the organization of production processes. In particular, thanks to the digitization and automation of foundry production in Ukraine, there is an opportunity to create a powerful potential that will contribute to the recovery of the country. Due to the expansion of the use of computer systems for the design and 3D printing of polymer foundry patterns with ventilation channels, it became possible to develop one of the methods of metal casting according to gasifying patterns (LFC) with the use of printed patterns (models), which corresponds to the growing trend of digitalization and automation of foundries processes. This became possible due to the increase in the intensity of evacuation of the products of gasification of printed patterns in the foundry mold using the vacuum of this mold. The developed method allows you to get a total benefit both from fairly fast computer-oriented 3D processes of designing and printing a foundry pattern, as well as from short-term processes of forming and punching out castings due to the use of dry sand foundry molds at LFC. At the same time, the digital transformation of LFC is combined with the resource efficiency of the reversible use of molding materials without changing the current standards of control of metal products of foundries. And the adaptation of production to additive technologies allows direct interaction with the buyer of the product, which is designed according to his individual digital project, with the help of the Internet. The latter corresponds to the concept of "manufacturing as a service" (Maas). Also, this implementation of the use of computer systems and new digital processes in traditional foundry processes shortens the time gap from the creation of prototypes and tools to the mass production of metal products.

Keywords: computer systems, 3D technologies, 3D printing, one-time foundry pattern, pattern gasification, foundry production.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-53-58>.

Вступ

В контексті впровадження концепції «Індустрія 4.0» цифровізація та автоматизація сьогодні стали вже не просто основою конкурентної переваги при виробництві товарів (робіт, послуг), у багатьох сферах вони сприймаються як необхідна умова організації виробничих процесів [1]. Інформаційні технології впроваджуються у дедалі більше галузей, що дозволяє оперативніше і точно виконувати поставлені завдання, здійснювати постійний моніторинг виробництва та бізнес-процесів, виключати зайві етапи роботи та оптимізувати її. Зокрема, завдяки цифровізації та автоматизації ливарного виробництва в Україні є можливість створення потужного потенціалу, що сприятиме відновленню країни.

Актуальність

Як одна з галузей цифровізації, 3D-друк (адитивне виробництво) з застосуванням сучасних комп'ютерних систем дозволяє змінювати як конфігурацію ливарної продукції, так і конструкцію ливарних моделей виключно за рахунок внесення змін в цифрову модель продукції без наступного переформатування виробничого базису. Серед ливарних технологій відомий «ЛГМ-процес» (Lost Foam Casting Process), який вирізняється тією характерною особливістю, що здійснюється шляхом лиття металу за разовими полімерними (піно-полімерними) ливарними моделями, які газифікуються – випаровуються в ливарній

формі одночасно з заміщенням цих моделей розплавленим металом. Цей процес має значний потенціал як до впровадження 3D-технологій, так і до створення різновидів способів з підвищенням гнучкості щодо випуску дрібносерійної, разової (зокрема кастомізованої) продукції для швидкого реагування на потреби ринку, а також в плані екологізації з наближенням до технологій, що не шкодять довкіллю.

Мета

Мета статті полягає розробці способу застосування комп'ютерних систем для проектування та 3D-друку полімерної ливарної моделі з вентиляційними каналами в її стінках та описі прикладу застосування такої моделі в ливарному процесі виготовлення металевих виливків широкою номенклатурою

Огляд відомих технічних рішень і аналіз їх недоліків

В Україні запатентовано способи 3D-друку об'ємних (тривимірних) виробів із тугоплавких матеріалів [2] з застосуванням плазмотрону, а також спосіб тривимірного друку металевого виробу [3] шляхом пошарової побудови виробу, що включає створення 3D-моделі виробу в програмі комп'ютерного (автоматизованого) моделювання (CAD), виведення її в управляючій пристрій 3D-принтера з подальшим поділом на горизонтальні шари, подачу у зону друку розплавленого модельного матеріалу з подальшим його застиганням, а як модельний матеріал використовують металевий електроіскровий електрод.

Недоліками цих двох способів являються застосування високої вартості енергоємне обладнання, що є унікальним для вітчизняних заводів. Також плавлення і друк вказаних у цих способах матеріалів і металу потребує значних витрат енергії та захисної атмосфери чи вакуумування для камери друку. Все це приблизно на порядок збільшує собівартість металовиробів порівняно з відпрацьованими ливарними способами. Також не розроблено вітчизняних стандартів сертифікації друківаних металевих та виробів із тугоплавких матеріалів щодо відповідності марки їх матеріалу діючим нормам.

Прикладом іншого і значно простішого напряму впровадження 3D-технологій в ливарне виробництво є 3D-друк разових полімерних ливарних моделей для ЛГМ-процесу, за якими виконують лиття металу методом їх газифікації у вакуумованих ливарних формах з сипкого піску [4]. В традиційній технології ЛГМ застосовують моделі з пінополістиролу (ППС) як разове оснащення, на заміну якого останнім часом завдяки дослідженням прагнуть впровадити 3D-друковані полімерні моделі. Такі полімерні друковані ливарні моделі призначені для формування в піску ливарної форми і газифікації їх при заливанні цієї форми металом. При цьому, оскільки вилівок утворюється при випаруванні (газифікованій) моделі, то контроль якості затверділого вилівка та відповідність марки його металу не відрізняється від традиційно застосовуваних, відпрацьованих і унормованих ливарних операцій в розрізі діючих стандартів.

Розв'язання задачі

В розробленому і описаному нижче способі [5], порівняно з традиційними різновидами ЛГМ-процесу, значно (в рази або навіть на порядок) скорочується тривалість виготовлення разової друкованої ливарної моделі. Підготовка до 3D-друку з застосуванням комп'ютерної системи полягає в тому, що в цифровому кресленні металеві деталі на персональному комп'ютері відображають ливарну технологію, цим самим це креслення «перетворюють» в креслення ливарної моделі, а в ньому додатково креслять вентиляційні газивидні канали в стінках ливарної моделі для їх виконання на етапі друкуванні цієї моделі. За готовою друкованою моделлю виконують досить швидко (протягом хвилини) формовку цієї моделі в сипкому піску з подальшим застосуванням традиційних операцій ЛГМ-процесу, недорогого за вартістю вилитої металопродукції (порівняно зі способами [1, 2]).

Розглянемо подробиці способу [5]. В цілому, застосування друкованих моделей дає суттєвий вииграш від значного скорочення тривалості підготовки виробництва нової продукції, таке виробництво не потребує оснастки (прес-форм) для виготовлення ливарних моделей, яка є нерідко складною і дорогою за вартістю. Це дозволяє розширити геометрію виливків, друкувати разові моделі навіть неможливої раніше конфігурації з високою чистотою поверхні, змінюючи дизайн металовиробу лише за рахунок внесення змін в його цифрову модель в комп'ютерній системі без будь-якої зміни обладнання в ливарному цеху. Швидкий автоматизований 3D-друк з цифрових даних ливарних моделей (навіть разової конструкції за індивідуальним замовленням або складної геометричної конфігурації) і по ним - металевих виливків все більше є предметом досліджень провідних ливарних і машинобудівних компаній світу і відповідає загальному напрямку цифровізації ливарного виробництва.

Проте, проблема полягає в тому, що друковані полімерні моделі мають більшу густину і, відповідно, газотвірність, ніж традиційні моделі з ППС, тому такі причини поки не дозволяють при ЛГМ отримувати в промислових масштабах вилівки стабільної якості відомими способами за друкованими моделями і, отже, технологія лиття за такими моделями зараз знаходиться лише на стадії експериментального випробовування і адаптивної трансформації ЛГМ-процесу до застосування в ньому друкованих ливарних моделей. Сьогодні основні недоліки полягають в тому, що надмірний тиск газів від газифікації більш масивної (проти моделі з ППС) друкованої моделі може призвести як до викидів металу з ливарної системи, так і до гальмування заповнення ним форми з утворенням браку виливків по недоливам. А також сучасний друкований матеріал моделей дає більший вуглецевий (коковий чи зольний) зали-

шок, ніж ППС, що також негативно впливає на якість виливків.

В способі [4] задача зниження надмірного тиску газів від газифікації моделі з виведенням їх з піщаної форми вирішується шляхом використання оболонкових порожнистих друківаних ливарних моделей, стінки яких мають поєднані між собою порожнини з внутрішніми тонкостінними каркасами чи розпірками. Ці порожнини зменшують масу (та газовиділення) моделей і поєднані з трубками, якими гази від газифікації цих моделей виводять за межі ливарної форми. Таке сполучення порожнин, що грають роль каналів, моделей з повітрям цеху зменшує газовий тиск від газифікації моделей до атмосферного. В цьому способі завдяки окисленню (спаленню) газів від моделі на поверхні форми зроблено акцент на екологізації ЛГМ з наближенням до технологій, що не шкодять довкіллю.

На жаль, порожнисті моделі [4] мають ряд таких недоліків, як можливість застосування лише для достатньо товстостінних виливків, адже дві протилежні стінки навколо порожнини повинні бути достатньо міцними і щільними, щоб запобігти їх деформації при засипанні в форму піску і вібрації форми. Такі ливарні моделі практично неможливо видрукувати цільними, а треба склеювати з оболонок, вони придатні для виливків обмеженої номенклатури, таких як крупні лопати тощо. Програми друкування оболонкових порожнистих моделей (порівняно з друкуванням цільних) більш складні, друкування потребує високошвидкісних принтерів, а збирання з установкою внутрішніх тонкостінних каркасів чи розпірок в порожнинах моделей – механічної обробки, ручної праці і прецизійного контролю кінцевої геометрії моделі при склейці оболонок і серцевини.

Тому з метою зниження витрат на виготовлення цільної 3D-друкованої ливарної моделі і забезпечення її газовідвідними вентканалами застосували досі незадіяний при друкуванні моделі потенціал комп'ютерної системи. За допомогою апаратного комплексу персонального комп'ютера, що забезпечує введення, оброблення, збереження та виведення інформації, в стінках ливарної моделі на цифровому кресленні її конструкції були внесені вентканали для виводу з моделі газів протягом всього періоду її газифікації при русі металу вздовж цих каналів. Це дає перспективу значного розширення номенклатури виробництва, в тому числі тонкостінних виливків, а також сприяє інтенсифікації виводу продуктів газифікації з ливарної форми за допомогою цих каналів і знімає перешкоди застосування друківаних моделей для ЛГМ, пов'язаної з ростом виділення продуктів газифікації.

На нинішньому початковому етапі застосування друківаних ливарних моделей цифрове 3D-креслення металовиробу створює конструктор в комп'ютерній системі CAD і передає виробникові для друку, або виробник сам може створити таке 3D-креслення (наприклад, скануванням готового виробу-прототипу). Потім 3D-креслення (3D-модель) цього виробу в комп'ютерній системі CAD доповнюють змінами (наносять ливарну технологію) з урахування усадки металу відповідно до розмірів ливарної моделі, припусків на механічну обробку тощо, конвертують файл в формат STL для 3D-друку і друкують цю ливарну модель. Оскільки 3D-друк лише починає застосовуватись для ЛГМ, то вентиляційні канали в ливарній моделі вздовж її стінок по мірі поступового заміщення моделі металом не друкували. Такої інформації не виявлено. В традиційній для ЛГМ моделі з ППС за потреби вентиляційні канали виконували механічним способом. При друкуванні ливарних моделей складної геометричної форми та тонкостінних конструкцій виконати вздовж її стінок канали (навіть з багатьма згинами) найпростіше при її друкуванні за кресленням цифрової 3D-моделі, в якому згідно розробленому способу [5] слід відобразити ці канали.

Таким чином, в перелік операцій процесу 3D-друку ливарної моделі, що складає створення 3D-моделі у програмі CAD, виведення цієї 3D-моделі у форматі STL в управляючий пристрій 3D-принтера з поділом на горизонтальні шари та пошарове адитивне вирощування ливарної моделі з полімерного термопластичного матеріалу цим принтером, нами внесено операцію відображення вентиляційних каналів на кресленні цифрової моделі і отриманні їх у друкованій ливарній моделі для виводу газів в напрямку руху розплавленого металу при газифікації ливарної моделі в піщаній ливарній формі.

Після 3D-друку вентиляційної ливарної моделі за цією моделлю виготовляється ливарна форма з сухого піску, яка заливається розплавленим металом при її вакуумуванні і газифікації теплом металу ливарної моделі з відведенням газових продуктів газифікації крізь газовідвідні вентканали. Для виходу газів у пори піску форми ці канали продовжують полімерними трубками, вихідні кінці яких закривають газопроникним вентами, що не пропускають пісок. Крім того, в разі застосування вставок з ППС в комплекті з 3D-друкованою ливарною моделлю канали для виводу газів можуть друкувати по стику цих вставок з друкованою частиною ливарної моделі шляхом друку борозенок в ній. Також полімерні трубки застосовували зі стінками достатньої міцності для запобігання їх деформації при дії на них вакууму в піску форми, або з цією ж метою вставляли в них металевий дріт у вигляді спіралі, або газопроникні пробки з піщаної суміші, які служили вентами.

Приклад проектування ливарної друкованої моделі для розробленого нами способу проілюстровано на рис. 1, а – в, де на рис. 1, а показано варіанти конструкцій зубчастих валків 1, для лиття яких застосовано новий спосіб. Це деталі соломорізки складної геометричної форми. Поруч з одним з варіантів валка

показано приклад моделі ливникової системи 2 з ППС.

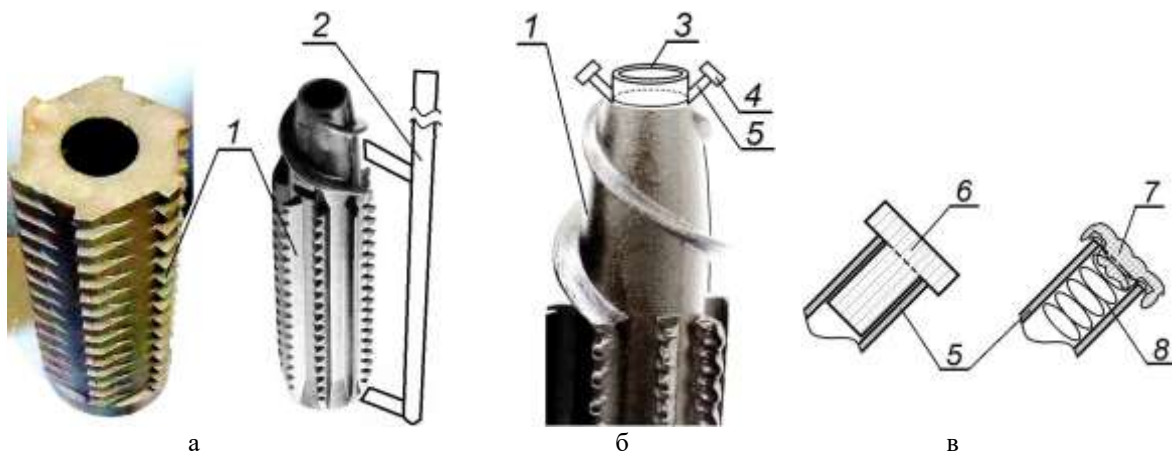


Рисунок 1 – Валки і конструкції їх модельних комплектів: а – приклади валків і ливникової системи; б - верхня частина моделі валка; в – приклади вент в поздовжньому розрізі; 1 - приклади валків; 2 - модель ливникової системи; 3 - патрубок з ППС; 4 – вента; 5 – трубка; 6 – вента - піщана пробка; 7 – вента з вати; 8 – спіраль з дроту.

Подібної конструкції валок (як аналог), модель якого без вентканалів вирізують по частинам на 3D-фрезері з блочного ППС, а потім склеюють ці частини, описано в роботі [6]. Така механічна обробка подібних моделей має той недолік, що супроводжується утворенням відходів у вигляді стружки, витратами по вивозу її у відвал, а також потребує прецизійного інструменту та ручної роботи по склеюванню. Поверхня моделі з ППС має більшу шорсткість ніж друкованої моделі.

На рис. 1, б показано верхню частину моделі валка 1, в центральний повздовжній внутрішній канал якої, вставлено на всю довжину моделі 1 тонкостінний патрубок 3 (циліндричної форми з внутрішнім каналом) з ППС низької густини. Робочою частиною валка є зовнішня, а внутрішній центральний канал служить для полегшення маси виливка і при формувці заповнюється піском. На внутрішній стороні вздовж центрального циліндричного каналу моделі 1 при друкуванні виконано борозенки (не показано), які при стику з патрубком 3 утворюють повздовжні вентканали, які продовжено вставленими в них полімерними (з поліпропілену) трубками 5 з вентами 4. На рис. 1, б показано дві трубки 5, але при відпрацюванні способу ЛГМ друкували не менше чотирьох борозенок, кожна з яких утворювала канал з трубкою 5 і вентом 4. Приклади виконання вент показано на рис. 1, в. Виготовлена з піщаної суміші вента 6 служить пробкою, а вента 7 виконана з вати, що опирається спіраль 8 з металевого дроту. Замість трубки можливе утворення патрубку обертанням плівки «скотч» навколо спіралі 8.

Модель валка 1 має таку геометричну форму, що її складно виготовити цільною з ППС відомими способами, її зубці мають ложкоподібні виїмки (рис. 1, б), тому оптимальним виявився 3D-друк. Повздовжня стінка моделі 1 з центральним каналом досить тонка, тому, щоб не ослаблювати конструкцію, вентканали виконали на поверхні цього центрального каналу з прямолінійних борозенок, які стикуються із вставкою – циліндричним патрубком 3 і сполученні з трубками 5. Венту-пробку 6 виготовили з піщано-рідкоскляної наливної суміші з високою газопроникністю, а вента 7 з вати утримується стінками трубки і спіраллю, яка потрібна в разі застосування м'якої трубки. Аналогічно часто армують гнучкі трубопроводи побутових пылесосів. Для виконання вентканалів методом утворення борозенок, крім застосування вставок типу патрубку 3 з ППС, також можливо борозенки з тонкими щілинами з боку поверхні моделі заклеювати смужками синтетичної плівки типу «скотч».

Для випробування способу моделі друкували методом пошарового наплавлення (FDM) з полілактиду (PLA) – біорозкладного термопластичного полієфіру, який є одним з найбільш широко використовуваних і недорогих за вартістю термопластиків для друку. PLA має густину 1240 кг/м³, температуру плавлення 150-160 °С, температуру кипіння 227 °С. Принцип роботи FDM заснований на плавленні, екструзії термопластичних полімерних ниток (філаментів) і подальшому осадженні розплавленого матеріалу шар за шаром для формування деталі, що використовується на найбільш поширених нескладних принтерах. Зараз такі порівняно низько бюджетні принтери часто навіть називають «шкільними», маючи на увазі їх поширення для навчання дітей в школі азам 3D-друку.

Випробування способу в ливарному цеху ЛГМ відбувалось наступним чином. 3D-друковану модель валка 1 з ливниковою системою 2, вставкою 3 і трубками 5 покрили протипригарною фарбою, не фарбуючи трубки і венти. При формуванні в контейнері моделі сухим піском з його вібраційним ущільненням контейнер зверху загерметизували синтетичною плівкою, вивели крізь неї верхню частину моделі ливникової системи і поставили на неї керамічну воронку для спрямування струменю металу.

Заливання розплаву високоміцного чавуну у форму виконували при її вакуумуванні, під'єднавши до трубопроводу цехової вакуумної системи, в якій підтримували залишковий тиск повітря на рівні 40-50 кПа. При підведенні по ливниковій системі головним чином знизу до моделі металу, він спричиняв газифікацію моделі при русі знизу вгору, гази від газифікації моделі по вентканалах відкачувались крізь трубки 5 і венти 4, далі в пісок форми і попадали крізь трубопровід від форми до вакуумної системи цеху, де проходили очищення. Рівень вакууму на поверхні венти наближався до рівня на поверхні моделі, залежав від відстані венти до вакуумного фільтра контейнерної форми, але газопроникність вент була вищою, ніж газопроникність типових для ЛГМ протипригарних фарб. При заливанні металу за рахунок інтенсивної газифікації моделі рівень залишкового газового тиску в зазорі «метал-модель» був вищим, ніж на поверхні «модель-форма», що забезпечувало стабільність стінки форми в момент контактування її з металом. Після заливання металом форми, охолодження в ній вилівка протягом кількох годин і видалення його з форми отримали вилівок високої якості. Короткі металеві стовпчики на місцях газифікації трубок 5 видалили механічним способом під час операції відокремлення від вилівки елементів ливникової системи.

Застосування комп'ютерних систем для проектування та 3D-друку ливарної моделі з вентиляційними каналами в її стінках знижує витрати на виготовлення таких вентиляційних моделей за рахунок автоматизації їх виконання друкуванням, такі канали нерідко непросто, чи навіть неможливо, інакше виконати в стінках складних за конфігурацією моделей. Для ЛГМ-процесу за моделями, які мають більшу масу на одиницю об'єму і дають більше газів при їх газифікації, ніж традиційні ливарні моделі з ППС, вентканали зменшують масу моделі та дозволяють інтенсифікувати відкачування газів завдяки вакууму форми. Протягом всього процесу газифікації моделі завдяки вакууму в піску форми іде примусове видалення (відсмоктування) газів у вакуумований пісок форми крізь ці канали моделі, продовжені трубками з вентами. Водночас канали спрямовують потоки металу, сприяючи течії створенням в них низького газового тиску.

Таким чином, для друкованих моделей задіяно принцип: чим більше газів утворюється в ливарній порожнині форми, яку заповнює метал, випаровуючи модель, тим більше слід застосувати засобів їх видалення разом з підсиленням впливу вакууму форми для відкачування як газів, так і рідкого металу, що рухається вслід за газами, для створення кращих умов заміщення моделі, ніж за раніше відомими способами ЛГМ. Відкачування газів також дозволить разом з ними вивести дрібні частинки сажі чи так званого коксового залишку, що запобігатиме їх негативному впливу на деякі сплави, що можуть з ними реагувати. Друковану модель з таким створенням в ній направленою газівідводу під впливом вакууму за своєю функцією в ідеалі можна розглядати як вакуумпровід для відкачки продуктів від власної газифікації. Також можливий такий термін, як «друкована модель з направленою пористістю».

Описаний спосіб ЛГМ за друкованою моделлю з вентканалами, реалізація якого стала можливою завдяки застосуванню комп'ютерних систем, дозволив використання вакууму ливарної форми для відсмоктування газів по видрукованим каналам за алгоритмом «чим більше газів від газифікації ливарної моделі, тим інтенсивніший спосіб потрібний для їх видалення з ливарної форми», що дозволить замінити моделі з ППС на друковані і розширити номенклатуру виливків за друкованими моделями при ЛГМ, забезпечуючи стабільну якість литва. Це сприятиме виробництву широкої номенклатури виливків зі зниженням витрат при виготовленні 3D-друкованих ливарних моделей, особливо різноманітних одиничних чи дрібних партій виливків за індивідуальними замовленнями покупців. Останнє відповідає концепції «виробництво як послуга» (Manufacturing as a Service, MaaS).

Описаний спосіб служить засобом подолання основної перешкоди застосування друкованих моделей для ЛГМ, пов'язаної з їх більшою масою і газотвірністю, порівняно з моделями з ППС. Адаптація ливарного виробництва до адитивних технологій дозволяє за допомогою мережі Інтернет пряму взаємодію з покупцем товару, який проектується за його індивідуальним цифровим проектом, зокрема через NFC-систему (бездротової передачі даних та платежів). Також таке поєднання нових цифрових процесів з традиційними виробничими скорочує часовий розрив від створення прототипів і інструментів до масового виробництва.

Висновки

Адитивні технології виробництва дозволяють змінювати як конфігурацію ливарної продукції, так і конструкцію ливарних моделей виключно за рахунок внесення змін в цифрову модель продукції без наступного переформатування виробничого базису. Завдяки розкриттю потенціалу застосування комп'ютерних систем для проектування та 3D-друку ливарної моделі з вентиляційними каналами було розроблено один із способів ЛГМ за друкованими моделями, що відповідає зростаючому тренду цифровізації і автоматизації ливарних процесів. Виконання таких каналів в друкованій моделі дало можливість підвищити інтенсивність евакуації продуктів газифікації цієї моделі у ливарній формі з використанням вакууму форми. Це дозволяє отримати сумарну вигоду як від достатньо швидкоплинних 3D-процесів виготовлення ливарної моделі, так і від короткотривалих процесів формовки та вибивки виливків завдя-

ки використанню при ЛГМ форм з сухого піску. При цьому цифрова трансформація ЛГМ поєднується з ресурсоефективністю оборотного застосування формувальних матеріалів без зміни діючих стандартів контролю металопродукції ливарних цехів, а адаптація виробництва до адитивних технологій дозволяє за допомогою мережі Інтернет взаємодію з покупцем товару, який проектується за його індивідуальним цифровим проектом. Також таке поєднання нових цифрових процесів з традиційними виробничими скорочує часовий розрив від створення прототипів, пілотних зразків продукції і інструментів до масового виробництва.

