науково-практичний симпозіум

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ:
СИСТЕМИ ТА РІШЕННЯ

2025

ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
КАФЕДРА СПЕЦІАЛІЗОВАНИХ КОМП'ЮТЕРНИХ СИСТЕМ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

науково-практичний симпозіум

ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ: СИСТЕМИ ТА РІШЕННЯ (ТІР:СТ – 2025)

24 жовтня 2025 року
м. Тернопіль

Збірник матеріалів науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення» (ТІР:СТ - 2025), Тернопіль, 2025. -122 с.

До збірника увійшли тези доповідей, подані учасниками науково-практичного симпозіуму «Технології Інтернету речей: системи та рішення», який проводився 24 жовтня 2025 р. у ЗУНУ кафедрою спеціалізованих комп'ютерних систем спільно з ГО «Кібербезпека і автоматизація».

Адреса організаторів:

вул. Олени Теліги 8, м. Тернопіль 46003,
кафедра спеціалізованих комп'ютерних систем,
Західноукраїнський національний університет.

Контакти: conferenceakit@gmail.com.

ЗМІСТ

УДК 004

Максим ПЕЧЕНЮК, Тарас ЦАВОЛИК

Західноукраїнський національний університет

ЕВОЛЮЦІЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ТА СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ IoT

Вступ. Стрімке зростання кількості пристроїв Інтернету речей (IoT) створює нові виклики для забезпечення інформаційної безпеки. За прогнозами аналітиків, кількість підключених IoT-пристроїв досягне 50 мільярдів одиниць, створюючи потенційний ринок обсягом понад 14 трильйонів доларів. Однак це зростання супроводжується критичним збільшенням кіберзагроз. За даними 2025 року, IoT-інфраструктура зазнає в середньому 820 тисяч спроб зламу щоденно, що становить зростання на 46% порівняно з попереднім роком. Традиційні методи криптографічного захисту та системи виявлення вторгнень, розроблені для класичних комп'ютерних систем, виявляються недостатньо ефективними через специфічні обмеження IoT-пристроїв – низьку обчислювальну потужність, обмежені енергетичні ресурси та гетерогенність протоколів. Це зумовлює необхідність еволюції криптографічних методів та систем виявлення вторгнень для адаптації до унікальних вимог IoT-екосистем.

Мета: Проаналізувати еволюцію криптографічних методів та систем виявлення вторгнень для IoT-пристроїв, визначити переваги та недоліки традиційних підходів порівняно з сучасними ML-базованими рішеннями, та надати рекомендації щодо вибору оптимальних механізмів захисту залежно від класу IoT-систем та їх специфічних обмежень.

1. Еволюція криптографічних методів для IoT-пристроїв

Забезпечення конфіденційності та цілісності даних в IoT-середовищах вимагає застосування криптографічних алгоритмів, адаптованих до обмежених обчислювальних ресурсів пристроїв. Традиційні криптографічні рішення, такі як AES-256 та RSA, хоча й забезпечують високий рівень безпеки, часто накладають значні обчислювальні та енергетичні витрати, що перевищують можливості легковагових сенсорів, вбудованих контролерів та периферійних пристроїв [1].

Алгоритм AES (Advanced Encryption Standard) залишається широко використовуваним блоковим шифром завдяки стандартизації NIST та всебічному криптоаналізу. Проте, в програмних реалізаціях без апаратного прискорення AES демонструє підвищене споживання пам'яті та енергії, особливо для пристроїв з 32-бітною архітектурою [2]. Дослідження на платформах Raspberry Pi 3 та Beagle Bone Black показали, що AES у режимах ECB та CBC має нижчу швидкість шифрування порівняно з потоковими шифрами при обробці файлів розміром від 1 МБ до 128 МБ.

ChaCha20 є потоковим шифром, розробленим Деніелом Бернстайном, що був стандартизований у RFC 7539 та включений до TLS 1.3. Алгоритм ChaCha20-Poly1305 поєднує шифрування ChaCha20 з автентифікатором Poly1305, забезпечуючи автентифіковане шифрування з асоційованими даними (AEAD). Порівняльні

дослідження показують, що ChaCha20 постійно перевершує AES за швидкістю та ефективністю пам'яті на процесорах загального призначення без AES-NI (апаратного прискорення AES) [3]. На 32-бітних мікроконтролерах ChaCha20-Poly1305 споживає приблизно 0,45 мкДж/байт, що на 20-30% ефективніше, ніж AES-GCM (0,52 мкДж/байт). Крім того, ChaCha20 не використовує таблиці підстановки (S-box), що робить його стійким до атак на основі аналізу часу виконання (cache-timing attacks), на відміну від загальних реалізацій AES [4].

На рисунку 1 представлено порівняльний аналіз продуктивності криптографічних алгоритмів для IoT-пристроїв.

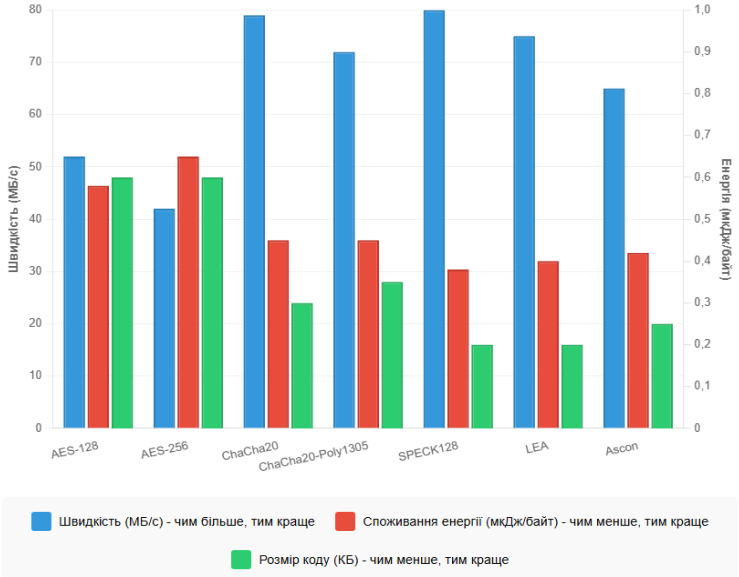


Рисунок 1 - Порівняння продуктивності криптографічних алгоритмів на 32-бітних ARM процесорах

NIST організував конкурс Lightweight Cryptography для вибору стандартизованих легковагових алгоритмів. Переможцем став алгоритм Ascon, що використовує губчасту конструкцію (sponge construction) та оптимізований для IoT-пристроїв з обмеженими ресурсами [5]. Однак Ascon, будучи спеціалізованим рішенням, не може використовувати існуючі високопродуктивні реалізації AES, такі як інструкції Intel AES-NI. Легковагові блокові шифри, такі як SPECK128 та LEA, демонструють швидкість 75-85 МБ/с при дуже низькому енергоспоживанні та малому розмірі коду, що робить їх привабливими для ресурсно-обмежених пристроїв [6].

Вибір криптографічного алгоритму для кожного рівня IoT-архітектури визначається балансом між рівнем безпеки, продуктивністю та ресурсними обмеженнями. На рівні пристрою (Device Layer) рекомендується використання легковагових симетричних шифрів (ChaCha20, SPECK, LEA, Ascon) для шифрування даних та криптографії на еліптичних кривих (ECC) замість RSA для асиметричного шифрування, оскільки вони забезпечують менший розмір ключів при еквівалентній стійкості. Рівень периферії/шлюзу (Edge/Gateway Layer) має підтримувати як легковагові, так і традиційні алгоритми для забезпечення сумісності та трансляції між протоколами різної складності [7].

2. Системи виявлення вторгнень: від сигнатурних до ML-базованих

Традиційні системи виявлення вторгнень (IDS), що базуються на сигнатурах або правилах, не здатні ідентифікувати нові та еволюціонуючі загрози в динамічних IoT-мережах. Це призвело до активного розвитку IDS на основі машинного навчання (ML) та глибокого навчання (DL), які здатні адаптуватися до складних та мінливих загроз в IoT-середовищах [8].

Сигнатурні IDS базуються на базі даних відомих патернів атак та порівнюють мережевий трафік з цими сигнатурами для виявлення загроз. Основною перевагою такого підходу є низька кількість хибних спрацювань (85-90% точності) та швидкість виявлення відомих атак. Однак критичним недоліком є неможливість виявлення нових, раніше невідомих атак (zero-day exploits) та необхідність постійного оновлення бази сигнатур [9].

Аномально-базовані IDS використовують статистичні методи для визначення нормальної поведінки мережі та виявлення відхилень від неї. Такі системи здатні виявляти невідомі типи атак, проте характеризуються високою кількістю хибних спрацювань (80-85% точності) через складність точного визначення "нормальної" поведінки в гетерогенних IoT-середовищах [10].

На рисунку 2 представлено архітектуру ML-базованої системи виявлення вторгнень для IoT.

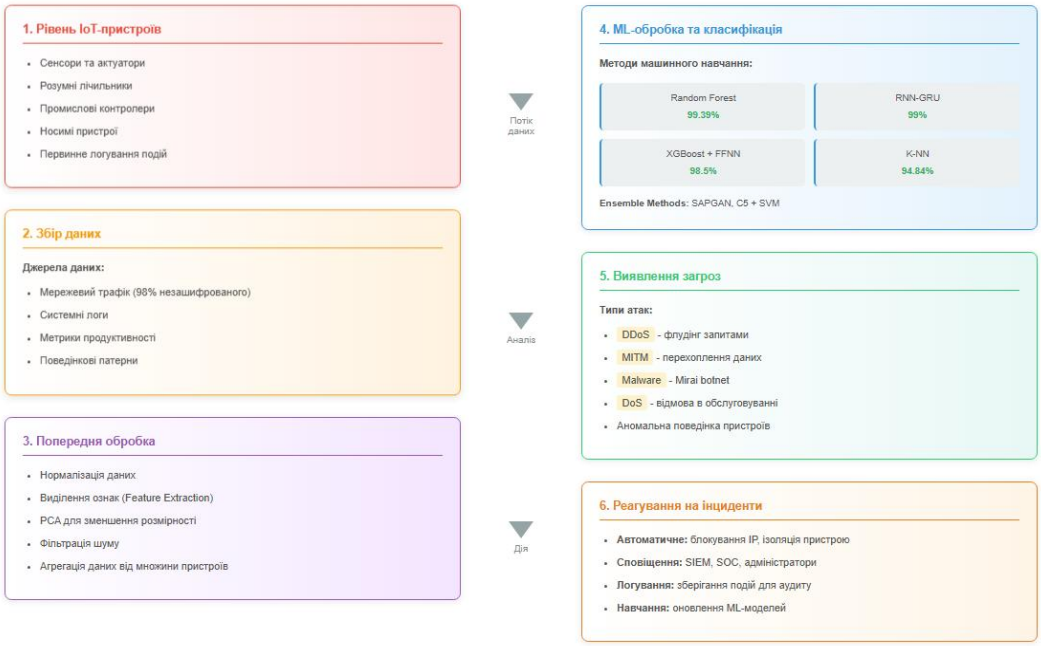


Рисунок 2 - Архітектура ML-базованої IDS для IoT-мереж

Порівняльний аналіз методів машинного навчання показує, що Random Forest (RF) демонструє найвищу точність (99,39%) серед класичних алгоритмів при виявленні аномалій в IoT-мережах, тоді як K-Nearest Neighbor (KNN) показує найнижчу продуктивність (94,84%) [11]. Гібридна модель, що поєднує Feed Forward Neural Networks (FFNN) та XGBoost, покращує точність виявлення атак при мінімізації обчислювальних витрат через застосування Principal Component Analysis (PCA) для відбору ознак.

Дослідження показують високу ефективність гібридних підходів, що поєднують різні архітектури нейронних мереж. Khan та співавтори запропонували модель RNN-GRU (Recurrent Neural Network - Gated Recurrent Units) для класифікації атак на всіх трьох рівнях IoT-архітектури (фізичний, мережевий, прикладний), досягнувши точності 99% на датасеті ToN-IoT для мережевого трафіку та 98% для трафіку прикладного рівня [12]. Іншим прикладом є фреймворк SAPGAN (Self-Attention Progressive Generative Adversarial Network), що інтегрує механізми самоуваги з генеративно-змагальними мережами для виявлення безпекових загроз в IoT-мережах.

Ансамблеві методи також демонструють високу ефективність. Jabbar та співавтори запропонували ансамблевий класифікатор на основі Random Forest та Average One-Dependence Estimator (AODE), що вирішує проблему залежності атрибутів у Naïve Bayes та підвищує точність при одночасному зменшенні кількості хибних спрацювань [13]. Khraisat та колеги розробили метод стекінгу (stacking ensemble), що комбінує дерево рішень C5 та One-Class Support Vector Machine, досягнувши точності класифікації шкідливого ПЗ 94%.

Важливим для ML-базованих IDS є можливість виявлення складних багатоетапних атак (Advanced Persistent Threats - APT). Традиційні сигнатурні системи виявляють лише окремі етапи атаки, тоді як ML-моделі здатні аналізувати послідовності подій та виявляти корельовані аномалії на різних рівнях IoT-архітектури [14].

Висновок. Аналіз еволюції криптографічних методів та систем виявлення вторгнень для IoT демонструє значний прогрес у адаптації технологій безпеки до специфічних обмежень та вимог IoT-пристроїв. Дослідження показує, що традиційні криптографічні алгоритми, такі як AES, хоча й забезпечують високий рівень безпеки, часто є неоптимальними для ресурсно-обмежених пристроїв через високе енергоспоживання та обчислювальні витрати.

Сучасні легковагові алгоритми, зокрема ChaCha20-Poly1305, SPECK та переможець конкурсу NIST Lightweight Cryptography – Ascon, демонструють значні переваги для IoT-застосувань. ChaCha20-Poly1305 досягає на 20-30% вищої енергоефективності порівняно з AES-GCM на 32-бітних мікроконтролерах, забезпечуючи при цьому стійкість до атак на основі аналізу часу виконання.

У сфері систем виявлення вторгнень спостерігається парадигмальний зсув від традиційних сигнатурних підходів до ML-базованих рішень. Експериментальні дані підтверджують, що Random Forest досягає точності 99,39% у виявленні аномалій, тоді як гібридні моделі RNN-GRU показують 99% точності на датасеті ToN-IoT. Ці результати значно перевершують традиційні сигнатурні системи (85-90% точності) та аномально-базовані підходи (80-85% точності).

Ключовим є необхідність застосування багаторівневого підходу до безпеки IoT, де криптографічні методи та системи виявлення вторгнень інтегруються на всіх рівнях архітектури – від пристрою до хмари. Вибір конкретних механізмів захисту повинен визначатися класом IoT-системи, обчислювальними ресурсами пристроїв та специфічними вимогами до безпеки застосування.

Перспективними напрямками подальших досліджень є розробка адаптивних

систем безпеки, що динамічно регулюють рівень захисту залежно від контексту та поточних загроз, інтеграція квантово-стійких криптографічних алгоритмів для забезпечення довгострокової безпеки, та застосування федеративного навчання для покращення ML-моделей виявлення вторгнень без компрометації конфіденційності даних.

Перелік використаних джерел.

1. Sharma V., Kumar R. A systematic review of lightweight cryptographic schemes for security and privacy in IoT. Discover Computing. 2025. Vol. 28. Article 15.
2. Alassaf N., Gutub A. Performance Evaluation of Cryptographic Ciphers on IoT Devices. arXiv preprint. 2018. arXiv:1812.02220.
3. Patel S., Mehta K. Comparative Performance Analysis of AES and ChaCha20 in Resource-Constrained Environments. International Journal for Multidisciplinary Research. 2025. Vol. 7, No. 6. P. 1-12.
4. Bernstein D. J. ChaCha, a variant of Salsa20. Workshop Record of SASC. 2008. Vol. 8. P. 3-5.
5. Dobraunig C., Eichlseder M., Mendel F., Schläffer M. Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology. 2021. Vol. 34. Article 33.
6. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L. The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive. 2013. Report 2013/404.
7. Kumar P., Singh A. Secure Data Management Via Lightweight Cryptographic Techniques in IoT. Proceedings of 13th ICAIIT. 2025. P. 1-8.
8. Nguyen T. T., Reddi V. J. Machine Learning-Based Intrusion Detection Methods in IoT Systems. Electronics. 2024. Vol. 13, No. 18. Article 3601.
9. Khan N. W., Alshehri M. S., Khan M. A., Almakdi S., Moradpoor N., Gidlund M., Alharbi S. A hybrid deep learning-based intrusion detection system for IoT networks. Mathematical Biosciences and Engineering. 2023. Vol. 20, No. 8. P. 13491-13520.
10. Ahmed S., Hassan M. Machine learning based intrusion detection framework for detecting security attacks in internet of things. Scientific Reports. 2024. Vol. 14. Article 23659.
11. Mahmud M. Z., Hossain M. S., Alam S., Andersson K. Optimized IoT Intrusion Detection using Machine Learning Technique. arXiv preprint. 2024. arXiv:2412.02845.
12. Chen Y., Wang L., Zhang H. Enhanced intrusion detection system IoT network security model by feed forward neural network and machine learning. Scientific Reports. 2025. Vol. 15. Article 1847.
13. Jabbar M. A., Aluvalu R., Reddy S. S. S. Cluster based ensemble classification for intrusion detection system. Proceedings of the 9th International Conference on Machine Learning and Computing. 2017. P. 253-257.
14. Saba T., Rehman A., Sadad T., Kolivand H., Bahaj S. A. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering. 2022. Vol. 99. Article 107810.

УДК 004.65

Аліна ДАВЛЕТОВА

Західноукраїнський національний університет

ПРОЕКТУВАННЯ ЗАХИЩЕНИХ БАЗ ДАНИХ У РОЗПОДІЛЕНИХ IoT-СИСТЕМАХ

Вступ. Розвиток технологій Інтернету речей (IoT) створює нові виклики щодо збереження та обробки великих обсягів даних, що генеруються численними сенсорами та пристроями [1, 2]. Ефективне проектування баз даних (БД) та забезпечення їх безпеки є критично важливими для надійної роботи IoT-систем і захисту конфіденційної інформації користувачів [3, 4].

Метою є дослідження методологічних та технічних аспектів проектування та захисту БД в системах IoT.

1. Методологічні основи проектування баз даних

Системи IoT характеризуються великою кількістю підключених пристроїв, що безперервно генерують дані різного типу, наприклад числові показники, текстові повідомлення, мультимедійні потоки або події. Такі дані мають високу швидкість надходження та значний обсяг, що створює специфічні вимоги до БД щодо їх зберігання, обробки та аналізу.

Для ефективного управління даними IoT застосовуються різні типи БД:

– реляційні (SQL) для структурованих даних,

– нереляційні (NoSQL, документні, графові) для напівструктурованих або розподілених потоків,

– спеціалізовані БД для зберігання сенсорних показників у часових рядах.

Розподілена архітектура БД у IoT-системах забезпечує масштабованість, стійкість до відмов і високу доступність даних (рисунок 1).

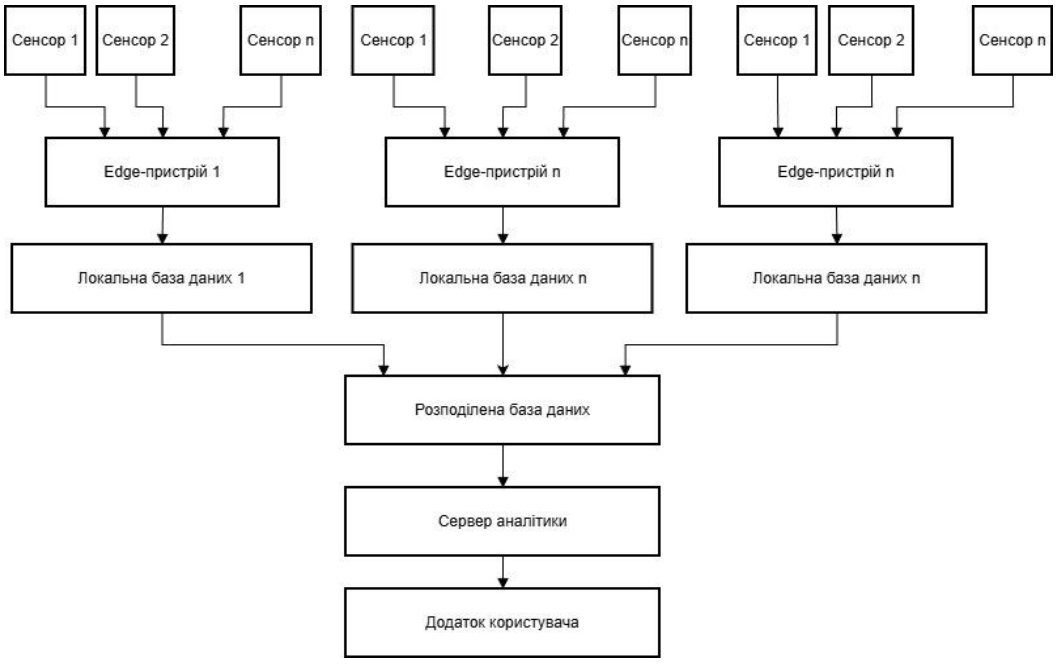


Рисунок 1 – Розподілена архітектура БД у IoT-системах

У таких IoT системах важливо оптимізувати запити, використовувати індексацію та кешування, щоб прискорити доступ до даних і забезпечити своєчасну обробку подій у реальному часі. Крім того, дані IoT часто передаються через мережі з обмеженими ресурсами, що накладає додаткові вимоги на ефективність протоколів передачі та інтеграцію з БД.

Проектування БД для систем IoT потребує комплексного методологічного підходу, що враховує як специфіку даних, так і особливості розподілених архітектур. Основними етапами проектування є аналіз вимог, моделювання даних, вибір типу БД та планування механізмів безпеки.

На етапі аналізу визначаються джерела даних, частота їх оновлення, обсяг і структура. Для IoT-систем характерні дані у форматі часових рядів, подій або мультимедійних потоків, що вимагає визначення оптимального формату зберігання та схеми БД.

Моделювання даних передбачає створення концептуальної та логічної схеми БД з урахуванням можливих сценаріїв доступу та обробки даних. Для IoT-систем часто використовують розподілені або гібридні архітектури, що поєднують локальні БД на edge-пристроях та централізовану розподілену БД у хмарі.

Вибір типу БД визначається характером даних та потребами аналітики: реляційні БД ефективні для структурованих даних і транзакцій, тоді як NoSQL і Time-Series бази дозволяють ефективно обробляти великі обсяги напівструктурованих або потокових даних.

Додатково, на етапі проектування враховуються методи забезпечення безпеки: аутентифікація, контроль доступу, шифрування та резервне копіювання. Усе це дозволяє створити БД, здатну забезпечити надійну та ефективну роботу IoT-систем у реальному часі.

2. Технічні аспекти захисту баз даних IoT

Захист БД у системах IoT є важливим етапом проектування та компонентом архітектури, оскільки середовище IoT характеризується високим числом підключених пристроїв та великим потоком даних. Технічні аспекти безпеки включають багаторівневу модель захисту, що охоплює

- контроль доступу,
- шифрування,
- моніторинг та управління подіями безпеки.

Контроль доступу реалізується на рівнях користувачів і пристроїв за допомогою ролей та політик доступу (RBAC/ABAC), що забезпечує обмеження операцій до необхідного мінімуму. Для захисту даних при зберіганні застосовують симетричне та асиметричне шифрування (AES, RSA), а для передачі – протоколи TLS/SSL та VPN.

Моніторинг подій БД включає збір журналів транзакцій, аналіз аномалій та використання систем виявлення вторгнень (IDS/IPS). Інтеграція з SIEM-платформами, такими як Wazuh, Elastic Security або QRadar, дозволяє централізовано відстежувати інциденти безпеки та реагувати на потенційні загрози у реальному часі.