Список літератури

- [1] Кабінет Міністрів України. (2021, лип. 21). *Постанова № 750. Щодо сприяння впровадженню технологічного підходу «Індустрія 4.0»*. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/750-2021-%D0%BF#Text>.
- [2] В. М. Коржик, М. П. Лютик, В. Ю. Хаскін і В. Ю. Шевченко. «Спосіб вирощування (3D-друку) об'ємних (тривимірних) виробів із тугоплавких матеріалів», *Патент України 118616. МПК В29С 64/153, В33У 10/00, В22F 3/105, В23К 26/342*. 11.02.2019.
- [3] М. О. Васильєв В. П. Бевз, К. М. Храновська. «Спосіб тривимірного друку металевого виробу», *Патент України 93424. МПК В41N 1/00, В41М 99/00*. 25.09.2014.
- [4] О. Й. Шинський, В. С. Дорошенко. «Спосіб лиття металу за адитивно виготовленими разовими ливарними моделями, що газифікуються у вакуумованих формах з сипкого піску, з окисленням продуктів газифікації», *Патент України 150121. МПК В22С 7/02, В22С 9/04*. 05.01.2022.
- [5] П. Б. Калюжний, І. А. Шалевська, О. В. Нейма, С. О. Кротюк, В. С. Дорошенко. «Спосіб лиття металу за 3D-друкованими моделями, що газифікуються у вакуумованих формах з сипкого піску», *заявка України u202305216. МПК В22 С7/02, В22С 9/04*. 3.11.2023.
- [6] М. Miller. «Why Lost Foam?», *Modern Casting*, no. 8, pp. 41-42. 2020.

Стаття надійшла: 22.11.2023 р.

References

- [1] Cabinet of Ministers of Ukraine. (2021, July 21). Resolution No. 750. Regarding promoting the implementation of the technological approach "Industry 4.0". Retrieved from: <https://zakon.rada.gov.ua/laws/show/750-2021-%D0%BF#Text>. [in Ukrainian].
- [2] Pat. 118616 UA, IPC B29C 64/153, B33U 10/00, B22F 3/105, B23K 26/342, Method of growing (3D-printing) volumetric (three-dimensional) products from refractory materials, Korzyk V. M., Lyutyk M. P., Haskin V. Yu., Shevchenko V. Yu., Publ. 11.02.2019. [in Ukrainian].
- [3] Pat. 93424 UA, IPC B41N 1/00, B41M 99/00, Method of three-dimensional printing of a metal product, Vasiliev M. O., Bevs V. P., Khranovska K. M., Publ. 25.09.2014. [in Ukrainian].
- [4] Pat. 50121 UA, IPC B22C 7/02, B22C 9/04, Method of casting metal using additively produced one-time foundry models that are gasified in vacuumed forms from loose sand, with oxidation of gasification products, Shinsky O. Y., Doroshenko V. S., Publ. 05.01.2022. [in Ukrainian].
- [5] Pat. Appl. u202305216 UA, IPC B22C7/02, B22C9/04, Method of metal casting according to 3D-printed models, which are gasified in vacuum molds from loose sand, Kalyuzhny P. B., Shalevska I. A., Neyma O. V., Krotiyuk S. O., Doroshenko V. S., Publ. 3.11.2023. [in Ukrainian].
- [6] M. Miller. «Why Lost Foam?», *Modern Casting*, no. 8, pp. 41-42. 2020.

Відомості про авторів

Дорошенко Володимир Степанович – доктор технічних наук, старший науковий співробітник, провідний науковий співробітник відділу фізико-хімії ливарних процесів.

Янченко Олександр Борисович – кандидат технічних наук, доцент кафедри галузевого машинобудування.

V. S. Doroshenko¹, O. B. Yanchenko²

APPLICATION OF COMPUTER SYSTEMS FOR DESIGNING AND 3D PRINTING OF A FOUNDRY PATTERN WITH VENTILATION CHANNELS IN ITS WALLS

¹Physical-technological Institute of Metals and Alloys, of the National Academy of Sciences of Ukraine, Kyiv

²Vinnitsia National Technical University, Vinnitsia

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОБЧИСЛЮВАЛЬНІ МЕТОДИ

УДК 004.627

О. О. Кавка, В. П. Майданюк, О. Н. Романюк, Є. К. Завальнюк

АНАЛІЗ АЛГОРИТМІВ СТИСНЕННЯ ЗОБРАЖЕНЬ ІЗ
ВТРАТАМИ

Вінницький національний технічний університет, Вінниця

Анотація. У статті розглянуто та проведено аналітичний огляд алгоритмів стиснення зображень зі втратами. Обґрунтовано актуальність дослідження за допомогою статистичних даних. Розглянуто та проаналізовано метод кольірної субдискретизації. Розглянуто, описано та проаналізовано метод квантування кольорів, зокрема наявні дослідження із застосування квантування кольорів у поєднанні з дискретним косинусним перетворенням. Виділено недоліки наявного дослідження та сформульовано можливість подальшого дослідження з використанням розширеної вибірки зображень. Детально розглянуто та проаналізовано стиснення на основі дискретного косинусного перетворення. Виділено пошук оптимальних матриць квантування як перспективний напрямок подальших досліджень з підвищення ефективності застосування дискретного косинусного перетворення. Виділено адаптивне виділення більших, кратних стандартному, блоків даних, як перспективний напрямок дослідження. Розглянуто та проаналізовано метод стиснення зображень на основі вейвлет-перетворення. Сформульовано напрямки подальших досліджень із застосування інших вейвлетів окрім вейвлета Коен-Добеші-Фюво та вейвлета ЛеГал-Табатабай для стиснення зображень. Розглянуто та проаналізовано метод фрактального стиснення. Сформульовано напрямки подальших досліджень, таких як обмеження глибини пошуку і застосування фрактального стиснення у поєднанні із дискретним косинусним перетворенням. Підсумовано напрямки подальших досліджень для покращення функціональних характеристик розглянутих алгоритмів. Основним науковим результатом проведеного дослідження є виділення переліку перспективних тем досліджень, що дозволять збільшити обсяг даних про методи, моделі та засоби стиснення зображень. Практична цінність проведеного дослідження полягає у тому, що воно містить перелік тем досліджень, які можуть бути використані науковими працівниками як матеріал для подальшої наукової діяльності.

Ключові слова: стиснення зображень, стиснення даних, кольорна субдискретизація, квантування кольорів, дискретне косинусне перетворення, вейвлет-перетворення, фрактальне стиснення.

Abstract. The article discusses and conducts an analytical review of lossy image compression algorithms. Substantiated the relevance of the research with the help of statistical data. Considered and analyzed the color subsampling method. Reviewed, described, and analyzed the color quantization method, in particular, existing studies on the application of color quantization in combination with the discrete cosine transform. Highlighted the shortcomings of the existing research and formulated the possibility of further research using an expanded sample of images. Considered and analyzed in detail the compression based on the discrete cosine transform. Singled out the search for optimal quantization matrices as a promising direction of further research on improving the efficiency of the application of discrete cosine transformation. Highlighted the adaptive allocation of larger, multiples of the standard data blocks as a promising direction of research. Considered and analyzed the image compression method based on the wavelet transform. Formulated the direction of further research on the use of wavelets other than Cohen-Dobechy-Feuvo and LeGall-Tabatababay wavelet for image compression. Considered and analyzed the method of fractal compression. Formulated directions for further research, such as limiting the search depth and applying fractal compression in combination with discrete cosine transformation. Summarized directions for further research to improve the functional characteristics of the considered algorithms. The main scientific result of the conducted research is the selection of a list of promising research topics that will allow increasing the amount of data on methods, models and means of image compression. The practical value of the research is that it contains a list of research topics that can be used by researchers as material for further research.

Key words: image compression, data compression, chroma subsampling, color quantization, discrete cosine transform, wavelet transform, fractal compression.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-59-64>.

Вступ

В епоху цифрових технологій більша частина людства отримала доступ до приладів, здатних створювати медійні матеріали, такі як фото, відео та звукозаписи. Обсяги цифрового контенту невпинно зростають, що зберігає актуальний статус проблеми пошуку шляхів підвищення ефективності збереження цифрових медіаданих. Одним із таких шляхів є покращення алгоритмів стиснення зображень із втратами, адже такі алгоритми дозволяють досягати значно нижчих показників надлишковості даних у порівнянні із алгоритмами стиснення зображень без втрат.

Актуальність

Кількість цифрових фото- та відеоматеріалів постійно зростає. За оцінками, у 2020 році було зроблено 1,12 трильйона фотографій і передбачалось зростання кількості нових фото до 1,4 трильйона у 2021 році [1]. Разом з цим, постійно зростає і роздільна здатність фотокамер. До прикладу, iPhone 3G, що вийшов у продаж в 2008 році, мав основну камеру на 2 мегапікселі. У свою чергу, iPhone 14 Pro, презентований в 2022 році, мав основну камеру на 48 мегапікселів, що покращує якість зйомки, а також призводить до збільшення розміру відповідного файлу зображення. Зрештою, опосередкованим

маркером актуальності проблеми є дослідження 2022 року [2], яке прогнозує, що ринок зберігання даних протягом 2023-2030 років буде зростати в середньому на 17,8% щороку.

Таким чином, пошук шляхів зменшення надлишковості при зберіганні цифрових зображень залишається актуальною проблемою.

Мета

Метою статті є аналіз сучасних алгоритмів стиснення зображень із втратами для визначення потенційних векторів дослідження для підвищення ефективності стиснення даних.

Задачі

1. Аналітичний огляд сучасних методів стиснення зображень із втратами.
2. Визначення перспективних напрямків дослідження для підвищення ефективності методів стиснення зображень із втратами.

Аналітичний огляд сучасних методів стиснення зображень із втратами

Виділимо сучасні методи стиснення зображень із втратами для проведення дослідження. До таких методів відносяться:

1. Колірна субдискретизація.
2. Квантування кольорів.
3. Стиснення даних на основі дискретного косинусного перетворення [3].
4. Стиснення даних на основі вейвлет-перетворення.
5. Фрактальне стиснення.

Колірна субдискретизація базується на особливості людської візуальної системи, яка полягає у більшій чутливості зору людини до яскравості зображення, аніж до кольоровості [4]. Цей метод широко використовується у стисненні зображень у поєднанні з іншими методами – до прикладу, в форматі JPEG. Для застосування цього методу зображення має бути приведено до кольорового простору YCbCr. Коефіцієнт стиснення даних залежить від формату субдискретизації:

$$J: a: b$$

де J – частота дискретизації каналу яскравості (ширина блоку), a – число вибірок кольірних сигналів у першому рядку з J пікселів, b – число вибірок кольірних сигналів у другому рядку з J пікселів.

Зазвичай, коефіцієнт J дорівнює 4, тобто ширина блоку для субдискретизації становить 4 пікселі. За винятком деяких специфічних випадків, коефіцієнт b зазвичай або дорівнює 0, або відповідає коефіцієнту a . Коефіцієнт a конфігурує роздільну здатність по горизонталі, а коефіцієнт b – по вертикалі (рис. 1).

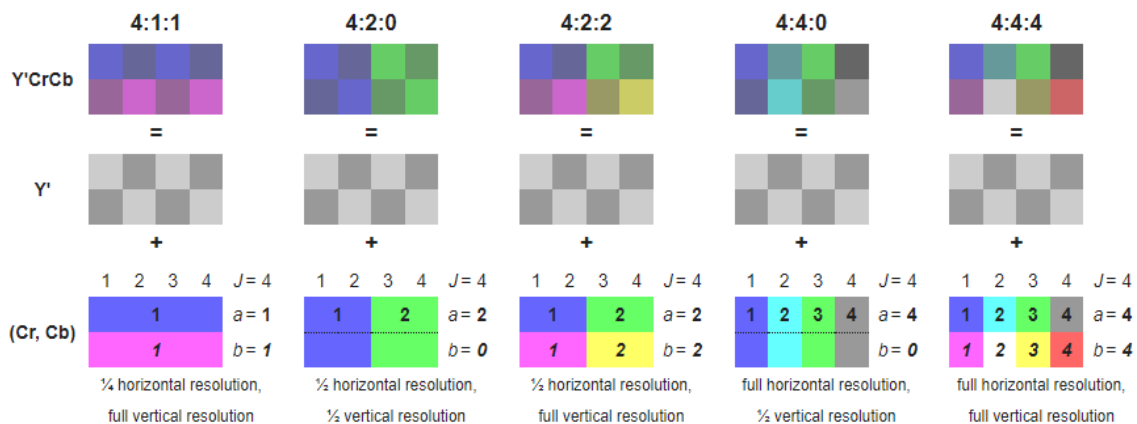


Рисунок 1 – Візуалізація методу колірної субдискретизації

Квантування кольорів – ще одна техніка, що застосовується у стисненні зображень із втратами. Суть цього методу полягає у квантуванні простору кольорів, що містяться на зображенні (рис. 2). Таким чином досягається зменшення розміру зображення із візуально незначними втратами у якості.

Більшість стандартних алгоритмів квантування кольорів розглядають цю проблему як задачу кластеризації точок у тривимірному просторі, де осі відповідають кольоровим каналам [5]. Квантування кольорів не застосовується у методах стиснення, що використовують дискретне косинусне перетворення, оскільки результат зазвичай характеризується погіршеною якістю зображення, а також меншим коефіцієнтом стиснення [6]. Тим не менш, як у статті зазначають самі автори, дослідження проведено на

невеликій вибірці, тому наявне дослідження не є вичерпним і наявний потенціал для подальших спроб покращення методів стиснення зображень у цьому напрямку.

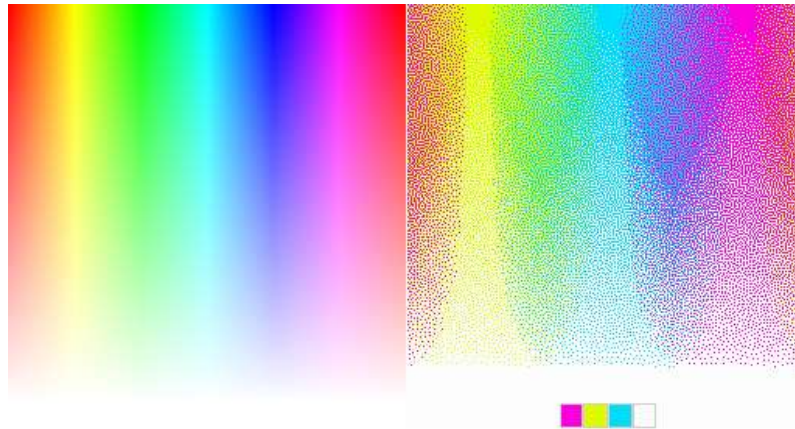


Рисунок 2 – Кольоровий спектр, зведений до палітри з 4 кольорів

Стиснення зображень за стандартом JPEG зазвичай складається з кількох етапів:

1. Зображення переводиться з RGB у YCbCr. Цей етап може бути пропущено.
2. До зображення, представленого в кольоровому просторі YCbCr, застосовується колірна субдискретизація (найчастіше в форматі 4:2:0 – тобто роздільна здатність колірної компоненти зменшується удвічі як за горизонталлю, так і за вертикаллю).
3. Кожен колірний канал розбивається на блоки 8x8, для кожного з яких застосовується дискретне косинусне перетворення.
4. Отримані в результаті перетворення значення частот квантуються за попередньо визначеними стандартом матрицями (які визначають коефіцієнт стиснення, а також впливають на втрату якості зображення). На рисунку 3 наведено приклад матриці квантування. Значення поступово зростають від лівого верхнього до правого нижнього кута, що призводить до відкидання менш значних частотних характеристик.
5. Отримані в результаті квантування блоки кодується за допомогою алгоритмів стиснення даних без втрат – спершу через кодування довжин серій (run-length encoding), після цього – через кодування Хафмана.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Рисунок 3 – Приклад матриці квантування JPEG-1 з коефіцієнтом стиснення 50%

Коефіцієнт стиснення в даному методі залежить переважно від вибору матриці квантування. Відповідно, перспективним є пошук більш оптимальних матриць квантування. Наприклад, дослідження 2022 року розглядає застосування частотного аналізу зображення для підбору оптимальної матриці квантування для конкретного зображення [7]. Враховуючи суттєве зростання пропускної здатності мереж, а також ємності носіїв даних, може бути доцільним формування великого набору матриць квантування і їх вибіркоче застосування в залежності від частотних характеристик конкретних зображень.

Ще одним шляхом до оптимізації стиснення зображень є адаптивне виділення більших блоків даних (16x16, 32x32, 64x64), їх масштабування до блоків 8x8 і подальше стиснення за допомогою звичайного дискретного косинусного перетворення. Такий метод може суттєво покращити коефіцієнт стиснення зображень з високою роздільною здатністю, але невеликою варіативністю – наприклад,

пейзажів, градієнтів, тощо. При цьому, застосування кратного розміру блоків спрощує масштабування, розширюючи діапазон можливих алгоритмів масштабування зображення.

Також є можливим застосування частотного аналізу для виділення повторюваних блоків і зменшення надлишковості при їх повторному кодуванні.

Алгоритм стиснення зображень за допомогою вейвлет-перетворення описано в стандарті JPEG 2000. Попри те, що стандарт JPEG 2000 не набув поширеності свого попередника, таке стиснення характеризується вищою якістю результуючого зображення, а також більш ефективним стисненням [8].

За цим стандартом, спершу виконується приведення кольорових компонент з RGB до іншого кольорового простору – або до YCbCr (незворотне перетворення, оскільки в результаті виникає похибка округлення дробових чисел), або до варіації YUV (зворотне перетворення).

Після кольорового перетворення проводиться розбиття зображення на блоки – над відміну від JPEG-1, не обов'язково розміром 8x8, але після вибору розміру блоку він застосовується до всього зображення. Зображення також може складатись лише з одного блоку. Перевагою такого підходу є можливість декодувати частину зображення, що покращує користувацький досвід у випадку роботи з дуже великими зображеннями, повне завантаження яких у оперативну пам'ять може бути проблемою. Недоліком такого підходу є зниження якості зображення. Використання великої кількості блоків може призводити до артефактів на декодованому зображенні, подібних до тих, що виникають при застосуванні JPEG-1.

Утворені блоки проходять через одне з двох вейвлет-перетворень:

1. Вейвлет Коен-Добеші-Фюво [9] для стиснення із втратами.
2. Вейвлет ЛеГал-Табатабай [10] для стиснення без втрат.

Після вейвлет-перетворення коефіцієнти квантуються задля зменшення кількості інформації, що призводить до втрати якості. Результат цих операцій – набір цілочисельних коефіцієнтів – кодується за процедурою EBCOT [11].

Перспективним вектором дослідження є застосування інших вейвлетів для стиснення зображень.

Фрактальне стиснення є перспективним методом стиснення зображень, що дозволяє забезпечити високі коефіцієнти стиснення при помірних втратах якості у порівнянні із дискретним косинусним перетворенням, особливо при стисненні текстур чи пейзажів. Фрактальне стиснення супутникових зображень дозволило досягнути коефіцієнту стиснення 172:1 [12].

Головною проблемою застосування фрактального стиснення є висока обчислювальна складність. Можливим способом подолання цієї проблеми є обмеження глибини пошуку і застосування у поєднанні із дискретним косинусним перетворенням [13].

Висновки

1. Наявні дослідження застосування квантування кольорів у поєднанні із дискретним косинусним перетворенням при стисненні зображень не є вичерпними, що свідчить про потенційну користь подальших досліджень у цьому напрямку.

2. Перспективним напрямком досліджень є використання розширеного набору таблиць квантування при стисненні зображень із застосуванням дискретного косинусного перетворення.

3. Перспективним напрямком досліджень є адаптивне виділення більших блоків даних (16x16, 32x32, 64x64), їх масштабування до блоків 8x8 і подальше стиснення за допомогою звичайного дискретного косинусного перетворення.

4. Є можливим застосування частотного аналізу для виділення повторюваних блоків і зменшення надлишковості при їх повторному кодуванні.

5. Одним зі шляхів розвитку методів стиснення зображень за допомогою вейвлет-перетворень є практичне дослідження застосування інших вейвлет-перетворень, окрім вейвлету Коен-Добеші-Фюво чи вейвлета ЛеГал-Табатабай.

6. Перспективним напрямком досліджень оптимізації фрактального стиснення є обмеження глибини пошуку і застосування методу у поєднанні з іншими методами стиснення – наприклад, дискретним косинусним перетворенням.

Список літератури

- [1] Pantic, N. (2022, February 2). *How Many Photos Will Be Taken in 2021?* – Mylio Blog. Mylio Blog. <https://blog.mylio.com/how-many-photos-will-be-taken-in-2021-stats>
- [2] *Data Storage Market Size, Share, Trends | Growth [2023-2030]*. (n.d.). <https://www.fortunebusinessinsights.com/data-storage-market-102991>
- [3] N. Ahmed, T. Natarajan and K. R. Rao, "Discrete Cosine Transform" in *IEEE Transactions on Computers*, vol. C-23, no. 1, pp. 90-93, Jan. 1974, doi: 10.1109/T-C.1972.223784.
- [4] Van Den Branden Lambrecht, C. J. (2001). *Vision Models and Applications to Image and Video Processing*. Springer Science & Business Media.

- [5] P. Heckbert. "Color Image Quantization for Frame Buffer Display", *Computer Graphics*, Vol 16, #3, pp. 297-303, 1982.
- [6] Leonardo C. Araujo, Joao P. H. Sansao, and Mario C. S. Junior. (2020). Effects of Color Quantization on JPEG Compression. *International Journal of Image and Graphics*. <https://doi.org/10.1142/s0219467820500266>
- [7] Qijun Wang, Ping Liu, Lei Zhang, Fan Cheng, Jianfeng Qiu, and Xingyi Zhang. (2022b). Rate-distortion optimal evolutionary algorithm for JPEG quantization with multiple rates. *Knowledge Based Systems*, 244, 108500. <https://doi.org/10.1016/j.knosys.2022.108500>
- [8] S. Naveen Kumar, M. V. Vamshi Bharadwaj and S. Subbarayappa, "Performance Comparison of Jpeg, Jpeg XT, Jpeg LS, Jpeg 2000, Jpeg XR, HEVC, EVC and VVC for Images," *2021 6th International Conference for Convergence in Technology (I2CT)*, Maharashtra, India, 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9418160.
- [9] M. Unser and T. Blu, "Mathematical properties of the JPEG2000 wavelet filters," in *IEEE Transactions on Image Processing*, vol. 12, no. 9, pp. 1080-1090, Sept. 2003, doi: 10.1109/TIP.2003.812329.
- [10] D. Le Gall and A. Tabatabai, "Sub-band coding of digital images using symmetric short kernel filters and arithmetic coding techniques," *ICASSP-88., International Conference on Acoustics, Speech, and Signal Processing*, New York, NY, USA, 1988, pp. 761-764 vol.2, doi: 10.1109/ICASSP.1988.196696.
- [11] Fresia, M., Natu, A., & Lavagetto, F. (2023b). Turbo Codes for the Transmission of JPEG2000 Compressed Imagery over Flat Rayleigh Fading Channels. *ResearchGate*. https://www.researchgate.net/publication/228943799_Turbo_Codes_for_the_Transmission_of_JPEG2000_Compressed_Imagery_over_Flat_Rayleigh_Fading_Channels
- [12] Wee Meng Woon, Anthony Tung Shuen Ho, Tao Yu, Siu Chung Tam, Siong Chai Tan and Lian Teck Yap, "Achieving high data compression of self-similar satellite images using fractal," *IGARSS 2000. IEEE 2000 International Geoscience and Remote Sensing Symposium. Taking the Pulse of the Planet: The Role of Remote Sensing in Managing the Environment. Proceedings* (Cat. No.00CH37120), Honolulu, HI, USA, 2000, pp. 609-611 vol.2, doi: 10.1109/IGARSS.2000.861646
- [13] Ali, A. H., Abbas, A. N., George, L. E., & Mokhtar, M. R. (2019). Image and audio fractal compression: Comprehensive review, enhancements and research directions. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(3), 1564-1570.