Важливим аспектом є забезпечення цілісності та відновлюваності даних через резервне копіювання та реплікацію у розподілених базах. Крім того, застосування

токенізації та маскування даних дозволяє мінімізувати ризик витоку конфіденційної інформації.

Таким чином, технічні рішення захисту БД IoT повинні бути інтегровані на всіх рівнях архітектури, від edge-пристроїв до центрального сервера аналітики, забезпечуючи комплексну безпеку та відповідність сучасним стандартам інформаційного захисту.

3. Моделі контролю доступу та політики авторизації

Доступ до БД повинен регламентуватися на основі принципів мінімальних привілеїв, поділу обов'язків та багатофакторної автентифікації. На рисунку 2 наведено багаторівневу модель контролю доступу до БД, яка включає етапи автентифікації, авторизації, застосування політик доступу та аудит дій користувачів. Модель побудована за принципом послідовного проходження всіх механізмів безпеки - від перевірки особи до формування журналів подій та виявлення аномалій.

Необхідними компонентами захисту БД також є моніторинг SQL-запитів, фіксація дій адміністраторів, виявлення аномальної активності та централізована система журналювання (ELK Stack, Splunk).

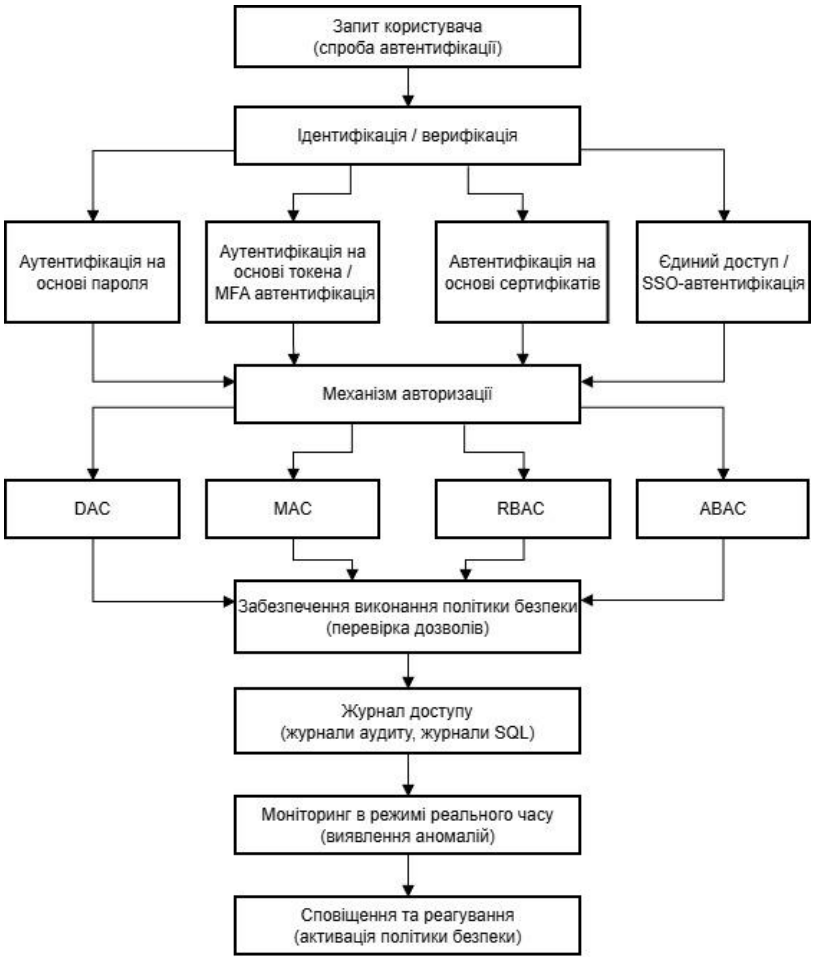


Рисунок 2 – Модель контролю доступу

На початковому рівні автентифікації користувач надсилає запит на доступ. Система виконує ідентифікацію за допомогою одного з способів, що дозволяє підтвердити особу користувача перед наданням доступу до ресурсу.

Після успішної автентифікації, на наступному рівні - авторизації, система визначає, які саме дії користувач має право виконувати, застосовуючи один з механізмів авторизації:

- DAC – контроль, заснований на правах власника;
- MAC – сувора ієрархія доступу за рівнями секретності;
- RBAC – найпоширеніша модель, що базується на ролях;
- ABAC – гнучкий контроль доступу на основі атрибутів користувача та контексту.

Цей етап забезпечує логічний розподіл прав і мінімізацію надлишкових привілеїв.

На рівні застосування політик (Policy Enforcement Point), після проходження авторизації система перевіряє чи відповідає операція дозволеним діям користувача, чи не порушує вона політики безпеки, чи не потребує вона підвищеного контролю. На даному рівні фактично приймається рішення про дозвіл або заборону.

На рівні аудиту та моніторингу (Logging and Monitoring) усі дозволені та заборонені операції фіксуються у журналах: SQL audit logs; login attempts logs; failed access logs; privileges escalation logs. На основі цих журналів здійснюється моніторинг у режимі реального часу, виявлення аномалій, сповіщення та реагування на інциденти. Журнали передаються до SIEM або SOC, що дозволяє виявляти інциденти на ранній стадії.

Переваги наведеної моделі контролю даступу є комбінація автентифікації, авторизації, контролю привілеїв і журналювання, що значно зменшує ризик несанкціонованого доступу, інсайдерських загроз та атак через компрометовані облікові записи. Підтримка різних механізмів авторизації гарантує гнучкість та можливість адаптації під будь-які вимоги. Принцип мінімальних привілеїв дозволяє скоротити площу атаки та зменшує ризик випадкових чи навмисних порушень.

Висновок. Проектування БД для IoT-систем потребує комплексного підходу, що поєднує високу продуктивність з надійним захистом даних. Використання сучасних технологій управління даними та безпеки дозволяє забезпечити безперервну роботу IoT-систем і мінімізувати ризики втрати або компрометації інформації. Запропонована багаторівнева модель контролю доступу забезпечує комплексне посилення захисту БД. Така архітектура підвищує стійкість IoT системи до зовнішніх і внутрішніх загроз, забезпечуючи керованість, прозорість та відповідність сучасним вимогам безпеки.

Перелік використаних джерел.

1. Trabelsi R., Fersi G., Jmaiel M.. 2023. Access control in Internet of Things: A survey. Comput. Secur. 135, C (Dec 2023). https://doi.org/10.1016/j.cose.2023.103472

2. Golightly L., Modesti P., Garcia R., Chang V. Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN, Cyber Security and Applications, Volume 1, 2023, 100015,https://doi.org/10.1016/j.csa.2023.100015.

3. Ulybyshev D., Rogers M., Kholodilo V., Northern B. End-to-End Database Software Security. Software 2023, 2, 163-176. https://doi.org/10.3390/software2020007

4. Hu V.C. Access Control on NoSQL Databases. NIST Interagency (IR8504) National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8504

УДК 681.5:621.9

Сергій СОРОКА, Микола БЕРНАДСЬКИЙ, Оксана БУРЛАК

Західноукраїнський національний університет

МОДЕЛЬНО-ОРІЄНТОВАНЕ КЕРУВАННЯ ТИПУ INTERNAL MODEL CONTROL В СИСТЕМАХ РЕГУЛЮВАННЯ ТЕМПЕРАТУРИ

Вступ. Системи автоматичного регулювання температури є невід'ємною складовою сучасних технологічних комплексів. Їх ефективність визначає не лише стабільність параметрів виробничого середовища, але й безпосередньо впливає на енерговитрати, якість продукції та тривалість технологічних циклів. У більшості випадків для таких задач використовують PID-регулятори, які завдяки простоті налаштування і реалізації залишаються промисловим стандартом. Однак їх застосування пов'язане з низкою труднощів, зокрема чутливістю до зміни параметрів об'єкта та складністю адаптації до збурень.

Проблема зберігає особливу актуальність у промислових системах, де температурні характеристики змінюються внаслідок старіння обладнання, сезонної залежності, коливань навантаження або впливу зовнішніх факторів. У таких умовах традиційні методи регулювання можуть виявитися неефективними, що стимулює пошук нових підходів. Одним із перспективних напрямів є модельно-орієнтоване керування (Model-Based Control), центральне місце в якому посідає метод Internal Model Control.

Об'єктом дослідження є система автоматичного керування температурою на основі методології Internal Model Control.

У роботі розглянуто принципи побудови систем автоматичного керування температурою на основі методології Internal Model Control (IMC). Проаналізовано особливості використання моделі об'єкта в контурі керування, наведено порівняння з класичними PID-регуляторами та визначено основні переваги застосування модельно-орієнтованого підходу в умовах змінних параметрів технологічного процесу. Показано, що використання структури IMC забезпечує підвищення точності та робастності системи, а також зменшення впливу зовнішніх збурень на регульовану величину.

Метою даного дослідження є порівняння моделі об'єкта в контурі керування з класичними PID-регуляторами та визначення переваги застосування модельно-орієнтованого підходу в умовах змінних параметрів технологічного процесу.

1. Теоретичні основи Internal Model Control

Концепція Internal Model Control ґрунтується на припущенні, що система керування може ефективно компенсувати вплив збурень лише за умови володіння інформацією про математичну модель об'єкта. Тобто, якщо регулятор має вбудовану модель процесу, він здатний передбачити його поведінку та сформувати оптимальний керуючий сигнал.

Структура IMC включає два ключові елементи:

−модель об'єкта, яка відтворює реакцію реального процесу,

−фільтр корекції, що впливає на динамічні властивості системи.

Регулювання за принципом Internal Model Control (IMC) використовує внутрішню модель процесу. Якщо регулятор є точною апроксимацією оберненої функції реального процесу, то вихідна величина завжди дорівнює заданій. Проте реалізація регулятора, що повністю відтворює обернену модель процесу, зазвичай є неможливою [1-3] (рисунок 1).

$$G_c(s) = G_p(s)^{-1}$$

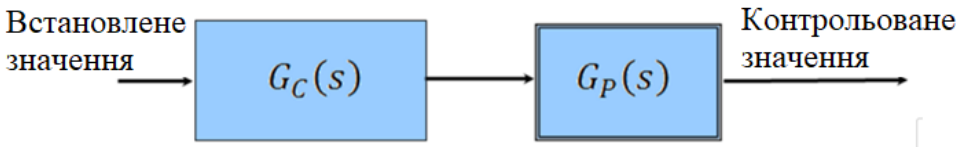


Рисунок 1 - Регулятор у вигляді оберненої моделі

Застосування зворотного зв'язку є необхідним, якщо модель процесу неточна або неповна. Система зі зворотним зв'язком частково компенсує похибки моделі та підвищує стійкість до збурень і шумів, що впливають на об'єкт керування (рисунок 2).

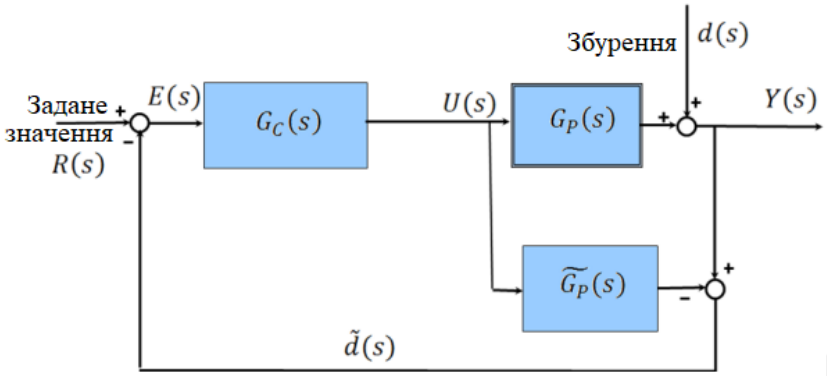


Рисунок 2 - Регулятор IMC із зворотним зв'язком

Позначення, використані на рисунку 2:

$d(s)$ – невідоме збурення, що діє на об'єкт;

$U(s)$ – сигнал керування;

$Y(s)$– вихід системи;

$\tilde{d}(s)$ – різниця між реакцією системи та моделі.

Згідно з теорією, на якій базується IMC, система із правильною внутрішньою моделлю ідеально компенсує зовнішні впливи. У реальних промислових умовах це твердження дещо обмежене неточністю моделей, однак IMC дозволяє гнучко регулювати міру їх впливу, що робить метод ефективним навіть у випадку невизначеностей об'єкта.

2. Побудова моделі об'єкта температурного керування

Для реалізації IMC необхідно сформувати математичну модель об'єкта. У випадку температурних систем найчастіше використовують інерційні моделі першого порядку з запізненням. Передавальна функція такого процесу описується виразом:

$$G_c(s) = \frac{K}{T_s + 1} e^{-Ls},$$

де K - коефіцієнт передачі, T - постійна часу, L - час запізнення.

Модель може бути отримана експериментальним шляхом, зокрема методом реакції на одиничний стрибок, або із застосуванням сучасних методів ідентифікації, включаючи нейронні мережі. Це особливо важливо для систем, де властивості об'єкта змінюються під час експлуатації.

Після побудови моделі формується зворотний регулятор, який мінімізує похибку між реальним об'єктом і моделлю. У класичному випадку керуючий сигнал визначається з урахуванням зворотної моделі:

$$u(t) = G^{-1}(s)f\big(\epsilon(t)\big),$$

де $\varepsilon(t)$ – похибка регулювання.

Щоб уникнути некоректної інверсії, пов'язаної з нестійкістю, застосовується фільтр $Q(s)$, який задає допустиму смугу пропускання системи:

$$Q(s) = \frac{1}{(\lambda s + 1)^n},$$

де параметр λ визначає компроміс між швидкодією та робастністю.

На рисунку 3 видно характерні перерегулювання температури під час зміни заданого значення. Їх можна усунути шляхом застосування допоміжного фільтра. Застосування такого фільтра усуває перерегулювання, проте збільшує час наростання температури до заданої величини.

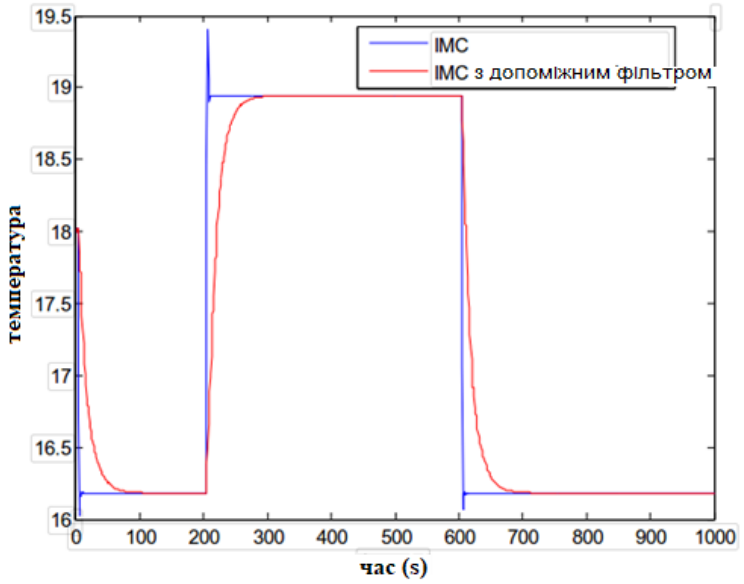


Рисунок 3 - Реакція спроєктованого регулятора IMC на стрибок заданої величини

3. Порівняння IMC з PID-регулюванням

Хоча IMC і PID мають різну теоретичну основу, між ними існує прямий зв'язок: регулятор IMC можна перетворити у PID зі зміненими параметрами. Це робить IMC універсальним інструментом для налаштування PID-регулятора.

Для порівняння дії регуляторів можуть бути використані два параметри:

- вхідна чутливість S_r (здатність системи точно відтворювати задану траєкторію);
- вихідна (збурювальна) чутливість S_d (стійкість системи до зовнішніх збурень і рівень їх пригнічення регулятором).

У таблиці 1 наведено аналітичні вирази, що визначають вхідну та збурювальну чутливість для порівнюваних структур регулювання.

Таблиця 1 - Аналітичні вирази, що визначають вхідну та збурювальну чутливість

Параметр	Регулятор	
	PID	IMC
S_r	$\frac{G_c * G_p}{1 + G_c * G_p}$	$\frac{G_c * G_p}{1 + G_c * (G_p - \widetilde{G}_p)}$
S_d	$\frac{1}{1 + G_c * G_p}$	$\frac{1 - G_c * G_p}{1 + G_c * (G_p - \widetilde{G}_p)}$

Порівняльні характеристики IMC та PID-регулювання показано у таблиці 2.

Таблиця 2 – Порівняльні характеристики IMC та PID-регулювання

Характеристика	PID	IMC
Робастність до збурень	середня	висока
Залежність від зміни об’єкта	висока	низька
Налаштування	потребує експериментів	має системний підхід
Чутливість до шуму	значна	помірна

Регулятори PID і IMC є системами з одним ступенем свободи, тому під час налаштування потрібно шукати компроміс між швидкістю реакції на зміни заданого значення та стійкістю до збурень.

Використання IMC у системах регулювання температурою забезпечує:

−зменшення інтегральної похибки типу IAE,

−зниження часу перехідного процесу,

−підвищення стійкості до параметричних змін,

−легкість адаптації під різні режими роботи.

У результаті модельно-орієнтоване керування є надійним рішенням для систем із непостійними характеристиками, що неможливо гарантувати в рамках PID-підходу.

Висновок. Метод Internal Model Control є ефективним інструментом підвищення точності та надійності систем автоматичного регулювання температури. Його застосування дозволяє компенсувати збурення, адаптуватися до зміни параметрів об’єкта та забезпечити високу якість регулювання. Завдяки здатності до інтеграції з класичними структурами IMC має значний потенціал для впровадження в промислові системи керування.

Перелік використаних джерел

1. Nath U. M., Sahu P. K., Panda R. C. Review on IMC-Based PID Controller Design Approach. - International Journal of Systems Science, 2023, Vol. 54(2), pp. 157–176.

2. Ningsih W., Putra E., et al. Performance Analysis of IMC-PID Controller on Pressure Control System. - Indonesian Journal of Electronics and Instrumentation Systems, 2024, Vol. 14(1), pp. 45–54.

3. Ranjan A., Patel S. Modified Internal Model Control for Nonlinear Processes. - Control Engineering Practice, 2023, Vol. 133, pp. 1–12.

УДК 681.5

Михайло КОБЕЛЯ

Західноукраїнський національний університет

ДОСЛІДЖЕННЯ ТА ОПТИМІЗАЦІЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВИСОКОТЕМПЕРАТУРНОЮ ТЕХНОЛОГІЧНОЮ УСТАНОВКОЮ

Вступ. Високотемпературні технологічні установки посідають ключове місце в металургії, машинобудуванні, хімічній промисловості та енергетиці, забезпечуючи виконання процесів плавлення, нагріву, термообробки та інших операцій із значним енергоспоживанням.

Сучасні вимоги до ефективності виробництва, стабільності режимів роботи та безпеки персоналу зумовлюють необхідність широкого впровадження автоматизованих систем управління (АСУ). Вони дозволяють реалізувати точний контроль параметрів, зменшити вплив людського фактора, підвищити якість технологічного процесу й оптимізувати витрати енергії [1-3].

Актуальність теми зумовлена необхідністю модернізації існуючих систем керування, які часто не забезпечують належного рівня адаптивності, швидкодії та надійності в умовах змінних технологічних режимів. Використання сучасних алгоритмів оптимізації та інструментів промислової автоматизації дає можливість підвищити продуктивність агрегатів, забезпечити діагностику та попередження аварійних ситуацій, а також інтегрувати установку в загальну систему управління підприємством.

Додаткову цінність становить впровадження технологій Інтернету речей (IoT), які забезпечують розширені можливості віддаленого моніторингу, збору телеметрії в реальному часі та аналітики параметрів роботи установки. Це дозволяє підвищити точність керування, оперативність реагування на відхилення та підтримку оптимальних режимів роботи за рахунок взаємодії сенсорних вузлів, контролерів і хмарних сервісів.

Метою роботи є дослідження та вдосконалення АСУ технологічною установкою сталеплавильного виробництва для підвищення її ефективності, надійності та стабільності функціонування.

1. Дослідження будови та принципу дії об’єкта управління

Сталеплавильне виробництво є одним із найбільш енергоємних технологічних процесів (ТП) у промисловості. Значна частка сталі у світі виробляється в електродугових печах (ЕДП), робота яких характеризується високою динамічністю, впливом випадкових збурень та складними нелінійними залежностями. Електрична дуга є нестабільним об’єктом керування, оскільки параметри плавки змінюються в залежності від хімічного складу шихти, теплового стану футеровки, коливань електродів та умов подачі кисню [4].

ЕДП оснащуються АСУ, які дозволяють підтримувати оптимальні режими плавлення, зменшувати енерговитрати та підвищувати безпеку експлуатації. Проте традиційні системи регулювання не завжди забезпечують достатню стійкість та

точність керування в умовах дії складних динамічних збурень, тому актуальним є питання розробки та оптимізації систем регулювання.

На рисунку 1 наведений приклад АСУ ЕДП [3]. До складу системи входять коплекс технічних засобів автоматизації (ТЗА), що включає: датчики та перетворювачі температури, тиску, положення, витратоміри рідинних або газових середовищ, виконавчі гідравлічні механізми, промислові контролери (PLC) з підтримкою стандартних протоколів обміну даними.

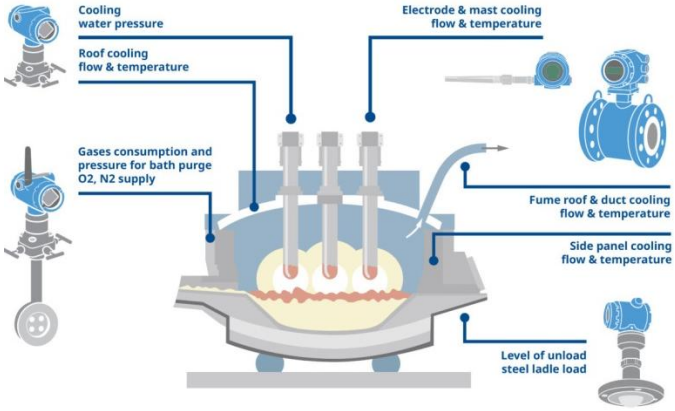


Рисунок 1 – Схема автоматизації ЕДП

Перелічені ТЗА забезпечують безперервне вимірювання параметрів та формування керуючих впливів для підтримання стабільного теплового режиму та безпечної роботи обладнання.

АСУ ЕДП, як правило, включає такі основні контури регулювання:

−керування електричною дугою (положення електродів, струм дуги);

−контроль температури металу, футеровки та газоходів;

−регулювання витрати охолоджувальної води;

−керування кисневою інтенсифікацією;

−контроль тиску та параметрів димових газів.

2. Моделювання та оптимізація автоматизованої системи управління

На основі проведених досліджень АСУ ЕДП побудовано передавальні функції окремих елементів, зокрема регулятора, виконавчого механізму, органу регулювання та технологічної ланки. Узагальнена передавальна функція розімкнутої системи має вигляд:

$$G_{cl}(s) = \frac{8}{0{,}001s^4 + 0{,}1205s^3 + 2{,}06s^2 + s}.$$

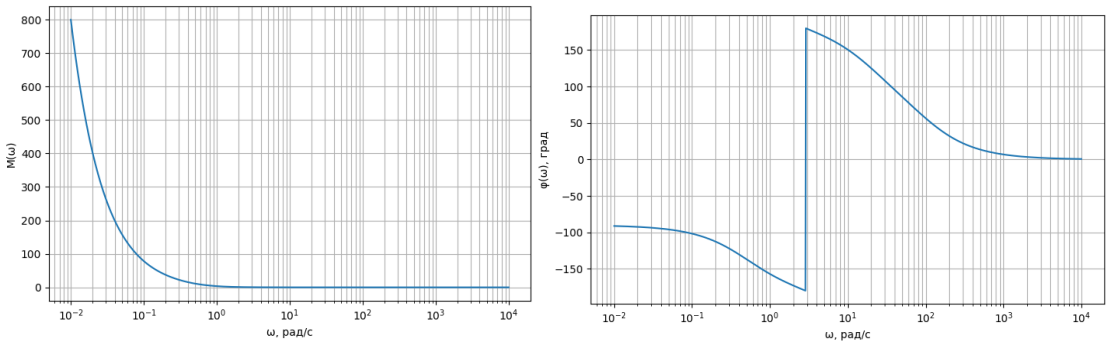
Замкнута система описується:

$$G_{cl}(s) = \frac{G_x(s)}{1 + G_x(s)}.$$

Було виконано аналіз полюсів, побудовано перехідні процеси, амплітудно-частотні (АЧХ) (рисунок 2а) та фазо-частотні (ФЧХ) (рисунок 2б) характеристики розімкнутої системи. Отримані результати вказують на ризик нестійкості системи та чутливість до збурень.

На рисунку 3 наведено реакцію замкнутої системи керування ЕДП на одиничний стрибковий сигнал, яка вказує на те, що система є стійкою, але має значне

перерегулювання (80.74 %), малий запас стійкості та коливальний характер реакції, y(t) то перевищує, то недосягає значення 1.



а) б)

Рисунок 2 – Характеристики розімкнутої системи

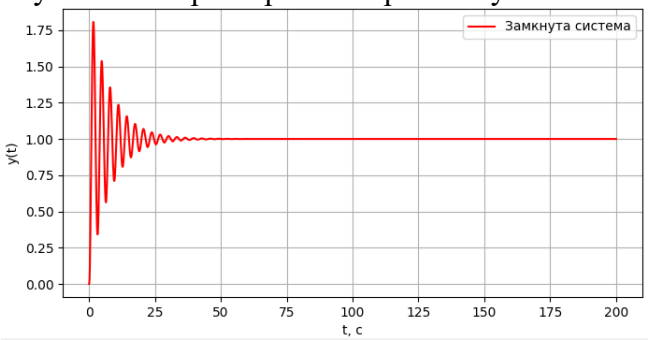


Рисунок 3 – Перехідний процес замкнутої системи

Проведені дослідження показали, що система схильна до коливань, чутлива до збурень і не забезпечує технологічної надійності процесу плавлення, тому виникає потреба в оптимізації.

Для динамічних контурів із швидкою реакцією (довжина дуги, струм дуги) застосовуються PID-регулятори, для температурних контурів - PI/PID. Обчислення керуючої дії здійснюється за виразом:

$$u(t) = K_p e(t) + K_i \int e(t)dt + K_d \frac{de(t)}{dt},$$

де $e(t) = r(t) - y(t)$ - похибка регулювання.

Використані математичні моделі та передавальні функції ЕДП дозволяють виконати налаштування регуляторів на основі частотних і перехідних характеристик.

Для покращення характеристик використано метод оптимізації на основі генетичного алгоритму, який проводив пошук оптимальних значень регулятора. Критерій оптимізації враховував перерегулювання, час встановлення, інтегральну похибку та плавність реакції системи

$$J = \int_0^{t_k} e(t)^2 dt + \alpha u(t)^2,$$

За результатами оптимізації сформовано оновлені параметри PID-регулятора, які забезпечують значне покращення якості перехідних процесів

$$K_p = 1.3395, K_i = 1.2945, K_d = 0.8481.$$

На рисунку 4 наведено результати моделювання, що демонструють перехідні процеси базової та оптимізованої системи. Застосування отриманих параметрів

регулятора забезпечують підвищення демпфування, зменшення коливань і пришвидшення перехідного процесу.

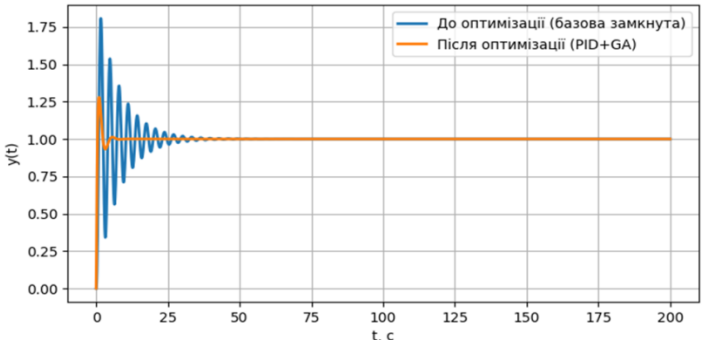


Рисунок 4 - Порівняльний аналіз якості перехідних процесів

Оптимізація АСУ дозволяє зменшити зношування гідроприводів, стабілізувати електричну дугу, знизити енерговитрати, мінімізувати ризики аварій та отримати передбачуване керування. В таблиці 1 наведено порівняння характеристик системи.

Таблиця 1 – Порівняльні характеристики АСУ

Показник	До оптимізації	Після оптимізації
Перерегулювання	80.74 %	27.94 %;
Час встановлення	0,9 с	0,5 с
Коливання	є	відсутні
Статична похибка	0	0
Стійкість	низька	висока

Висновок. У роботі проведено повне дослідження автоматизованої системи керування дуговою піччю: від аналізу технологічного процесу до математичного моделювання та оптимізації. Отримані результати підтверджують ефективність застосування генетичних алгоритмів для покращення параметрів регулювання складних технологічних об’єктів.

Оптимізована система забезпечила значне зменшення перерегулювання, усунення коливань та підвищення стійкості, що є критично важливим для дугового сталеплавильного виробництва. Робота має практичне значення та може бути використана для вдосконалення існуючих АСУ ТП металургійних підприємств

Перелік використаних джерел.

1. Технологія виробництва сталі: повний процес від руди до готового металу. [Електронний ресурс].- Режим доступу: https://kompositstal.com.ua/технологія-виробництва-сталі/

2. З чого виготовляють сталь? [Електронний ресурс].- Режим доступу: https://mskukraine.com/uk/blog-uk/z-chogo-vygotovlyayut-ta-yak-vyroblyayut-stal/

3. Як передові технології автоматизації сприяють переходу до виробництва зеленої сталі. [Електронний ресурс].- Режим доступу: https://www.emersonautomationexperts.com/2023/measurement-instrumentation/how-advanced-automation-technology-driving-transition-green-steel-manufacturing/

4. Електродугова піч для виробництва сталі. [Електронний ресурс].- Режим доступу: https://hanmetallurgy.com/electric-arc-furnace-steelmaking/

УДК 004.056.5

Віталій КЛІМ, Тарас ЦАВОЛИК

Західноукраїнський національний університет

АРХІТЕКТУРА СИСТЕМИ БЕЗПЕКИ KUBERNETES

Вступ. Стрімке поширення контейнеризації та використання Kubernetes як домінуючої платформи оркестрації призводить до суттєвого ускладнення вимог до кібербезпеки. Динамічність кластерів, автоматичне масштабування, часті оновлення контейнерних образів та велика кількість взаємодіючих мікросервісів створюють середовище, у якому традиційні статичні політики безпеки втрачають ефективність. Контроль доступу, перевірка конфігурацій та моніторинг активності повинні реагувати на зміни у режимі реального часу, інакше в інфраструктурі виникають критичні прогалини безпеки. Сучасні системи DevOps та GitOps вимагають автоматизованого й адаптивного управління політиками, що забезпечує їх узгодженість у всіх середовищах. Динамічне застосування політик стає ключовим елементом захисту Kubernetes, оскільки дозволяє мінімізувати людський фактор, забезпечити відповідність конфігурацій та автоматично блокувати потенційні загрози без втручання адміністратора. Такий підхід дозволяє не лише підвищити рівень безпеки, а й підтримувати стабільність сервісів у системах високого навантаження. Додатково впровадження політик дає можливість стандартизувати процеси безпеки, що особливо важливо при роботі великих команд та у розподілених інфраструктурах.

Мета. Метою дослідження є обґрунтування концепції динамічного застосування політик безпеки у Kubernetes та визначення механізмів, які забезпечують адаптивність, автоматичне реагування на аномалії та підвищення стійкості контейнеризованих інфраструктур. Одним із ключових завдань є встановлення взаємозв'язку між поведінковим моніторингом, автоматизованими інструментами контролю та інтелектуальними системами аналізу загроз, що дозволяють сформувати сучасну модель кіберзахисту.

1. Основи реалізації динамічних політик безпеки.

Механізм політик у Kubernetes реалізується через Admission Controllers – модулі, які перехоплюють запити до API-серверу перед створенням або модифікацією об'єктів. Додаткове розширення можливостей надають інструменти Kyverno та Open Policy Agent (OPA) Gatekeeper, що дозволяють формувати політики на мові декларативних правил [1].

Динамічне застосування політик передбачає зміну правил залежно від:

– подій у системі моніторингу (наприклад, Falco або eBPF-сенсор фіксує аномалію);

– контексту запиту (namespace, роль користувача, тип застосунку);

– аналітики поведінки контейнерів (виявлення нетипових дій, спроб доступу до host-ресурсів).

Така архітектура забезпечує принцип Policy-as-Code, коли всі політики зберігаються у Git-репозиторії та оновлюються автоматично через GitOps-процеси (ArgoCD або Flux). Це мінімізує людський фактор і гарантує узгодженість конфігурацій у всіх середовищах.

2. Інтеграція політик з системами виявлення аномалій.

Динамічні політики безпеки ефективні лише у зв'язці з механізмами моніторингу. Інструменти, що базуються на технології eBPF, дозволяють аналізувати системні виклики ядра й миттєво ініціювати реакцію – наприклад, блокування контейнера, що перевищив дозволені права.

Типовий цикл роботи системи такий:

1. Сенсор Falco фіксує подію (наприклад, exec у привілейованому контейнері);

2. Подія передається у систему автоматизації (Kyverno Controller або OPA Webhook);

3. Динамічна політика змінюється - блокує запуск подібних контейнерів у майбутньому;

4. Зміни синхронізуються у Git-репозиторії, забезпечуючи audit-trace.

Таблиця 1 - Взаємозв'язок між рівнем реагування та типом події

Тип події	Реакція політики	Інструмент реалізації
Підозріла активність у контейнері	Блокування, alert	Falco, Kyverno
Спроба зміни конфігурації	Автоматичне відхилення	OPA Gatekeeper
Вразливий контейнерний образ	Оновлення політики CI/CD	Trivy, ArgoCD
Нетипова мережева активність	Заборона доступу	Cilium, Calico

Висновок. Динамічні політики безпеки є ключовою складовою сучасної моделі захисту Kubernetes. Вони забезпечують автоматичне реагування на зміни у кластері, адаптацію політик у реальному часі, інтеграцію з поведінковим моніторингом та значно зменшують ризики, пов'язані з людським фактором. Завдяки поєднанню Policy-as-Code, eBPF-моніторингу, GitOps-підходів та SIEM-аналітики формуються самонавчальні системи кіберзахисту. У майбутньому очікується інтеграція машинного навчання, яке дозволить прогнозувати загрози та формувати політики автоматично, що зробить Kubernetes платформою з автономним рівнем безпеки. Крім того, розвиток поведінкових моделей дозволить створювати системи, здатні передбачати потенційні атаки та блокувати їх до фактичного здійснення, що істотно підвищить рівень кіберзахисту підприємств.

Перелік використаних джерел.

1. Kyverno Policy Engine for Kubernetes. [Електронний ресурс]. - Режим доступу: https://kyverno.io/

2. Open Policy Agent Gatekeeper. [Електронний ресурс]. - Режим доступу: https://openpolicyagent.org/

3. Falco Runtime Security Project. [Електронний ресурс]. - Режим доступу: https://falco.org/

4. ArgoCD GitOps Continuous Delivery. [Електронний ресурс]. - Режим доступу: https://argo-cd.readthedocs.io/

5. Trivy Vulnerability Scanner. [Електронний ресурс]. - Режим доступу: https://aquasecurity.github.io/trivy/

УДК 004.056

Світозар ВАСЕНКО, Степан ІВАСЬЄВ

Західноукраїнський національний університет

ВІДСТЕЖЕННЯ ДІЙ КОРИСТУВАЧА НА ОСНОВІ РЕЄСТРУ WINDOWS

Вступ. У сучасних комп'ютерних системах питання забезпечення кібербезпеки та цифрової криміналістики постає особливо гостро у зв'язку зі зростанням кількості інцидентів, спрямованих на несанкціоновану зміну або приховування даних. Суттєву роль у дослідженні таких інцидентів відіграє аналіз реєстру Windows, який містить велику кількість системних параметрів і артефактів активності користувача [1, 2].

Реєстр накопичує інформацію про запуск програм, відкриття документів, роботу з провідником Windows, зміну конфігурацій та параметрів системи. Ці дані є надзвичайно інформативними для реконструкції поведінки користувача та визначення потенційно шкідливих дій, оскільки деякі артефакти зберігаються навіть тоді, коли журнали подій були видалені або модифіковані [3].

Завдяки автоматизації збору, обробки та аналізу ключів реєстру можливо реалізувати гнучкі системи моніторингу, що дозволяють ідентифікувати загрози та оцінювати відхилення у поведінці користувача. Документація Microsoft підтверджує, що багато системних компонентів Windows залишають цифрові сліди взаємодії у структурі реєстру [4].

Мета: Метою роботи є дослідження артефактів поведінки користувача в реєстрі Windows та розробка високоефективного програмного модуля для автоматичного відстеження, збирання й аналізу даних про дії користувача із формуванням бази подій та побудови поведінкових моделей.

1. Аналіз артефактів реєстру Windows

Реєстр Windows являє собою ієрархічну базу, що складається з гілок, ключів і параметрів, які містять налаштування операційної системи та користувача [1]. Для аналізу активності користувача найбільш інформативними є такі гілки:

- RunMRU - історія команд, введених у вікно «Виконати» (Win+R), що дозволяє відстежувати запуск програм [2];
- TypedPaths - шляхи, введені в адресний рядок провідника Windows, що відображають файлову навігацію [4];
- RecentDocs - список нещодавно відкритих документів різних типів;
- UserAssist - бінарні структури, що зберігають інформацію про використані програми, з частотою запусків та часовими мітками [2];
- ShellBags – дані про перегляд каталогів та їх відображення у провіднику, що широко використовуються у цифровій криміналістиці [5].

Дослідження показали, що Windows оновлює відповідні ключі при кожній взаємодії з програмами, файлами чи системними компонентами, що дозволяє з високою точністю реконструювати послідовність дій користувача [1, 2].

Перспективним є автоматизований збір артефактів: наприклад, читання гілок реєстру, що містять цю інформацію, (рисунок 1), налаштувань безпеки, мережевих налаштувань, автозапуску тощо.

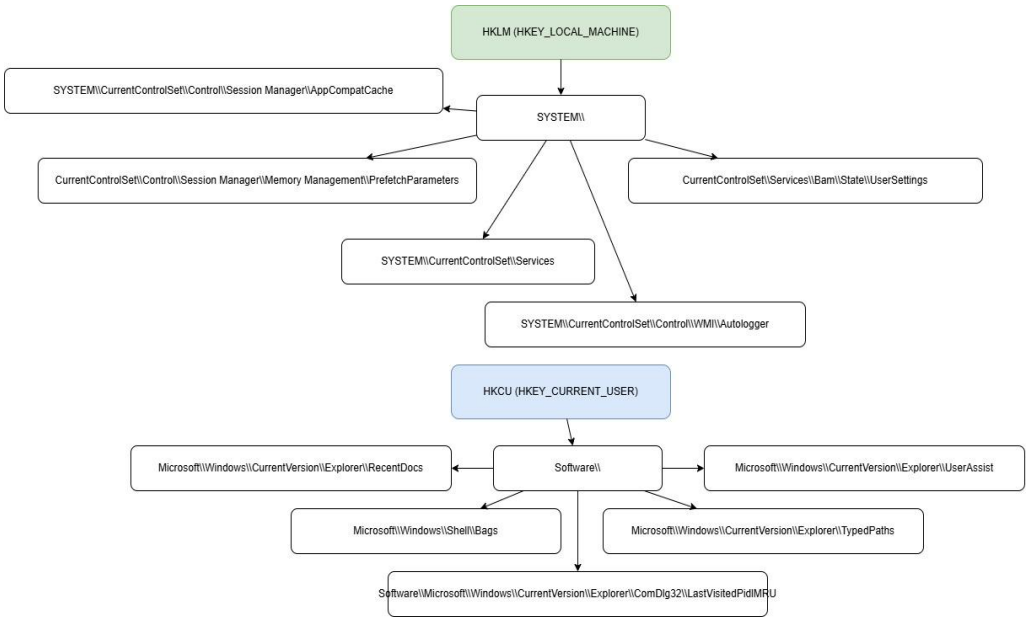


Рисунок 1 – Гілки реєстру Windows що містять чутливу інформацію

2. Розробка програмного модуля аналізу реєстру

Python має стандартний модуль winreg, який дозволяє працювати з «живим» реєстром на поточній системі Windows: відкривати гілки реєстру (HKLM, HKCU тощо), перераховувати підключі та значення, читати типи даних (REG_SZ, REG_DWORD, REG_BINARY тощо), створювати, змінювати й видаляти ключі (у форензіці зазвичай обмежуються читанням). Існують сучасніші бібліотеки, орієнтовані саме на DFIR (Digital Forensics and Incident Response), наприклад, модуль для читання офлайн-реєстру, «парсери» для типових артефактів (BAM/DAM, Amcache, ShimCache, UserAssist, ShellBags тощо), готові CLI-утиліти на Python, які можна запускати з командного рядка для аналізу гілок. Перевага таких бібліотек – наявність вбудованої логіки форензичного аналізу: розробнику не потрібно вручну розбирати структуру бінарних значень, достатньо викликати відповідний парсер.

На основі виконаного аналізу було розроблено програмний модуль на Python, основні функції якого: експорт системних ключів реєстру за допомогою стандартних засобів Windows [4], парсинг .reg-файлів, створених командою експорту, створення структурованих таблиць CSV та запис у базу SQLite для подальшого аналізу, класифікація подій за типами активності: ProgramRun, FileOpen, PathNavigation, побудова графіків активності та візуалізація інтенсивності дій користувача.

Методологічна основа побудови інструменту спирається на описи внутрішніх механізмів Windows, описаних у роботах Russinovich та Ionescu [1], а також на методи цифрової криміналістики, наведені у книгах Carvey і Casey [2, 5].

Розроблене рішення дозволяє автоматично формувати базу подій з часовими мітками, що робить можливим подальший поведінковий аналіз та побудову моделей взаємодії користувача з системою.

3. Експериментальне дослідження системи

Експериментальні дослідження проводилися у віртуальному середовищі VirtualBox з ОС Windows 10. На основі серії сценаріїв (запуск програм, відкриття

файлів, зміна конфігурацій, робота з командним рядком) здійснювався поетапний експорт реєстру.

У результаті встановлено:

- ключ RunMRU точно відображає послідовність запуску системних утиліт та сторонніх програм [2];
- TypedPaths дозволяє відтворити дії користувача у провіднику, зокрема переміщення між каталогами [4];
- RecentDocs містить артефакти роботи з різними типами документів, що має важливе значення для криміналістики;
- UserAssist забезпечує додаткову інформацію щодо частоти запусків програм, що ускладнює спроби приховати активність [5].

ShellBags - один з найточніших артефактів реконструкції переміщення користувача по файловій системі. ComDlg32 MRU - останні файли у діалогах “Відкрити/Зберегти”. BAM/DAM - фіксують детальну інформацію про запуск виконуваних файлів та взаємодію процесів із системою. PrefetchParameters - дає інформацію, чи працює Prefetch, що допомагає оцінити достовірність Prefetch-файлів у форензіці. AppCompatCache (ShimCache) - зберігає інформацію про запуски програм, яку використовує механізм сумісності. Services - налаштування системних служб, драйверів, параметрів завантаження. Autologger - Дозволяє відстежувати низькорівневі події системи, які не потрапили у звичайні журнали подій.

Результати експериментів узгоджуються з висновками, викладеними у роботах Carvey та Casey, де підкреслюється важливість реєстру як джерела доказової інформації [2, 5].

Висновок. У роботі доведено, що реєстр Windows є одним з найбільш інформативних джерел даних для відстеження активності користувача. Розроблений програмний модуль дозволяє збирати, систематизувати та аналізувати дані з різних гілок реєстру, у тому числі при відсутності стандартних логів Windows. Методика може бути інтегрована у системи моніторингу безпеки підприємств, а також застосована у цифровій криміналістиці.

Подальші дослідження можуть включати розширення набору аналізованих артефактів, впровадження засобів обробки даних у режимі реального часу та використання алгоритмів машинного навчання для автоматичної класифікації поведінки користувача [5].

Перелік використаних джерел

1. Russinovich M., Solomon D., Ionescu A. Windows Internals. 7th ed. Microsoft Press, 2017. 1248 p.

2. Carvey H. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. 2nd ed. Syngress, 2016. 330 p.3. Mandia K., Prosise C., Pepe M. Incident Response and Computer Forensics.

4. Mandia K., Prosise C., Pepe M. Incident Response and Computer Forensics. 3rd ed. McGraw-Hill, 2014. 736 p.

5. Microsoft. Windows Registry API and System Behavior. Microsoft Learn Documentation. Available at: https://learn.microsoft.com/en-us/windows/).

УДК 681.05

Володимир ДМИТРУСЬ, Ренат ДАВЛЕТОВ

Західноукраїнський національний університет

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ АВТОНОМНОЮ ЕНЕРГЕТИЧНОЮ УСТАНОВКОЮ

Вступ. Сучасні енергетичні системи потребують автономних джерел електроживлення, здатних забезпечувати стабільну роботу критично важливих об’єктів у умовах обмеженого доступу до централізованих мереж. Автономні енергетичні установки (АЕУ) застосовуються в промисловості, комунальному секторі, транспорті, телекомунікаційній сфері та об’єктах оборонного призначення [1-3]. Високі вимоги до надійності, енергоефективності та безпеки їх функціонування зумовлюють необхідність використання сучасних автоматизованих систем управління.

Впровадження автоматизованих систем управління (АСУ) дозволяє підвищити точність контролю технологічних параметрів, мінімізувати людський фактор, забезпечити оптимальні режими роботи агрегату та зменшити витрати на експлуатацію. Актуальність теми визначається розвитком технологій дистанційного моніторингу та керування, які дозволяють реалізувати адаптивне управління та діагностику технічного стану устаткування в реальному часі. Особливого значення набуває інтеграція IoT рішень, що забезпечують безперервний збір телеметрії, віддалений контроль ключових параметрів роботи АЕУ та аналітичну обробку даних.

Метою є дослідження та розробка АСУ АЕУ, яка забезпечує стабільність функціонування, підвищення енергоефективності та безпеки експлуатації, а також можливість адаптивного контролю та діагностики в різних режимах роботи.

1. Газотурбінний генератор як об’єкт автоматизації

Газотурбінні генератори малої потужності (ГТГ) є АЕУ, що застосовуються в енергетичних комплексах для живлення промислових підприємств, об’єктів нафтогазової сфери, систем критичної інфраструктури та резервного електроживлення. Їх перевагами є компактність, швидкий пуск, висока питома потужність та можливість роботи на різних видах газового палива.

ГТГ складається з компресора, камери згоряння, турбіни, генератора та допоміжних систем (мастило, охолодження, паливоподача). Принцип дії ГТГ (рисунок 1) включає послідовні етапи: стиснення повітря, подачу палива, змішування та згоряння газоповітряної суміші, розширення газів у турбіні та перетворення механічної енергії в електричну на валу генератора [4].