Стаття надійшла: 19.09.2023

References

- [1] Pantic, N. (2022, February 2). *How Many Photos Will Be Taken in 2021? – Mylio Blog*. Mylio Blog. <https://blog.mylio.com/how-many-photos-will-be-taken-in-2021-stats>
- [2] *Data Storage Market Size, Share, Trends | Growth [2023-2030]*. (n.d.). <https://www.fortunebusinessinsights.com/data-storage-market-102991>
- [3] N. Ahmed, T. Natarajan and K. R. Rao, "Discrete Cosine Transform" in *IEEE Transactions on Computers*, vol. C-23, no. 1, pp. 90-93, Jan. 1974, doi: 10.1109/T-C.1972.223784.
- [4] Van Den Branden Lambrecht, C. J. (2001). *Vision Models and Applications to Image and Video Processing*. Springer Science & Business Media.
- [5] P. Heckbert. "Color Image Quantization for Frame Buffer Display", *Computer Graphics*, Vol 16, #3, pp. 297-303, 1982.
- [6] Leonardo C. Araujo, Joao P. H. Sansao, and Mario C. S. Junior. (2020). Effects of Color Quantization on JPEG Compression. *International Journal of Image and Graphics*. <https://doi.org/10.1142/s0219467820500266>
- [7] Qijun Wang, Ping Liu, Lei Zhang, Fan Cheng, Jianfeng Qiu, and Xingyi Zhang. (2022b). Rate-distortion optimal evolutionary algorithm for JPEG quantization with multiple rates. *Knowledge Based Systems*, 244, 108500. <https://doi.org/10.1016/j.knosys.2022.108500>
- [8] S. Naveen Kumar, M. V. Vamshi Bharadwaj and S. Subbarayappa, "Performance Comparison of Jpeg, Jpeg XT, Jpeg LS, Jpeg 2000, Jpeg XR, HEVC, EVC and VVC for Images," *2021 6th International Conference for Convergence in Technology (I2CT)*, Maharashtra, India, 2021, pp. 1-8, doi: 10.1109/I2CT51068.2021.9418160.
- [9] M. Unser and T. Blu, "Mathematical properties of the JPEG2000 wavelet filters," in *IEEE Transactions on Image Processing*, vol. 12, no. 9, pp. 1080-1090, Sept. 2003, doi: 10.1109/TIP.2003.812329.
- [10] D. Le Gall and A. Tabatabai, "Sub-band coding of digital images using symmetric short kernel filters and arithmetic coding techniques," *ICASSP-88., International Conference on Acoustics, Speech, and*

- Signal Processing*, New York, NY, USA, 1988, pp. 761-764 vol.2, doi: 10.1109/ICASSP.1988.196696.
- [11] Fresia, M., Natu, A., & Lavagetto, F. (2023b). Turbo Codes for the Transmission of JPEG2000 Compressed Imagery over Flat Rayleigh Fading Channels. *ResearchGate*. https://www.researchgate.net/publication/228943799_Turbo_Codes_for_the_Transmission_of_JPEG2000_Compressed_Imagery_over_Flat_Rayleigh_Fading_Channels
- [12] Wee Meng Woon, Anthony Tung Shuen Ho, Tao Yu, Siu Chung Tam, Siong Chai Tan and Lian Teck Yap, "Achieving high data compression of self-similar satellite images using fractal," *IGARSS 2000. IEEE 2000 International Geoscience and Remote Sensing Symposium. Taking the Pulse of the Planet: The Role of Remote Sensing in Managing the Environment. Proceedings* (Cat. No.00CH37120), Honolulu, HI, USA, 2000, pp. 609-611 vol.2, doi: 10.1109/IGARSS.2000.861646.
- [13] Ali, A. H., Abbas, A. N., George, L. E., & Mokhtar, M. R. (2019). Image and audio fractal compression: Comprehensive review, enhancements and research directions. *Indonesian Journal of Electrical Engineering and Computer Science*, 15(3), 1564-1570.

Відомості про авторів

Кавка Олексій Олександрович – аспірант кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця

Kavka Oleksii Oleksandrovych – Graduate Student of the Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia

Майданюк Володимир Павлович – к. т. н., доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця

Maidaniuk Volodymyr Pavlovych – Doctor of Philosophy (Tech.), Associate Professor of the Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia

Романюк Олександр Никифорович – д. т. н., професор, завідувач кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця

Romanyuk Oleksandr Nykyforovych – Doctor of Science (Tech.), Professor of the Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia

Завальнюк Євген Костянтинович – аспірант кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця

Zavalniuk Yevhen Kostiantynovych – Graduate Student of the Department of Software Engineering, Vinnytsia National Technical University, Vinnytsia

O. O. Kavka, V. P. Maidaniuk, O. N. Romanyuk, Y. K. Zavalniuk

ANALYSIS OF THE LOSSY IMAGE COMPRESSION ALGORITHMS

Vinnytsia National Technical University, Vinnytsia

УДК 004.8

Д. А. Ткачик, Р. Н. Кветний

АСИМЕТРИЧНИЙ АНАЛІЗ ТОНАЛЬНОСТІ ДІЛОВИХ НОВИН В СИСТЕМАХ ПРОГНОЗУВАННЯ ДАНИХ НА ФІНАНСОВИХ РИНКАХ

Вінницький національний технічний університет, Вінниця

Анотація. Прогнозування даних на фінансових ринках - актуальне завдання у сучасному світі. Здатність передбачити напрямки руху ринку допомагає інвесторам уникнути очевидних ризиків і позбавити себе додаткових витрат. Було розроблено багато різних торгових платформ, щоб швидко отримувати доступ до великих обсягів історичних даних, що дозволяє аналізувати фінансовий ринок з будь-якого куточка планети в режимі реального часу, використовуючи лише ноутбук або персональний комп'ютер. Такі платформи дозволяють розробляти унікальні стратегії та підходи на основі фундаментального або технічного аналізу, які враховують новини про певну компанію, її прибуток, капіталізацію та кількість дивідендів, які вона повинна виплачувати вчасно. Ділові новини є важливим джерелом інформації про стан економіки та ринків. Вони можуть використовуватися для прогнозування майбутніх подій. Одним із методів прогнозування на основі ділових новин є аналіз тональності. Аналіз тональності дозволяє оцінити позитивність або негативність ділових новин. Традиційні методи аналізу тональності використовують симетричний підхід. Це означає, що позитивні та негативні новини однаково враховуються при прогнозуванні. Однак у реальному світі позитивні новини можуть мати більший вплив на ринки, ніж негативні новини. Це пов'язано з тим, що позитивні новини можуть стимулювати економічну активність, а негативні новини можуть її гальмувати.

У статті розглядається застосування асиметричного аналізу тональності ділових новин у системах прогнозування фінансових ринків. Проаналізовано різні методи аналізу тональності ділових новин, їхні переваги та недоліки. Запропоновано новий підхід до аналізу тональності ділових новин, який комплексно використовує штучні нейронні мережі та метод головних компонент.

Ключові слова: історичні дані, ділові новини, аналіз тональності, прогнозування асиметрія, фундаментальний аналіз

Abstract. Forecasting data in financial markets is a pertinent task in the modern world. The ability to predict market movements helps investors avoid obvious risks and spare themselves additional expenses. Numerous trading platforms have been developed to quickly access extensive historical data, enabling real-time analysis of the financial market from any corner of the planet using only a laptop or personal computer. Such platforms allow the development of unique strategies and approaches based on fundamental or technical analysis, taking into account news about a particular company, its earnings, capitalization, and the amount of dividends it is expected to pay on time. Business news is a crucial source of information about the state of the economy and markets. They can be used for forecasting future events.

One method of forecasting based on business news is sentiment analysis. Sentiment analysis allows assessing the positivity or negativity of business news. Traditional sentiment analysis methods employ a symmetric approach. This means that positive and negative news are equally considered in forecasting. However, in the real world, positive news may have a greater impact on markets than negative news. This is because positive news can stimulate economic activity, while negative news may hinder it.

The article explores the application of asymmetric sentiment analysis of business news in financial data forecasting systems. Various methods of sentiment analysis of business news, their advantages, and disadvantages are analyzed. A new approach to sentiment analysis of business news is proposed, which comprehensively utilizes artificial neural networks and principal component analysis.

Key words: historical data, business news, sentiment analysis, asymmetry forecasting, fundamental analysis

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-65-75>.

Вступ

Ділові новини є важливим джерелом інформації про стан економіки та ринків. Вони можуть використовуватися для прогнозування майбутніх подій. Одним із методів прогнозування на основі ділових новин є аналіз тональності. Аналіз тональності дозволяє оцінити позитивність або негативність ділових новин. Традиційні методи аналізу тональності використовують симетричний підхід. Це означає, що позитивні та негативні новини однаково враховуються при прогнозуванні. Однак у реальному світі позитивні новини можуть мати більший вплив на ринки, ніж негативні новини. Це пов'язано з тим, що позитивні новини можуть стимулювати економічну активність, а негативні новини можуть її гальмувати [1].

Асиметричний аналіз тональності враховує асиметрію тональності, яка вказує на нерівномірність вираження позитивних та негативних відтінків в тексті. У контексті аналізу текстів, таких як новини або відгуки, асиметрія тональності виражається у тому, що кількість та інтенсивність позитивних або негативних висловлювань неоднакові. При цьому позитивні новини враховуються з більшим вагомистію, ніж негативні новини. Це дозволяє поліпшити точність прогнозування.

Нижче наведено основні етапи асиметричного аналізу тональності ділових новин (рисунок 1).

Метою роботи є підвищення точності прогнозування фінансових ринків, з використанням аналізу тональності ділових новин

Результати досліджень

Асиметричний аналіз тональності ділових новин - це метод прогнозування майбутніх подій, який враховує асиметрію впливу позитивних і негативних новин на ринки.



Рисунок 1 - Основні етапи асиметричного аналізу тональності ділових новин

Традиційні методи аналізу тональності використовують симетричний підхід, тобто позитивні та негативні новини однаково враховуються при прогнозуванні. Однак у реальному світі позитивні новини можуть мати більший вплив на ринки, ніж негативні новини. Це пов'язано з тим, що позитивні новини можуть стимулювати економічну активність, а негативні новини можуть її гальмувати. Асиметричний аналіз тональності враховує цю асиметрію. При цьому позитивні новини враховуються з більшим вагомистю, ніж негативні новини. Це дозволяє поліпшити точність прогнозування [2].

Асиметричний аналіз тональності ділових новин може бути використаний для прогнозування різних економічних показників, таких як фондовий ринок, курс валют та інфляція.

Асиметричний аналіз тональності ділових нових складається з наступних етапів:

1. Збір даних: зібрати дані ділових новин за певний період часу.
2. Аналіз тональності: оцінити позитивність або негативність кожної новини.
3. Врахування асиметрії: врахувати асиметрію тональності при прогнозуванні.
4. Прогнозування: зробити прогноз майбутніх подій.

На першому етапі необхідно зібрати дані ділових новин. Ці дані можна зібрати з різних джерел, таких як веб-сайти новин, соціальні мережі та агенції новин.

На другому етапі необхідно оцінити позитивність або негативність кожної новини. Це можна зробити за допомогою різних методів, таких як:

- Лексичний аналіз: використання словників для визначення позитивних та негативних слів.

- Статистичний аналіз: використання статистичних методів для визначення позитивності або негативності тексту.

- Штучний інтелект: використання штучних інтелектуальних методів, таких як машинне навчання та штучні нейронні мережі.

На третьому етапі необхідно врахувати асиметрію тональності при прогнозуванні. Це можна зробити за допомогою різних методів, таких як:

- Використання вагових коефіцієнтів: позитивні новини можна враховувати з більшими ваговими коефіцієнтами, ніж негативні новини.

- Використання спеціальних алгоритмів: розробити спеціальні алгоритми прогнозування, які враховують асиметрію тональності.

На четвертому етапі необхідно зробити прогноз майбутніх подій. Це можна зробити за допомогою різних методів, таких як:

- Лінійне прогнозування: використовувати лінійні моделі для прогнозування майбутніх значень.

- Нелінійне прогнозування: використовувати нелінійні моделі для прогнозування майбутніх значень.

- Глибоке навчання: використовувати штучні нейронні мережі для прогнозування майбутніх значень.

Існує кілька різних методів асиметричного аналізу тональності ділових новин.

Ось деякі з них:

- Метод розкладу на основні компоненти (МГК) МГК - це статистичний метод, який використовується для зменшення розмірності даних. У контексті аналізу тональності ділових новин МГК може бути використаний для виділення двох основних компонентів: позитивного тону та негативного тону. Метод штучних нейронних мереж

- Штучні нейронні мережі - це тип машинного навчання, який може бути використаний для навчання на складних даних. У контексті аналізу тональності ділових новин штучні нейронні мережі можуть бути навчені на наборі даних ділових новин, щоб визначати позитивні та негативні тони.

- Метод обробки природної мови (NLP) NLP - це галузь комп'ютерних наук, яка займається обробкою природної мови. У контексті аналізу тональності ділових новин NLP може використовуватися для виявлення позитивних та негативних слів і фраз у ділових новинах.

- Метод статистичного аналізу Статистичний аналіз може використовуватися для оцінки тона ділових новин за допомогою статистичних методів, таких як частотний аналіз або аналіз дисперсії.

У цій статті розглядається застосування штучних нейронних мереж (ШНМ) у комплексі з методом головних компонент (МГК) для асиметричного аналізу тональності ділових новин. МГК використовується для зменшення розмірності даних, що покращує продуктивність ШНМ [3].

Нейронні мережі — це комп'ютерні моделі, які імітують роботу нейронних систем у мозку. Вони використовуються для вирішення завдань у сферах розпізнавання образів, класифікації, прогнозування, та багатьох інших областях.

Тут ми розглянемо декілька типів нейронних мереж та їх особливості:

1. Персептрон (рисунки 2) — це найпростіший вид нейронної мережі, яка складається з входів, ваг, суматора та функції активації. Його основна функція — класифікація вхідних даних на два класи (наприклад, "так" чи "ні").

2. Рекурентні нейронні мережі (РНМ) - мають здатність зберігати інформацію в попередніх станах, що робить їх ефективними для роботи з послідовностями даних, такими як мовлення або часові ряди.

Рекурентні нейронні мережі (РНМ) є особливим класом нейронних мереж, які призначені для роботи з послідовнісними даними, такими як текст, часові ряди або мовлення. Одна з головних відмінностей РНМ від інших типів нейронних мереж полягає в їхній здатності утримувати та

використовувати інформацію з попередніх кроків часу. Важливим елементом РНМ є зворотні зв'язки, які дозволяють передавати інформацію від одного часового кроку до іншого [4].

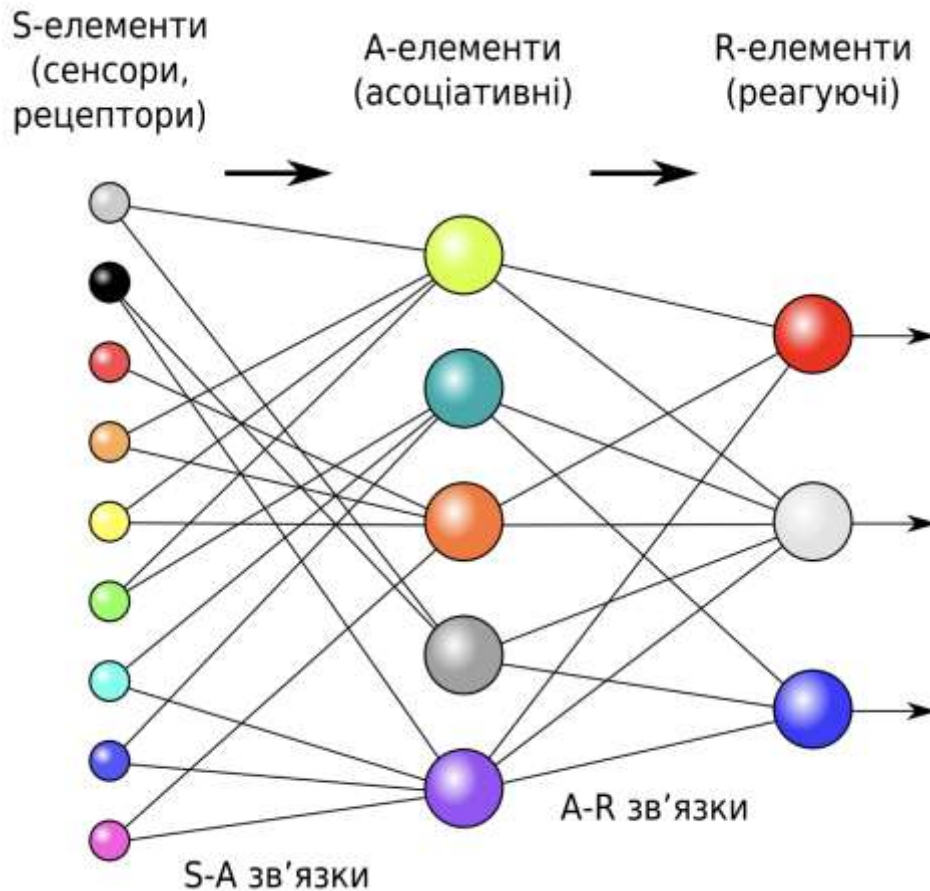


Рисунок 2 - Логічна схема перцептрону з трьома виходами

Основна ідея РНМ полягає в тому, що вона має внутрішні стани, які оновлюються на кожному кроці часу від вхідних даних та попереднього стану. Основна формула для одного часового кроку РНМ може бути виражена наступним чином:

$$h_t = \tanh(W_{hh}h_t - 1 + W_{xh}x_t + b_h), \quad (1)$$

де h_t - вектор прихованого стану на часі t , x_t - вектор вхідних даних на часі t , W_{hh} - матриця ваг для прихованого стану, W_{xh} - матриця ваг для вхідних даних, b_h - зміщення для прихованого стану, \tanh - гіперболічний тангенс, який може використовуватися як функція активації.

Ця формула показує, як оновлюється прихований стан h_t на кожному кроці часу, враховуючи попередній прихований стан h_{t-1} та вхідні дані x_t . Функція активації \tanh допомагає контролювати значення, які може приймати h_t , утримуючи їх у діапазоні від -1 до 1.

3. Згорткові нейронні мережі (ЗНМ) - азвичай використовуються для обробки зображень. Мають здатність до виявлення просторових шаблонів через згорткові шари.

Згорткові нейронні мережі є ефективними для обробки візуальної інформації, такої як зображення. Вони використовують операцію згортки для виявлення локальних патернів та особливостей відображення, що дозволяє їм автоматично вивчати властивості зображень [5]. Основні компоненти згорткових нейронних мереж включають в себе згорткові шари підсемплінгу, і повнозв'язані шари, що використовуються для класифікації.

Основна формула для операції згортки може бути виражена так:

$$C(i, j) = \sigma(\sum_m \sum_n I(i + m, j + n) \cdot K(m, n) + b), \quad (2)$$

де $C(i, j)$ - вихідний піксель після операції згортки, $I(i + m, j + n)$ - значення пікселя вхідного зображення, $K(m, n)$ - вага фільтра (ядро) для операції згортки, b - зміщення, σ - функція активації.

Операція згортки відбувається шляхом руху фільтра (ядра) по вхідному зображенню і обчислення взваженої суми значень пікселів [6]. Це дозволяє виявляти локальні патерни та особливості вхідного зображення. Шар підсемплінгу використовується для зменшення просторового розміру ознак та зниження кількості параметрів в мережі. Загальна формула для операції підсемплінгу може виглядати так:

$$P(i, j) = \max_{m, n}(I(s \cdot i + m, s \cdot j + n)), \quad (3)$$

де $P(i, j)$ - вихідний піксель після підсемплінгу, $I(s \cdot i + m, s \cdot j + n)$ - значення вхідного пікселя, s - фактор підсемплінгу.

Оскільки в даному дослідженні проводиться аналіз тональності новин (текстів), то доцільніше обрати саме рекурентні нейронні мережі.

Метод аналізу головних компонентів (МГК) є статистичним методом зменшення розмірності даних, зберігаючи при цьому їх варіативність. Основна ідея полягає в перетворенні оригінальних змінних у новий набір лінійно некорельованих змінних, які називаються головними компонентами.

Принцип дії МГК:

1. Стандартизація даних: Дані стандартизуються для забезпечення однакового масштабу.
2. Розрахунок матриці коваріацій: Визначається матриця коваріацій для оригінальних змінних.
3. Розрахунок головних компонент: Визначаються власні значення та власні вектори матриці коваріації, і вони використовуються для створення головних компонент.
4. Вибір головних компонент: Вибираються головні компоненти, які пояснюють найбільшу частку варіативності.

Використання МГК:

1. Зменшення розмірності даних: Використовується для візуалізації та аналізу даних.
2. Видалення кореляції між змінними: Допомагає уникнути мультиколінеарності у моделях.
3. Покращення ефективності моделей: Використовується для відбору важливих змінних та покращення роботи моделей машинного навчання.

Загальна схема математичних перетворень в МГК зображена на рисунку 3.

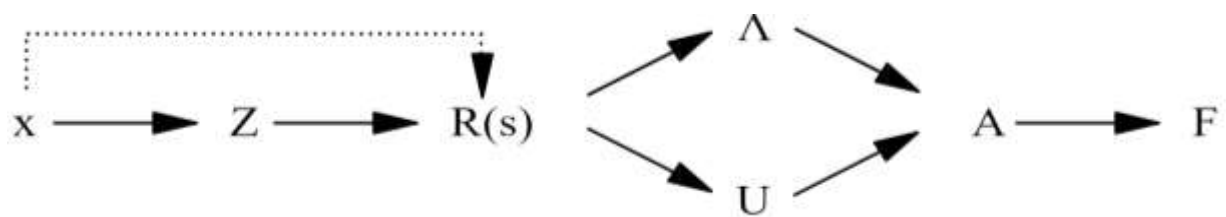


Рисунок 3 - Загальна схема математичних перетворень в МГК

На рисунку 3 позначення: X — матриця вихідних даних розмірністю $n \times m$ (n — число об'єктів спостереження, m — число елементарних аналітичних ознак); Z — матриця центрованих і нормованих значень ознак; R — матриця парних кореляцій. Λ — діагональна матриця власних (характеристичних) чисел. A — матриця факторного відображення, її елементи a_{ij} — вагові коефіцієнти. Спочатку A має розмірність $m \times m$ — за кількістю елементарних ознак X_j , потім в аналізі залишається r найвагоміших компонент, $r \leq m$. Обчислюють матрицю A за відомими даними матриці власних чисел Λ і нормованими власними векторами V за формулою $A = V\Lambda^{1/2}$. F — матриця значень головних компонент розмірністю $r \times n$.

Тексти новин для аналізу потрібно токенизувати на окремі слова або токени, і потім перетворити їх у вектори [7]. Один з підходів - використання словника, де кожне унікальне слово має відповідний

вектор. Це можна реалізувати за допомогою предтренованих векторів слів (наприклад, GloVe або Word2Vec) або з нуля, використовуючи ембедінги слів в нейронній мережі.

Модель для аналізу тональності може бути заснована на рекурентних нейронних мережах (RNN), довільних різновидностях Long Short-Term Memory (LSTM) або Gated Recurrent Unit (GRU), або трансформерних архітектурах (наприклад, BERT).

Оскільки моделі типу BERT мають обмеження, нам треба скорочувати розмір тексту, не втративши нічого корисного. У цій частині завдання є кілька підходів. Наведемо кілька можливих:

За допомогою синтаксичного дерева:

- використовуючи синтаксичний аналізатор із бібліотеки SpaCy, ми будемо синтаксичне дерево, у якого в кожному вузлі знаходиться слово або знак пунктуації;

- починаючи з знайденого вузла, що містить сутність, запускаємо на дереві «алгоритм забарвлення»: спочатку помічаємо вузли дерева на m рівнів вище знайденого, потім вузли на n рівнів нижче позначених (m і n - параметри, що налаштовуються) [8];

- всі помічені вузли об'єднуємо в текст, якщо між вузлами є перепустки, ставимо три крапки.

Простіший варіант: брати всі пропозиції, в яких згадується сутність, яка нас цікавить.

У новинах ми активно використовували набір бібліотек SpaCy як допоміжний інструмент:

- для отримання іменованих сутностей та їх нормалізації;

- розбиття статей на пропозиції;

- вилучення інформації з синтаксичного дерева для автоматичного виділення ключових іменованих сутностей та скороченого варіанта тексту.

Варто зазначити, що в тексті часто та сама сутність може зустрічатися у вигляді скорочень, псевдонімів або аббревіатур. Це відома проблема різного написання назв організацій залежно від видавництва, настрою автора, погоди, дня тижня тощо.

Для конкретного контрагента, наприклад Монобанк, вдасться знайти у статтях безліч варіантів написання: «Моно», «Монобанк», «Банк Моно» тощо.

Для приведення сутностей до єдиної форми ми використовуємо словник можливих написань для кожної сутності та нечіткий пошук за допомогою бібліотеки FuzzyWuzzy [9]. Це також важливо для завдання матчінгу новини та бази контрагентів, за якими ми хочемо проводити аналіз.

Для кожної новини:

1. Виділяємо сутності та робимо оцінку тональності новини щодо кожної;

2. Наводимо різні варіанти вживання однієї сутності єдиного виду;

3. Робимо заміну ключової сутності на X ;

4. Утискаємо текст вихідної новини до 512 токенів щодо X .

У результаті ми отримуємо N^* прикладів та навчаємо BERT із додатковим вихідним шаром класифікації.

Підготовка даних і навчання моделі зображено на рисунку 4.

$$\text{Точність} = \frac{\text{Кількість правильних прогнозів}}{\text{Кількість всіх прогнозів}} \quad (4)$$

Для бінарної класифікації точність також може бути обчислена за допомогою критерію k щодо позитивних і негативних рейтингів, наступним чином:

$$k = \frac{TP+TN}{TP+TN+FP+FN}, \quad (5)$$

де TP - правильно визначені позитивні результати, TN - правильно визначені негативні результати, FP - неправильно визначені позитивні результати і FN - неправильно визначені негативні результати.

Отримані результати слід розглядати як обнадійливі. Отримана точність 0,7301. Якість моделі можна покращити за рахунок збільшення навчальної вибірки та підбору параметрів моделі. Незважаючи на помилки, модель помиляється в сусідні класи, при цьому явно не плутаючи негативні та позитивні приклади.

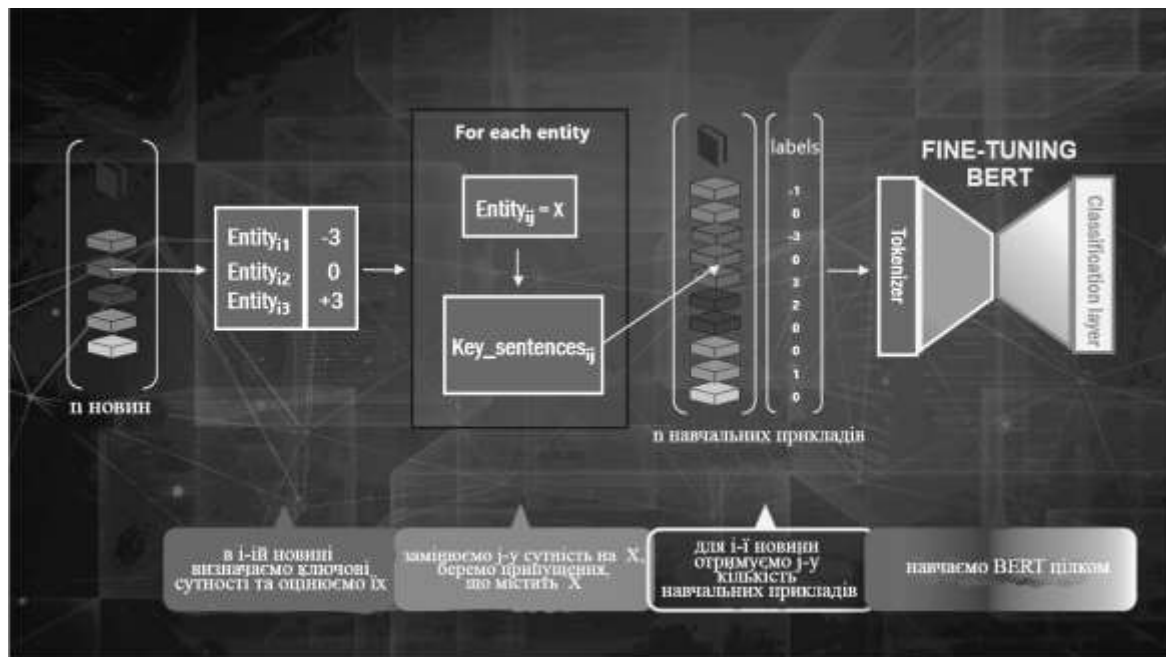


Рисунок 4 – Підготовка даних і навчання моделі BERT

Результати навчання моделі зображено на рисунку 5 у вигляді матриці помилок.



Рисунок 6 – Матриця помилок

Точність є одним із показників для оцінки моделей класифікації. Неформально, точність - це частка прогнозів, які модель вірно визначила. Формально точність має наступне визначення:

При використанні навченої моделі (рисунку 6) ми видаємо оцінки для кількох найважливіших сутностей новини. При цьому важливість визначається як зважена кількість згадок про сутність у тексті новини. Коли вона зустрічається як підмет, ми беремо її з великою вагою. Зрештою, ми просто відсікаємо всі неважливі сутності, частка згадки яких не перевищує заданий поріг.

Чи є суть підметом чи його частиною, ми визначаємо за допомогою синтаксичного дерева, що видається SpaCy.

Беремо новину та отримуємо ключові сутності.

Для кожної ключової сутності:

1. Наводимо різні варіанти вживання однієї сутності єдиного виду;
2. Робимо заміну ключової сутності на X;
3. Утискаємо текст прикладу до 512 токенів щодо X;
4. Подасмо в навчену модель;
5. Отримуємо можливості класів шкали тональностей, вибираємо найбільш можливий клас.

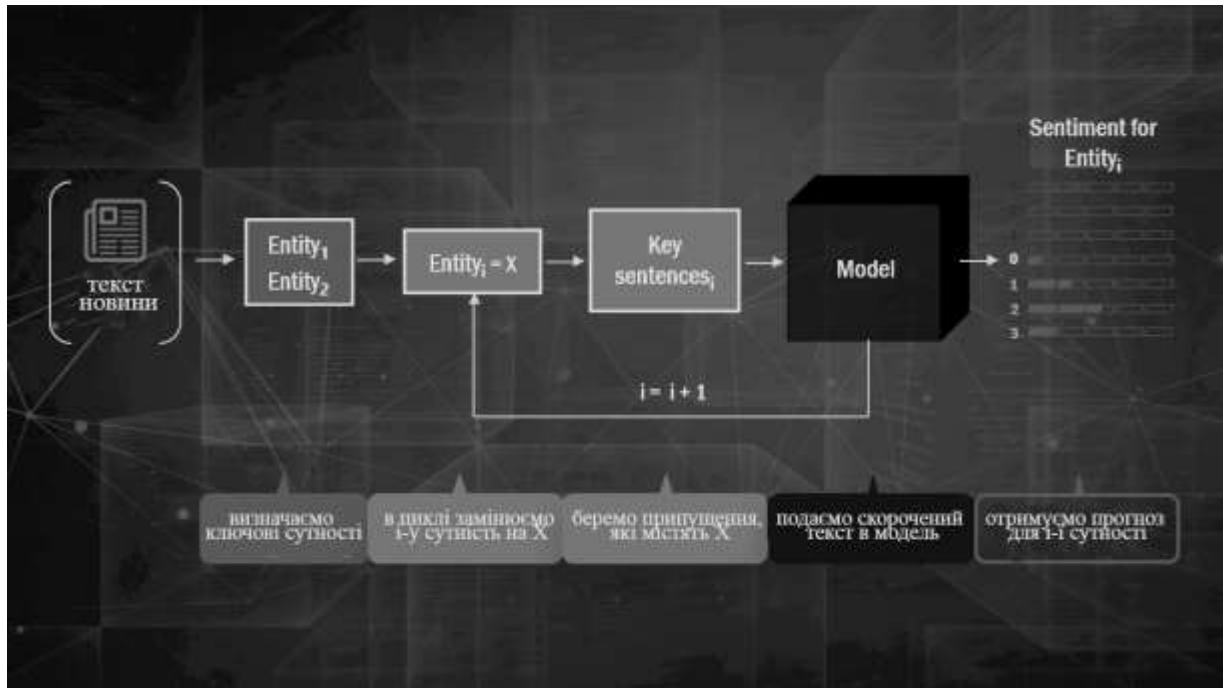


Рисунок 6 – Використання навченої моделі

Після отримання класів тональності за допомогою Штучних Нейронних Мереж (ШНМ), можна використовувати метод головних компонент (МГК), щоб зменшити розмірність цих класів та виокремити головні компоненти, які найкраще описують варіативність даних. Детальний процес буде описано нижче.

Нехай X буде матрицею, де кожний рядок представляє класів тональності для відповідної новини. Перш за все, слід стандартизувати дані, щоб забезпечити однаковий масштаб. Це важливо для вірного роботи МГК. Використовуємо бібліотеку `scikit-learn` для визначення головних компонент.

Після визначення головних компонент можна також оцінити, яку частку варіативності вони зберігають, що показує, яку частку загальної варіативності виявлено кожним з головних компонент. Можна також оцінити важливість кожного головного компонента за допомогою власних значень, які вказують на зміну варіативності, яку вони представляють.

Отримані приклади даних, що наведені в таблиці 1, можна використовувати як вхід для подальших моделей прогнозування, таких як класифікатори для прогнозування ринкової реакції на основі тональності новин.

Таблиця 1 – Приклад вихідних даних

Новина	Клас тональності	Головна компонента
1	0.8	0.7
2	-0.3	-0.5
3	0.1	0.2

В цілому комплексне використання штучних нейронних мереж та методу головних компонент має кілька переваг, які можуть зробити його кращим варіантом для аналізу тональності тексту та прийняття рішень на фінансових ринках порівняно з іншими методами:

- ШНМ відмінно пристосовані для аналізу складних залежностей у великих текстових даних, що може сприяти точнішій класифікації тональності, а комбінація ШНМ і МГК дозволяє створити комплексну модель, яка здатна краще виявляти та розуміти складні зв'язки між текстом і факторами, що впливають на тональність.

- МГК допомагає зменшити розмірність текстових даних, зберігаючи при цьому інформацію, що є важливою для аналізу. Зменшення розмірності дозволяє підвищити продуктивність моделі більше ніж на 50%, дозволяючи швидше обробляти великі об'єми текстової інформації та знижуючи витрати обчислювальних ресурсів.

- МГК дозволяє визначити головні компоненти, які найкраще виражають варіативність даних, забезпечуючи інтерпретованість зменшених даних. Інтерпретованість є важливою при прийнятті фінансових рішень, і цей метод забезпечує збереження важливих характеристик від зменшених даних.

- ШНМ адаптовані до змін у текстових даних, що може бути важливим для аналізу фінансових новин. Комплексне використання ШНМ та МГК дозволяє ефективно працювати з динамічними текстовими даними, що мають значний вплив на фінансові ринки.

- комбінація точної класифікації ШНМ та зменшення розмірності МГК дозволяє покращити прогнозування ринкової реакції на основі тональності новин. Застосування обох методів допомагає створити модель, яка краще адаптується до змін у тексті та забезпечує більш точні та надійні прогнози.

Таким чином описаний в статті підхід та використані в ньому методи збільшують продуктивність систем для прогнозування фінансових ринків. За рахунок використання штучних нейронних мереж та зменшення розмірності даних для аналізу зменшується час на прийняття рішень та підвищується точність прогнозів.

Висновки

Розвиток систем прогнозування даних є актуальним, оскільки в сучасному комп'ютеризованому світі значна кількість людей має доступ до Інтернету і володіє особистим комп'ютером, що надає швидкий доступ до фондових бірж та дозволяє переглядати котирування в режимі реального часу не залишаючи дім [10].

У даній статті розглянуто використання штучних нейронних мереж (ШНМ) та методу аналізу головних компонент (РСА) для аналізу тональності фінансових новин та прийняття рішень на фінансових ринках.

Процес прийняття рішення при цьому включає такі етапи:

1. Підготовка Даних: Зчитування та підготовка текстових та фінансових даних.
2. Використання ШНМ для Аналізу Тональності:
 - Тренування моделі (наприклад, LSTM або BERT) на текстах новин для аналізу тональності.
 - Отримання векторів тональності для кожної новини.
3. Стандартизація та Використання РСА:
 - Стандартизація отриманих векторів для однакового масштабу.
 - астосування РСА для зменшення розмірності та отримання головних компонент.
4. Прогноз Ринкової Реакції:
 - Використання зменшених даних в якості вхідних для моделі прогнозування ринкової реакції.
5. Прийняття Управлінських Рішень:
 - На основі прогнозу приймаються управлінські рішення, такі як оптимізація портфеля чи розробка стратегій.

Цей підхід дозволяє об'єднати сильні сторони ШНМ у роботі з текстовою інформацією та PCA для зменшення розмірності даних, полегшуючи подальший аналіз та використання в прийнятті рішень [11]. Для подальшого розвитку запропонованого підходу для досягнення найкращих результатів важливо налагоджувати параметри моделей та валідувати їх на реальних історичних даних.

Список літератури

- [1] Д. А. Ткачик, Р. Н. Кветний, "Розробка ефективних комбінацій моделей технічного аналізу для прогнозування ринку" Матеріали XLIX Науково-технічної конференції ВНТУ, Вінниця, 27-28 квітня 2020 р.. 2020. [Online]. Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2020/paper/view/9600>.
- [2] Goodfellow, I., Bengio, Y., Courville, A. (2016). "Deep Learning." MIT Press.
- [3] Tsai, C. F., & Wang, C. C. (2018). "Using deep neural network models for risk prediction and classification in real-time financial market." *Expert Systems with Applications*, 95, 12-27.
- [4] D. P. Kroese, S. J. Rubinstein, P. I. Frazier, et al. (2019). "Statistical Machine Learning for Asset Management." *Journal of Financial Data Science*, 1(1), 2-19.
- [5] Tsantekidis, A., Passalis, N., Tefas, A., et al. (2017). "Using deep learning and Google Trends to predict the stock price of a large IT company." *Expert Systems with Applications*, 73, 125-139.
- [6] Stock Market Sentiment Analysis in 2023, 2022. URL: <https://research.aimultiple.com/sentiment-analysis-stock-market/>
- [7] Types of Sentiment Analysis and How Brands Perform Them, 2020. URL: <https://www.analyticsinsight.net/types-of-sentiment-analysis-and-how-brands-perform-them/>
- [8] Aspect-based sentiment analysis via affective knowledge enhanced graph convolutional networks / B. Liang et al. *Knowledge-Based Systems*. 2022. Vol. 235. P. 107643. URL: <https://doi.org/10.1016/j.knosys.2021.107643>
- [9] Zhang, Y., Watson, J., & Johnson, J. (2019). "Deep learning in finance." *Journal of Economic Dynamics and Control*, 98, 1-16.
- [10] Yu, L., Wang, S., & Lai, K. K. (2017). "A deep learning and cross-domain approach for stock price movement prediction." *Expert Systems with Applications*, 83, 56-66.
- [11] Hagenau, M., Liebmann, M., & Neumann, D. (2013). "Automated news reading: Stock price prediction based on financial news using context-capturing features." *Decision Support Systems*, 55(3), 685-697.

Стаття надійшла: 19.09.2023

References

- [1] D. A. Tkachyk, R. N. Kvyetnyy, "Rozrobka efektyvnykh kombinatsiy modeley tekhnichnoho analizu dlya prohozuvannya rynku" Materialy XLIX Naukovo-tekhnichnoyi konferentsiyi VNTU, Vinnytsya, 27-28 kvitnya 2020 r.. 2020. [Online]. Rezhym dostupu: <https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2020/paper/view/9600>.
- [2] Goodfellow, I., Bengio, Y., Courville, A. (2016). "Deep Learning." MIT Press.
- [3] Tsai, C. F., & Wang, C. C. (2018). "Using deep neural network models for risk prediction and classification in real-time financial market." *Expert Systems with Applications*, 95, 12-27.
- [4] D. P. Kroese, S. J. Rubinstein, P. I. Frazier, et al. (2019). "Statistical Machine Learning for Asset Management." *Journal of Financial Data Science*, 1(1), 2-19.
- [5] Tsantekidis, A., Passalis, N., Tefas, A., et al. (2017). "Using deep learning and Google Trends to predict the stock price of a large IT company." *Expert Systems with Applications*, 73, 125-139.
- [6] Stock Market Sentiment Analysis in 2023, 2022. URL: <https://research.aimultiple.com/sentiment-analysis-stock-market/>
- [7] Types of Sentiment Analysis and How Brands Perform Them, 2020. URL: <https://www.analyticsinsight.net/types-of-sentiment-analysis-and-how-brands-perform-them/>
- [8] Aspect-based sentiment analysis via affective knowledge enhanced graph convolutional networks / B. Liang et al. *Knowledge-Based Systems*. 2022. Vol. 235. P. 107643. URL: <https://doi.org/10.1016/j.knosys.2021.107643>
- [9] Zhang, Y., Watson, J., & Johnson, J. (2019). "Deep learning in finance." *Journal of Economic Dynamics and Control*, 98, 1-16.

- [10] Yu, L., Wang, S., & Lai, K. K. (2017). "A deep learning and cross-domain approach for stock price movement prediction." *Expert Systems with Applications*, 83, 56-66.
- [11] Hagenau, M., Liebmann, M., & Neumann, D. (2013). "Automated news reading: Stock price prediction based on financial news using context-capturing features." *Decision Support Systems*, 55(3), 685-697.

Відомості про авторів

Ткачик Денис Анатолійович – аспірант кафедри автоматизації та інтелектуальних інформаційних технологій ВНТУ

Квєтний Роман Наумович – доктор технічних наук, професор, професор кафедри автоматизації та інтелектуальних інформаційних технологій ВНТУ

D.A. Tkachuk, R. N. Kvietnyi

**ASYMMETRIC SENTIMENT ANALYSIS OF BUSINESS NEWS IN HISTORICAL
DATA FORECASTING SYSTEMS**

Vinnitsia National Technical University

БІОЛОГІЧНІ ТА МЕДИЧНІ ПРИЛАДИ І СИСТЕМИ

UDC 615. 471.03:616.073

S.V. PAVLOV¹, WALDEMAR WÓJCIK², R.L. HOLYAKA³,

O.D. AZAROV¹, L.E. NYKYFOROVA⁴, YANG LONGYIN¹

DEVELOPMENT OF A MATHEMATICAL MODEL OF THE THERMAL FIELD OF AN INTEGRAL STRUCTURE IN THE IMPLEMENTATION OF SENSORS FOR BIOMEDICAL RESEARCH

¹Vinnitsia National Technical University, Vinnitsia, Ukraine,

²Lublin University of Technology, Poland

³Lviv Polytechnic National University, Ukraine

⁴National University of Life and Environmental Sciences of Ukraine

Анотація. В статті розглянуто реалізація комплексної методики для електротеплового моделювання вимірювальних перетворювачів теплових сенсорів потоку, який поєднує синтез кола заміщення імпульсної температурної релаксації та спосіб формування ВАХ перетворювачів в режимі їх самонагріву струмом живлення. Розглянуто питання оцінювання нестабільності ітераційних процесів при аналізі ВАХ вимірювальних перетворювачів з від'ємним диференціальним опором, що обумовлено самонагрівом цих перетворювачів. Розроблено експрес-метод визначення меж, в яких забезпечується коректний електротепловий DC аналіз для застосування в біомедичних приладах та системах.

Ключові слова: електротеплове моделювання, вимірювальні перетворювачі, самонагрів перетворювачів, біомедичні прилади та системи.

Abstract. The paper deals with the implementation of a complex technique for electrothermal modeling of measuring transducers of thermal flow sensors, which combines the synthesis of the impulse temperature relaxation substitution circuit and the method of forming the I-V converters in the mode of their self-heating by the supply current. The issue of assessing the instability of iteration processes in the analysis of I/V measuring converters with negative differential resistance, which is caused by self-heating of these converters, is considered. An express method for determining the limits in which correct electrothermal DC analysis is provided for use in biomedical devices and systems has been developed.

Keywords: electrothermal modeling, measuring transducers, self-heating of transducers, biomedical devices and systems.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-76-83>.

Introduction

Information signal of the primary thermal flow sensors converters is their temperature that depends on the intensity of the heat exchange between the structure of the converter and the flow medium (gas or fluid). Modeling studies of the circuits of the above-mentioned measuring converters, carried out for the optimization of their structure and supply modes, require the combination of the analysis of the electric and thermal processes in a single complex.

Unfortunately, known packages of circuit modeling, in particular, PSpice and MicroCAP, do not allow combining electric and thermal analysis - in the course of such modeling studies the temperature of the elements cannot change if the electric power, released in these elements, varies. That is why, the problem of the development of the adaptation method of the circuit modeling procedure in the given packages for the realization of the possibility of the complex analysis of electric and thermal processes in the circuits of primary thermal flow sensors converters, was put forward. The realization of this task requires the creation of the model (equivalent circuit) of the elements, volt-ampere characteristic of which is influenced in the process of self-heating of these elements.

Techniques and models of calculation of the temperature fields of the electronic equipment and, in particular, solid-state and hybrid integrated circuits have already been adequately discussed in numerous publications. A number of specialized programming products are available, namely: WinTherm (developer ANALYSIS TECH; www.analysisstech.com), T3Step and Thermodel (developer MICRED; www.micred.com), BETASoft Board (developer DYNAMIC SOFT ANALYSIS; www.betasoft-thermal.com), etc. [54-65]. Taking

into consideration, that the scientific aspects of the greater part of thermal calculations are comprehensive, at least, from the point of view of the tasks, put forward in the given research, further we will suggest only the description of the thermal model in general form and partial examples of the results of thermal fields of the integrated structures of the thermal hot-wire anemometers calculations. The material of the given subsection should be considered only as the initial data for the developed new approaches of the electric thermal modeling, presented in the next parts of the monograph, where the dynamic, thermal and circuit calculations of elements, the temperature of which is the informative value of the signal converter of the thermal flow are combined.

Method

In the process of the thermal calculation of the integral structures, they are divided into the sections, in particular, into layers and parallelograms, each of them is described by the independent system of parameters - thermal conductivity factor, heat capacity, heat release power, etc. The system of heat conduction equations in the Cartesian coordinate system x, y, z for the i -th layer of the multilayer structure (assuming that the bottom boundary of the i -th layer corresponds to the coordinate $z_i = \delta_i$, and the upper - $z_i = \delta_i$, where δ_i - is the hickness of the i -th layer) has the form [172, 173]:

$$\frac{\partial^2 T_i}{\partial x^2} + \frac{\partial^2 T_i}{\partial y^2} + \frac{\partial^2 T_i}{\partial z^2} = 0$$

Boundary conditions are:

- on lateral edges if $x = 0, x = L_x, y = 0, y = L_y$:

$$\frac{\partial T_i}{\partial x} = 0; \quad \frac{\partial T_i}{\partial y} = 0;$$

- on the boundary of the i -th and $(i+1)$ -th layers if $z_i = \sigma_i, z_{i+1} = 0$:

$$T_i = T_{i+1}; \quad \lambda_i \left(\frac{\partial T_i}{\partial z_i} \right) = \lambda_{i+1} \left(\frac{\partial T_{i+1}}{\partial z_{i+1}} \right);$$

- on the surface S if $z_1 = 0$

$$\frac{\partial T_1}{\partial z_1} = -\frac{1}{\lambda_1} \sum_{j=1}^k \frac{P_j}{a_j b_j} h_j(x) h_j(y) h_j(z) + \frac{\alpha_0}{\lambda_1} T_1;$$

- on the surface S_N if $z_N = \delta_N$:

$$\frac{\partial T_N}{\partial z_N} = \frac{1}{\lambda_N} \sum_{j=1}^k \frac{P_j}{a_j b_j} h_j(x) h_j(y) h_j(z) - \frac{\alpha_N}{\lambda_N} T_N,$$

where T_i - is the excessive temperature (temperature of overheating) of the i -th layer over the ambient temperature ($i = 1, 2, 3... N$); N - is a number of layers; λ_i - is the thermal conductivity of the i -th layer; P_j - is the power of the j -th source of heat ($j = 1, 2, 3... k$); k - is the number of heat sources; a_j, b_j - are dimensions of the heat sources with the number j on axes x and y , correspondingly; $h_j(x), h_j(y)$ - are coordinate-dependent functions which take the value of 1 in the area of the source and 0 outside the area of the j -th source of heat; $h_j(z)$ - are coordinate-dependent functions, which take the value of 1 on the surface S_N and 0 - on the surface S_0 , correspondingly; α_0, α_N - are heat transfer coefficients from the surfaces S_0, S_N .

Calculation of the temperature field, stipulated by the location of the source of heat on the surface S_N , can be performed by means of numerical methods, applying series:

$$\begin{aligned}
 \frac{T_{ij}}{P_j} = & \frac{(1-k_i)Z_c\alpha_0 + 1}{Z_c\alpha_0\alpha_N + \alpha_0 + \alpha_N} \frac{1}{L_x L_y} + \frac{8L_x}{\pi^2 a_i a_j L_y} \times \\
 & \times \sum_{n=1}^{\infty} \frac{W(n,0,k_i)}{n^2} \cos n\pi \frac{\phi_i}{L_x} \cos n\pi \frac{\phi_j}{L_x} \sin n\pi \frac{a_j}{2L_x} \sin n\pi \frac{a_i}{2L_x} + \\
 & + \frac{8L_y}{\pi^2 b_i b_j L_x} \sum_{m=1}^{\infty} \frac{W(0,m,k_i)}{m^2} \cos m\pi \frac{\psi_i}{L_y} \sin m\pi \frac{b_i}{2L_y} \cos m\pi \frac{\psi_j}{L_y} \times \\
 & \times \sin m\pi \frac{b_j}{2L_y} + \frac{64L_x L_y}{\pi^4 a_i a_j b_i b_j} \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{W(n,m,k_i)}{n^2 m^2} \cos n\pi \frac{\phi_i}{L_x} \cos n\pi \frac{a_i}{2L_x} \times \\
 & \times \cos n\pi \frac{\phi_j}{L_x} \sin n\pi \frac{a_j}{2L_x} \sin m\pi \frac{\psi_i}{L_y} \sin m\pi \frac{b_i}{2L_y} \cos m\pi \frac{\psi_j}{L_y} \sin m\pi \frac{b_j}{2L_y},
 \end{aligned}$$

where T_{ij} – is the average temperature of the i -th section, heated by the j -th source of heat; a_i, a_j, b_i, b_j – are dimensions of the sections; ϕ_i, ϕ_j – are the coordinates of the centers of sections on the axis x ; ψ_i, ψ_j – are the coordinates of the centers of sections on the axis y ; L_x, L_y – are the dimensions of the structure on the

$$Z_c = \sum_{l=1}^N \frac{\delta_l}{\lambda_l}$$

axes x and y ; δ_l – is thermal resistance; δ_l, λ_l – thickness and thermal resistance of the l -th layer ($l = 1, 2, 3,$

$$W(n, m, k_i) = (G_N(1 - k_i) + k_i) \frac{Z_N}{Z_N \alpha_N + 1}$$

... N); N – is a number of the structure layers.