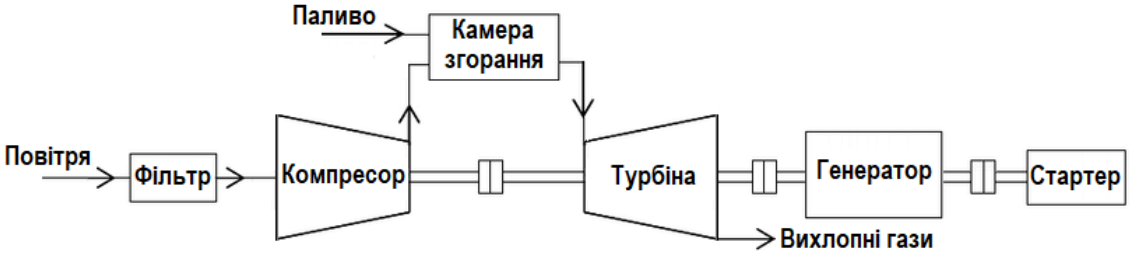


Рисунок 1 - Принципова схема роботи ГТГ

Компресор, зазвичай має роторний (осьовий або відцентровий) тип. Повітря атмосферного тиску всмоктується через повітряний фільтр, що очищує його від пилу та механічних домішок. Обертові лопаті компресора нагнітають повітря між нерухомими напрямними лопатками, унаслідок чого тиск і температура повітря зростають. На виході компресора утворюється потік повітря під високим тиском, який далі подається до камери згорання, що забезпечує стабільне згоряння суміші та рівномірний розподіл температури по потоку, що необхідно для безпечної роботи турбіни.

Газова турбіна сприймає енергію гарячих газів, що розширюються, та перетворює її на механічну енергію обертання вала. Потік газів, проходячи через лопатки турбіни, виконує роботу, обертаючи ротор, який з'єднано з компресором і генератором. Температура відпрацьованих газів на виході з турбіни становить близько 350–400 °C, після чого вони можуть бути використані для нагріву в регенераторі або викидаються в атмосферу Газова турбіна з'єднана з генератором змінного струму, який перетворює механічну енергію обертання вала на електричну енергію

Основними технологічними параметрами, що визначають ефективність роботи ГТГ і підлягають автоматичному контролю та регулюванню, є:

– частота обертання ротора;
– температура газів перед турбіною;
– тиск та витрата паливного газу;
– температура повітря після компресора;
– тиск мастила, температура охолодження;
– електричні параметри генератора.

2. Проектування автоматизованої системи управління

Для забезпечення надійної та безпечної роботи ГТГ запропоновано АСУ, яка виконує моніторинг, регулювання та діагностику основних технологічних параметрів. Система оснащена наступними технічними засобами автоматизації:

- перетворювачі тиску для вимірювання тиску газу та мастила;
- диференційні датчики тиску для контролю фільтрів;
- термопари типів K/N та датчики для вимірювання температур;
- датчики витрати газу ультразвукового або термодинамічного типу;
- датчики рівня в мастильному баку (радарні або поплавкові);
- датчики вібрації та обертів на основі акселерометрів;
- електричні трансформатори струму та напруги для контролю електричних параметрів;
- датчики полум'я (UV/IR) для контролю наявності горіння;
- позиціонери для моніторингу ступеня відкриття паливної арматури.

Виконавча частина АСУ формує керуючі впливи та включає:

- регулюючий паливний клапан швидкодіючого типу зі зворотним зв'язком;
- редуктори тиску паливного газу;
- електричні та пневматичні приводи клапанів;
- соленоїдні відсічні клапани (нормально закриті);
- клапани аварійного скидання газу;

- насоси мастила та охолодження із частотним керуванням;
- система запалювання високої енергії;
- виконавчі механізми направляючих апаратів.

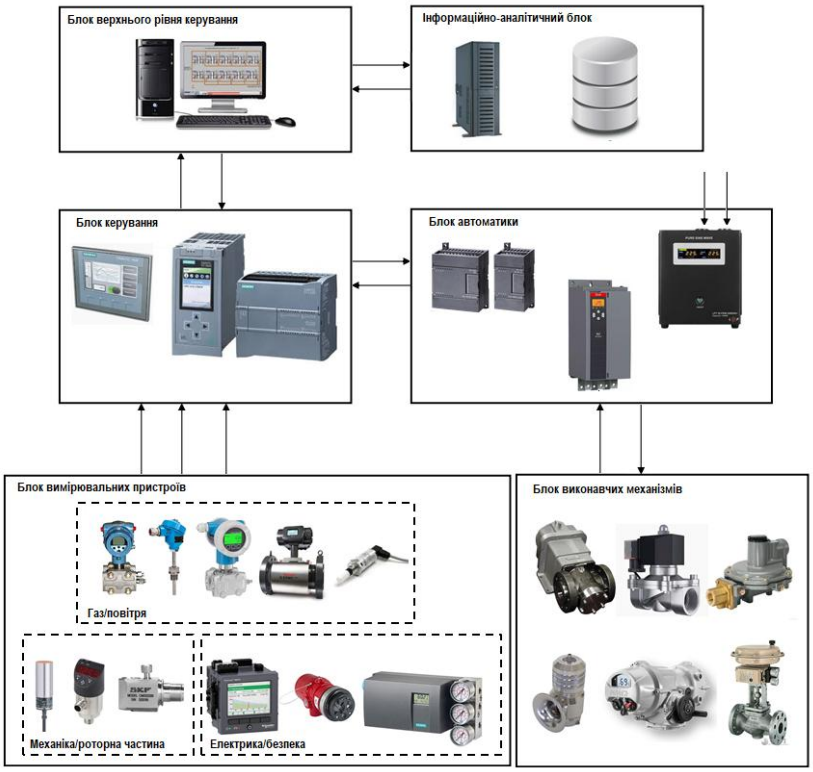


Рисунок 2 – Архітектура АСУ ГТГ

Центральним елементом системи є контролер (ПЛК), що здійснює опитування датчиків (AI, DI, HART, Modbus, Profibus/Profinet), реалізацію контурів регулювання частоти, температури та тиску, логіку протиаварійного захисту (ПАЗ/ESD), діагностику виконавчих механізмів та передавання даних на панель оператора та SCADA-систему.

3. Дослідження системи автоматичного керування

Основним контуром регулювання АСУ є регулювання частоти обертання ротора ГТГ шляхом зміни подачі палива. Для цього використано ПІ-регулятор із антинасиченням, що запобігає накопиченню інтегральної складової при насиченні керуючого сигналу.

Математичну модель побудовано як послідовність інерційних та підсилювальних ланок, що відображають динаміку камери згоряння, турбіни та генератора

$$G(s) = G_v(s) \cdot G_c(s) \cdot G_{comb}(s) \cdot G_{turb}(s) \cdot G_{mech}(s) \cdot G_m(s),$$

де $G_v(s)$ - динаміка виконавчого механізму (паливний клапан), $G_c(s)$ - динаміка компресора, $G_{comb}(s)$ - камера згоряння (затримка нагріву газів), $G_{turb}(s)$ – турбіна, $G_{mech}(s)$ - механічна частина (вал + генератор), $G_m(s)$ - фільтр вимірювального тракту.

На рисунку 3 наведено графіки перехідних процесів. У базовій моделі АСУ частоти обертання ротора ГТГ значення параметрів ПІ-регулятора задавалися згідно з типовими налаштуваннями для систем із домінуванням теплової та механічної інерційності $K_i = 1{,}0$ та $T_i = 6{,}0$. Такі значення забезпечили працездатність

регулятора та допустиму динаміку, однак результати моделювання показали, що початково система має час регулювання близько 2,0–2,2 с, невелике перерегулювання на рівні 5–6 %, підвищену чутливість до різких змін навантаження та повільну компенсацію збурень у режимі пуску.

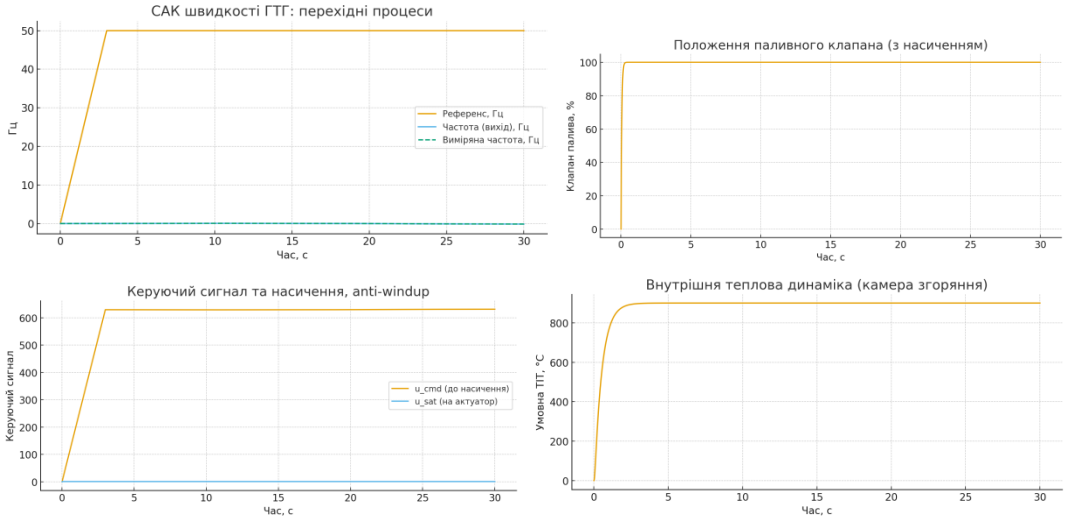


Рисунок 2 – Результати моделювання роботи АСК

Для підвищення якості регулювання застосовано критерій IAE: $IAE = \int_0^{30} |e(t)| dt$, що дозволило визначити оптимальні параметри $K_i^{opt} = 2{,}3$ та $T_i^{opt} = 4{,}5$, які забезпечують скорочення часу регулювання до 1,5 с, зменшення перерегулювання до 3 % та стабільність режимів роботи при пуску та зміні навантаження.

Висновок. У роботі проведено комплексне дослідження структури, параметрів та принципів роботи ГТГ малої потужності. Проаналізовано технічні засоби автоматизації та розроблено архітектуру АСУ ГТГ. Побудовано математичну модель об’єкта керування й виконано моделювання роботи ПІ-регулятора. Оптимізація параметрів за інтегральним критерієм показала можливість зменшення часу перехідних процесів і підвищення стабільності роботи установки. Отримані результати можуть бути використані при проектуванні систем керування мікротурбін, резервних енергоблоків та автономних енергетичних комплексів.

Перелік використаних джерел.

1. Gas Turbine Power Plant – Layout & Schematic Diagram. [Електронний ресурс].- Режим доступу: https://www.electricalengineeringinfo.com/2014/12/gas-turbine-power-plant-or-gas-power-station-layout.html

2. У Бучанській громаді запрацювала перша когенераційна установка. [Електронний ресурс].- Режим доступу: https://mistoinform.com.ua/u-buchanskij-gromadi-zapraczyuvala-persha-kogeneraczijna-ustanovka/

3. "Укрнафта" планує побудувати у 2026 році 420 МВт газової генерації. [Електронний ресурс].- Режим доступу: https://ua-energy.org/uk/posts/ukrnafta-planuie-pobuduvaty-u-2026-rotsi-420-mvt-hazovoi-heneratsii

4. Boukrouma E., & Bendib R., & Zennir Y. (2024). Assessing Fire and Explosion Risks Associated with Gas Turbines Using the Fire and Explosion Index. 2.6.

УДК 004.056

Степанюк О.В., Прончук Д.С.

Західноукраїнський національний університет

СУЧАСНІ ПЕРСПЕКТИВИ АВТОМАТИЗОВАНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

Вступ. У сучасних умовах стрімкого розвитку цифрових технологій та зростання обсягів інформації [1] особливої важливості набуває забезпечення комплексної безпеки об’єктів, інформаційних ресурсів і критично важливої інфраструктури [2].

Автоматизовані системи контролю доступу (АСКД) є ключовим елементом систем фізичного та інформаційного захисту, оскільки вони забезпечують керування доступом до приміщень, ресурсів та інформаційних систем на основі чітко визначених правил і прав користувачів [3].

Актуальність дослідження АСКД зумовлена кількома факторами. По-перше, зростає кількість загроз, пов’язаних із несанкціонованим доступом. По-друге, сучасні організації переходять до інтегрованих систем безпеки, де АСКД взаємодіють з відеоспостереженням, охоронною сигналізацією, біометричними датчиками та інформаційними платформами. По-третє, розвиток хмарних технологій, Інтернету речей та мобільних застосунків стимулює появу нових архітектур АСКД, що вимагають відповідності сучасним стандартам безпеки.

Таким чином, дослідження АСКД є вкрай актуальним, оскільки дозволяє підвищити ефективність захисту об’єктів, забезпечити надійність управління доступом, адаптувати системи до сучасних викликів кібербезпеки.

Мета: дослідити сучасні перспективи розвитку автоматизованих систем контролю доступу.

1. Перспективи автоматизованих систем контролю доступу

Програмні засоби Security information and event management (SIEM) - управління подіями інформаційної безпеки – стали доступними для придбання приблизно 1997 р. Їх функціонал дозволяв зменшити кількість «хибних спрацьовувань» систем виявлення мережевих вторгнень (IDS - intrusion detection system), які загрожували системам IDS. Аналіз експертних думок виявив напрямки з найбільшим потенціалом зростання, які сприятимуть технологічним рішенням АСКД, зокрема концепції SIEM, яка швидко розвивається:

- автоматизація відповіді на кіберінциденти;
- розвиток експертизи у сфері управління системою;
- одавання нового функціоналу SIEM за рахунок методів моніторингу поведінки об'єктів UBA;
- застосування хмарних обчислень як джерела інформації та надання інформації в рамках моделі «as a service»;
- аналіз ситуації на кінцевих вузлах та аналізу трафіку.

Протягом останніх 15 років під SIEM розуміють інструмент для збору

інформації з різних систем і засобів кореляції, при цьому дослідження отриманих масивів даних має на увазі тільки кореляційний аналіз.

Для того, щоб підвищити рівень моніторингу подій безпеки необхідно визначити такі параметри:

- правила, за якими відбуватиметься нормалізація;
- пакети із правилами виявлення загроз;
- методи налаштування джерел даних;
- методику активації джерел;
- зміст правил детектування;
- рекомендації для ситуацій спрацьовування правил.

На даний момент частка покриття SIEM-технології дорівнює 50-60%. Іншим трендом потенційного розвитку SIEM-рішень є автоматизація відповіді на інциденти. Виходячи з результатів опитування, проведеного Positive Technologies, одна четверта частина всіх опитаних спеціалістів у сфері ІБ працює в SIEM-системі щодня 2–4 години. Самими трудомісткими завданнями були названі: аналіз інцидентів (назвали 52% учасників опитування) та обробка хибних спрацьовувань - внесення змін до правил кореляції (58%). Налаштування джерел даних, а також моніторинг їх працездатності займають значну кількість часу на думку 30% фахівців. Така ситуація сприяє еволюції SIEM-рішень у бік програмних рішень Security orchestration and automated response (SOAR), які вирішують питання автоматичного реагування та оркестрації систем безпеки. Для цієї технології покриття приблизно дорівнює 60-70%.

Як третій напрямок для розвитку SIEM слід вказати взаємопроникнення технологій аналізу логів (SIEM-рішення), аналіз мережевого трафіку (Network Traffic Analysis, NTA-рішення), а також аналіз ситуації на кінцевих вузлах (Endpoint Detection & Response, EDR-рішення). За відсутності можливостей, що надаються EDR-системами та детального аналізу трафіку, моніторинг не можна вважати повним. Аналіз мережевого трафіку в найближчі роки буде обов'язковою процедурою при проведенні SIEM, аналіз ситуації на кінцевих вузлах стане опціональною можливістю функціоналу. Для цієї технології частка покриття дорівнює 60-70%.

Четвертою тенденцією можна назвати додавання можливостей UEBA-рішень (механізмів аналізу поведінки об'єктів) до інструментів SIEM, що дасть можливість отримання повної картини ситуації в інфраструктурі на єдиному екрані. Принципова різниця між UEBA та SIEM полягає в тому, що кошти UEBA розробляють моделі поведінки, а SIEM-рішення є деяким конструктором, що збирає логи. В алгоритмах пошуку та вивчення інцидентів можуть використовуватись різні підходи: машинне навчання, глибоке навчання, статистичний аналіз тощо. Ці підходи дають оператору інформацію про те, які об'єкти ведуть себе нетиповим для них чином і чому така поведінка нехарактерна для них. Частка покриття цієї технології складає 70-80%.

Наступний тренд у розвитку SIEM пов'язаний з використанням хмарних технологій. Дослідження, яке провела компанія Enterprise Strategy Group у 2019 р. на замовлення Intel Corp. і Dell Technologies, показало, що 64% організацій планували збільшення витрат на публічні хмарні платформи порівняно з попереднім роком. Ця тенденція стимулює вендорів до додавання найбільш широко використовуваних платформ (Google Cloud Platform, Microsoft Azure, Amazon Web Services) у перелік

підтримуваних джерел SIEM. Крім того, пропонуються системи SIEM за допомогою підходу «as a service», доповнюючи способи розгортання, налаштування та управління системою SIEM (хмарних, віртуальних пристроїв - virtual appliance). На думку експертів, покриття технології дорівнює 60-70%.

Деякі з цих тенденцій вже зараз виявляються певною мірою (рисунок 1), інші з них стануть актуальними протягом 1-3 років. Ці технології покращують рівень якості роботи з системами SIEM і дають можливість знизити навантаження на операторів, які здійснюють моніторинг і реагують на інциденти.

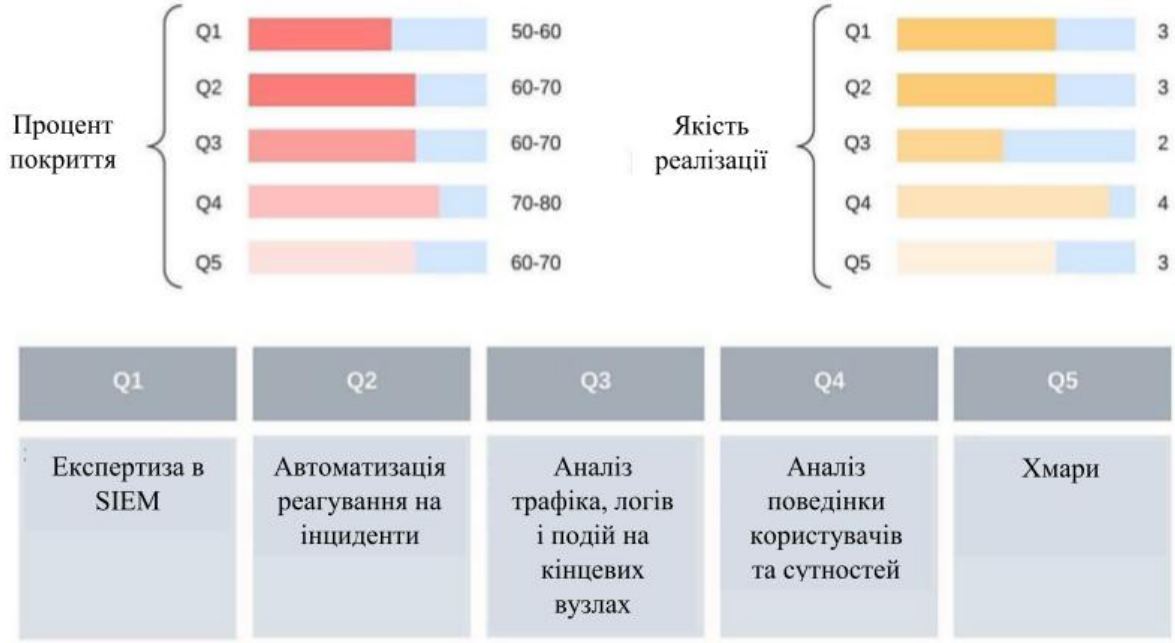


Рисунок 1 - Тренди розвитку SIEM-систем (оцінки якості реалізації: 1 - реалізовано погано; 2 - якість реалізації нижче середнього; 3 - якість реалізації середня; 4 - якість реалізації вище середнього; 5 - реалізовано добре

Подана інформація є експертною оцінкою компанії Positive Technologies. Тенденції є актуальними для компаній-лідерів на ринку SIEM (кількість компаній-лідерів було визначено з допомогою інформації, наданої IDC).

Висновок. Досліджено перспективи розвитку автоматизованих систем контролю доступу, визначено сучасні тенденції та продемонстровано експертні оцінки компанії Positive Technologies.

Перелік використаних джерел.

1. Gil-Garcia J.R., Flores-Zúñiga M.Á. Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. Government Information Quarterly. 2020. Vol.37. No. 4. P. 101518..

2. Li F., Lu H., Hou M., Cui K., Darbandi M. Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. Technology in Society. 2021. Vol.64. No.5. P.101487.

3. Elia G., Margherita A., Passiante G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process. Technological Forecasting and Social Change. 2020. Vol.150. P.119791.

УДК 004.5

Олександр КУХАРУК

Західноукраїнський національний економічний університет

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ АНАЛІЗУ ТА МОНІТОРИНГУ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ

Вступ. Зростання вартості активів, що управляються смарт-контрактами в блокчейн-мережах, робить питання їх безпеки пріоритетним. За даними Halborn Security, у 2023-2024 роках понад 60% втрат у DeFi-секторі стало наслідком вразливостей у смарт-контрактах. Це зумовлює необхідність розробки комплексного підходу до забезпечення безпеки на всіх етапах життєвого циклу розробки програмного забезпечення.

Існує значний розрив між швидкістю розробки нових DeFi-проектів та якістю забезпечення їх безпеки. Багато розробників недооцінюють важливість формальних методів верифікації та комплексного тестування, що призводить до критичних вразливостей у продакшн-середовищі.

Мета. Систематизувати та проаналізувати сучасні заходи та інструменти забезпечення безпеки смарт-контрактів, розробити практичні рекомендації щодо їх застосування.

1. Аналіз предметної області та існуючих засобів забезпечення безпеки смарт-контрактів

Смарт-контракти стали основою для широкого спектра децентралізованих застосунків - від фінансових платформ до логістичних систем. Водночас їхня безпека визначає надійність усієї екосистеми. На відміну від централізованих сервісів, де помилки можна виправити оновленням, смарт-контракти після деплою є незмінними. Це робить критичним аналіз засобів та методів, які сьогодні застосовуються для забезпечення їхньої безпеки.

1. Сфера смарт-контрактів стикається з такими ключовими викликами:
2. Незмінність коду - помилка може призвести до значних фінансових втрат.
3. Публічність та відкритість - код є видимим усім користувачам, зокрема зловмисникам.
4. Складність логіки - високорівневі сценарії взаємодій часто важко передбачити.
5. Зовнішні виклики - смарт-контракти можуть викликати інші контракти, що збільшує ризики.

Відомі інциденти, такі як DAO Hack або експлойти у DeFi-платформах (Cream Finance, Poly Network), підтверджують, що вади у смарт-контрактах здатні призвести до втрати сотень мільйонів доларів.

У сучасній практиці використовуються такі групи інструментів:

1) Статичні аналізатори – перевіряють код на типові патерни вразливостей:
   - Slither - швидкий і гнучкий аналізатор Solidity.
   - Mythril - інструмент для виявлення логічних вразливостей.

- Securify 2.0 - формалізований підхід ETH Zurich.

2) Динамічне тестування (fuzzing, symbolic execution) – дозволяє виявити приховані помилки під час виконання контракту: Echidna; Foundry fuzzing; MythX symbolic analysis.

3) Формальна верифікація – математичний доказ правильності функцій контракту. Застосовується у критичних фінансових контрактах (наприклад, у стандарті ERC-20 для великих бірж).

4) Аудит безпеки - це огляд коду вручну фахівцем. Найчастіше застосовується у великих проектах перед деплоєм. Популярні аудиторські компанії: CertiK; Trail of Bits; PeckShield; OpenZeppelin.