Variable k_i takes the value 1 in the point, located on the surface S_N , and 0 – on the surface S_N . Functions G and S_N are calculated in the consecutive order, passing the layers of the structure, starting from the first and ending with $N = m$, using the recurrent expressions:

$$Z_i = \frac{v\lambda_i Z_{i-1} + 1 + (v\lambda_i Z_{i-1} - 1)e^{-2v\delta_i}}{v\lambda_i Z_{i-1} + 1 - (v\lambda_i Z_{i-1} - 1)e^{-2v\delta_i}}; G_i = \frac{G_{i-1} 2v\lambda_i Z_{i-1} e^{-v\delta_i}}{v\lambda_i Z_{i-1} + 1 + (v\lambda_i Z_{i-1} - 1)e^{-2v\delta_i}},$$

$$v = \sqrt{\frac{n^2 \pi^2}{L_x^2} + \frac{m^2 \pi^2}{L_y^2}}$$

where i – is the number of the layer

In addition to the above-mentioned equations systems of mathematical description of the temperature fields, in the thermal flow sensors it is necessary to calculate the interaction of the heated structure of the primary converter of the flow sensor. In general case the dependence between the temperature parameters of thermoanemometric primary converter and parameters of the flow can be written in the form of the equation [1-5]:

$$P_{\text{H}} = K_1 \alpha F \Delta t,$$

where K_1 – is the coefficient, which is introduced, as in greater part of cases it is not the difference of the temperature of the heat exchange surface and the fluid that is measured but another value Δt ; α – is the coefficient of the convective heat transfer; F – is heat exchange surface; Δt – is the temperatures difference.

Main parameter of the thermal model is Nusselt criterion Nu , which characterizes the heat exchange between the surface of the heater and flow medium:

$$Nu = A Re^n Pr^b Gr^c \left(\frac{Pr_p}{Pr_c} \right)^d,$$

where Re – is Reynolds criterion, which characterizes the ratio of the inertia and viscosity forces and determines the character of fluid (gas); Pr – is Prandtl number, which characterizes the physical properties of the

fluid (gas); Gr – is Grashof number, which characterizes the lifting force, which appears in the fluid (gas) as a result of densities difference.

Prandtl similarity criterion is a physical parameter, which characterizes the properties of the flow. Grashof number also does not contain the velocity of the flow and only characterizes the interaction of the molecular friction and lifting force, this is stipulated by the densities difference in separate points of the flow due to its non-isothermality. Only Reynolds criterion Re contains the flow velocity, we are interested in. That is why, in general case the connection between Nusselt criterion, which contains the coefficient of the convective heat transfer and Reynolds criterion, which contains flow velocity V , can be written in the form:

$$Nu = C Re^n,$$

where C – is specific heat of the measuring environment; or:

$$\frac{\alpha d}{\lambda} = C \left(\frac{v d \rho}{\mu} \right)^n,$$

It follows:

$$\alpha = C \frac{\lambda d^{n-1} \rho^n}{\mu^n} v^n = C \frac{\lambda d^{n-1}}{\mu^n} G_M^n,$$

where d – is the diameter of the tube, where the flow velocity is measured; v – is the flow velocity ρ , μ , λ – is the density, viscosity, heat conduction of the measured medium; G_M – is a mass flow rate.

It should be noted, that for practical realization, as a rule, criterion equations, obtained as a result of the experimental research, are used.

Modeling

A number of the results of the thermal calculations of two typical constructive solutions of the integral structures of the thermal flow sensors, carried out by us, are given below. The first of them (Figure 1a) - it is the crystal (B) of the silicon integrated circuit, in the centre of which on the membrane (M) one heater (H) is formed, and on the periphery - two or four sensors (S1, S2) of the difference temperature $\Delta T = T_{S2} - T_{S1}$. To minimize the heat transfer from the heater to the sensors the thermal resistance of the membrane must be as high as possible - in ideal case the heat transfer must be performed only through the medium (gas or fluid) of the measuring flow. That is why, the thickness of the membrane is minimal, typically - not more than 0.05 mm.

The sensors of the difference temperature must also have maximum heat resistance relatively the structure of the integrated circuit, that is why, they are formed with dielectric sublayer with low thermal conductivity (figure 1). Instead the thermal resistance of the integrated circuit structure on the whole must have minimal thermal resistance with the heat sink on which this circuit is mounted. It provides the fixed temperature of the structure and the lack of the temperature gradients, stipulated by the direct heat transfer across the membrane to the sensors.

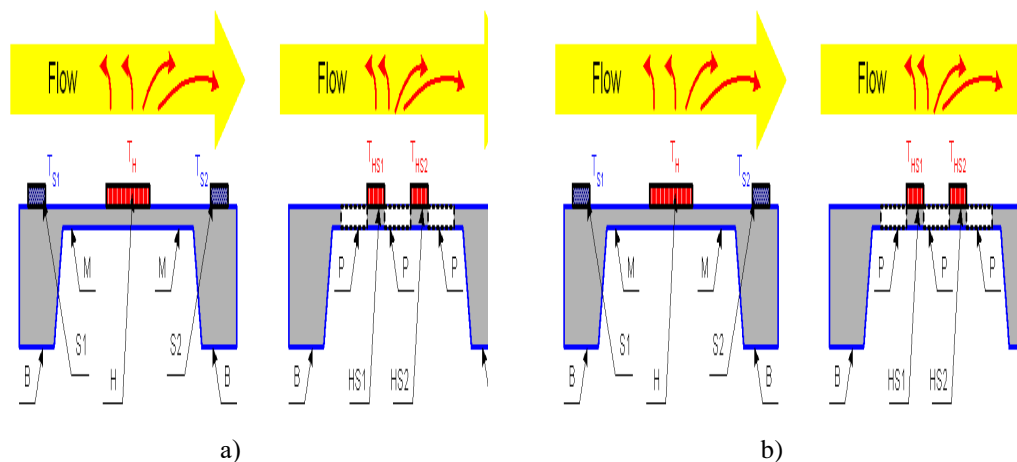


Figure 1 – Typical constructive solutions of the thermal flow sensors

The realization of the above-mentioned requirement is not a problem as the thermal conductivity coefficient λ_{Si} of the silicon (basic semiconductor of the solid-state integrated circuits) and eutectic alloy gold-silicon λ_{Si-Au} (the layer that connects the crystal of the integrated circuit with the radiator) is rather high – $\lambda_{Si} = 120 \text{ W/(m}\cdot\text{K)}$, $\lambda_{Si-Au} = 150 \text{ W/(m}\cdot\text{K)}$, correspondingly. Instead, thermal conductivity coefficient of the majority of the dielectric layers, on which temperature sensors are formed (oxide or silicon nitride) is several tens of times

less that provides good thermal insulation of the temperature sensors from the crystal of the integrated circuit of the primary converter of the flow sensor.

The examples of the calculations results of the temperature field of the flow sensor structure without the available flow are shown in Figure 2a in the process of heat transfer across the flow (at various values of the normalized flow rate 1 ... 4) - in Figure 3. Temperature field has three characteristic sections: B - crystal of the integrated circuit, temperature of which is practically stable, M - peripheral part of the membrane and H - central part of the membrane, where the heater is located.

At very small flow rates (Flow 1) the temperature field remains practically unchanged and temperature difference between the sections of temperature Sensors 1 and Sensor 2 location is small. Increase of flow rate 2 and flow rate 3 leads to the transfer of heat in the direction of its motion and corresponding increase of temperature difference $\Delta T = T_{S2} - T_{S1}$. The temperature of the heater decreases, this stipulates nonlinearity of the flow sensor conversion function.

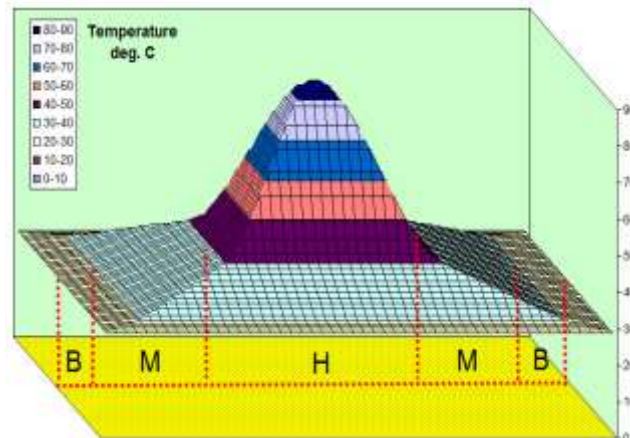


Figure 2 – Temperature field of the integrated structure (Figure 1a) without the impact of the heat transfer across the flow

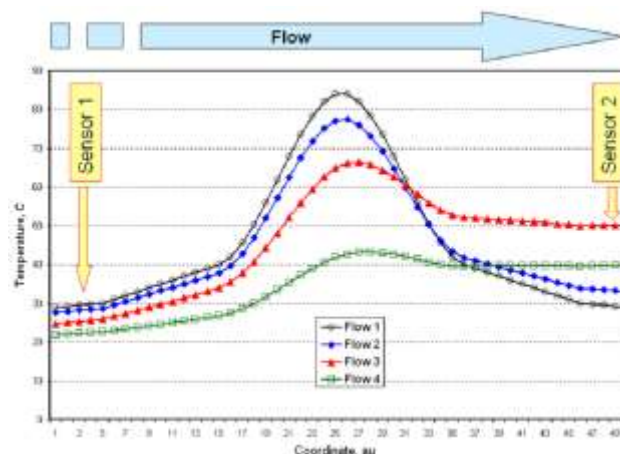


Figure 3 –Temperature field of the integrated circuit (see Figure 1a) at different flow rates (in normalized units – Flow1...4)

Further increase of the flow rate (Flow 4) leads to considerable cooling of the heater at non-sufficient heating of the flow medium, this stipulates the decrease of the structure heating in the section where temperature Sensor 2 is located and the decrease of temperature difference ΔT . Figure 4 shows typical dependence of the temperature difference ΔT on the flow rate. This dependence is the determining for the development of the structure of the primary flow sensor converter and determines the linearity of the conversion function and admissible measurement range.

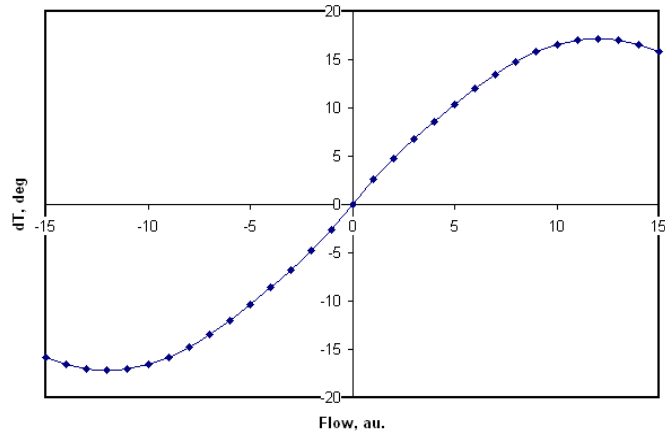


Figure 4 – Dependence of temperatures difference $\Delta T = T_{S2} - T_{S1}$ on the flow rate

Similar calculations were carried out also for the second typical construction of the primary converter of the thermal flow sensor structure (see Figure 1b), which contains two integrated elements (HS1, HS2), each of these elements serves both as a heater and temperature sensor. In order to minimize the heat transfer these elements are made in the form of bridges, contacting with the structure of the crystal only in two points. Lateral sides of the elements are suspended, i.e., heat exchange is carried out only across the medium (P) of the flow.

Typical picture of the temperature field of such structure without the impact of the heat transfer across the flow is shown in Figure 5.

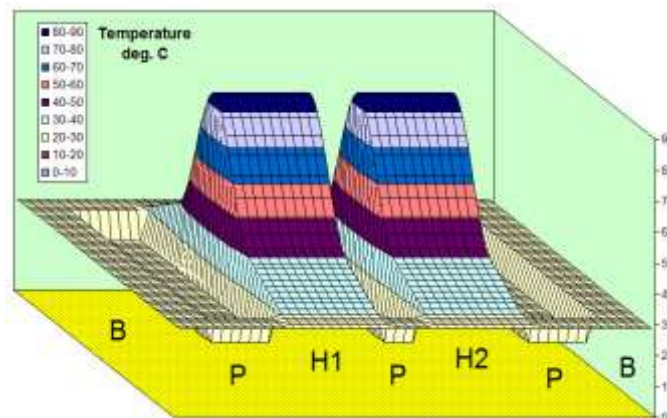


Figure 5 – Temperature field of the integral structure (see Figure 1b) without the impact of the heat transfer across the flow

The temperature of the medium between the integrated elements (HS1, HS2) we assume to be a stable value (in the Fig. it is represented by the lowered sections P). Information value of the primary converter of the flow sensor is the temperatures difference of the integrated elements $\Delta T = T_{HS2} - T_{HS1}$.

The example of the calculation of the temperature field of the structure with two integrated elements at certain flow rate is shown in Figure 6. Similarly to the above-mentioned calculations the increase of temperatures difference

$\Delta T = T_{HS2} - T_{HS1}$, is observed in case of flow rate increase, it is stipulated by the decrease of the convective heat exchange between the heaters and the flow in the direction of its propagation. In the given case it is stipulated by the increase of the medium temperature of the flow while its passage above the heaters (taking into account the large gradients of the temperatures in the flow, its temperature is not presented in the figure- it is assumed to be the fixed value $T_A = 20^\circ\text{C}$). As in the previous case with one heater at certain critical rate of the flow the function of temperature difference takes the extreme value, after that the temperatures difference decreases. This limits the range of the flow rate measurement.

The analysis, carried out, confirms the data, published in literature [1-5], that the function of thermal flow sensors conversion is nonlinear and at certain value of the flow rate there comes the mode at which the gradient of the temperatures ceases to increase and starts to decrease at the increase of the flow rate.

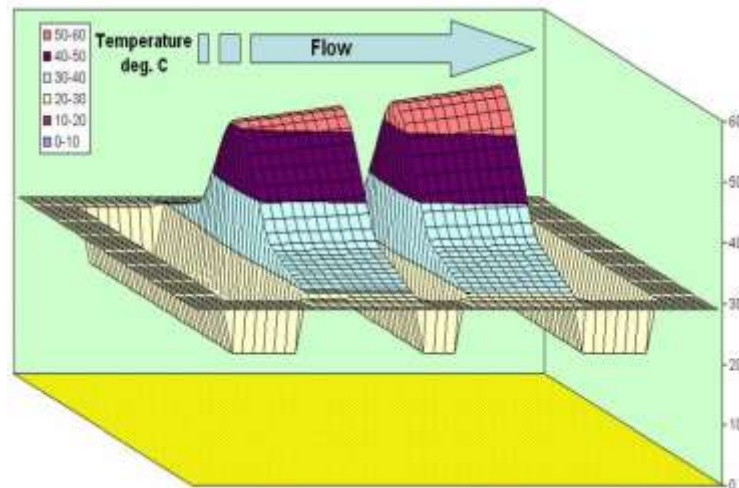


Figure 6 –Temperature field of the integrated circuit (see Figure 1b) at a certain flow rate

Conclusions

1. A complex method of electro-thermal modeling of measuring transducers of thermal flow sensors has been developed, which includes the synthesis of a substitution circuit for pulsed temperature relaxation and a method of forming I-V converters in the mode of their self-heating by the supply current.
2. Considered problems of instability of iterative processes in the analysis of I/V measuring converters with negative differential resistance due to self-heating of these converters. An express method of determining the limits in which correct electrothermal DC analysis is provided has been developed.

References

- [1] Y. Fang and W. W. Liou. Computations of the Flow and Heat Transfer in Microdevices Using DSMC With Implicit Boundary Conditions // *J. Heat Transfer*. – 2002. – Vol. 124. – P. 338–345.
- [2] W.W. Liou and Y. Fang. Implicit Boundary Conditions for Direct Simulation Monte Carlo Method in MEMS Flow Predictions // *CMES*. – 2000. – Vol. 1, No. 4, – P. 119–128.
- [3] Y. Weiping, L. Chong, L. Jianhua, M. Lingzhi and N. Defang. Thermal distribution microfluidic sensor based on silicon // *Sensors and Actuators B*. – 2005. – Vol. 108. – P. 943–946.
- [4] B.W. van Oudheusden. Silicon thermal flow sensors // *Sensors and Actuators A: Phys.* – 1992. № 30. – PP. 5–26.
- [5] M. Ashauer, H. Glosch, F. Hedrich, N. Hey, H. Sandmaier, W. Lang. Thermal flow sensor for liquids and gases based on combinations of two principles // *Sensors and Actuators A*. – 1999. Vol. 73. – PP. 7–13.
- [6] F. Jiang, Y.-C. Tai, C.-M. Ho, R. Karan, M. Garstener. Theoretical and experimental studies of micromachined hot-wire anemometers // *International Electron Devices Meeting (IEDM)*, San Francisco, December 11–14. – 1994. PP. 139–142.
- [7] J.J. van Baar, R.W. Wiegerink, T.S.J. Lammerink, G.J.M. Krijnen, M. Elwenspoek. Micromachined structures for the thermal measurements of fluid and flow parameters // *J. Micromech. Microeng.* – 2001. – № 11. – PP. 311–318.
- [8] T. S. T. Lammerink, N. R. Tas, M. Elwenspoek, J. H. J. Fluitman. Micro-liquid flow sensor // *Sensors and Actuators A*. – 1993. – PP. 45–50.
- [9] P.M. Handford, P. Bradshaw. The pulsed-wire anemometer // *Exp. Fluids* 7. – 1989. – PP. 125–132.
- [10] Ellis Menga, Po-Ying Li, Yu-Chong Tai. A biocompatible Parylene thermal flow sensing array // *Sensors and Actuators A*. – 2008. № 144. –PP. 18–28.
- [11] A. Margelov. Honeywell gas flow sensors [Electronic resource] / A. Margelov // *Chip News*. — 2005. — № 9 (102). — C.56—58. — www.chip-news.ru.
- [12] Z.Yu. Gotra, R.L. Holyaka, S.V. Pavlov, S.S. Kulenko, O.V. Manus Differential thermometer with high resolution // *Technology and construction in electronic equipment*. - 2009. - No. 6 (84). - P. 19 - 23.3.Ю.
- [13] Pavlov S. V. *Information Technology in Medical Diagnostics* //Waldemar Wójcik, Andrzej Smolarz, July 11, 2017 by CRC Press - 210 Pages.
- [14] Wójcik W., Pavlov S., Kalimoldayev M. *Information Technology in Medical Diagnostics II*. London: (2019). Taylor & Francis Group, CRC Press, Balkema book. – 336 Pages.

- [15] Highly linear Microelectronic Sensors Signal Converters Based on Push-Pull Amplifier Circuits / edited by Waldemar Wojcik and Sergii Pavlov, Monograph, (2022) NR 181, Lublin, Comitet Inzynierii Srodowiska PAN, 283 Pages. ISBN 978-83-63714-80-2.
- [16] Pavlov Sergii, Avrunin Oleg, Hrushko Oleksandr, and etc. System of three-dimensional human face images formation for plastic and reconstructive medicine // Teaching and subjects on bio-medical engineering Approaches and experiences from the BIOART-project Peter Arras and David Luengo (Eds.), 2021, Corresponding authors, Peter Arras and David Luengo. Printed by Acco cv, Leuven (Belgium). - 22 P. ISBN: 978-94-641-4245-7.
- [17] Kukharchuk, Vasyl V., Sergii V. Pavlov, Volodymyr S. Holodiuk, Valery E. Kryvonosov, Krzysztof Skorupski, Assel Mussabekova, and Gaini Karnakova. 2022. "Information Conversion in Measuring Channels with Optoelectronic Sensors" *Sensors* 22, no. 1: 271. <https://doi.org/10.3390/s22010271>
- [18] Avrunin, O.G.; Nosova, Y.V.; Pavlov, S.V.; Shushliapina, N.O.; and etc. Research Active Posterior Rhinomanometry Tomography Method for Nasal Breathing Determining Violations. *Sensors* 2021, 21, 8508. doi: 10.3390/s21248508, <https://www.mdpi.com/1424-8220/21/24/8508>.
- [19] Avrunin, O.G.; Nosova, Y.V.; Pavlov, S.V.; and etc. Possibilities of Automated Diagnostics of Odontogenic Sinusitis According to the Computer Tomography Data. *Sensors* 2021, 21, 1198. <https://doi.org/10.3390/s21041198>.
- [20] Vasyl V. Kukharchuk, Sergii V. Pavlov, Samoil Sh. Katsyv, and etc. "Transient analysis in 1st order electrical circuits in violation of commutation laws", PRZEGLĄD ELEKTROTECHNICZNY, ISSN 0033-2097, R. 97 NR 9/2021, p. 26-29, doi:10.15199/48.2021.09.05.
- [21] Sensors of electric magnetic radiation for bioengineering research / G. S. Tymchyk; V. I. Skytsiuk, M. A. Waintraub, T. R. Klochko. – K. : S.E. Lesia, 2004. – 64 p.
- [22] Osadchuk O. V Microelectronic frequency converters on the base of the transistor structures with negative resistance / O. V. Osadchuk. – Vinnytsia: UNIVERSUM- Vinnytsia, 2000. – 303 p.

Надійшла до редакції 01.11.2023

Видано за грантової підтримки Національного фонду досліджень України в рамках проекту 2022.01/0135 "Розробка лазерно-фотонного лікувально-діагностичного комплексу медичної реабілітації пацієнтів з політравмами різного ступеня важкості"

Information about authors

Pavlov Sergii – D.Sc., Professor of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

Wójcik Waldemar – D.Sc., Professor, director of the Institute of Electronics and Information Technology at Lublin University of Technology. Doctor Honoris Causa of five Universities in Ukraine and Kazakhstan

Holyaka Roman – D.Sc., Professor of Electronic Device of Information-Computer Technologies Department, Lviv Polytechnic National University

Azarov Olexiy – D.Sc. Professor, head of Computer Technology Department, Vinnytsia National Technical University

Nykyforova Larysa - Doctor of Technical Sciences, Professor of the Department of Automation and Robotic Systems named after Academician I.I. Martynenko, National University of Life and Environmental Sciences of Ukraine

Yang Longyin – M.Sc., post-graduated student of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

С.В.Павлов¹, Вальдемар Вуйцік², Р.Л. Голяка³, О.Д. Азаров¹,
Л.Є. Никифорова⁴, Ян Лунінь¹

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ТЕПЛОВОГО ПОЛЯ ІНТЕГРАЛЬНОЇ СТРУКТУРИ ПРИ РЕАЛІЗАЦІЇ СЕНСОРІВ ДЛЯ БІОМЕДИЧНИХ ДОСЛІДЖЕНЬ

¹Вінницький національний технічний університет

²Люблінський університет технологій, Польща

³Національний університет «Львівська Політехніка»

⁴Національний університет біоресурсів та природокористування України

Li Jingiong, Sergii Pavlov

EXPERT BIOINFORMATION SYSTEM FOR DIAGNOSING FORMS OF ACUTE LEUKEMIA BASED ON ANALYSIS OF BIOMEDICAL INFORMATION

Vinnytsia National Technical University, Vinnytsia

Анотація. В статті представлено значення лейкемії в здоров'ї людини та проблеми, пов'язані як з діагностикою, так і з терапією. Мета статті - надати інформаційно-технологічне рішення цієї проблеми, тим самим покращуючи доступ для пацієнтів і прогнозування. Запропонована концептуальна модель експертної системи діагностики острих лейкозів, яка дозволить знизити неоднозначність в інтерпретації об'єктів дослідження. Розглянуто фактори, що впливають на правильне розпізнавання складних об'єктів (виявлення бластних і небластних клітин крові) за допомогою експертної системи на основі методів комп'ютерної мікроскопії.