2. Модель забезпечення безпеки

Запропонована концепція системного підходу до забезпечення безпеки смарт-контрактів, яка поєднує існуючі інструменти в єдину багаторівневу систему забезпечення безпеки, орієнтовану не лише на аналіз вразливостей, але й на побудову безпечної архітектури ще до написання коду (рисунок 1).

Рисунок 1 – Узагальнена схема моделі безпеки смарт-контракту

Запропонована модель включає 5 взаємопов’язаних етапів:

Етап 1. Архітектурне проєктування (до написання коду): визначення ролей; сценарії взаємодій; обмеження доступу; мінімізація зовнішніх викликів; використання шаблонів OpenZeppelin; моделювання потенційних атак (threat modeling).

Етап 2. Безпечна розробка:

- використання рекомендованих патернів (Ownable, Pausable, ReentrancyGuard);
- перевірка функцій на gas-ефективність;
- поділ логіки на незалежні модулі;
- використання бібліотек із доведеною безпекою.

Етап 3. Автоматизований аналіз – на цьому етапі застосовуються інструменти, описані у розділі 1, але комбіновано і послідовно:

- Статичний аналіз (Slither)
- Математична верифікація (Certora, Scribble)
- Fuzzing (Echidna)
- Символічне виконання (MythX)

Етап 4. Аудит та інтеграційне тестування – особливість моделі включення двоетапного аудиту:

- внутрішній аудит командою розробки;
- зовнішній аудит (за можливості).

Етап 5. Моніторинг після деплою – це критично важливо, оскільки атаки можуть

бути відкладеними. Інструменти моніторингу:

- Forta Network (виявлення аномалій)
- Tenderly (трасування викликів)
- EigenPhi / DeFiLlama (аналіз транзакцій)

Практичні рекомендації з упровадження:

1. Використання стандартів (ERC-20, ERC-721, ERC-1155) – забезпечує передбачувану поведінку контрактів.

2. Мінімізація зовнішніх викликів – це основна міра проти re-entrancy атак.

3. Використання модифікаторів доступу – наприклад: onlyOwner, onlyAdmin, nonReentrant.

4. Використання «економічних» тестів – аналіз впливу gas-вартості на функціонування контракту.

5. Використання проксі-контрактів – дозволяє оновлювати логіку без деплою нового контракту.

Висновок. У роботі виконано комплексний аналіз проблем безпеки смарт-контрактів і визначено основні вразливості, що мають найбільший вплив на децентралізовані системи. Розглянуто сучасні інструменти і методи аудиту, тестування та верифікації. Запропонована авторська модель SSCL (Secure Smart Contract Lifecycle) забезпечує багаторівневий підхід до безпеки: безпека на рівні архітектури; безпечні патерни розробки; автоматизована перевірка; аудит і моніторинг; можливість безпечного оновлення системи. Запропонований підхід може використовуватись у практиці проєктування і впровадження безпечних смарт-контрактів у DeFi, NFT-платформах та корпоративних рішеннях.

Перелік використаних джерел.

1. Antonopoulos, A. M., Wood, G. Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media, 2018.

2. Solidity Documentation. Solidity Programming Language. Доступно: https://docs.soliditylang.org/

3. Trail of Bits. Smart Contract Security Recommendations. Trail of Bits Security Reports, 2022.

4. CertiK. Security Leaderboard and Audit Reports. CertiK Research Publications, 2021–2024.

5. OpenZeppelin. Contracts Library Documentation. OpenZeppelin Docs, 2024. Доступно: https://docs.openzeppelin.com/

6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

7. Ethereum Foundation. Ethereum Yellow Paper: A Formal Specification of Ethereum Protocol. Ethereum Foundation Technical Reports, 2015–2024.

8. Binance Research. DeFi Attacks and Vulnerabilities: Analytical Reports. Binance Research Publications, 2020–2024.

9. Esposito, D. Blockchain Security and Smart Contract Auditing. Springer, 2021.

10. PeckShield. Annual Blockchain Security Reports. PeckShield Cybersecurity Research, 2021–2024.

УДК 004.056

Наталія ЯЦКІВ, Аліна МИКОЛАЙСЬКА

Західноукраїнський національний університет

КЛАСИФІКАЦІЯ КІБЕРРИЗИКІВ У ХМАРНИХ СЕРВІСАХ

Вступ. Широке впровадження хмарних сервісів у бізнес-процеси, державне управління та повсякденну діяльність користувачів супроводжується зростанням кількості та складності кіберризиків. Модель спільної відповідальності провайдера та споживача, багатокористувацьке середовище, віртуалізація ресурсів, географічно розподілене зберігання даних і автоматизоване масштабування створюють якісно новий простір загроз, який не повністю покривається традиційними підходами до інформаційної безпеки.

У таких умовах особливої ваги набуває системна класифікація кіберризиків у хмарних сервісах, що дозволяє структурувати загрози, уразливості й наслідки інцидентів, узгодити підходи до оцінки ризиків і обґрунтувати вибір організаційних та технічних заходів захисту відповідно до стандартів ENISA, NIST, ISO/IEC 27001 [1].

Мета. Систематизувати та обґрунтувати класифікацію кіберризиків у хмарних сервісах як основу для подальшої розробки методики їх кількісної та якісної оцінки.

1. Підходи до класифікації кіберризиків у хмарних сервісах

Класифікація кіберризиків у хмарних сервісах може здійснюватися за різними критеріями: за джерелом походження (зовнішні/внутрішні), за природою (технічні, організаційні, правові), за об’єктом впливу (дані, сервіси, інфраструктура, користувачі), за етапами життєвого циклу послуг (планування, міграція, експлуатація, виведення з експлуатації). ENISA у своїх звітах пропонує ризик-орієнтовану класифікацію, яка базується на сценаріях інцидентів, типах активів і виявлених уразливостях, що дозволяє охопити як технологічні, так і організаційні аспекти [1].

NIST застосовує ризик-орієнтований підхід, що поєднує класифікацію ризиків з моделлю загроз та рекомендаціями щодо контролів, орієнтуючись на публічні хмарні середовища та модель спільної відповідальності [2].

У контексті хмарних сервісів доцільно будувати класифікацію кіберризиків у кількох взаємопов’язаних вимірах:

- за рівнем (організаційний, технологічний, бізнес-рівень);
- за доменом (безпека даних, безпека інфраструктури, ідентифікація та доступ, відповідність, безперервність бізнесу);
- за моделлю використання (SaaS, PaaS, IaaS) та розгортання.

Такий багатовимірний підхід дозволяє пов’язати виявлені ризики з конкретними сервісними моделями, відповідальністю сторін, нормативними вимогами та наборами контролів [3].

2. Організаційно-політичні ризики

До організаційно-політичних ризиків належать ризики, пов’язані з управлінням, контрактами, відповідністю і взаємовідносинами між провайдером та клієнтом. ENISA

виокремлює, зокрема, ризики: залежність від постачальника, втрата контролю над даними й процесами, виклики відповідності, репутаційні ризики через дії «сусідів» по хмарі, припинення надання сервісів або їх поглинання іншим провайдером, проблеми ланцюга постачання.

Залежність від постачальника проявляється у складності або неможливості міграції даних і сервісів до іншого провайдера через закриті формати даних, нестандартні API, відсутність процедур повернення або знищення даних. Це призводить до довготривалої залежності, підвищення витрат і ускладнює реагування на інциденти безпеки чи зміну політик провайдера. Ризик втрати контролю пов'язаний із передачею значної частини функцій управління IT-інфраструктурою зовнішній організації; у результаті замовник може не мати достатньої прозорості щодо реального стану безпеки, журналів доступу, механізмів резервного копіювання та відновлення [1].

Ризики відповідності стосуються невідповідності регуляторним вимогам (GDPR, національне законодавство, галузеві стандарти), особливо за умови розміщення даних у різних юрисдикціях та використання субпідрядників. Відсутність прозорості щодо місця зберігання та обробки даних, субобробників та сертифікацій провайдера ускладнює оцінку відповідності. Такі ризики класифікуються як бізнес-критичні, бо можуть призвести до значних штрафів та обмеження діяльності організації [2].

3. Технічні ризики інфраструктури та віртуалізації

Технічні ризики охоплюють уразливості інфраструктури, гіпервізора, механізмів ізоляції віртуальних машин, мережевої сегментації, засобів моніторингу й управління ресурсами. У хмарних середовищах особливо критичними є ризики порушення ізоляції між тенантами (наприклад, через уразливості гіпервізора), некоректної конфігурації мережевих політик, а також зловживання обчислювальними ресурсами для проведення атак (DDoS, brute force, «cryptojacking» тощо).

До цієї групи належать також ризики, пов'язані з неправильним управлінням ресурсами, помилками у налаштуванні систем балансування навантаження, механізмів авто-масштабування, резервного копіювання та реплікації. Неправильні параметри масштабування можуть призвести як до відмови сервісу, так і до неконтрольованого споживання ресурсів та витрат. ENISA виокремлює сценарії, пов'язані з виснаженням ресурсів, відмовою сервісів та збоями в ланцюгу постачання [4].

Суттєвою групою є ризики управління доступом до панелей адміністрування хмарної платформи, API та інтерфейсів управління. Компрометація цих інтерфейсів (наприклад, через фішинг, повторне використання паролів, відсутність багатофакторної автентифікації) дозволяє зловмиснику змінювати конфігурацію мережі, створювати нові ресурси, отримувати доступ до сховищ даних та журналів. Стандарти NIST та ISO/IEC 27017 наголошують на необхідності чітких політик керування доступом і сегментації адміністративних повноважень між провайдером і клієнтом [2].

4. Ризики безпеки даних та приватності

Ризики безпеки даних у хмарних сервісах пов'язані з конфіденційністю, цілісністю, доступністю та приватністю персональних даних. До них належать: несанкціонований доступ до даних через вразливості застосунків або інтерфейсів,

втрата чи пошкодження даних через помилки реплікації або резервного копіювання, витік даних унаслідок неправильно налаштованих сховищ (наприклад, публічні S3-бакети чи відкриті об'єктні сховища), недостатнє або некоректне шифрування даних «на спокої» та «в транзиті».

Окрему підгрупу становлять ризики приватності та захисту персональних даних, що регулюються стандартами ISO/IEC 27018 та національним/наднаціональним законодавством. До них відносять: незаконну обробку персональних даних, передачу даних у треті країни без належних гарантій, відсутність механізмів реалізації прав суб'єктів даних (право на забуття, переносимість тощо), а також недостатній контроль субобробників провайдера.

Класифікуючи ризики безпеки даних, доцільно розрізняти:

- ризики, пов'язані з конфігурацією (misconfiguration: відкриті сховища, надлишкові права доступу, відсутність шифрування);
- ризики, пов'язані з обробкою та зберіганням (неналежне резервування, недостовірне відновлення, незахищені журнали);
- ризики, пов'язані з життєвим циклом даних (неналежне видалення, повторне використання носіїв, неконтрольований доступ до «сміттєвих» копій).

Такий поділ дозволяє цілеспрямовано підбирати контролі: шифрування, токенізацію, DLP, контроль життєвого циклу даних, аудит доступу, а також вимоги до знищення і повернення даних після завершення контракту [2].

5. Ризики, пов'язані з відповідністю, аудитом і спільною відповідальністю

Хмарна безпека реалізується в рамках моделі спільної відповідальності, де частина контролів належить провайдеру, а частина – клієнту. Неправильне розуміння цієї моделі формує окрему категорію ризиків: організація вважає, що за безпеку повністю відповідає провайдер, і недооцінює власні завдання щодо налаштування сервісів, керування доступом, шифрування, моніторингу та реагування. ISO/IEC 27017 прямо орієнтований на уточнення розподілу повноважень та контролів між сторонами.

Ризики комплаєнсу та аудиту пов'язані з відсутністю або недостатністю доказової бази (логів, звітів, сертифікатів) для підтвердження відповідності регуляторним вимогам і внутрішнім політикам. Якщо провайдер не надає прозорих і стандартизованих механізмів аудиту (регулярні звіти, атестації за ISO/IEC 27001, 27017, SOC 2 тощо), це ускладнює управління ризиками та може призвести до санкцій з боку регуляторів або партнерів.

6. Ризики появи нових типів загроз та еволюції атак

Динамічний характер хмарних середовищ обумовлює появу нових класів загроз, у тому числі тих, що використовують специфічні можливості хмарної інфраструктури:

- «Cybercrime as a Service», коли хмарні ресурси використовуються як платформа для розгортання ботнетів, сервісів DDoS за запитом, ферм для майнінгу криптовалют;
- атаки на метадані і контрольні площини, спрямовані на отримання повного контролю над тенантським середовищем;

- атаки на ланцюги CI/CD та DevOps-процеси, характерні для хмарних застосунків (контейнерні образи, інфраструктура як код);
- зловживання API, які відкривають доступ до управління ресурсами та даними [5].

Такі ризики важко повністю описати в рамках статичних класифікацій, тому сучасні підходи рекомендують поєднувати базову таксономію ризиків із моделями загроз, що постійно оновлюються. Це дозволяє враховувати появу нових векторів атак без повного перегляду структури класифікації.

Висновки. Класифікація кіберризиків у хмарних сервісах є важливою передумовою ефективної методики їх оцінки. Багатовимірний підхід (за рівнем, доменом, сервісною моделлю, життєвим циклом даних) дозволяє пов'язати конкретні ризики з відповідними контролями, відповідальністю сторін та нормативними вимогами.

Безпека даних і приватність у хмарі вимагають окремої, деталізованої класифікації ризиків. Поділ на ризики конфігурації, обробки, зберігання та життєвого циклу даних дозволяє точніше обирати засоби захисту.

Еволюція хмарних технологій породжує нові типи загроз, що доповнюють традиційні категорії ризиків. Практичне застосування запропонованих класифікацій створює основу для побудови формалізованих методик оцінки кіберризиків у хмарних сервісах, що, у свою чергу, дозволяє обґрунтовано обирати архітектурні рішення, моделі розгортання, інструменти моніторингу та реагування, а також оптимізувати витрати на забезпечення кібербезпеки в умовах зростаючої залежності від хмарних технологій.

Перелік використаних джерел.

1. Cloud Computing Risk Assessment. [Електронний ресурс].- Режим доступу: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

2. Jansen, W. A., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. . [Електронний ресурс].- Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

3. Cloud computing: benefits, risks and recommendations for information security. [Електронний ресурс].- Режим доступу: https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%20-%20Cloud%20Computing%20-%20final.pdf

4. Cayirci, E., Garaga, A., Santana de Oliveira, A., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. Journal of Cloud Computing, 5 (1), 14.

5. Marinos, L. (2016). ENISA Threat Taxonomy: A tool for structuring threat information. ENISA,Heraklion. [Електронний ресурс].- Режим доступу: https://www.um.es/documents/2096502/4937674/Enisa.pdf/2374a6a9-3c9d-422c-b5ad-b047a2fb8568

УДК 004.056

Володимир ПРАЦІНЬ, Ігор ПІТУХ

Західноукраїнський національний університет

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ КОМПЛЕКСОМ ЗБЕРІГАННЯ НАФТОПРОДУКТІВ

Вступ. Резервуарні парки нафтопродуктів (РПН) є критичними об’єктами інфраструктури нафтобаз, терміналів та промислових підприємств, що забезпечують приймання, зберігання, перекачування та відвантаження палива. Високі вимоги до безпеки, екологічної надійності та точності контролю параметрів обумовлюють необхідність упровадження сучасних автоматизованих систем управління (АСУ) [1, 2]. Особливого значення набувають системи, здатні забезпечувати точний контроль параметрів технологічного процесу (ТП), а також реалізувати протиаварійний захист (ПАЗ) та дистанційне керування виконавчими механізмами.

Мета дослідження полягає у дослідження технологічні процеси резервуарного парку як об’єкта автоматизації та розробці АСУ РПН.

1. Дослідження систем автоматизації резервуарного комплексу

Комплекси зберігання нафтопродуктів (резервуарні парки, резервуарне господарство нафтобаз) відіграють ключову роль у логістичних ланцюгах паливно-енергетичного сектору. Резервуарний комплекс включає групу вертикальних або горизонтальних резервуарів, систему обв’язки трубопроводами, насосні станції, вузли налива/зливу, засоби пожежогасіння та газовідведення, а також контрольно-вимірювальні прилади (КВП) (рисунок 1) [3].

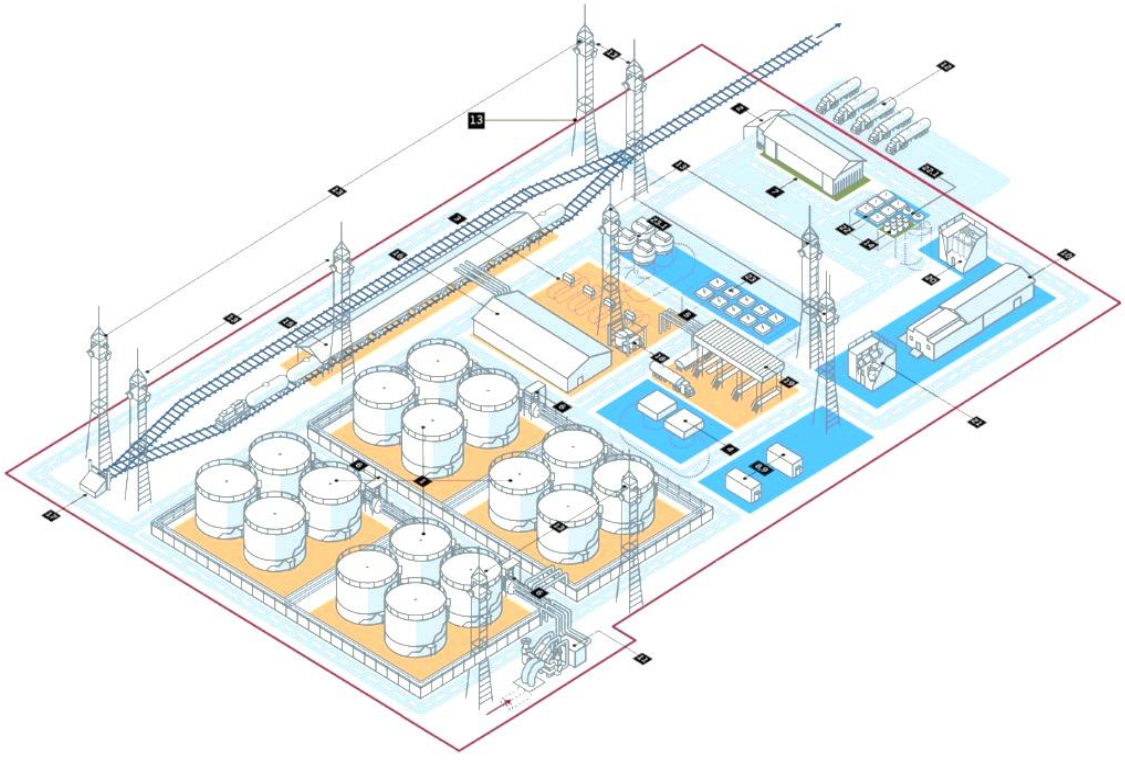


Рисунок 1 – Структура резервуарного комплексу

В результаті проведеного дослідження ТП РПН визначено основні етапи, зокрема:

- приймання нафтопродуктів (залізничний або автомобільний транспорт);
- перекачування та фільтрацію продукту;
- заповнення резервуарів із контролем рівня та тиску;
- зберігання з урахуванням температурних режимів і газової подушки;
- відвантаження палива через вузли обліку;
- протиаварійні заходи при переливі, розгерметизації, перевищенні тиску, температури, витрат.

На кожному із етапів АСУ реалізують контроль та керування основних технологічних параметрів [4]: рівень рідини в резервуарах; температура нафтопродукту та стінок резервуара; надлишковий тиск у газовому просторі; рівень води; витрати під час налива/зливу; стан запірно-регулюючої арматури; параметри пожежної безпеки.

На рисунку 2 наведено приклад реалізації АСУ резервуарним господарством.

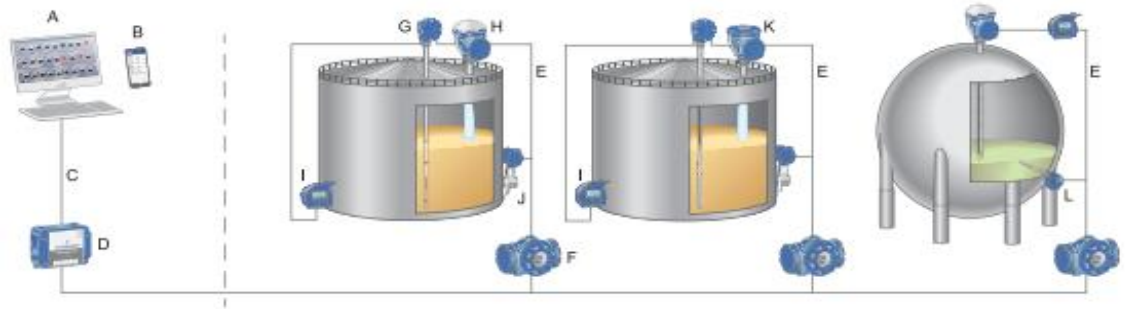


Рисунок 2 – Структура АСУ

Проведений аналіз промислових рішень показав, що більшість АСУ працює за принципом модульної побудови та базується на поєднанні вимірювальних датчиків, мікропроцесорних контролерів, комунікаційних шлюзів та SCADA-систем. Актуальним є застосування технологій IoT, які забезпечують безперервний збір даних від датчиків рівня, тиску, температури та газоаналізу, віддалений моніторинг стану резервуарів і трубопроводів, а також оперативний аналіз даних у реальному часі. Використання IoT-рішень підвищує швидкість реагування на відхилення, забезпечує прозорість технологічних операцій і сприяє підвищенню загальної безпеки РПН. Основні вимоги до сучасної АСУ РПН визначаються такими критеріями:

- точність вимірювання та обліку технологічних параметрів;
- надійність та відмовостійкість роботи в агресивних умовах;
- оперативність протиаварійного реагування;
- масштабованість та можливість нарощування кількості резервуарів;
- інтеграція з корпоративними інформаційними системами;
- захист інформаційних потоків згідно вимог кібербезпеки;
- мінімізація експлуатаційних ризиків під час налива/зливу.

2. Проектування архітектури автоматизованої системи управління

Архітектура АСУ РПН (рисунок 3) побудована за багаторівневим принципом, що забезпечує модульність, масштабованість, відмовостійкість та можливість інтеграції з корпоративними інформаційними системами підприємства. Система включає

наступні основні рівні:

- низовий рівень датчиків (рівень, тиск, температура, витрата) та виконавчих механізмів (кульові клапани, засувки, насоси, ПЧ);
- рівень контролю та керування;
- верхній диспетчерський рівень управління та SCADA;
- канали взаємодії через Profinet/Profibus/Modbus.

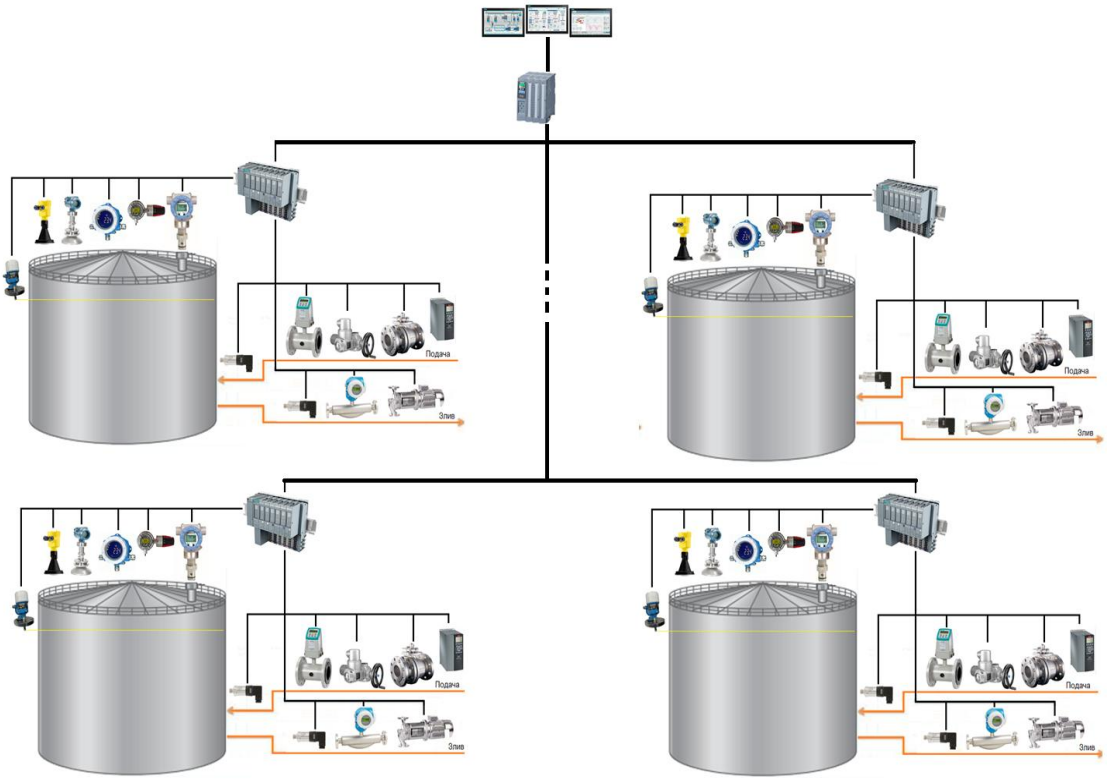


Рисунок 3 - Архітектура проектованої АСУ

Низовий рівень є основою АСУ, оскільки забезпечує безпосередній збір інформації про стан ТП зберігання нафтопродуктів та реалізацію команд керування. Основні функції рівня включають:

- вимірювання рівня нафтопродукту (радарні, гідростатичні рівнеміри);
- контроль температури продукту та резервуара (термопари, Pt100);
- вимірювання тиску у газовому просторі резервуара;
- виявлення водяної подушки;
- вимірювання витрат під час налива/зливу;
- керування насосами (пуск, зупинка, аварійні режими);
- керування запірно-регулюючою арматурою;
- збір даних систем пожежогасіння (датчики диму, полум'я, температури);
- виконання аварійних блокувань (запобігання переповненню, перевищенню тиску).

Рівень контролю та керування забезпечує локальне управління ТП, обробку сигналів та реалізацію алгоритмів контролю. Основними функціями, що реалізуються на даному рівні є:

- оцифрування та фільтрація даних, отриманих від датчиків;

- локальні алгоритми регулювання;
- моніторинг роботи контурів автоматизації;
- забезпечення роботи протиаварійного захисту;
- керування насосним обладнанням за заданими алгоритмами;
- взаємодія між резервуарами під час перерозподілу потоків;
- збір, архівація та передавання даних на верхній рівень;
- резервування каналів зв'язку та автономність роботи у разі втрати зв'язку зі SCADA.

Верхній рівень забезпечує загальне управління, моніторинг, аналітику та інтеграцію з інформаційними системами підприємства. Функції SCADA-рівня перебдвачають візуалізацію ТП, архівування параметрів, трендів та графіків, облік операцій налива/зливу, формування журналів подій, дистанційне керування обладнанням, планування режимів роботи насосних станцій, а також контроль відповідності технологічних параметрів нормативам.

У межах архітектури виділено також мережевий рівень, який забезпечує надійну передачу даних між компонентами АСУ.

Для реалізації АСУ проаналізовано та обґрунтовано вибір комплексу технічних засобів автоматизації (ТЗА) та ПЗА, що наведений в таблиці 1. Критеріями вибору виступали точність, стійкість до корозійного середовища, вибухозахищене виконання, сумісність з протоколами промислового зв'язку та відповідність стандартам.

Таблиця 1 - Перелік технічних засобів автоматизації

Вимірювання рівня у резервуарах	Діапазон вимірювання: до 30 м. Похибка: ±2 мм. Вибухозахист: ATEX, IECEx
Вимірювання температури	Діапазон: –50…+200 °C. Вибухозахист: ATEX Ex ia
Вимірювання тиску	Діапазон: від 0–0,1 бар до 0–400 бар. Похибка: 0.065%. Стійкість до вібрацій: 10 g
Вимірювання витрати	Похибка: ±0.4%. Температура продукту: –10…+150 °C
Електроприводна засувка	Крутний момент: 10–1000 Н·м. Інтерфейси: Profibus DP, Modbus RTU. Температура: –25…+70 °C
Кульовий клапан	DN: 25–300. Допустимий тиск: до 40 бар
Насос відцентровий	Продуктивність: 5–1400 м³/год. Напір: до 160 м. Температура продукту: до 200 °C.
Частотний перетворювач	Потужність: 0.75–560 кВт. Інтерфейси: Profibus, Profinet, Modbus. Функції: PID-регулятор, плавний пуск
Датчик загазованості	Тип газу: бензинові пари (VOC), CH_4, H_2S. Похибка: < ±2%.Вибухозахист: ATEX Ex d
Сигналізатор переливу	Тип: вібраційний рівневий сигналізатор. Вибухозахист: ATEX, SIL2
Модульний контролер	Пам'ять: 250 кБ – 1,5 МБ RAM. Комунікації: Profinet, Profibus, Modbus TCP. Ступінь захисту: IP20. Температура: –20…+60 °C
Модуль I/O	Інтерфейси: Profinet. Модулі: DI, DO, AI, AO. Ступінь захисту: IP20 / IP65

3. Аналіз ефективності проектованої системи

З метою оцінки ефективності проектованої АСУ проведено моделювання аварійних режимів її роботи, що включало аналіз таких ситуацій:

- відмова датчика рівня;
- перевищення тиску газової подушки (заклинювання засувки);
- відсутність зв'язку з контролером;
- переповнення резервуара (збільшення притоку).

Реакція системи у кожному сценарії (рисунок 4) відповідає алгоритмам ПАЗ, зокрема закриття клапана, вимкнення насоса, переведення системи у безпечний стан, формування аварійних сигналів.

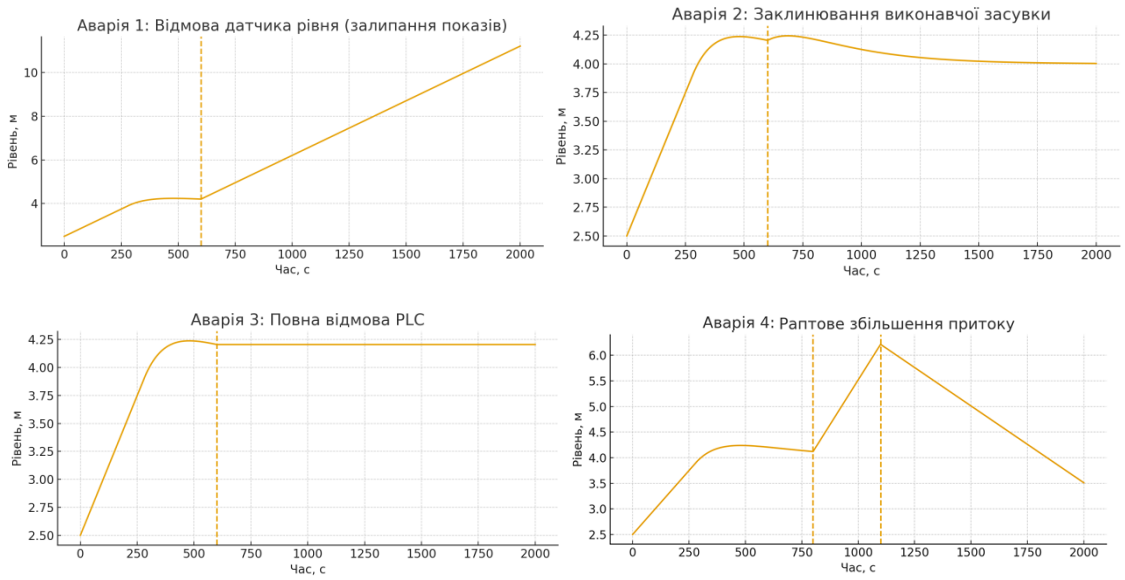


Рисунок 4 - Моделювання аварійних режимів роботи АСУ

Виконано структурно-логічне моделювання відмов, що дозволило визначити ключові фактори ризику та оцінити загальну надійність системи автоматизації.

Висновок. Результати дослідження підтвердили ефективність запропонованої АСУ. Система забезпечує безпечне керування технологічними процесами, автоматичний захист від аварійних ситуацій, точний контроль параметрів та можливість масштабування та інтеграції з мережами підприємства.

Перелік використаних джерел.

1. Григоров А.Б. Зберігання нафти та нафтопродуктів в умовах нафтобаз. – Харків-Тернопіль: НТУ «ХПІ», Видавництво «Крок», 2022. – 184 с.

2. UA-Systems – АС «КМ Парк». [Електронний ресур].- Режим доступу: https://www.ua-systems.com.ua/avtomatizaciya-parkiv-zberigannya-p

3. Бугай Ю.М., Глоба В.М., Нагорний В.П., Венгерцев Ю.О. Спорудження нафтобаз і газонафтосховищ: Підручник для студентів вищих навчальних закладів. – К..: "ВІПОЛ", 2000, - 606

4. Основні вимоги до резервуарів для зберігання пального та нафтопродуктів. . [Електронний ресур].- Режим доступу: https://petroline.ua/osnovni-vymogy-do-rezervuariv-dlia-palnogo/

УДК 681.51

Якименко Н., Слободян В., Якименко Ю., Хомяк Р.

Західноукраїнський національний університет

МЕТОД КІЛЬКІСНОЇ ОЦІНКИ КІБЕРРИЗИКІВ НА ОСНОВІ ДОСТОВІРНИХ СТАТИСТИЧНИХ ІМОВІРНІСНИХ МОДЕЛЕЙ

Вступ. Кількісна оцінка кіберризиків залишається однією з найбільш складних і актуальних проблем сучасних організацій [1]. Незважаючи на зростання обізнаності щодо загроз інформаційній безпеці, керівники служб інформаційної безпеки (CISO) часто стикаються з труднощами у визначенні пріоритетних напрямів захисту. Зокрема, виникають сумніви щодо того, які ризики становлять більшу небезпеку - фізичні інциденти, пов'язані з втратою пристроїв, чи соціоінженерні атаки.

Сучасний ринок пропонує широкий спектр рішень для забезпечення кібербезпеки, однак постачальники цих рішень рідко надають кількісні оцінки впливу своїх технологій на загальний рівень ризику організації [2].

Унаслідок цього спостерігається тенденція до неефективного розподілу ресурсів та здійснення інвестицій у безпеку без належного обґрунтування. Типовим прикладом є ситуація, коли аналітики з безпеки переоцінюють внутрішні загрози (зловмисні дії інсайдерів), тоді як фактичні дані свідчать про значно більшу частоту зовнішніх атак, наприклад, на веб-сайти та веб-додатки.

Аналіз інцидентів упродовж п'ятирічного періоду в окремих організаціях показав, що реальні ризики, пов'язані з кібератаками на вебресурси (зокрема SQL-ін'єкції, дефейси тощо), значно перевищують загрозу від інсайдерських дій, хоча інтуїтивно може здаватися навпаки.

Відсутність достовірних методів кількісного вимірювання ефективності заходів кібербезпеки ускладнює прийняття стратегічних рішень щодо оптимізації витрат і розподілу бюджету. Інвестиції у шифрування даних, навчання персоналу з протидії фішингу або модернізацію мережевого обладнання часто здійснюються без порівняльної оцінки потенційного зниження ризику. Це призводить до низької ефективності витрат і нераціонального використання обмежених ресурсів.

Мета: розробка методу кількісного оцінювання кіберризиків на основі достовірних статистичних імовірнісних моделей.

1 Концептуальні основи моделювання кіберризиків на основі даних про інциденти

Кіберризик складається з поширених інцидентів з невеликим впливом у поєднанні з рідшими інцидентами, що мають більший вплив. Необхідно оцінити всю криву ризику, щоб особи, які приймають рішення, могли зрозуміти обидва типи ризику: історичні інциденти, які вже трапилися, а також нові сценарії, які, можливо, ще не траплялися. Оцінка цих двох типів інцидентів може вимагати різних методів моделювання [3].

У випадку кібербезпеки аналітики можуть використовувати експертні думки або моделі сценаріїв, які ще не відбулися, щоб отримати більш повну оцінку всієї кривої

ризику. Використовуючи цю структуру, кіберризик можна моделювати в трьох режимах (рисунок 1):

- модель на основі даних: базується на історичних подіях, якщо дані існують і є стабільними у часі;
- модель на основі сценаріїв: використовується для моделювання інцидентів, які ще не відбулися (зазвичай інциденти з великим впливом);
- режим перекриття: поєднує модель на основі даних та модель на основі сценаріїв шляхом перекриття кривих ризику, щоб уникнути подвійного підрахунку інцидентів.

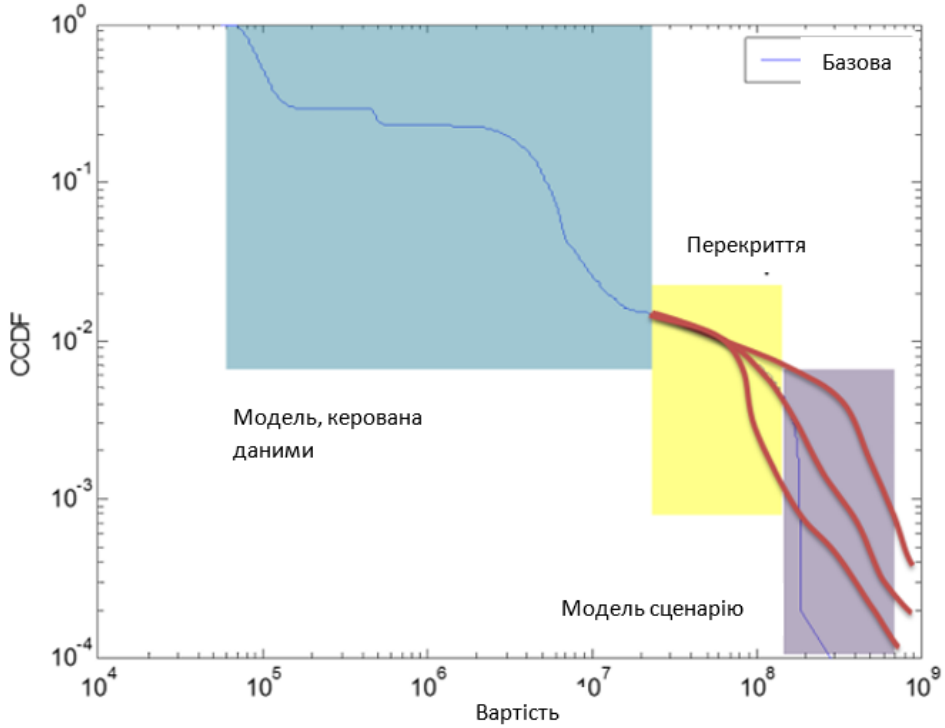


Рисунок 1 – Три режими кривої ризику: модель на основі даних, модель на основі сценаріїв та режим перекриття

Після об’єднання цих трьох режимів особа, яка приймає рішення, отримує повну характеристику кіберризику, з яким стикається організація.

2 Оцінка ризиків за допомогою моделювання методом Монте-Карло

Після моделювання розподілу різних типів атак, їх частоти та впливу, криву ризику на основі даних можна обчислити за допомогою моделювання методом Монте-Карло. Крім того, розподіл вхідних даних може базуватися на історичних даних (у випадку режиму на основі даних) або сценаріях (у випадку більш масштабних інцидентів).

Тому інциденти, що моделюються, могли відбутися в минулому, але також можуть бути новими сценаріями, які ще не спостерігалися. Іншими словами, модель Монте-Карло узагальнюється в метод моделювання навіть для інцидентів, які ще не відбулися.

Інциденти моделюються із заданою частотою, і кожен інцидент має відповідний вплив, взятий з розподілу. Вартість кожного інциденту розраховується в доларах.

Модель моделює один рік кіберінцидентів, хоча це можна легко змінити. Наприкінці моделювання всі витрати підсумовуються, щоб отримати загальні річні витрати. На основі великої кількості прогонів (n=10 000) розраховується доповнювальна кумулятивна функція розподілу.

Більш формально визначено наступні терміни для використання в моделюванні (таблиця 1).

Таблиця 1 – Терми для використання в моделюванні кіберризиків

Символ	Значення
C	Вартість
I	Позначення інциденту
J	Позначення типу інциденту (веб-сайт, ел. пошта, шкідливе ПЗ, тощо)
H	Години
V	Ф-ції індикатора
P_i	Ймовірність втрати для інциденту типу i
DC_i	Прямі витрати для інциденту типу i
PI_i	Втрата конфіденційної і-ції для інциденту типу i
RD_i	Втрата репутації для інциденту типу i
IP_i	Втрата інтелектуальної власності для інциденту типу i
BI_i	Втрати від переривання бізнесу для інциденту типу i

Загальна вартість кіберінцидентів в організації за рік – це просто сума вартості кожного інциденту, що стався.

$$\text{Річна вартість} = \sum_i \boldsymbol{C_i}. \quad (1)$$

Загальна вартість кожного інциденту визначається шляхом підсумовування кожної категорії впливу, а саме: витрати на розслідування, прямі витрати, переривання діяльності, шкода репутації, моніторинг кредитоспроможності та втрата інтелектуальної власності.

Припускається, що кожна година розслідування коштує 100 доларів, тому кількість годин, витрачених на розслідування інциденту, множиться на 100. У цій моделі робиться спрощене припущення, що витрати є умовно нерелевантними, враховуючи години розслідування. Можуть виникнути певні ситуації, в яких це припущення не спрацьовує, наприклад, коли втрата інтелектуальної власності збільшує ймовірність шкоди репутації. Загальна вартість визначається:

$$\boldsymbol{C_i = H_i * \$100 + DC_i + BI_i + RD_i + PI_i + IP_i}. \quad (2)$$

Категорії впливу (переривання бізнесу, шкода репутації тощо) можуть залежати від типу j інциденту (електронна пошта, веб-сайт, витік даних тощо). Вартість інциденту i типу j є функцією годин розслідування інциденту i, розподілу впливу, функцій індикаторів та умовних ймовірностей. Наприклад, вартість інциденту і типу «витік даних» можна записати наступним чином:

$$\boldsymbol{C_i = H_i * \$100 + RD_i + PI_i}. \quad (4)$$

В результаті інциденту з витоком даних можуть виникнути лише витрати часу на розслідування, шкода репутації та розкриття конфіденційної інформації. Витрати можна додатково розбити на такі складові:

$$\boldsymbol{C_i = H_i * \$100 + V(H_i) * (RD_i + PI_i)}. \quad (5)$$

$$\boldsymbol{V(H_i) = \begin{cases} 1 \ if \ H_i \geq 500 \\ 0 \ else \end{cases}}. \quad (6)$$

$$\boldsymbol{PI_i = \{Uniform\ (60k\ to\ 5M)\}}. \quad (7)$$

$$\boldsymbol{RD_i = \begin{cases} Uniform\ (1M\ to\ 2M), & \text{з ймовірністю } 0,45 \\ Beta\ Dist\ (100M\ to\ 160), & \text{з ймовірністю } 0,05 \\ 0, & \text{з ймовірністю } 0,5 \end{cases}}. \quad (8)$$

Іншими словами, збитки від шкоди репутації та витрати на інформацію про приватність виникають лише в тому випадку, якщо час розслідування перевищує 500 годин, звідси і походить функція індикатора $V(H_i)$. Якщо це відбувається, з розподілу вибирається випадкова змінна, щоб отримати рівень збитків від інциденту.

Втрати конфіденційної інформації вибираються з рівномірного розподілу, а шкода репутації - з кускового розподілу, що представляє три типи результатів. Після того як вартість кожного інциденту вибрана з розподілів і обчислена, криву ризику можна отримати шляхом багаторазового моделювання та формування кумулятивної функції розподілу або, в даному випадку, додаткової кумулятивної функції розподілу.

На рисунку 2 показано діаграму рішень щодо кібербезпеки в організації та те, як частота, вплив і тип інциденту впливають на загальну вартість.

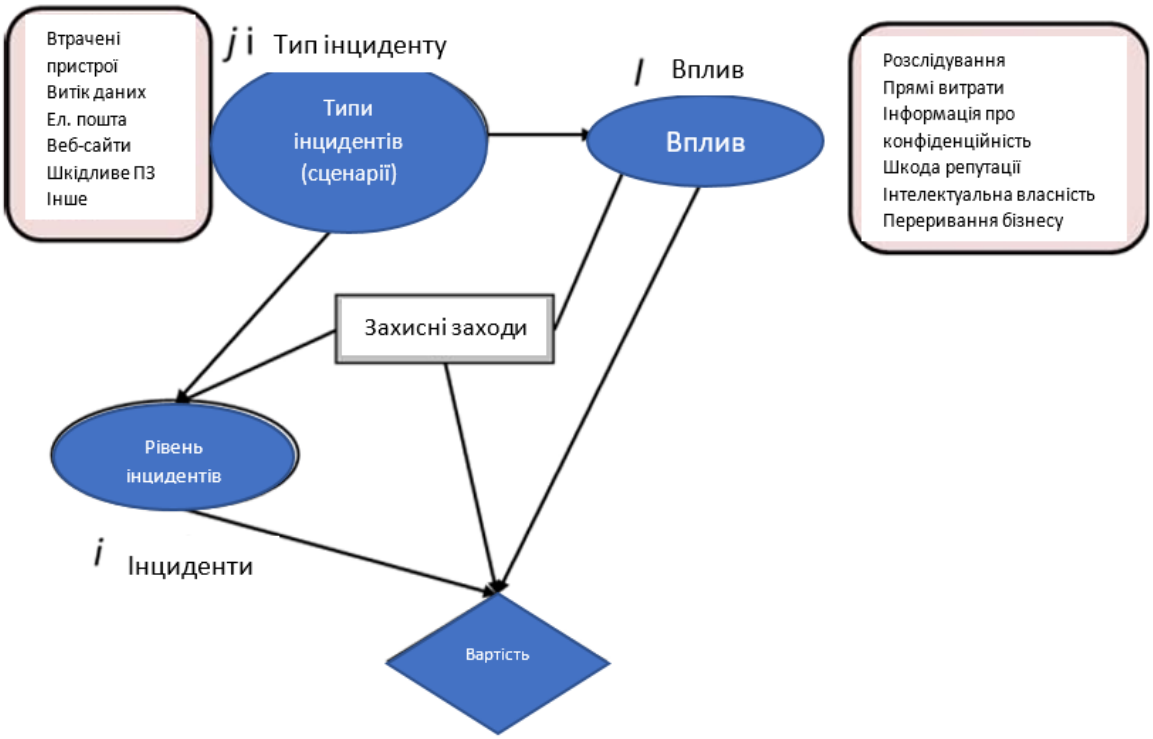


Рисунок 2 – Для розрахунку кривих ризику використовується моделювання методом Монте-Карло

Використання моделі, заснованої на інцидентах, є зручним, оскільки деякі невизначеності стають умовно нерелевантними для вартості, враховуючи інформацію про частоту, тип і вплив атак. Наприклад, аналітики можуть робити висновки про зловмисника, але ці дані не потрібні для розрахунку рентабельності інвестицій у засоби захисту. Для моделювання діаграми прийняття рішень, використовується метод Монте-Карло.