Ключові слова: гострий лейкоз, діагностика та терапія, біомедичне зображення, зображення бластних і небластних клітин крові

Abstract. The introductory chapter established the context for this paper by stressing the significance of leukemia in healthcare and the challenges associated with both diagnosis and therapy. The paper ultimate objective is to provide an information technology solution to these issues, thereby improving patient care and prognosis. A conceptual model of an expert system for the diagnosis of acute leukemia is proposed, which will reduce the ambiguity in the interpretation of research objects. Factors influencing the correct recognition of complex objects (images of blast and non-blast blood cells) using an expert system based on computer microscopy methods are considered.

Keywords: acute leukemia, diagnosis and therapy, biomedical image, images of blast and non-blast blood cells

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-84-93>.

Introduction

Blood cancers, including leukemia, are a major global health concern because they affect people of all ages and demographics. The disease's annual incidence rate of 13 cases per 100,000 individuals illustrates how widespread it is and how much it strains international health systems (Begum et al, 2020). Acute leukemia, which makes up 1-2% of cases, is the deadliest subtype of malignant neoplasms. This cancer is associated with distinct demographic patterns: men are more susceptible than women, and the majority of victims are Caucasians (Rehman et al., 2018). While acute myeloid leukemia is more common in older adults, acute lymphocytic leukemia usually affects teenagers. Age is yet another crucial component (Singha et al., 2021). Moreover, chronic lymphocytic leukemia and chronic myelogenous leukemia differ in their epidemiological characteristics [1,2,3,4].

Leukemia's epidemiology demonstrates the diverse nature of this group of blood cancers, with differences observed in several demographic factors. One such component that exhibits intriguing patterns to help make sense of the intricate relationships between lifestyle, environment, and genetic factors is gender (Rehman et al., 2018). Men are frequently slightly more likely than women to develop leukemia. Gender differences in leukemia susceptibility point to potential underlying causes (Vosberg & Greif, 2019). All subtypes show a general consistency in this greater occurrence in men's pattern, suggesting a stable tendency. Acute lymphocytic leukemia is one notable exception, though. In this subtype, there is little recorded female predominance (Begum et al, 2020). It is a difficult challenge to identify the factors that contribute to these gender-specific variances in leukemia development, including genetic, hormonal, and environmental factors [5,6,7,].

Potential causes of these gender-based variances in leukemia incidence include genetic variations, hormonal variations, and differing exposures to environmental toxins. The genetic susceptibilities of men and women to leukemia may differ, thus influencing their respective risk profiles (Rehman et al., 2018). Hormonal differences may also be significant because they affect the development and progression of some leukemia subtypes, particularly those linked to puberty and pregnancy (Ansari et al., 2023). discrepancies in lifestyle and profession may also contribute to the observed discrepancies between men and women, as they often have distinct exposure patterns to possible carcinogens [8,9,10].

The purpose of this work is to develop a conceptual model of an expert system for diagnosing acute leukemia using computer microscopy methods, as well as to analyze the influence of factors that influence the result of recognition of poorly formalized objects (images of blast and non-blast cells).

Objectives: To design and implement an information technology system for the rapid and reliable detection of acute leukemia; To develop a forecasting model that can assist healthcare professionals in making informed treatment decisions based on the patient's condition and characteristics; To assess the performance and effectiveness of the developed information technology solution through rigorous testing and evaluation.

Problems

There is no doubt that racial and ethnic disparities affect the prevalence of leukemia, with Caucasians having a larger risk than other racial groupings. The fundamental causes of the racial disparities in leukemia incidence have been the subject of extensive research (Singha et al., 2021). One important component that may account for these discrepancies is genetic predisposition. There is proof that some genetic mutations and circumstances increase the likelihood of developing leukemia (Vosberg & Greif, 2019). Caucasians may have greater rates of leukemia because some racial or ethnic groupings may have a higher prevalence of these genetic variants (Begum et al, 2020). Understanding the genetic underpinnings of leukemia across different ethnic groups is essential for more effective tailoring of diagnostic and treatment strategies.

A further factor influencing the variations in leukemia incidence throughout ethnic groups is environmental exposure. Exposure to toxins or carcinogens is one environmental element that may affect a person's risk of leukemia (Rehman et al., 2018). Examples of how various racial and ethnic groups may be more or less exposed to environmental risk factors include variations in lifestyle, occupation, and site of residence (Abdeldaim et al., 2018). Examining these environmental exposures within specific ethnic populations is essential to reduce disparities in leukemia incidence and to find effective preventive interventions [11,1213,14].

Furthermore, differences in healthcare access and consumption may potentially contribute to the differences in leukemia incidence throughout ethnic groups. Socioeconomic position, cultural barriers, and variations in the healthcare system can all affect the accessibility and quality of treatment (Abdeldaim et al., 2018). Minority populations could experience difficulties accessing healthcare services, which could lead to delayed diagnosis and less satisfactory treatment outcomes. Reducing these gaps in healthcare consumption and access is necessary to guarantee that all individuals, irrespective of their ethnicity, have equitable access to early diagnosis and appropriate treatment for leukemia (Begum et al, 2020). Work of this nature can help close the gap in leukemia incidence between different racial and ethnic groupings.

Age is a key demographic factor in the epidemiology of leukemia that significantly affects the variations in incidence and frequency of distinct leukemia subtypes. Age-specific patterns in leukemia offer valuable insights into the relationship between age and disease susceptibility, particularly in the context of acute myeloid leukemia (AML) and acute lymphocytic leukemia (ALL) (Rehman et al., 2018). When it comes to leukemia, age plays a big role in determining the prevalence of different disease subtypes. Acute lymphocytic leukemia (ALL) is largely a pediatric disease, with the majority of cases occurring in children between the ages of two and five (Abdeldaim et al., 2018). Because ALL mostly affects children, its age distribution highlights its unique traits.

Methodology

Because of the peculiar characteristics of pediatric ALL, including specific genetic alterations and treatment modalities, this age group needs specialist care. Acute myeloid leukemia (AML), on the other hand, has an extremely clear age-related pattern (Rehman et al., 2018). Over 60 years of age, the incidence of AML rises dramatically, leading to a higher diagnosis rate in this age group. The complex interplay between several aging-related factors, including alterations in the bone marrow microenvironment, cumulative genetic mutations, and exposure to environmental risk factors over time, result in this age-specific rise in AML incidence (Begum et al, 2020). Because older persons are more likely to develop AML, the disease mostly affects the elderly.

The age-related patterns in ALL and AML highlight the heterogeneity of leukemia and the importance of tailoring diagnostic and treatment strategies to the individual needs and characteristics of patients of different ages. Treatment strategies for pediatric ALL are often less aggressive than those for adults since children are more tolerant of rigorous therapy than adults are (Arber et al., 2017). On the other hand, for older persons with AML, therapeutic approaches specific to age-related comorbidities and treatment tolerance may be required. To make an accurate diagnosis and offer tailored therapy, medical professionals need to understand how aging impacts the epidemiology of leukemia (Williams et al., 2019). Additionally, it advances ongoing research that aims to develop age-specific strategies to improve treatment results for leukemia patients of all ages (Begum et al, 2020). By comprehending the minute variations in leukemia incidence among age groups, medical practitioners can enhance patient care and results.

Beyond general demographic trends, distinct subtypes of leukemia display age-related patterns and distinctive characteristics. These variations highlight the complexity of leukemia as a blood cancer class with a

broad spectrum of risk factors and clinical presentation (Rehman et al., 2018). This variety is best demonstrated by the age distribution of two subtypes: chronic lymphocytic leukemia (CLL) and chronic myelogenous leukemia (CML). The age distribution of chronic myelogenous leukemia (CML) is unique; it is bimodal. This suggests that the incidence rates of CML show two distinct peaks at different phases of life (Ansari et al., 2023). In early adulthood, the initial peak often occurs between the ages of 25 and 30. There may be a link between specific genetic abnormalities or risk factors that impact this age range and the early start of CML. The incidence of CML peaks again after late adulthood, with greater rates observed in individuals over 60 (Begum et al., 2020). It is critical to comprehend this bimodal age distribution to adapt therapy and diagnostic strategies to individuals at different phases of life.

However, there is a notable difference in the age-related pattern of chronic lymphocytic leukemia (CLL). The majority of patients with this subtype of leukemia are elderly adults; the typical diagnostic age is almost 70 years (Zolfaghari & Sajedi, 2022). When compared to bimodally distributed CML, late adulthood is the primary age at which CLL affects individuals. This age-related tendency in CLL may result from the intricate interactions between immunological changes, genetic variables, and cumulative exposure to environmental factors throughout time. Because these age-related trends in CML and CLL affect diagnosis and treatment decisions, healthcare providers need to be aware of them (Ansari et al., 2023). The unique characteristics of these subtypes—such as the bimodal distribution in CML and the prevalence of elderly persons in CLL—require specialized methods of care. The patient's age, comorbidities, and potential drug adverse effects may need to be considered in treatment approaches (Begum et al., 2020). Moreover, leukemia epidemiology research continues to explore the underlying causes of these diverse age-related trends, providing insights into the mechanisms driving the formation of distinct leukemia subtypes over a range of age ranges.

An approach to solving the problem of diagnosis and treatment of leukemia

Leukemia diagnosis and treatment provide complex problems for medical professionals, necessitating a multimodal approach to address the complex psychological, emotional, and physical elements of this illness. Leukemia patients deal with the emotional toll of managing their illness and its effects on their lives in addition to the physical difficulties of the disease (Shah et al., 2021). Further highlighting the need for sophisticated, precise, and quick diagnostic techniques are the complexity of leukemia subtypes, variations in patient demographics, and the wide range of survival rates.

The unchecked growth of abnormal white blood cells, which compromises the body's capacity to fight infections and generate healthy blood cells, is a hallmark of leukemia, a kind of blood cancer. Blood counts, bone marrow biopsies, and cytogenetic analysis are among the tests used in the diagnosis of leukemia to identify the particular subtype of the disease (Ahmed et al., 2023). Treatment strategies differ based on the kind of leukemia, patient age, and general health, and frequently entail stem cell transplantation, radiation therapy, and chemotherapy. For patients and their families, receiving a leukemia diagnosis and treatment can be extremely taxing emotionally. Anxiety, despair, and social isolation might result from treatment-related adverse effects, uncertainty about the disease's course, and dread of recurrence (Zolfaghari & Sajedi, 2022). To address these issues and improve patients' quality of life, effective communication, emotional support, and psychological treatment are essential.

The wide range of leukemia subtypes, each with unique genetic abnormalities and clinical manifestations, makes fast and correct diagnosis extremely difficult. Although helpful, traditional diagnostic approaches can be time-consuming and interpreted differently (Zolfaghari & Sajedi, 2022). It is critical to have reliable diagnostic instruments that can quickly and precisely detect leukemia subtypes. There are notable differences in leukemia incidence and survival rates among various demographic groups. Social class, age, gender, and ethnicity can all affect treatment outcomes, access to high-quality care, and the likelihood of developing leukemia (Shah et al., 2021). Comprehending these demographic disparities is crucial in formulating focused preventive measures and enhancing healthcare parity.

Excessive production of abnormal blood cells occurs in the bone marrow, the source of leukemia, a group of blood malignancies. Even though leukemia therapy has advanced significantly in recent years, survival rates for the various cancer subtypes still vary significantly (Ahmed et al., 2023). In the continuous efforts to create more effective medicines and individualized treatment plans for leukemia patients, an understanding of these discrepancies is essential. The increase in survival rates is one of the most positive advances in leukemia research and treatment (Ansari et al., 2023). This advancement is the result of numerous variables, such as improved leukemia patient supportive care, more precise treatment protocols, focused therapy development, and advancements in diagnostic techniques (Shah et al., 2021). Many people with leukemia now have higher survival rates and improved quality of life as a result of these advancements.

Significance of the Study

The creation of an efficient and reputable technique for identifying acute leukemia is one of the main goals of this research. This is significant because it can revolutionize the present diagnostic procedure, which is

laborious and dependent on human interpretation (Arber et al., 2017). Healthcare practitioners now have access to a diagnostic tool that is more accurate and efficient thanks to information technology solutions. This may result in the early identification of acute leukemia, allowing for the timely start of treatment and maybe enhancing the prognosis for affected individuals (Singha et al., 2021). Quick diagnosis is especially important when it comes to acute leukemia because of its quick and aggressive progression.

Another important factor contributing to the study's significance is its emphasis on predictive capacities. Making predictions about how acute leukemia patients will progress and respond to therapy could completely change how medical practitioners make decisions (Arber et al., 2017). The research can provide clinicians with valuable insights about the expected course of a patient's sickness by utilizing computer processing techniques and biomedical data (Ahmed et al., 2023). This in turn makes it easier to make well-informed treatment decisions, enabling a more efficient and individualized method of providing care (Shah et al., 2021). Patients with leukemia may experience better results and a higher quality of life as a result of this customized care.

This study's potential to solve current gaps in leukemia management highlights its significance. Leukemia is a broad and complicated group of diseases, each having specific traits, treatment options, and prognoses (Singha et al., 2021). By facilitating a systematic and data-driven approach to leukemia care, information technology solutions can assist in harmonizing the diagnosis and treatment procedures. This harmonization can be especially helpful in raising the standard of care across medical facilities and geographical areas, guaranteeing that patients receive the finest care available wherever they seek care. Furthermore, the study has significant ramifications for medical practitioners that go beyond leukemia treatment (Arber et al., 2017). Through the utilization of computer processing techniques and information technology, this research can provide physicians with a multitude of data-driven insights (Kadia et al., 2016). In turn, these insights are a potent tool that enables medical practitioners to make decisions based on accurate forecasts and verifiable data.

This shift in the process of making decisions has broad implications. With these cutting-edge resources at their disposal, healthcare professionals may feel more confident in the treatments they choose to administer (Arber et al., 2017; Rose-Inman & Kuehl, 2017). They can now make decisions based on tailored insights derived from each patient's biology data, rather than on guesswork or broad methods, which gives them a sense of confidence (Ahmed et al., 2023). The reduction of the uncertainty that sometimes accompanies the treatment of complicated medical illnesses, including leukemia, is one very notable feature of this transition. Even the most skilled medical practitioners may encounter difficulties due to the complexities and particular patient-specific characteristics that these illnesses frequently exhibit (Kadia et al., 2016). Information technology solutions have the potential to greatly lessen this uncertainty load.

Healthcare providers can handle leukemia cases more skillfully if they have a deeper comprehension of the unique requirements and prognosis of each patient. Consequently, this opens the door for the provision of more patient-centered care (Singha et al., 2021). Instead of depending exclusively on traditional, one-size-fits-all methods, medical professionals can customize treatment regimens to meet the unique needs of every patient. As a result, patients now receive care at a higher standard that is more sensitive to the unique circumstances of each patient and the dynamic nature of leukemia (Shah et al., 2021). This study essentially serves as a cornerstone in the effort to equip medical personnel with the information, resources, and understanding necessary to provide more efficient, individualized, and patient-centered treatment (Arber et al., 2017). The research eventually helps patients and healthcare professionals by contributing to a larger paradigm shift in healthcare through the reduction of ambiguity, improvement of evidence-based decision-making, and provision of customized insights.

Method

One of the first stages in the diagnosis of acute leukemia is the study of peripheral blood for the presence of blast cells. This procedure is associated with a number of difficulties, the main of which is the high variability of blast cells and the similarity of the images of some of them with non-blast cells, which causes errors in their classification. It should be noted that such an expert system serves as a tool for a hematologist in diagnosing acute leukemia.

The main advantage of the system being developed is a reference selection of digital images, the descriptions of which are stored in the knowledge base. An important component of the system is the analytical subsystem, which includes many rules by which decisions are made [15,16,17,18].

Mathematical models based on spatially connected preparation have been developed. The essence of spatially connected preparation (SCP) consists in finding the intensity differences between readings of the discretized image according to the eight ranks of connectivity (Fig. 1), forming two-level detection signals, transforming the collection of detection signals into a collection of SCP, forming SCP functions and forming by summing masked ones separately functions of CSP of positive, negative and zero generalized spatially connected preparations (GSCP).

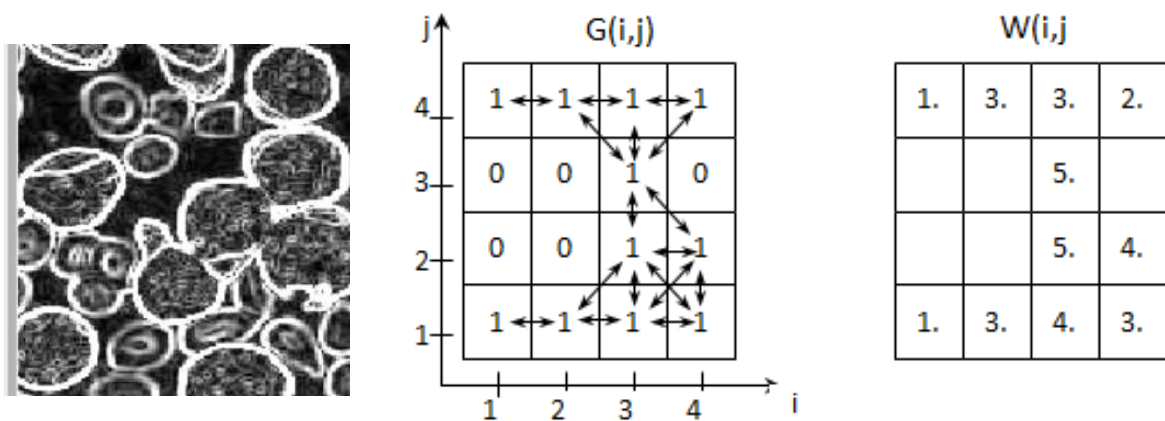


Figure 1 – Finding the intensity differences between counts of the discretized image by eight ranks of connectivity

We form the functions of spatially connected preparations, obtaining a system of functions of the PZKP:

$$\begin{cases} f_{i,j(\beta)}^{(\bar{\alpha}_1)} = \begin{cases} 1, & \text{if } r_{i,j(\beta)}^{+(\bar{\alpha}_1)} = \beta \\ 0, & \text{that,} \\ \dots \end{cases} \\ \dots \\ f_{i,j(\beta)}^{(\bar{\alpha}_8)} = \begin{cases} 1, & \text{if } d_{i,j(\beta)}^{+(\bar{\alpha}_8)} = \beta \\ 0, & \text{that} \end{cases} \end{cases}$$

In accordance with the method of generalized spatial connectivity, we form the system of functions of SCP from the system of functions of GSCP in the form [19, 20, 21]:

$$\left\{ \begin{array}{l} F_{|\bar{\alpha}_V|=1(\beta)}^{i,j} = \sum_{v=1}^8 (f_{i,j|\bar{\alpha}_V|=1(\beta)}^{(\bar{\alpha}_v)} \omega_{i+l,j+\tau, \xi_k, \eta_k}) \\ \dots \\ F_{|\bar{\alpha}_V|=S(\beta)}^{i,j} = \sum_{v=1}^8 (f_{i,j|\bar{\alpha}_V|=S(\beta)}^{(\bar{\alpha}_v)} \omega_{i+l,j+\tau, \xi_k, \eta_k}) \end{array} \right. , \quad (1)$$

where $F_{|\bar{\alpha}_V|(\beta)}^{i,j}$ - is the generalized SCP function.

The local spectrum of spatial connectivity (SCP) $W_{\wedge(i,j)}^{\bar{Z}_{V(\beta)}}$ is defined by the expression:

$$W_{\wedge(i,j)}^{\bar{Z}_{V(\beta)}} = \sum_{|\bar{\alpha}_V|=1}^S F_{\bar{\alpha}(\beta)}^{i,j} = \sum_{|\bar{\alpha}_V|=1}^S F_{\bar{\alpha}(0)}^{i,j} \cup \sum_{|\bar{\alpha}_V|=1}^S F_{\bar{\alpha}(-1)}^{i,j} \cup \sum_{|\bar{\alpha}_V|=1}^S F_{\bar{\alpha}(+1)}^{i,j}. \quad (2)$$

Then the full SCP $W_n^{\bar{\alpha}(\beta)}$ of the image $g(i,j)$ can be determined using expression (1), obtaining the input information for the PI transformation [22,23].

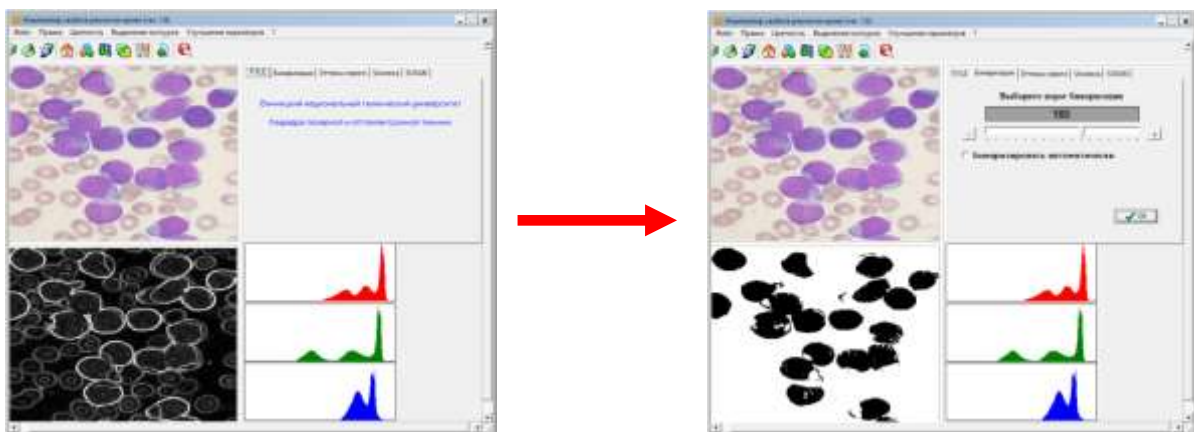
$$W_n^{\bar{\alpha}(\beta)} = \begin{pmatrix} \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{1,1} & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{1,2} & \dots & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{1,m_g} \\ \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{2,1} & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{2,2} & \dots & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{2,m_g} \\ \dots & \dots & \dots & \dots \\ \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{n_g-1,1} & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{n_g-1,2} & \dots & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{n_g-1,m_g} \\ \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{n_g,1} & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{n_g,2} & \dots & \sum_{|\bar{\alpha}_v|=1}^S F_{\bar{\alpha}_v(\beta)}^{n_g,m_g} \end{pmatrix}. \quad (3)$$

Realization of expert system is of peripheral blood for the presence of blast cells

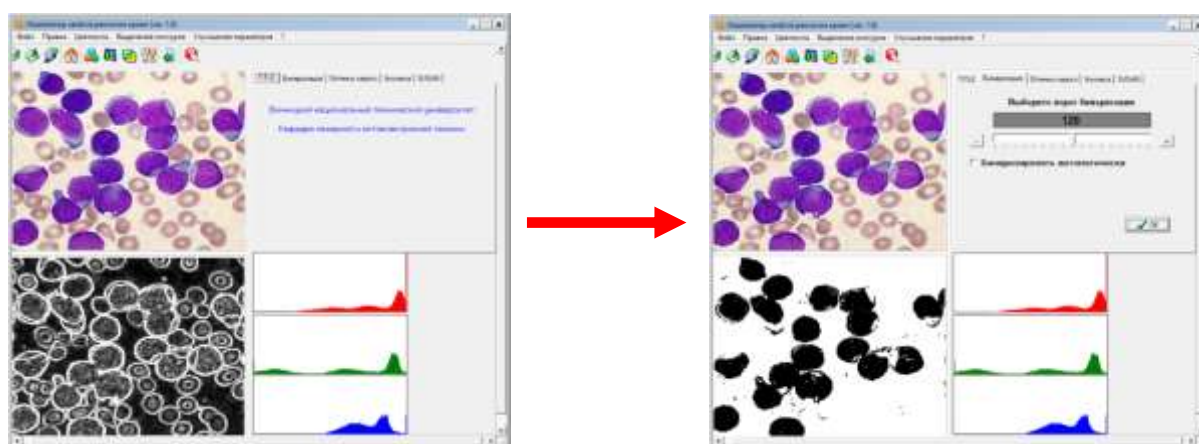
The result of the work of the expert system is a conclusion about whether a cell belongs to a certain type, indicating a probabilistic assessment, which requires the creation of the required volume of a representative reference sample of cell images. The peculiarity of the expert system under consideration is that, along with the knowledge of experts accumulated in it, a database is created based on the results of measuring quantitative characteristics obtained as a result of automated image processing. The authors developed an automated method for processing and isolating blast cells and software "Blood Rheology Analyzer" for a hematologist. In Fig. 2. An example of the processing of blast and non-blast cells is presented.



a) Determination of blast cells against the background of lymphocytes



b) an example of an atypical mononuclear



c) Determination of blast cells

Figure 2 – Example of processing blast and non-blast cells

Recommendations for the development of an expert system for studying peripheral blood for the presence of blast cells

We formulate recommendations for the creation of a system for assessing dynamic changes in biomedical images using the application of monitoring peripheral blood for the presence of blast cells in the following way (Figure 3):

- Processing of images taken per hour of one patient visit;
- Preservation and preservation of the results of digitalization and maintenance of the image database;
- Visualization of the results of the main stages of processing, analysis and alignment of blood cells;
- Organization of interactive interaction with the computer behind an additional graphical interface, which allows you to control the necessary parameters in the process of tracking and data processing, which will ensure the output of the necessary inputs and output data to the doctor in a manual format for processing;
- Notify and prompt the doctor of the results of syntactic and logical control of the data that is entered;
- Formation of a report on the results of processing both one and several biomedical images;
- Implementation of classification algorithms, saving parameters of mask templates, forming a selection with valued sign values, assessing the reliability of diagnosis.
- The adherence to such recommendations gives doctors a low priority, and itself:
- improve all the main structures and change the microcirculatory bed;
- the system is simple, easy to use and easy to use;
- the establishment of a clear scoring gradation will facilitate quantitative analysis and statistical processing of tracking results;
- detailed assessment of dynamic indicators that change during biomedical investigations and course treatment.

A comprehensive characterization of dynamic indicators makes it possible to assess the adequacy of the administered drug dose, the course of treatment, the correction of doses of pharmacological drugs and drug therapy regimens, as well as There are other methods of bathing.

For the system under consideration, instrumental factors can be classified into two groups: the first – factors determined by the instrumental capabilities of the equipment; the second is factors determined by the influence of external conditions. The first group of instrumental factors includes image sensor noise, color and brightness distortions of the camera, diffraction effects of the optical system of the microscope, uneven spectral characteristics of the illuminator in the microscope, uneven illumination of the sample in the field of view of the camera, etc. The factors of the second group include factors determined by the external conditions of use of the system.

When developing measurement techniques, it is necessary to resolve the problems of ambiguity in the interpretation of the measured quantities (for example, cell size, nucleus size, taking into account the variety of shapes of these objects). When choosing measurement models, one should take into account (and for this it is necessary to conduct preliminary studies) the achievable accuracy in measuring the parameters under consideration (for example, the accuracy of measuring the nuclear-cytoplasmic ratio, which is one of the signs widely used by doctors to differentiate cells by type, depends on the accuracy of image segmentation nucleus and cytoplasm).

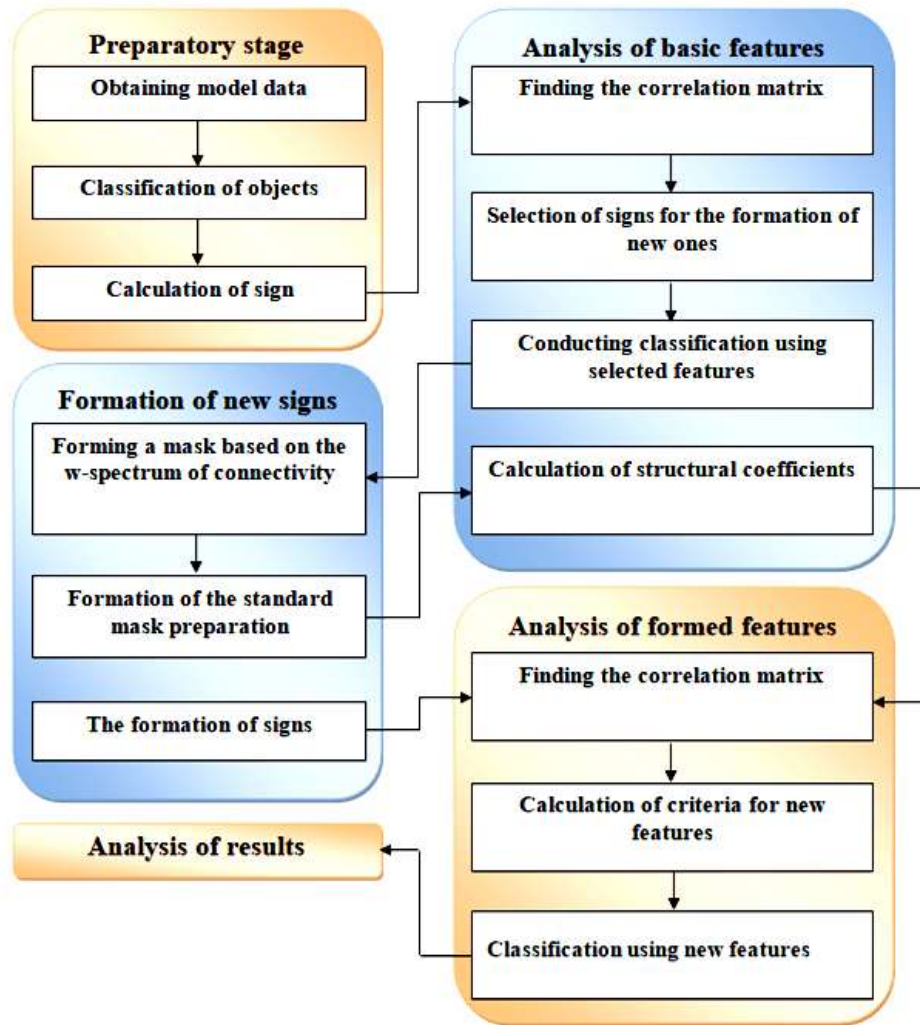


Figure 3 – Scheme of the robotic expert system algorithm for examining peripheral blood for the presence of blast cells

Conclusion

The introductory chapter established the context for this paper by stressing the significance of leukemia in healthcare and the challenges associated with both diagnosis and therapy. The paper ultimate objective is to provide an information technology solution to these issues, thereby improving patient care and prognosis. A conceptual model of an expert system for the diagnosis of acute leukemia is proposed, which will reduce the ambiguity in the interpretation of research objects. Factors influencing the correct recognition of complex objects (images of blast and non-blast blood cells) using an expert system based on computer microscopy methods are considered.

The upcoming chapters will address the impact of the suggested information technology system on the diagnosis and treatment of acute leukemia in addition to a thorough study of the research methodology, data analysis, and conclusions.

References

- [1] Abdeldaim, A. M., Sahlol, A. T., Elhoseny, M., & Hassanien, A. E. (2018). Computer-aided acute lymphoblastic leukemia diagnosis system based on image analysis. *Advances in Soft Computing and Machine Learning in Image Processing*, 131-147.
- [2] Ahmed, I. A., Senan, E. M., Shatnawi, H. S. A., Alkhraisha, Z. M., & Al-Azzam, M. M. A. (2023). Hybrid techniques for the diagnosis of acute lymphoblastic leukemia based on fusion of CNN features. *Diagnostics*, 13(6), 1026.

- [3] Ansari, S., Navin, A. H., Sangar, A. B., Gharamaleki, J. V., & Danishvar, S. (2023). A customized efficient deep learning model for the diagnosis of acute leukemia cells based on lymphocyte and monocyte images. *Electronics*, 12(2), 322.
- [4] Arber, D. A., Borowitz, M. J., Cessna, M., Ezzell, J., Foucar, K., Hasserjian, R. P., ... & Vardiman, J. W. (2017). Initial diagnostic workup of acute leukemia: guideline from the College of American Pathologists and the American Society of Hematology. *Archives of pathology & laboratory medicine*, 141(10), 1342-1393.
- [5] Begum, S., Sarkar, R., Chakraborty, D., & Maulik, U. (2020). Identification of biomarker on biological and gene expression data using fuzzy preference based rough set. *Journal of Intelligent Systems*, 30(1), 130-141.
- [6] Grimwade, L. F., Fuller, K. A., & Erber, W. N. (2017). Applications of imaging flow cytometry in the diagnostic assessment of acute leukaemia. *Methods*, 112, 39-45.
- [7] Kadia, T. M., Jain, P., Ravandi, F., Garcia-Manero, G., Andreef, M., Takahashi, K., ... & Kantarjian, H. M. (2016). TP53 mutations in newly diagnosed acute myeloid leukemia: clinicomolecular characteristics, response to therapy, and outcomes. *Cancer*, 122(22), 3484-3491.
- [8] Rehman, A., Abbas, N., Saba, T., Rahman, S. I. U., Mehmood, Z., & Kolivand, H. (2018). Classification of acute lymphoblastic leukemia using deep learning. *Microscopy Research and Technique*, 81(11), 1310-1317.
- [9] Rose-Inman, H., & Kuehl, D. (2017). Acute leukemia. *Hematology/Oncology Clinics*, 31(6), 1011-1028.
- [10] Shah, A., Naqvi, S. S., Naveed, K., Salem, N., Khan, M. A., & Alimgeer, K. S. (2021). Automated diagnosis of leukemia: a comprehensive review. *IEEE Access*, 9, 132097-132124.
- [11] Singha, A., Thakur, R. S., & Patel, T. (2021). Deep learning applications in medical image analysis. *Biomedical Data Mining for Information Retrieval: Methodologies, Techniques and Applications*, 293-350.
- [12] Vosberg, S., & Greif, P. A. (2019). Clonal evolution of acute myeloid leukemia from diagnosis to relapse. *Genes, chromosomes and cancer*, 58(12), 839-849.
- [13] Williams, P., Basu, S., Garcia-Manero, G., Hourigan, C. S., Oetjen, K. A., Cortes, J. E., ... & Daver, N. G. (2019). The distribution of T-cell subsets and the expression of immune checkpoint receptors and ligands in patients with newly diagnosed and relapsed acute myeloid leukemia. *Cancer*, 125(9), 1470-1481.
- [14] Zolfaghari, M., & Sajedi, H. (2022). A survey on automated detection and classification of acute leukemia and WBCs in microscopic blood cells. *Multimedia Tools and Applications*, 81(5), 6723-6753.
- [15] Timchenko, L., Wojcik, W., Kokriatskaia, N., Levchenko, O., Kryvinska, N. New methods of network modelling using parallel-hierarchical networks for processing data and reducing erroneous calculation risk. *CEUR Workshop Proceedings* this link is disabled, 2020, 2805, pp. 201-212
- [16] Timchenko, L.I. Multi-stage parallel-hierarchical network as a model of a neural-like computing scheme. *Cybernetics and System Analysis*, No. 2, 2000, pp. 114-134.
- [17] Metlitsky, E.A., Kaverznev, V.V. *Parallel Memory Systems: Theory, Design, Application*. In: Timokhin, V.I. (Ed.), Leningrad University Press, 1989, 240 pp.
- [18] Leonid Tymchenko, Natalia Kokriatska, Volodymyr Tverdome, Natalia Sachaniuk-Kavets'ka, Liudmyla Semenova, Olha Riabokon, Konrad Gromaszek, Aisha Mussabekova "Pyramidal method of generalized spatially connected processing and an example of its implementation in image processing", *Proc. SPIE 12476, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2022*, 124760E (12 December 2022) <https://doi.org/10.1117/12.2659202>
- [19] Pavlov S. V. *Information Technology in Medical Diagnostics* //Waldemar Wójcik, Andrzej Smolarz, July 11, 2017 by CRC Press - 210 Pages.
- [20] Wójcik W., Pavlov S., Kalimoldayev M. *Information Technology in Medical Diagnostics II*. London: (2019). Taylor & Francis Group, CRC Press, Balkema book. – 336 Pages.
- [21] *Highly linear Microelectronic Sensors Signal Converters Based on Push-Pull Amplifier Circuits* / edited by Waldemar Wojcik and Sergii Pavlov, Monograph, (2022) NR 181, Lublin, Comitet Inzynierii Srodowiska PAN, 283 Pages. ISBN 978-83-63714-80-2.
- [22] Pavlov Sergii, Avrunin Oleg, Hrushko Oleksandr, and etc. *System of three-dimensional human face images formation for plastic and reconstructive medicine // Teaching and subjects on bio-medical engineering Approaches and experiences from the BIOART-project Peter Arras and David Luengo* (Eds.), 2021, Corresponding authors, Peter Arras and David Luengo. Printed by Acco cv, Leuven (Belgium). - 22 P. ISBN: 978-94-641-4245-7.
- [23] Romanyuk O.N. *Microfacet distribution function for physically based bidirectional reflectance distribution functions* / O. N. Romanyuk, S. V. Pavlov, R. Yu. Dovhaliuk, N. P. Babyuk, M. D.

Obidnyk, P. Kisala, B. Suleimenov // Optical Fibers and Their Applications 2012. Lublin and Naleczow, Poland, Code 96466.

Надійшла до редакції 01.11.2023

Видано за грантової підтримки Національного фонду досліджень України в рамках проєкту 2022.01/0135 "Розробка лазерно-фотонного лікувально-діагностичного комплексу медичної реабілітації пацієнтів з політравмами різного ступеня важкості"

Li Jingiong – postgraduated student of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

Pavlov Sergii – D.Sc., Professor of Biomedical Engineering and Optic-Electronic Systems Department, Vinnytsia National Technical University

Лю Цзіньюн, Сергій Павлов
ЕКСПЕРТНА БІОІНФОРМАЦІЙНА СИСТЕМА ДІАГНОСТИКИ ФОРМ
ГОСТРОГО ЛЕЙКОЗУ НА ОСНОВІ АНАЛІЗУ БІОМЕДИЧНОЇ
ІНФОРМАЦІЇ

Вінницький національний технічний університет

РАДІОВИМІРЮВАЛЬНІ ПРИЛАДИ

УДК 621.395.7:004.738.5:339.138

М.І. Литвиненко, Н.В. Гармаш

АНАЛІЗ ПРОСУВАННЯ ТЕХНОЛОГІЇ 5G У СВІТІ
ТА ОЧІКУВАННЯ ДЛЯ УКРАЇНИ

Харківський національний університет Повітряних Сил імені Івана Кожедуба

Анотація. В статті проводиться аналіз просування, переваги та оцінка досягнень технології 5G у світі, наявні результати впровадження 5G у різні галузі економіки незважаючи на проблеми з його стрімким розвитком. Аргументовано підтверджено зростаючі потреби у швидкості та пропускну здатності передачі даних, збільшення кількості підключених пристроїв без втрати якості зв'язку, зниження затримок і підвищення надійності в проведенні дистанційних операцій в реальному часі, розвиток інновацій таких, як інтернет речей (IoT), розширена реальність (AR) та віртуальна реальність (VR), автономні транспортні засоби та промисловий сектор, зокрема на промислово автоматизацію та "розумні" фабрики, використання високопродуктивних датчиків та робототехніку в реальному часі. Приведено переваги технології 5G, що характеризують високу швидкість передачі даних, низьку затримку (латентність), велику ємність мережі, покращену мобільність. Описано епізоди використання 5G у військовій сфері в реальному часі, миттєвого зберігання та відтворення великих обсягів відео та графіки, смарт-міста, які використовують 5G підтримку великої кількості датчиків та сенсорів у місті, реалізують різноманітні послуги, управляють енергетикою, моніторинг громадського транспорту. Актуальність використання мобільної мережі 5G в Україні залишається високою. Розглянуто необхідні кроки в Україні таких, як розробка стандартів, виділення частот, створення інфраструктури та отримання необхідної кількості пристроїв, які підтримують 5G. Надамо прогноз очікуваних результатів таких, як розширення інфраструктури; доступ до широкого спектру діапазону частот, включаючи низькі та високі діапазони; здатність протистояти кібератакам із широкого кола джерел; енергоефективними; сумісними з існуючою інфраструктурою та іншими протоколами зв'язку. Зроблено висновок, що найскоріше впровадження мережі 5G надає поштовх для України з технічної та економічної точки зору.

Ключові слова: технологія 5G, мобільні мережі, передача даних, швидкість мережі, пропускна здатність, частоти, інфраструктура.

Abstract. The article analyzes the promotion, advantages and assessment of the achievements of 5G technology in the world, the available results of the implementation of 5G in various sectors of the economy despite the problems with its rapid development. The growing needs for speed and bandwidth of data transmission, increasing the number of connected devices without loss of communication quality, reducing delays and increasing reliability in conducting remote operations in real time, the development of innovations such as the Internet of Things (IoT), augmented reality (AR) and virtual reality (VR), autonomous vehicles and the industrial sector, in particular on industrial automation and "smart" factories, the use of high-performance sensors and real-time robotics. The advantages of 5G technology, characterized by high data transfer speed, low support (latency), large network capacity, and improved mobility, are given. Episodes of the use of 5G in the military field in real time are described, to instantly store and reproduce large volumes of video and graphics, smart cities that use 5G to support a large number of sensors and sensors in the city, to implement a variety of services, energy management, public transport monitoring. Considered, the relevance of using the 5G mobile network in Ukraine remains high. The necessary steps in Ukraine from the development of standards, the allocation of frequencies, the creation of infrastructure and the acquisition of the necessary number of devices that support 5G are considered. A forecast of expected results such as infrastructure expansion is provided; access to a wide range of frequencies, including low and high bands; the ability to resist cyber attacks from a wide range of sources; energy efficient; compatible with existing infrastructure and other communication protocols. It was concluded that the introduction of the 5G network as soon as possible will provide an impetus for Ukraine from a technical and economic point of view.

Key words: 5G technology, mobile networks, data transfer, network speed, bandwidth, frequencies, infrastructure.

DOI: <https://doi.org/10.31649/1999-9941-2023-58-3-94-103>.

Вступ

Обіцянка швидкого розвитку технології 5G вже багато років повторюється в діловому світі. Вища швидкість 5G, менша затримка та можливість підключати значно більшу кількість пристроїв, ніж попередні покоління мобільних технологій, пропонує більш ефективний та продуктивний майбутнього. Забезпечивши основу для повсюдного надшвидкого широкосмугового зв'язку 5G відкриє можливості далеко за межі охоплення 4G або Wi-Fi 6. На теперішній час це завдання стає більш актуальним, оскільки провідні компанії роздумують, як найкращим чином відновити, переглянути та реконфігурувати ринок [4].

За останні 20 років технології зв'язку та передавання даних фантастично просунулися. Сьогодні знаходячись постійно у русі користувач під'єднаний до інтернету, дивитися відео онлайн, ініціює конференц-зв'язок, контролює тварин через камеру з онлайн-доступом. Технологія 5G дозволяє створювати мережі нового типу, які забезпечують більш високі швидкості передачі даних, нижчу затримку та підтримують більшу кількість користувачів, пристроїв та послуг і одночасно мають більш високу ефективність.

5G підтримує три широкі категорії варіантів використання:

- послуги з високою пропускну здатністю для бездротового зв'язку;
- наднадійна та низька затримка зв'язку для критично важливих вимог;
- надійний зв'язок для мільярдів датчиків та контрольних пристроїв [3].

Епоха технології 5G вийде за рамки покращення продуктивності мережі та підвищення швидкості, надаючи користувачам нові інноваційні та покращені можливості підключення. 5G може

підвищити продуктивність бізнес-додатків, одночасно надаючи нові користувацькі інтерфейси та послуги в таких областях, як додатки з доповненою, віртуальною та змішаною реальністю (AR, VR та MR), відеоконференції, промислова автоматизація, автомобілі з автоматичним керуванням та підключені до мережі медичні пристрої [5].

Актуальність

Темі популяризації, підтримки та поширення 5G технології приділяють увагу багато авторів. Вчені та компанії вивчають наявність перспектив та шляхів розвитку комунікаційних технологій, фокусуючись на максимальному ефекті використання досліджень технології 5G, оптимізації пристроїв та застосунків, які забезпечують покращення наявних параметрів [3].

Розглядається, що технологія 5G має певні результати, які свідчать про технічний та економічний ефект від використання мереж [4], [5], [6], [7].

У роботі [4] проаналізовано економічний ефект широкого впровадження мереж 5G, прогнози в цьому дослідженні показують, що несприятливі умови не мають істотного впливу на довгостроковий економічний внесок 5G. Зроблено висновок, що за основними перевагами, такими як значно нижча затримка та значному росту швидкості передачі даних, мережа 5G розширює свій вплив на широким спектр розвитку сфери застосування такими, як охорона здоров'я, енергетика, транспорт, будівництво, критична інфраструктура. Очікується [7], що досягнення кращих показників від просування мереж п'ятого покоління потребуватиме застосування нових рішень. У роботі [10] розглянуто, що станом на початок 2023 року розгорнулася боротьба між технологічними компаніями Китаю та США і ЄС з впровадження технології 5G, контролю за безпекою у розвитку, прогнозовано кількісні показники користувачів та економічний ефект.

Вказані обставини, які спонукають до просування технології 5G в Україні [11-13], розглянути особливості по її використанню та очікування результатів спираючись на досвід провідних держав.

Мета

Провести аналіз просування, переваг та оцінки технічних та економічних аспектів мережі 5G у світі, визначення необхідних кроків та можливостей у вирішенні питань впровадження 5G в Україні та очікуваних результатів у розробці високотехнологічних рішень.

Задачі

Головним чинником швидкого розповсюдження технології п'ятого покоління – тотальна цифровізація. Від поширення 5G залежить розвиток всього суспільства. 5G – частина широкої еволюції, яка також охоплює хмарні технології та технології автоматизації для створення більш надійної та стійкої платформи для постачальників послуг [6].

Розв'язання задач

Щоб задовольнити зростаючий попит на швидку передачу даних і був розроблений 5G. Існує кілька відмінностей між 5G та 4G:

1. 5G - це уніфікована платформа, здатна більше ніж 4G (буде підтримувати всі типи спектру (ліцензовані, спільні, неліцензовані) та смуги, збільшений широкий набір можливостей застосування, а також нові способи взаємозв'язку (наприклад, як сітка від пристрою до пристрою та мульти-хоп-сітки));
2. 5G використовує спектр краще, ніж 4G (від низьких діапазонів нижче 1 ГГц, до середніх діапазонів від 1 ГГц до 6 ГГц, до високих діапазонів, відомих як міліметрова хвиля);
3. 5G швидше, ніж 4G (забезпечивши до 20 Гбіт/с пікових швидкостей передачі даних і 100+ Мбіт/с);
4. 5G має більшу ємність, ніж 4G (підтримуватиме 100-кратне збільшення пропускної здатності та ефективності мережі, підтримує мільйон пристроїв на квадратний кілометр);
5. 5G має нижчу затримку, ніж 4G (зменшення затримки в кінці в 10 разів до 1 мс) [9].

У європейських, азійських та американських країнах мобільна мережа 5G вже активно використовується. Лідером як в Азії, так і у світі є Південна Корея, що пропонує найвищу швидкість інтернету (до 430 Мбіт/с). Далі йдуть ОАЕ, Кувейт, Катар, Саудівська Аравія, Малайзія, Тайвань, Китай, Японія [4].

Не відстають і європейські країни, зокрема Швеція, Норвегія, Фінляндія, Португалія, Болгарія, Хорватія. Інші країни Європи – Польща, Швейцарія, Латвія, Бельгія, Австрія, Німеччина, Нідерланди теж запустили 5G, але швидкість там нижча, а зона покриття менша. У США, Канаді, Австралії та Новій Зеландії мережа 5G також активно розвивається вже кілька років. На африканському континенті п'яте покоління зв'язку для публічного використання наразі не запустили. Виняток становить лише острів Мадагаскар [10].

На рис. 1 наведена карта покриття 5G по всьому світу.



Рисунок 1 – Карта покриття 5G по всьому світу

Джерело: розроблено авторами за даними [8].

За прогнозами, на кінець 2026 року у світі буде 4,1 мільярда абонентів мобільного зв'язку 5G. Це еквівалентно 37,1% від загальної кількості глобальних мобільних підписок. На Азіатсько-Тихоокеанський регіон припадатиме найбільша частка світових мобільних з'єднань 5G – 64% на кінець 2026 року, за нею йдуть Європа, Північна Америка, Африка, Близький Схід і Латинська Америка [10].

Фактори прогресу мережі 5G:

- технічний (стандарти, доступність, допоміжна інфраструктура):
- економічний (регулювання ринку, бізнес-середовище, споживча готовність):

У технічному аспекті зміни будуть стосуватися:

- використання нових хвиль (низькочастотний 5G працює у діапазоні 600-850 МГц (700 МГц); середньочастотний 5G працює в діапазоні 2,5-3,7 ГГц (3,4-3,8 ГГц); високочастотний діапазон, який найчастіше асоціюється із 5G, охоплює частоти від 25 до 39 ГГц (26 ГГц);

- збільшення інфраструктури (більшої кількості станцій, оптоволоконні магістралі для передачі, підключення до електромережі). Зараз відомо, що радіус покриття від однієї 5G станції становить близько 500 м і це без перешкод. В той час як 4G пропонує радіус покриття від 50 км і до 150 км в залежності від місцевості і перешкод. Тобто, замість однієї 4G станції необхідно встановити більше 10-ти 5G станцій.