Висновки. У роботі запропоновано метод кількісної оцінки кіберризиків, який ґрунтується на достовірних статистичних та імовірнісних моделях, що забезпечують об'єктивніше та реалістичніше визначення рівня кіберзагроз для організації. Методика поєднує історичні дані про інциденти та сценарне моделювання майбутніх подій, що дозволяє будувати повну криву ризику з урахуванням як частих малозатратних інцидентів, так і рідкісних, але високовартісних атак.

Використання моделювання методом Монте-Карло дає змогу оцінити ймовірний розподіл щорічних збитків, враховуючи частоту, типи інцидентів і всі категорії їх впливу - прямі витрати, втрату конфіденційності, збитки репутації, порушення бізнес-процесів тощо. Такий підхід забезпечує можливість формування кількісних показників ризику, що є необхідними для прийняття обґрунтованих управлінських рішень щодо інвестицій у кібербезпеку.

Запропонована модель сприяє підвищенню ефективності розподілу ресурсів, оскільки дає змогу порівнювати очікуване зниження ризику від різних заходів кіберзахисту. Вона усуває залежність від суб'єктивних експертних оцінок та дозволяє уникнути переоцінки незначних загроз або недооцінки рідкісних, але критичних атак.

Таким чином, представлений метод є важливим інструментом у стратегічному управлінні кіберризиками, забезпечує прозорість і точність оцінювання, а також створює основу для економічно обґрунтованого планування заходів кібербезпеки.

Перелік використаних джерел.

1. Білявська Ю., Білявський В., Шестак Я., та інші. "Моніторинг кіберризиків у фінансовому секторі економіки." Financial and Credit Activity Problems of Theory and Practice, Том 3, № 62, 2025, с. 355–369.

2. Байдур О. Кількісна методологія оцінки ризиків кібербезпеки при відсутності фінансових даних про втрати." Кібербезпека: освіта, наука, техніка, Том 2, № 26, 2024, с. 95–114. https://doi.org/10.28925/2663-4023.2024.26.659

3. Franco, M.F., Mullick, A.R., Jha, S. "QBER: Quantifying Cyber Risks for Strategic Decisions." arXiv, 2024.

УДК 004.9

Підгурський Д.В.

Західноукраїнський національний університет

АНАЛІЗ КОНСТРУКЦІЇ ТА ТИПОВИХ ДЕФЕКТІВ ВІТРОВИХ ТУРБІН

Вступ. Розроблення ефективних систем накопичення енергії на основі водню, що використовують енергію вітру як первинне джерело, має потенціал стати одним із головних складників декарбонізованої енергетики України. Водночас підвищення надійності та ефективності роботи вітроенергетичних установок є необхідною умовою сталого розвитку цієї галузі.

Сучасна вітрова турбіна є складною електромеханічною системою, що перетворює кінетичну енергію вітру на електричну [1]. Її технічний стан безпосередньо впливає на продуктивність і економічні показники виробництва. Тому аналіз конструкції основних вузлів і характерних дефектів турбіни є ключовим етапом розроблення системи діагностики та прогнозування відмов.

Мета: проаналізувати конструкцію вітрової турбіни, визначити основні вузли та типові дефекти, що впливають на ефективність її роботи, а також окреслити напрями подальшої діагностики на основі алгоритмів штучного інтелекту.

1. Конструктивна схема вітрової турбіни

На рисунку 1 наведена конструктивна схема вітрової турбіни [2].

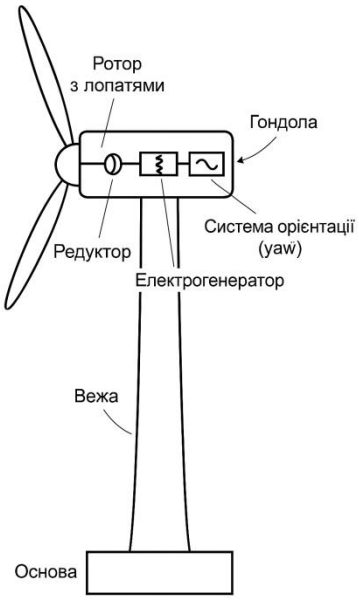


Рисунок 1 – Конструктивна схема вітрової турбіни

Типова горизонтально-осьова турбіна складається з таких основних частин (рисунок 1):

1. Ротор з лопатями. Складається з композитних лопатей, закріплених на маточині. Вони перетворюють кінетичну енергію повітряного потоку на механічну енергію обертання.

2. Головний підшипниковий вузол. Забезпечує передачу крутного моменту від ротора до вала, зменшуючи втрати на тертя. Підшипники є одним із найбільш

навантажених і вразливих елементів.

3. Редуктор. Підвищує частоту обертання вала для узгодження з номінальною швидкістю генератора. Має складну зубчасту структуру, що потребує ретельного мастила та моніторингу стану.

4. Електрогенератор. Перетворює механічну енергію обертання в електричну. Зазвичай використовується асинхронний або синхронний генератор з постійними магнітами.

5. Системи керування кутом атаки (pitch) і орієнтації (yaw). Регулюють напрямок і положення ротора відносно потоку вітру, забезпечуючи стабільну роботу при змінних швидкостях вітру.

6. Вежа та основа. Забезпечують механічну стабільність конструкції, утримуючи гондолу на необхідній висоті.

2. Типові несправності вітрових турбін та їх ознаки

Кожен із зазначених вузлів вітрової турбіни працює в умовах змінних навантажень, вібрацій та температурних коливань, що зумовлює поступове зношення деталей і появу дефектів. З огляду на складність конструкції, навіть незначні відхилення в роботі окремих елементів можуть спричинити суттєве зниження ефективності всієї установки або її аварійне зупинення. Тому систематичний аналіз типових несправностей, їхніх фізичних причин і діагностичних ознак є необхідною передумовою для побудови надійних методів моніторингу та автоматичної класифікації станів вітрових турбін.

Основні типи дефектів та їх характерні ознаки наведено в таблиці 1 [3, 4].

Таблиця 1 - Основні вузли вітрової турбіни, типові дефекти та їх діагностичні ознаки

Вузол / компонент	Типові дефекти	Діагностичні ознаки	Можливі наслідки
Підшипниковий вузол	Знос, піттінг, тріщини, розбалансування	Зростання середньоквадратичного рівня вібрацій (RMS), імпульсні коливання, підвищення температури корпусу	Руйнування вала, зупинка генератора
Редуктор	Знос або поломка зубців, недостатнє мастило, розцентрування валів	Гармоніки на зубчастих частотах, збільшення шуму, перегрів мастила	Втрата крутного моменту, заклинювання передачі
Ротор і лопаті	Тріщини, деламінація, ерозія країв, обмерзання	Нерівномірні навантаження, збільшення рівня шуму, зміна швидкості обертання	Дисбаланс, падіння аеродинамічної ефективності

Генератор	Знос підшипників, пошкодження ізоляції, перегрів обмоток	Підвищена температура, вібрації на кратних частотах обертання, зміна струму	Вихід генератора з ладу, електричні втрати
Система керування pitch/yaw	Відмова приводів, збій датчиків, неточне позиціювання	Нестабільність швидкості обертання, відхилення кута атаки, вібрації в гондолі	Зниження ефективності, підвищене навантаження на лопаті
Вежа та основа	Металеві тріщини, ослаблення болтів, корозія	Поступове збільшення амплітуди вібрацій, нахил конструкції, акустичні шуми	Порушення стабільності, ризик аварії

Найчастіше дефекти виникають у підшипникових вузлах, редукторі, лопатях ротора та системах керування [5]. Їх своєчасне виявлення потребує комплексного підходу до моніторингу стану обладнання із застосуванням вібраційних, акустичних і температурних показників.

Висновок. Отримані висновки створюють основу для подальшої розробки методів автоматичної діагностики та класифікації дефектів вітрових турбін із використанням алгоритмів штучного інтелекту, зокрема нейромережевого підходу Ванга–Менделя.

Перелік використаних джерел.

1. Вітроенергетика / За заг. ред. С. О. Кудрі. – Київ: Інститут відновлюваної енергетики НАНУ, 2023. – 135 с.

Беднаровський А. С. Проектування мікромережі постійного струму малопотужної вітрової турбіни для живлення побутових споживачів: кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю „141 – електроенергетика, електротехніка та електромеханіка“ / А. С. Беднаровський. – Тернопіль: ТНТУ, 2023. – 89 с.

Дубчак, Л. О. Аналіз дефектів лопатей вітрових турбін засобами нейро-нечіткої системи. Scientific Bulletin of UNFU, 2025. 35(3), С. 108-113. https://doi.org/10.36930/40350311.

Баліцький О. І. Кіберфізична системи динамічного збору візуальних даних про дефекти об’єктів вітрової енергетики з використанням БПЛА : кваліфікаційна робота бакалавра : 123 Комп’ютерна інженерія / О. І. Баліцький ; Хмельниц. нац. ун-т. – Хмельницький, 2025. – 87 с.

Горлачук М. А. Розробка рекомендацій для попередження пошкодження вітрових турбін : робота на здобуття кваліфікаційного ступеня магістра : спец. 141 – електроенергетика, електротехніка та електромеханіка / наук. кер. В. П. Коваль. Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. 72 с.

УДК 004.056.5

Руслан ПАВЛЮК, Степан ІВАСЬЄВ

Західноукраїнський національний університет

АЛГОРИТМ ЗАСТОСУВАННЯ NMAP ДЛЯ ПОШУКУ ВРАЗЛИВОСТЕЙ МЕРЕЖЕВИХ РЕСУРСІВ

Вступ. У цифровому ландшафті проактивна ідентифікація та управління вразливостями є фундаментальною умовою для забезпечення кіберстійкості організацій. Серед безлічі доступних інструментів, Nmap (Network Mapper) зберігає статус де-факто індустріального стандарту для розвідки ережі та аудиту безпеки.

Проблематика даного дослідження полягає в тому, що "хаотичне" або несистематичне використання Nmap є неефективним. Запуск сканування за замовчуванням на великих мережевих сегментах генерує надлишковий "шум", який важко аналізувати , та, що більш важливо, вкрай легко виявляється і блокується сучасними системами виявлення та запобігання вторгненням (IDS/IPS). Таке блокування призводить до отримання хибно-негативних результатів (false negatives), коли аудитор вважає порт закритим, хоча насправді він просто фільтрується.

Це зумовлює гостру необхідність у розробці формалізованого алгоритму. Такий алгоритм повинен представляти собою систематичну методологію, що поєднує найефективніші техніки сканування, автоматизований аналіз вразливостей за допомогою скриптового рушія Nmap (NSE) та, за необхідності, адаптивні методи ухилення від виявлення.

Мета. Розробка та наукове обґрунтування комплексного алгоритму застосування Nmap для автоматизованого пошуку, ідентифікації та пріоритезації вразливостей мережевих ресурсів. Для досягнення поставленої мети необхідно вирішити наступні завдання дослідження:

- Проаналізувати фундаментальні механізми сканувань на базі протоколів TCP та UDP, їхні переваги, недоліки та вплив на точність результатів.
- Дослідити архітектуру та функціональні можливості Nmap Scripting Engine (NSE) як ключового інструменту для здійснення переходу від сканування портів до повноцінного виявлення вразливостей.
- Розробити практичний програмний модуль з використанням мови програмування Python, що реалізує запропонований алгоритм, з фокусом на автоматизації процесів сканування та структурованому управлінні отриманими даними.
- Систематизувати основні методи виявлення сканувань Nmap системами IDS/IPS та проаналізувати ефективність відповідних технік протидії та ухилення.

1. Аналіз методів та розробка алгоритму сканування

Основою роботи Nmap є концепція сканування "портів" - програмних абстракцій для ідентифікації сервісів - з використанням транспортних протоколів TCP

та UDP. Ефективність алгоритму критично залежить від правильного вибору методу сканування для кожного з протоколів [1].

У контексті протоколу TCP, який забезпечує надійну доставку даних, Nmap пропонує декілька підходів. Найбільш простим є метод TCP Connect Scan (-sT), що базується на встановленні повного з'єднання через процедуру "трьохстороннього рукостискання" (SYN, SYN/ACK, ACK).

Хоча цей метод не вимагає привілеїв адміністратора, він має суттєвий недолік - високий рівень "шуму". Цільова система гарантовано фіксує та логує факт встановлення з'єднання, що демаскує дії аудитора. Тому стандартом де-факто для професійного аудиту є метод TCP SYN Scan (-sS), також відомий як "напіввідкрите" сканування.

При його використанні Nmap надсилає пакет SYN, і отримавши відповідь SYN/ACK (що свідчить про відкритий порт), не завершує з'єднання, а надсилає пакет RST (Reset). Це робить сканування значно швидшим та менш помітним для засобів логування на рівні додатків.

На рисунку 1 представлено узагальнену блок-схему розробленого алгоритму, що візуалізує логіку прийняття рішень під час сканування.

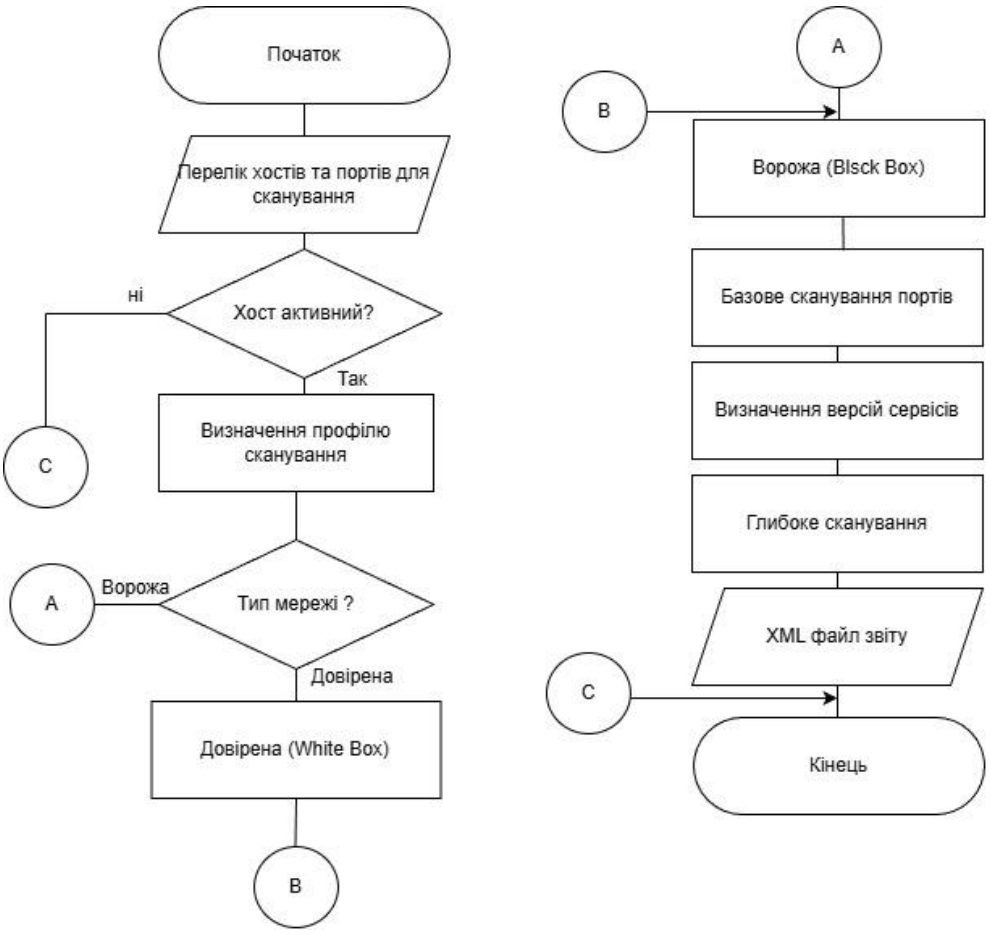


Рисунок 1 –Схема алгоритму автоматизованого пошуку вразливостей

Сканування протоколу UDP (-sU) представляє значно більшу складність, проте його ігнорування є критичною помилкою, оскільки важливі інфраструктурні сервіси (DNS, SNMP, DHCP) працюють саме на цьому транспортному рівні.

Основною проблемою UDP-сканування є низька швидкість та неоднозначність результатів. Більшість операційних систем, зокрема Linux, обмежують частоту відправки ICMP-повідомлень про помилки (Destination Unreachable), що змушує Nmap штучно сповільнювати процес сканування. Крім того, відсутність відповіді на UDP-пакет може трактуватися двояко: або порт відкритий, або пакет був відкинутий брандмауером (стан open|filtered) [2].

Для вирішення цієї проблеми розроблений алгоритм передбачає обов'язкове поєднання UDP-сканування з опцією визначення версій (-sV), що дозволяє верифікувати відкритість порту через аналіз відповіді на специфічний для протоколу запит. Ключовим етапом запропонованого алгоритму є перехід від виявлення портів до аналізу вразливостей. Цю функцію виконує Nmap Scripting Engine (NSE) - підсистема, що дозволяє виконувати скрипти мовою Lua. Хоча стандартна категорія скриптів vuln дозволяє виявляти відомі вразливості, цей підхід є статичним і обмеженим наявною базою скриптів.

Тому в роботі пропонується використання динамічного підходу на базі скрипту vulners. Алгоритм передбачає наступний ланцюжок дій: Nmap визначає точну версію сервісу (наприклад, "Apache 2.4.49"), після чого скрипт vulners звертається до зовнішньої бази даних через API та повертає список актуальних CVE (Common Vulnerabilities and Exposures) з оцінками критичності CVSS [3].

2. IPS програмна реалізація та протидія IDS/IPS

Практична реалізація алгоритму виконана у вигляді програмного модуля мовою Python. Вибір мови обумовлений наявністю потужних бібліотек для роботи з мережею та даними. Ключовим компонентом розробки є використання бібліотеки python-nmap, яка виступає програмною обгорткою над бінарним файлом Nmap [4].

Критично важливим аспектом автоматизації є управління даними. Nmap підтримує декілька форматів виводу, однак для програмної обробки єдиним прийнятним форматом є XML (-oX) [5].

На відміну від застарілого формату Grepable (-oG) або текстового виводу, XML забезпечує повну структурованість даних, включаючи складні вкладені структури, такі як результати виконання NSE-скриптів.

Розроблений програмний модуль виконує три ключові функції. По-перше, це оркестрація сканування, що включає формування командного рядка Nmap відповідно до обраного профілю (швидкий аудит або поглиблений пентест) та запуск процесу. По-друге, це парсинг результатів, де модуль автоматично зчитує згенерований XML-файл, перетворюючи його на об'єктну модель Python. По-третє, це збереження даних у реляційну базу даних SQLite [6].

Використання бази даних дозволяє перетворити результати одноразових сканувань на історичну базу знань, уможливлюючи виконання аналітичних запитів (наприклад, пошук нових відкритих портів у динаміці).

Логіка обробки та збереження даних, реалізована в програмному модулі, є критично важливою для перетворення "сирого" виводу Nmap у корисну інформацію.

На рисунку 2 наведено блок-схему, що деталізує алгоритм парсингу та збереження результатів сканування.

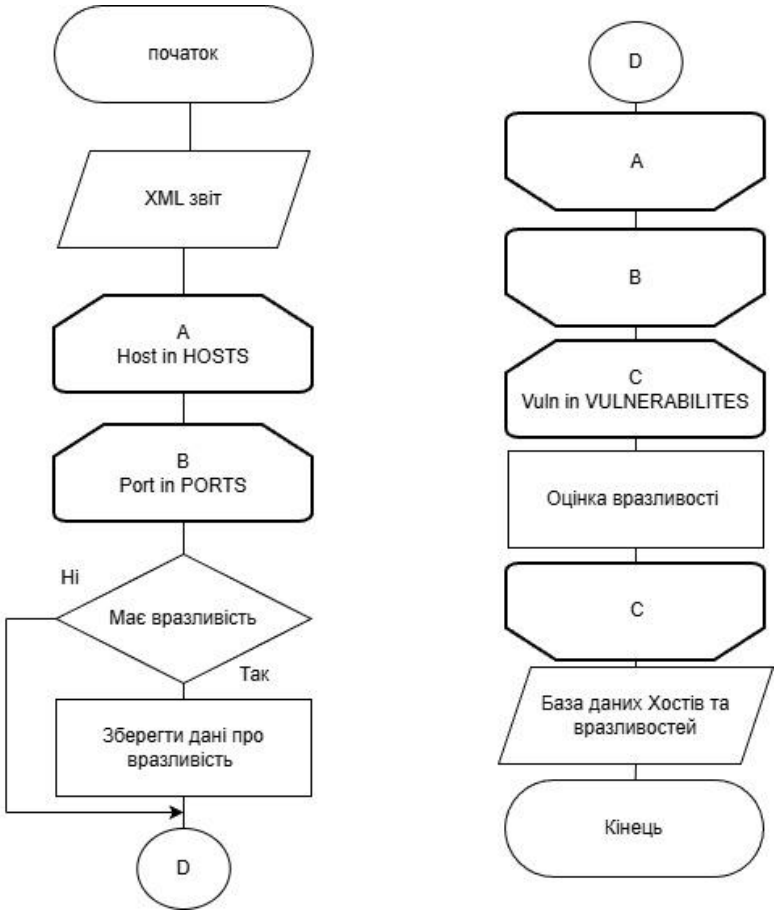


Рисунок 2 – Схема алгоритм парсингу та збереження даних сканування (деталізація)

Згідно з наведеною схемою, процес обробки є ієрархічним:

- на верхньому рівні відбувається ітерація по хостах, де зберігаються загальні метадані. Далі, для кожного відкритого порту фіксуються параметри сервісу.
- на найнижчому рівні, якщо скрипт NSE виявив вразливості, система розбирає їх список та створює записи в таблиці вразливостей, прив'язані до конкретного порту та хоста.

Така структура бази даних (Host -> Port -> Vulnerability) забезпечує нормалізацію даних та ефективний пошук.

3. Протидія системам виявлення вторгнень

Ефективність сканування у реальних умовах часто обмежується діяльністю систем IDS/IPS. Сучасні системи захисту використовують два основні методи виявлення сканувань: сигнатурний та поведінковий.

Для забезпечення успішного виконання алгоритму в "ворожому" середовищі було систематизовано та інтегровано методи ухилення (evasion techniques) [7].

Першим методом є фрагментація пакетів (-f), яка полягає у розділенні заголовка TCP на декілька дрібних IP-фрагментів. Це ускладнює роботу простих пакетних фільтрів та IDS, які не виконують повну дефрагментацію потоку перед аналізом, дозволяючи скануючим пакетам проходити непоміченими.

Другим методом є використання "приманок" (Decoys, -D). Ця техніка дозволяє

приховати реальну IP-адресу сканера серед множини підроблених адрес. Наприклад, команда nmap -D RND:10,ME генерує пакети від імені 10 випадкових хостів та реального сканера. Для аналітика SOC або автоматичної системи захисту це виглядає як одночасна атака з багатьох джерел, що унеможливлює автоматичне блокування реального джерела без ризику заблокувати легітимні адреси.

Третім, найбільш надійним методом обходу поведінкових аналізаторів, є маніпуляція таймінгами (-T, --scan-delay). Використання режимів -T1 (Sneaky) або -T2 (Polite) у поєднанні з примусовою затримкою між пакетами дозволяє знизити інтенсивність сканування нижче порогу спрацьовування тригерів IDS, заснованих на частоті запитів (rate-based detection).

Розроблений алгоритм є адаптивним: у режимі "Довірена" він віддає пріоритет швидкості (-T4), тоді як у режимі "Ворожа" автоматично активує комплекс методів ухилення (рандомізація хостів, приманки, фрагментація), жертвуючи швидкістю заради прихованості.

Висновок. У ході виконання роботи було розроблено комплексний алгоритм застосування Nmap, який формалізує процес пошуку вразливостей, трансформуючи його з ручного набору команд в автоматизований процес.