- в одній решітці може поміститися набагато більше антен (масиви MIMO);

- формування променя (найефективніший маршрут доставки даних конкретному користувачу);

- повний дуплекс (кремнієві транзистори, які діють як високошвидкісні перемикачі, щоб зупинити зворотний крен цих хвиль, дозволяючи їм передавати та приймати сигнали на одній частоті одночасно).

Щодо економічного впливу просування мережі 5G, стосується потенціалу підвищення ефективності та продуктивності, за рахунок чого підвищиться вплив на такі фактори, як надійність, швидкість, низьку затримку, економію енергії та збільшення об'ємів підключень як всередині системи, так і зовні. Результатом буде широкопasmовий доступ це не просто надшвидкий, але всюдисущий. При використанні 5G в поєднанні з III, розширеною реальністю (XR), периферійними обчисленнями та Інтернетом речей (IoT) надасть більші можливості для економіки та людей.

Еволюція розвитку технології 5G за період 2019-2023 роки та перспективи до 2025 року (див. рис. 2).

Ми проаналізували випадки використання 5G, як нові, так і відомі, у п'яти секторах: охорона здоров'я, розумні комунальні послуги, споживачі та медіа, промислове виробництво та фінанси послуги – і виявив, що в сукупності прийняття 5G додасть 1,3 трильйона доларів США до світового ВВП до 2030 року [4]. Серед яких:

- охорона здоров'я 530 млрд.;
- енергетика 330 млрд.;
- споживачі та медіа-додатки 254 млрд.;
- промислове виробництво 134 млрд.;

- програми фінансових послуг 85 млрд.



Рисунок 2 – Еволюція розвитку технології 5G
Джерело: розроблено авторами за даними [4]

Ці цифри кількісно виражають вплив, але, мабуть, важливіше наше дослідження висновки відображають цінність 5G.

Протягом перших років внесок 5G в економічне зростання буде справедливо скромним, оскільки телекомунікаційні компанії зосереджені на будівництві та розгортанні інфраструктури. Але, починаючи з 2025 року, враховуючи зростаючі інвестиції принесуть стимулюючий вплив на світову економіку, оскільки програми з підтримкою 5G стають більш поширені (див. рис. 3).

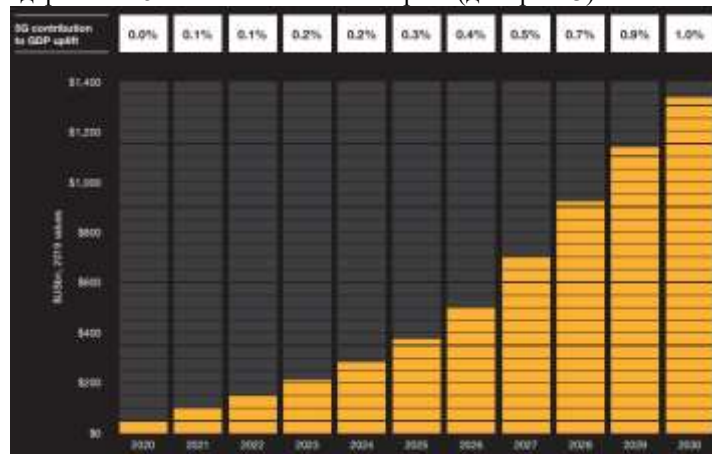


Рисунок 3 – Прогнозований внесок 5G у світовий ВВП до 2030 року
Джерело: розроблено авторами за даними [4]

На регіональному рівні найбільший відсоток зростання ВВП від просування мережі 5G відноситься до Північної Америки, потім йдуть Азія та Океанія, а потім Європа Близький Схід і Африка (ЕМЕА). В абсолютних доларах, Північна Америка також займе найвище місце, а також Азія. Прогнозується, що Океанія випередить ЕМЕА через її більшу загальну економіку. Масштаб національної економіки вплине на його абсолютний вплив на глобальний ВВП: 2% зростання економіки США приблизно в шість разів більше в доларовому еквіваленті 1,3% розширення в Японії економіка. Серед проаналізованих країн (див. рис. 4), ті, що мають потужні сучасні сектори промислового виробництва можуть отримати більше вигоди, ніж ті, які покладаються на сфери послуг наприклад, банківська справа.

Крім того, мережі 5G дозволяють використовувати дистанційно технології у критичних за часом додатках. Технологія 5G вплине на такі галузі, і це лише малий перелік:

- медицина;
- освіта;
- торгівля;
- транспорт;
- будівництво;
- сільськогосподарська діяльність;
- критична інфраструктура;
- добування корисних копалин [10].



Рисунок 4 – Прогнозований економічний вплив технології 5G за країнами до 2030 року
Джерело: розроблено авторами за даними [4]
Як використання технології 5G змінить життя навколо нас наведено на рис. 5.



Рисунок 5 – Використання пристроїв та з'єднань 5G навколо нас
Джерело: розроблено авторами за даними [10].

Кожне нове покоління стільникового зв'язку значно збільшує швидкість передачі даних. Так впроваджуються сучасні нові можливості обслуговування та нові формати сервісу. Люди отримують нові захоплення а нові аспекти у якості життя.

Планується, що до 2035 року інфраструктура 5G-мереж надасть 22 млн. робочих місць на планеті, а її внесок у всесвітній розвиток за період з 2020 по 2035 рік буде порівнянний з нинішнім розміром економіки Індії, який дорівнює \$2,4 трлн. З розвитком 5G значно зростуть прибутки Інтернету речей (IoT). У 2023 році вони можуть досягти позначки \$1,7 трлн.

Відповідно до “правила 10 років” на появу мереж 6G слід очікувати до 2030 року [6].

Передбачалося, що початок розгортання 5G у нашій країні відбудеться у 2022 році, але завадила російсько-українська війна. У цей час змінилися пріоритети, і на передній план вийшли справи захисту держави та ефективного використання ресурсів. Але головне, що є запит на використання 5G і впевненість у тому, що це відбудеться. Офіційних заяв щодо цього не було, але оптимістичні прогнози щодо розгортання мережі п'ятого покоління стосуються першої половини 2024 року. Тим часом, головною мережею для українців на найближчі роки залишиться 4G.

До кінця 2024 року держава планує, що 95% населення, громадських об'єктів і основних автодоріг матимуть покриття швидкісним 4G.

Враховуючи насамперед, економічну сферу застосування 5G запуснуть для великих підприємств та для сфер бізнесу. Особливо цифровізація буде важливою після перемоги, оскільки зможе полегшити та прискорити деякі процеси у роботі та відновленні критичної інфраструктури, а також в інших важливих галузях економіки [10].

Після цього мережу п'ятого покоління зможуть використовувати звичайні користувачі. Очікується, що спочатку 5G запуснуть у великих містах – Києві, Харкові, Дніпрі, Одесі, Львові. За кращого розвитку ситуації, лише через 5-6 років мережа 5G стане переважаючою в Україні [10].

Таблиця 1 - Як 5G змінить наше життя

Коло використання	Наслідки
Бізнес	Створення нових робочих місць, росту підприємництва та покращення ефективності в різних галузях
Автомобілі	У безпілотних (автономних) автомобілях зменшення затримки сигналу на великій швидкості, автомобілі зможуть підтримувати контакт один з одним та з дорожніми службами
Промисловість	Відігравати ключову роль в переосмисленні та трансформації виробництва через введення концепцій Індустрії 4.0, де машини можуть ефективно співпрацювати, оптимізуючи виробничі процеси
Сільське господарство	Використання датчиків для моніторингу вологості, температури та інших параметрів на полі, високоточний збір та обробку даних для кращого управління ресурсами, такими як ґрунт, вода, добрива та пестициди; реалізувати автоматизовані трактори та обладнання; ефективно моніторити процеси збирання врожаю та оптимізувати їх для досягнення максимальної продуктивності; впровадження систем відстеження та управління худобою; використовувати дрони для моніторингу великих областей землі, визначення стану посівів, розпізнавання шкідників та планування оптимальних сільськогосподарських дій; встановлювати ефективний обмін даними вздовж всього ланцюга постачання – від фермера до споживача
Освіта	Інтерактивне навчання, доступ до інформації в реальному часі, віддалене навчання, колективна робота та співпраця, інтерактивні додатки та сервіси, створення інтерактивних навчальних середовищ через VR-трансляцію з погляду викладача
Телемедицина	Забезпечити високоякісні віддалені консультації між лікарями та пацієнтами, можливості для проведення операцій в труднодоступних місцях або в обставинах, коли фахівець не може фізично знаходитися на місці подій, реалізувати системи моніторингу здоров'я в режимі реального часу, які автоматично передають дані лікарям, полегшити безпечний обмін медичними даними між лікарнями, клініками та іншими медичними закладами, використання телемедичинських додатків та пристроїв, використання штучного інтелекту для аналізу медичних зображень, діагностики та інших завдань, що вимагають великої обчислювальної потужності
Спілкування	Розширення аудиторії та можливостей спілкування на відстані так, як знаходячись один біля одного
Розваги	Швидка безпроводна передача відеоданих у надвисокій якості (4K, 8K), трансляція заходів з ефектом VR. Дуже стрімко зростає популярність відео та музики
Комп'ютерні ігри	Багатокористувацькі ігри без затримки сигналу та розширення аудиторії учасників, розвиток хмарних геймінгових платформ, створення більш іммерсивних ігрових вражень через AR та VR, онлайн-геймінг та масові мережеві битви, де велика кількість гравців.
Оборона	Ефективні дії навіть у віддалених і складних умовах; створення реалістичних сценаріїв навчання та моделювання, надаючи військовому персоналу більш реалістичний та ефективний досвід навчання

Джерело: розроблено авторами за даними [1, 6].

Прогнози розгортання 5G в Україні та частки населення, яке залишається невідключеним базуються на аналізі перешкод та бар'єрів, які зосереджується на чотирьох основних обмеженнях для впровадження мережі 5G, а саме наявність, доступність, актуальність і готовність:

1. Наявність: прогнозування проміжного стільникового покриття до 2030 року.
2. Доступність: розподіл доходів населення, ціна найдешевшого смартфона і місячну вартість найдешевших передплат мобільного передавання даних.
3. Актуальність: число глядачів онлайн-відео та користувачів соціальних мереж у країні.
4. Готовність: цифрова грамотність населення [8].

Щоб об'єднати результати, слід взяти першу обмежувальну умову – наявність покриття.

Зважаючи на вагомі позитивні наслідки цифровізації в Україні, значну фінансову і технологічну підтримку країн-партнерів та дій уряду над стартом розгортання мережі 5G постійно працюють. Це визначають відповідні кроки:

- У 2017 році вийшов Указ Президента України про впровадження 5G на території нашої країни.
- У 2019 році зустріч Президента України Володимира Зеленського з головними інвесторами розвитку телекомунікаційних технологій та готовність України до співпраці.
- У 2021 році вийшла Постанова Кабінету Міністрів України про початок тестування мобільної мережі 5G в Україні. У цьому році відбулося публічне тестування бездротового зв'язку п'ятого покоління. [10].
- 27 лютого 2023 року США та Україна підписали меморандум про взаєморозуміння та співпрацю в галузі телекомунікацій та впровадження мобільного зв'язку 5G.
- 28 лютого 2023 року Верховний Суд України відмовив ТОВ "Українські новітні технології" (колишній оператор Freshtel) у продовженні терміну дії ліцензії на користування радіочастотами у діапазоні 3400-3600 МГц. Рішення аргументували тим, що "Українські новітні технології" не використовували виділені частоти за призначенням, не у повному обсязі платили за користування радіочастотним ресурсом і припинили подавати звітність. Це рішення фактично відкрило двері для впровадження 5G провідними операторами мобільного зв'язку.

Які кроки потрібно зробити для впровадження 5G в Україні:

1. Встановити стандарти (сукупність параметрів радіохвиль, технологія передачі та протоколи);
2. Виділити частоти (здіяння частоти діапазону 30-300 ГГц).
Оператори (Vodafone Україна, Київстар, Lifecell) також наголосили, що розблокування частот у діапазоні 3400-3600 МГц загалом є позитивним кроком уряду і з технічного та юридичного погляду дійсно наближає впровадження 5G в Україні [7].
3. Оновити інфраструктуру (5G не замінить 4G, а працюватиме паралельно з існуючою інфраструктурою; пристрої перемикатимуться між мережами).

В цей час першочерговий фокус компаній – забезпечення безперебійного зв'язку та передавання даних для абонентів на основі наявних технологій, підтримання мережі в умовах відключення електроенергії та відновлення пошкодженої інфраструктури. Водночас оператори продовжують готувати технологічну основу для майбутнього впровадження наступних технологічних стандартів, зокрема 5G.

Орієнтація на технологічні компанії Huawei, Ericsson та Nokia, які інвестують кошти та борються за ринок України. Необхідно враховувати, що компанія Huawei знаходиться під санкціями у США та ЄС, які підозрюються в наявності прихованих програм в телекомунікаційному обладнанні цього виробника.

Дивлячись на це, скоріше за все ключові ролі у розвитку ринку в Україні зіграють виробники телекомунікаційного устаткування Ericsson і Nokia [7].

4. Збільшення кількості приладів з підтримкою 5G (абонентські пристрої повинні стати розумнішими та потужнішими, заміна SIM-карт з появою 5G).

Стандарт мобільного зв'язку п'ятого покоління передусім принесе користь бізнесу. Для звичайних абонентів швидкості та пропускної спроможності 4G вистачає з головою, навіть якщо йдеться про перегляд відео у форматі 4K. А от 5G необхідний для різних галузей промисловості [7].

Частка користувачів 4G до 2024 року в Україні становитиме 50%, 3G – 42%, ці дані було презентовано з посиланнями на GSMA. Проникнення смартфонів з підтримкою 5G у мережі Lifecell досі менше 10% від загальної кількості, що замало для широкого розгортання нової технології. Для порівняння, кількість споживачів 5G у США становитиме 63%, у Західній Європі 40%.

Вартість появи зв'язку 5G в Україні залежатиме від термінів її впровадження, від того, коли з'явиться частотний ресурс, як саме він використовуватиметься. Ці чинники впливатимуть обсяг інвестицій. Якщо оператори мобільного зв'язку, які зараз інвестують в мережі LTE, закладуть технічний базис для подальшого впровадження 5G, то подальші інвестиції будуть меншими.

Важливо, яку бізнес-модель використовуватиме оператор. Чи стане він чисто сервіс-провайдером або оператором, який розроблятиме програми, сервіси і продаватиме ці послуги [6].

Загалом, незважаючи на прийняття на державному рівні нормативно правових актів, спрямованих на використання радіочастот й упровадження мобільного зв'язку 5G, ми наразі перебуваємо серед аутсайдерів за впровадженням 5G унаслідок причин технічного, інституційного та економічного характеру. З метою результативного впровадження мобільного зв'язку п'ятого покоління держава має забезпечити здійснення науково обґрунтованих розрахунків та експертних оцінок вартості радіочастотного ресурсу 5G-зв'язку, удосконалення нормативно-правової бази, ліцензування використання радіочастот, проведення торгів та видачі ліцензій на його використання. Пріоритет у цьому – це забезпечення заходів націлених на підтримку впровадження 5G в Україні, використовуючи попит на продукцію та зацікавленість бізнесу [14].

Використання 5G в оборонній сфері може мати численні переваги для військових, що може покращити ефективність та можливості військових операцій. До найбільш вагомих маємо віднести:

- велику пропускну здатність та швидкість передачі даних, що особливо важливо для обміну великими обсягами інформації, такої як великі відео- та аудіопотоки, геопросторові дані, та великі файли;
- можливість підтримки великої кількості одночасно підключених пристроїв, що важливо для розвитку великих мереж військового обладнання, IoT-пристроїв, дронів та інших систем;
- впровадження AR та VR для симуляцій, навчання, розвідки та інших військових застосунків;
- керування та координація безпілотних транспортні засоби (БПЛА, роботи) у режимі реального часу, що може бути важливо для розвідки, рятувальних операцій та поставок;
- зростаючий фокус на кібербезпеці в зв'язку з великим обсягом даних та кількістю підключених пристроїв, удосконалення кіберзахисту військових систем;
- забезпечення гнучкості управління мережею та швидкого реагування на зміни в обстановці та вимоги військових операцій.

Можливі напрями використання технології 5G в оборонній сфері України, це насамперед:

1. Покращення військового спостереження та збору розвідданих (передачу відеоматеріалів з дронів та інших пристроїв спостереження, військовослужбовці можуть швидко та безпечно отримувати доступ до даних) [11].

2. Військовий зв'язок, командування та управління (забезпечувати швидший і безпечніший зв'язок, більш ефективне командування та контроль) [11].

3. Переваги безпеки 5G для оборонної промисловості (покращений контроль і покращена швидкість, пропускну здатність і надійність мереж 5G допоможуть оборонним організаціям захистити свої дані та мережі від потенційних загроз) [13].

4. Змінити військову логістику та управління ланцюгом поставок (моніторингу ресурсів у режимі реального часу, дозволяючи військовим швидко оцінювати рівень постачання та відповідно розгортати ресурси) [9].

5. Використання для автономних систем зброї в оборонній промисловості (використання 5G у розробці автономних систем зброї) [13].

Звісно, при впровадженні 5G в оборонній сфері необхідно враховувати питання кібербезпеки, стандартизації та управління сумісністю для забезпечення найвищого рівня ефективності та безпеки.

Оцінюючи, можливості використання 5G в оборонній сфері, слід зазначити, що це вимога часу за стратегічними перевагами, які зможуть допомогти покращити функціональність та ефективність оборонних сил. Підвищення швидкості, пропускну можливості, об'єму передачі даних, підключення великої кількості пристроїв (датчиків) та їх координацію, використання інтелектуальних систем та штучного інтелекту, керування та координації автономних транспортних засобів та ефективно виявлення та відвертати кібератак на системи оборони.

Ці функції роблять технологію 5G важливим елементом для модернізації та покращення оборонних систем. Однак, слід враховувати та ефективно вирішувати питання кібербезпеки, оскільки з використанням нових технологій збільшується і ймовірність кібератак.

Висновок

Одним з джерел труднощів у комунікації з потенційними споживачами 5G-послуг є розрив між їх очікуваннями та доступними можливостями. Але просування, оцінка переваг та досягнень мережі 5G показує перспективи у подальшому розвитку цієї сфери та значного зростання сегментів економіки держави, населення яке відчуває необхідність проникнення 5G пристроїв у побут та найімовірний прогрес його використання.

Важливими очікуваннями для України будуть економічне зростання, інновації в наукових дослідженнях, підтримка Індустрії 4.0, розвиток Smart Cities, швидкісний та стабільний інтернет, розвиток телемедицини, нарощування обороноздатності держави.

Важливо зауважити, що разом з перевагами використання 5G приходять питання щодо кібербезпеки, конфіденційності даних та інфраструктурної стійкості, які потрібно вирішувати для максимальної користі та безпеки.

Список літератури

1. Saad Z. Asif. (2019). 5G Mobile Communications: Concepts and Technologies / CRC Press, Taylor & Francis Group., P. 335.
2. Scott Fulton III. (2021). What is 5G? Business guide to the next generation of wireless technologies. <https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wirelesstechnology/>

3. Гармаш Н.В., Литвиненко М.І. (2023). Аналіз розвитку технології 5G. С. 282-283. <https://isg-konf.com/wp-content/uploads/2023/10/GLOBAL-PROBLEMS-OF-IMPROVING-SCIENTIFIC-INVENTIONS.pdf>
4. PwC. (2021). Вплив 5G на світову економіку. С. 22. <https://www.pwc.com/gx/en/industries/technology/publications/economic-impact-5g.html>.
5. F. Grijpink, E. Kutcher A. Ménard, S. Ramaswamy, D. Schiavotto, J. Manyika M. Chui, R. Hamill, E. Okan. (2020). Підключений світ: Еволюція підключення після революції 5G. <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution>.
6. В. Кордон. (2022). Як 5g може змінити наше життя? <https://www.unian.net/longrids/5G/>.
7. Все, що вам потрібно знати про 5G. (2019). <https://www.qualcomm.com/5g/what-is-5g>.
8. Попит на прогноз ринку 5G і доходів від послуг до 2026 року / Global Outlook Report / (2021). <https://www.researchandmarkets.com/reports/5451398/5g-market-demand-and-service-revenue-forecast-to>.
9. Україна 2030e – країна з розвинутою цифровою економікою (2019). <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>.
10. А. Нікітіна. (2023). Мережа 5G: коли з'явиться в Україні. <https://andro-news.com/ua/news/set-5g-kogda-poyavitsya-v-ukraine.html>.
11. Слюсар В.І., Сотник В. В., Купчин А. В., Шостак В.Г. (2020). Проривні технології в оборонній сфері України. / Озброєння та військова техніка. № 4. С. 13–23. https://www.slyusar.kiev.ua/OVT_4_2020_1.pdf.
12. Завербний А., Ломага Ю. (2022). Проблеми та перспективи формування логістичних ланцюгів постачання у воєнний період за умов активізації євроінтеграції / Економіка та суспільство, № 45. <https://doi.org/10.32782/2524-0072/2022-45-23>.
13. Горбулін В.П. (2019). Забезпечення оборони та безпеки України: актуальні проблеми і шляхи їх вирішення / Вісник Національної академії наук України. № 9. С. 3-18.
14. Князева І. (2021). Мобільний зв'язок п'ятого покоління та його місце в трансформаційних процесах цифровізації економіки. <https://doi.org/10.15407/econindustry2021.01.046>.

References

1. Saad Z. Asif. (2019). 5G Mobile Communications: Concepts and Technologies / CRC Press, Taylor & Francis Group. P. 335.
2. Scott Fulton III. (2021). What is 5G? Business guide to the next generation of wireless technologies. <https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wirelesstechnology/>
3. Harmash N.V., Lytvynenko M.I. (2023). Analysis of the development of 5G technology. P. 282-283. <https://isg-konf.com/wp-content/uploads/2023/10/GLOBAL-PROBLEMS-OF-IMPROVING-SCIENTIFIC-INVENTIONS.pdf>
4. PwC. (2021). The impact of 5G on the global economy. P. 22. <https://www.pwc.com/gx/en/industries/technology/publications/economic-impact-5g.html>.
5. F. Grijpink, E. Kutcher, A. Ménard, S. Ramaswamy, D. Schiavotto, J. Manyika, M. Chui, R. Hamill, E. Okan. (2020). A connected world: The evolution of connectivity after the 5G revolution. <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/connected-world-an-evolution-in-connectivity-beyond-the-5g-revolution>.
6. V. Kordon. (2022). How can 5g change our lives? <https://www.unian.net/longrids/5G/>.
7. Everything you need to know about 5G. (2019). <https://www.qualcomm.com/5g/what-is-5g>.
8. Demand for 5G market forecast and service revenues until 2026 / Global Outlook Report / (2021). <https://www.researchandmarkets.com/reports/5451398/5g-market-demand-and-service-revenue-forecast-to>.
9. Ukraine 2030e – a country with a developed digital economy (2019). <https://strategy.uifuture.org/kraina-z-foroventoyu-cifrovoyu-ekonomikoyu.html>.
10. A. Nikitina. (2023). 5G network: when it will appear in Ukraine. <https://andro-news.com/ua/news/set-5g-kogda-poyavitsya-v-ukraine.html>.
11. Slyusar V.I., Sotnyk V.V., Kupchyn A.V., Shostak V.G. (2020). Breakthrough technologies in the defense sphere of Ukraine. / Armament and military equipment. No. 4. P. 13–23. https://www.slyusar.kiev.ua/OVT_4_2020_1.pdf.
12. Zaverbny A., Lomaga Yu. (2022). Problems and prospects of the formation of logistics supply chains during the war period under the conditions of intensification of European integration / Economy and society, No. 45. <https://doi.org/10.32782/2524-0072/2022-45-23>.
13. Horbulin V.P. (2019). Ensuring the defense and security of Ukraine: current problems and ways to solve them / Bulletin of the National Academy of Sciences of Ukraine. No. 9. P. 3-18.

14. Knyazeva I. (2021). Fifth generation mobile communication and its place in the transformational processes of digitalization of the economy. <https://doi.org/10.15407/econindustry2021.01.046>.

Відомості про авторів

Литвиненко Михайло Іванович – к.т.н., доцент, доцент кафедри математичного та програмного забезпечення АСУ, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Lytvynenko Mykhailo Ivanovych – Ph.D., associate professor, associate professor of the Department of Mathematics and Software of ASU, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine.

Гармаш Наталія Вікторівна – старший викладач кафедри математичного та програмного забезпечення АСУ, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна.

Harmash Nataliia Viktorivna – senior lecturer of the Department of Mathematics and Software of ASU, Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine.

M. I. Lytvynenko, N. V. Harmash

**ANALYSIS OF PROMOTION OF 5G TECHNOLOGY IN THE WORLD
AND EXPECTATIONS FOR UKRAINE**

Ivan Kozhedub Kharkiv National Air Force University, Kharkiv