Обґрунтовано використання динамічного аналізу вразливостей через інтеграцію Nmap Scripting Engine зі скриптом vulners, що забезпечує кореляцію знайдених сервісів з глобальними базами CVE в реальному часі.

Розроблено програмну архітектуру на базі Python, яка автоматизує запуск сканування та парсинг XML-результатів, перетворюючи неструктуровані дані у реляційну базу знань.

Запропоновано адаптивний механізм вибору параметрів сканування, який враховує наявність засобів активного захисту (IDS/IPS) та автоматично застосовує техніки ухилення. Це дозволяє значно підвищити ефективність аудитів інформаційної безпеки, зменшити кількість рутинних операцій та мінімізувати ризик пропуску критичних вразливостей.

Перелік використаних джерел.

1. Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

2. UDP Scan (-sU) // Nmap.org. [Електронний ресур].- Режим доступу: https://nmap.org/book/scan-methods-udp-scan.html

3. Vulners.nse Script Documentation // Nmap.org. [Електронний ресур].- Режим доступу: https://nmap.org/nsedoc/scripts/vulners.html

4. Python-nmap: run nmap from python // PyPI. [Електронний ресур].- Режим доступу: https://pypi.org/project/python-nmap/

5. Output Formats - XML Output (-oX) // Nmap.org. [Електронний ресур].- Режим доступу: https://nmap.org/book/output-formats-xml-output.html

6. Argp. nmapdb: parses nmap's XML output files and inserts them into an SQLite database // GitHub. 2009. URL: https://github.com/argp/nmapdb

7. Bypassing Firewalls and Intrusion Detection Systems // Nmap.org. [Електронний ресур].- Режим доступу: https://nmap.org/book/man-bypass-firewalls-ids.html

УДК 681.5

Віталій КЛИМІВ, Аліна ДАВЛЕТОВА

Західноукраїнський національний університет

КОМП'ЮТЕРИЗОВАНА СИСТЕМА УПРАВЛІННЯ ПАРОВИМ ЕНЕРГЕТИЧНИМ АГРЕГАТОМ

Вступ. За рівнем автоматизації теплоенергетика займає одне з ведучих місць серед інших галузей промисловості. Теплоенергетичні установки характеризуються безперервністю процесів, що протікають у них. При цьому вироблення теплової й електричної енергії в будь-який момент часу повинно відповідати споживанню (навантаженню). Пароутворюючі енергетичні агрегати (ПЕА) є ключовими елементами технологічної інфраструктури промислових підприємств, забезпечуючи виробництво пари, необхідної для технологічних, енергетичних та теплових потреб [1, 2]. Стабільність та безпека роботи таких котлів прямо залежить від ефективності систем контролю й управління. У зв'язку з цим впровадження комп'ютеризованих систем управління (КСУ) є актуальним напрямом розвитку сучасної промислової автоматизації. Інтеграція технологій Інтернету речей (IoT) забезпечує можливість віддаленого моніторингу стану ПЕА, своєчасного збору даних, аналізу динаміки параметрів технологічного процесу (ТП) та оперативного реагування на відхилення. Використання IoT-рішень підвищує точність контролю, надійність роботи обладнання та сприяє переходу до концепції прогнозного обслуговування.

Метою роботи є проєктування та моделювання КСУ ПК, що дозволяє забезпечити точне регулювання технологічних параметрів, зменшення впливу людського фактора та підвищення безпеки ТП.

1. Дослідження будови та принципу дії пароутворюючих агрегатів

ПЕА промислового типу мають складну багатофункціональну структуру, яка включає топкову камеру, барабан, поверхні нагріву (радіаційні, конвективні та випарні), систему підготовки й подачі живильної води, системи дуття та відведення продуктів згоряння, а також контрольно-вимірювальні прилади та засоби автоматизації (рисунок 1) [3].

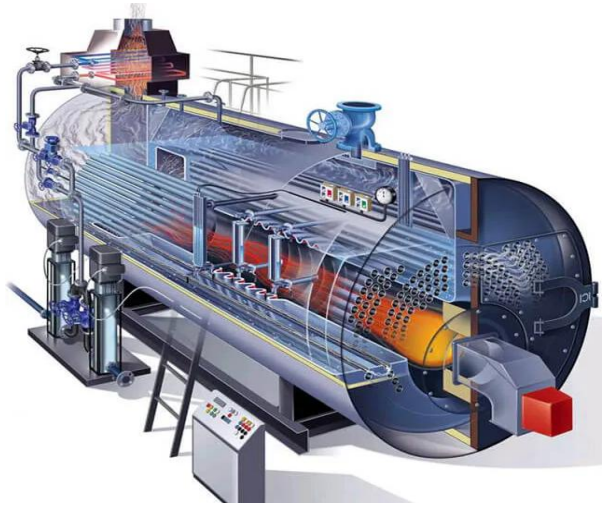


Рисунок 1 – Будова ПЕА

Топкова камера забезпечує стабільне горіння палива за рахунок подачі його у визначених витратах і дотримання оптимального співвідношення «повітря–паливо». Радіаційні поверхні призначені для інтенсивного теплообміну, тоді як конвективні поверхні забезпечують додатковий нагрів води та пари. Барабан виконує функції розподілу пароводяної суміші, відокремлення пари та підтримання необхідного рівня води.

Принцип роботи ПЕА (рисунок 2) базується на перетворенні хімічної енергії палива в теплову енергію, яка передається воді для утворення пари [4]. Процес включає подачу палива в топковий пристрій, змішування його з повітрям у необхідних пропорціях, організацію горіння та перенесення тепла через радіаційні та конвективні поверхні нагріву. У зонах випаровування вода перетворюється на пароводяну суміш, яка надходить у барабан для розділення на насичену пару та теплоносій.

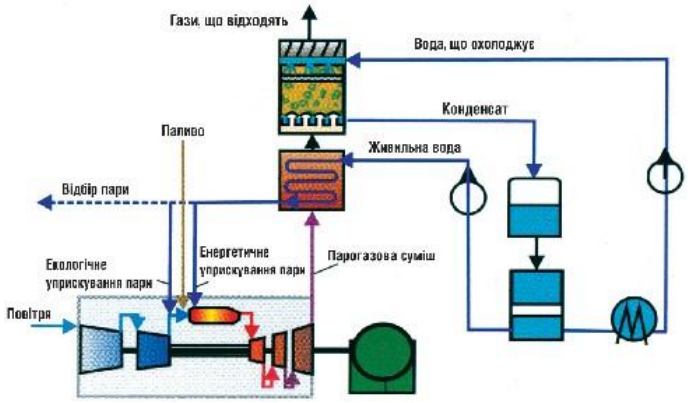


Рисунок 2 - Принципова схема ПЕА

Управління процесами горіння, випаровування та утворення пари вимагає підтримання визначених режимів роботи – температури у топковій камері, тиску та витрати пари, стабільного рівня води в барабані. Чутливість процесу до змін навантаження, коливань теплової потужності і режимів споживання пари робить необхідним застосування автоматизованих контурів регулювання.

За результатами дослідження встановлено, що принцип дії агрегатів передбачає багатоконтурне регулювання із взаємопов’язаними параметрами, а ефективна автоматизація забезпечує мінімізацію енергетичних втрат, покращення економічності та підвищення рівня безпеки роботи обладнання.

Стабільність пароутворюючого процесу визначається узгодженою роботою всіх вузлів ПЕА, а найбільш критичними параметрами є тиск пари, температура в топці, рівень води в барабані, витрата палива, витрата повітря та склад димових газів. Ці параметри характеризуються високою чутливістю до зовнішніх збурень і мають нелінійні взаємозв’язки, що обґрунтовує необхідність комплексної автоматизації. Проведене дослідження дозволило визначити структуру теплоенергетичного об’єкта, ідентифікувати його ключові елементи та сформувати вимоги до подальшого проєктування КСУ.

2. Проектування архітектури комп’ютеризованої системи управління

ТП пароутворення залежить від точності підтримання наступних базових параметрів: тиску, температури, рівня води в барабані, витрати палива/повітря та

співвідношення між ними. Невідповідність цих параметрів може спричинити аварійні режими, гідроудари, перегрів поверхонь нагріву або зниження економічності ПЕА.

Для контролю та регулювання визначених технологічних параметрів розроблено багаторівневу архітектуру КСУ, яка включає наступні рівні:

- рівень датчиків, перетворювачів та виконавчих механізмів;
- рівень контролерів (ПЛК), що реалізують алгоритми регулювання технологічних змінних;
- рівень управління, моніторингу, протоколювання, аварійної сигналізації, індикації станів.

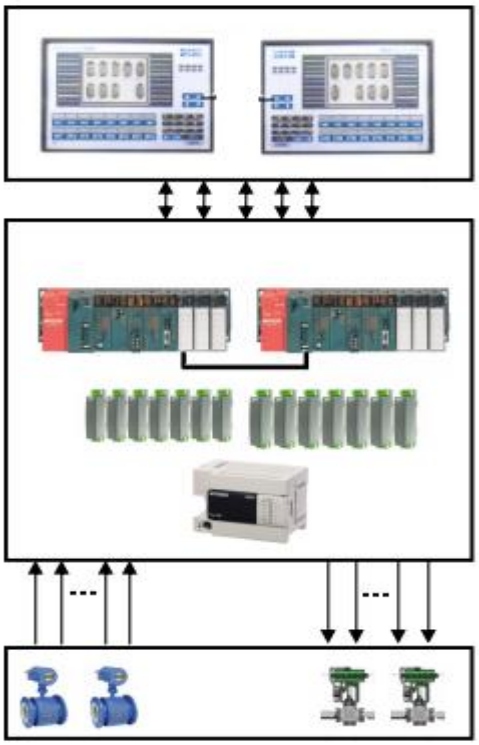


Рисунок 3 - Архітектура проектованої КСУ

Запропонована структура забезпечує високу живучість, модульність, можливість масштабування та інтеграції з існуючими системами підприємства.

На основі проведеного досліджень визначено та розроблено функціональну схему КСУ, що включає взаємопов’язані контури, які виконують окремі функції у загальному процесі керування:

- контур регулювання тиску пари, що підтримує стабільний тиск у паровому барабані за допомогою регулювання подачі палива.
- контур регулювання температури, що забезпечує оптимальний тепловий режим котла.
- контур регулювання рівня води, який реалізовано в одно-, дво- та трьохелементних варіантах.
- контур регулювання витрати, що компенсує зміну навантаження котла.
- контур регулювання співвідношення «повітря–паливо», що забезпечує повне згоряння палива й мінімізацію викидів.

Реалізація КСУ дозволяє забезпечити підтримку безпечного та енергоефективного режиму роботи ПЕА.

3. Дослідження ефективності проектованої системи

Проведене імітаційне моделювання дозволило дослідити динамічну поведінку проектованої КСУ при різних режимах роботи: пуск котла; зміна навантаження; відхилення параметрів; вплив збурень (раптове зростання витрати пари, зміна тиску газу тощо) (рисунок 4).

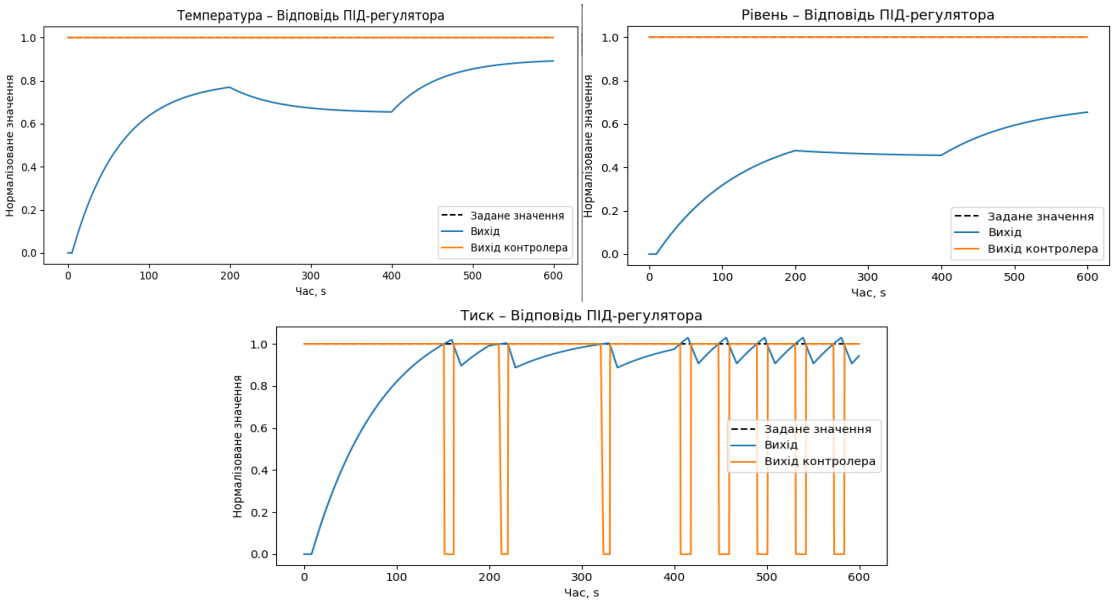


Рисунок 4 – Результати моделювання проектованої КСУ

Результати моделювання підтвердили адекватність побудованих моделей та працездатність розробленої архітектури системи.

Висновок. Розроблена КСУ ПЕА дозволяє забезпечити автоматичне, безпечне та енергоефективне функціонування котельної установки, зменшення впливу людського фактора, підвищення точності регулювання параметрів, удосконалення процесів контролю та діагностики та можливість інтеграції з цифровими системами управління підприємством. Отримані результати підтверджують ефективність впровадження сучасних методів автоматизації та перспективність використання алгоритмів з прогнозуванням стану для промислових пароутворюючих установок.

Перелік використаних джерел.

1. Gilman G.F. Boiler Control Systems Engineering. 2nd edition. Technical book. 2010. 217p.

2. Hasan Karrar. (2020). Study Operation of Steam Generation System Using Different Fuels. DOI: 10.13140/RG.2.2.12780.64648

3. Принцип роботи та влаштування парового котла – відмінності, переваги. [Електронний ресур].- Режим доступу: https://heatingmastak.com.ua/alternative-heating/princip-roboti-i-pristrij-parovogo-kotla-vidminnosti-perevagi.html

4. Створення та розвиток парогазових й газопарових установок, їх класифікація. [Електронний ресур].- Режим доступу: http://energetika.in.ua/ua/books/52-entsiklopediya/rozvitok-teploenergetiki-ta-gidroenergetiki/chasina-1-teploenergetika/rozdil-3-parovi-ta-gazovi-turbini/146-3-8-stvorennya-ta-rozvitok-parogazovikh-j-gazoparovikh-ustanovok-jikh-klasifikatsiya

УДК 681.32

Іван АЛБАНСЬКИЙ, Валерій ПАВЛІН, Михайло-Сергій ГОРОХІВСЬКИЙ, Володимир КИБА

Західноукраїнський національний університет

АВТОМАТИЗАЦІЯ ПРОЦЕСУ КЕРУВАННЯ ВИКОНАВЧИМИ МЕХАНІЗМАМИ РОБОТИЗОВАНОЇ ПЛАТФОРМИ

Вступ. Стрімкий розвиток робототехніки та систем автоматизації є однією з ключових тенденцій сучасної інженерії. Роботизовані платформи знаходять широке застосування у виробництві, логістиці, сільському господарстві, оборонній сфері, медицині та побутових пристроях. Висока динаміка розвитку цього напрямку зумовлена потребою підвищення продуктивності, мінімізації людського фактора та створення адаптивних систем, здатних самостійно функціонувати у складних або небезпечних умовах. Одним із найважливіших аспектів побудови роботизованих систем є керування виконавчими механізмами, від якого залежить точність переміщення, стабільність роботи, швидкодія та надійність усієї платформи.

Мета: дослідження систем автоматизації процесу керування виконавчими механізмами роботизованої платформи.

1. Актуальність процесів автоматизації промислових установок та мобільних платформ

Керування виконавчими механізмами охоплює процеси формування керуючих сигналів, регулювання сили, положення та швидкості, а також забезпечення зворотного зв’язку від сенсорних підсистем. У сучасних роботизованих платформах можуть бути використані різні типи виконавчих механізмів: електричні двигуни, сервоприводи, крокові двигуни, пневматичні та гідравлічні актуатори. Їхня узгоджена робота потребує впровадження інтелектуальних алгоритмів керування, систем стабілізації та засобів діагностики, які забезпечують безперервний моніторинг стану обладнання та коригування траєкторій руху в реальному часі.

Автоматизація цих процесів є необхідною для створення роботів, здатних виконувати складні технологічні операції, адаптуватися до змінних умов середовища та взаємодіяти з іншими технічними засобами. Саме тому дослідження, спрямовані на підвищення ефективності керування виконавчими механізмами, є актуальними не лише в науковому, але й у практичному аспектах. В сучасному інженерному середовищі розробка алгоритмів керування, удосконалення апаратної архітектури та оптимізація взаємодії між модулями роботизованої платформи стають важливою частиною технологічного прогресу.

Актуальність автоматизації процесу керування виконавчими механізмами роботизованих платформ визначається низкою технічних, економічних та соціальних чинників. Сучасні промислові та сервісні роботи повинні працювати швидко, точно та автономно. При цьому зношуваність механізмів, нестабільність навантаження, зовнішні дестабілізуючі фактори та складні умови експлуатації вимагають впровадження алгоритмів автоматичного коригування руху, адаптації та компенсації похибок [1].

Одним із ключових факторів актуальності є перехід від традиційних роботів до

мобільних та комбінованих систем, здатних взаємодіяти з людиною та навколишнім середовищем. У таких системах точність керування виконавчими механізмами набуває критичного значення, бо від неї залежить безпека персоналу, надійність виконання операцій і рівень інтеграції платформи в технологічні процеси.

Економічна актуальність полягає у тому, що правильно автоматизовані виконавчі механізми дозволяють мінімізувати втрати енергії, підвищити ресурс двигунів і зменшити витрати на технічне обслуговування. Це забезпечує зростання рентабельності використання роботизованих платформ у промислових масштабах.

Важливим є також зростаючий попит на роботизовані системи у військовій та екстремальній діяльності. У таких умовах виконавчі механізми мають працювати стабільно навіть при відмовах частини сенсорів або зміні зовнішніх умов, що ще більше підкреслює актуальність теми автоматизації керування.

2. Структура систем управління сервоприводами автоматизованих систем

Для розробки та налагодження системи автоматичного управління (САУ) необхідний моніторинг роботи кожного елемента системи керування. Важливо відзначити, що на початку розробки перевірку працездатності схемотехнічних та програмних рішень доцільно проводити до того, як буде створено реальний прототип пристрою. Тому актуально використовувати віртуальну модель системи керування. У цій роботі проводилося моделювання системи управління сервоприводами для влаштування паралельної кінематики.

Система управління сервоприводами складається з персонального комп'ютера (ПК) та керованого з нього, контролера сервоприводів (рисунок 1).

Рисунок 1 – Схема моделювання САУ на комп’ютері

Керуюча програма подає команди з комп'ютера на контролер, в яких міститься інформація про номер двигуна та його потрібне положення. Контролер відповідає про виконану команду і відправляє сигнали на серводвигуни їхнього повороту (рисунок 2) [2].

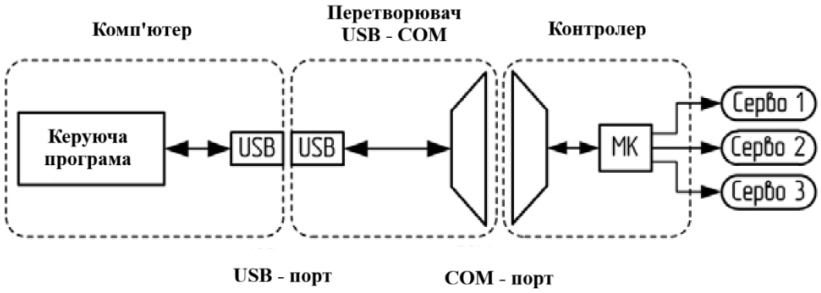


Рисунок 2 – Функціональна схема реальної САУ

Ця система управління повністю промодельована на комп'ютері, перш ніж було створено прототип. Моделювання роботи системи керування виконується за

допомогою трьох програм: Serial Port Monitor, Visual Serial Ports Driver, Proteus.Програма Serial Port Monitor є терміналом для обміну інформацією з послідовним портом. Розробник має можливість надсилати команди на пристрій та приймати повідомлення. Таким чином, імітується робота керуючої програми. За допомогою утиліти Virtual Serial Ports Driver емулюється послідовний порт RS-232, з'єднаний віртуальним нуль-модемним кабелем [3]. Створені два віртуальні послідовні порти в системі, з'єднаних один з одним для обміну інформацією. Ця програма моделює роботу портів комп'ютера та контролера, з'єднаних кабелем.

Засіб розробки та тестування Proteus моделює роботу електроніки, у тому числі серводвигунів та мікроконтролера Atmega-16. Для перевірки розробленої програми, що керує мікроконтролером, вона завантажується у віртуальну електричну модель пристроїв. Під час коректної роботи цією програмою буде запрограмовано реальний мікроконтролер. У середовищі налагодження Proteus є набір віртуальних приладів, таких як вольтметр, осцилограф, логічний аналізатор. Схему моделі САУ наведено на рисунку 3.

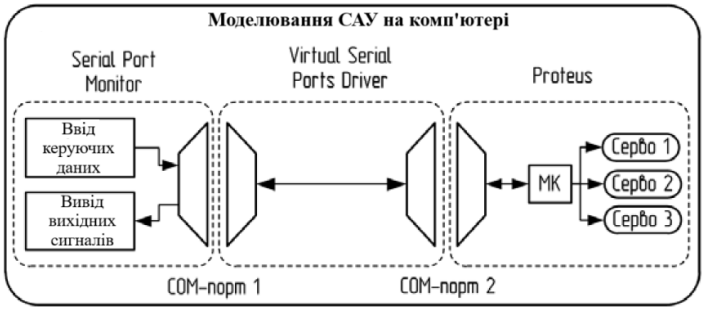


Рисунок 3 – Схема моделювання САУ за допомогою програмних комплексів

Наступним кроком є детальний аналіз елементів системи управління їх розробкою та налагодженням. Оскільки необхідні керуючі сигнали визначаються об'єктом управління, то спочатку потрібно вивчити пристрій роботи сервоприводу.

Сервомеханізм - слідкуюча система автоматичного регулювання, яка працює за принципом зворотного зв'язку і в якій один або більше системних сигналів, сформованих в сигнал, що управляє, надають механічний регулюючий вплив на об'єкт. Сервосистеми мають дві особливості: здатність посилювати потужність та інформаційний зворотній зв'язок. Посилення необхідне тому, що потрібна на виході енергія зазвичай велика (береться від зовнішнього джерела), але в вході незначна. Зворотний зв'язок є замкнутим контуром, в якому неузгодженість сигналів входу і виходу використовується для управління. Отже, у прямому напрямку контур передає енергію, а у зворотному забезпечує інформацію, необхідну точного управління (рисунок 4) [4].

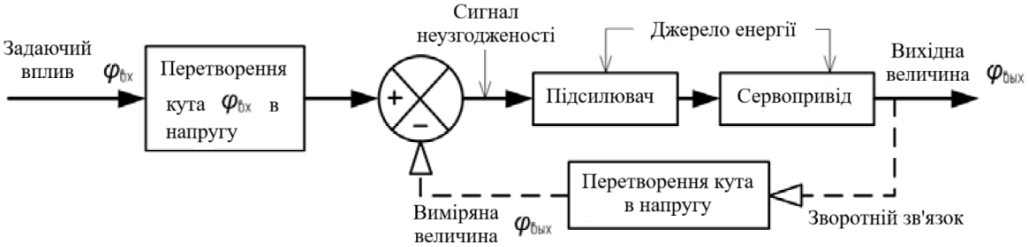


Рисунок 4 – Блок-схема системи керування серводвигуном

Керуючі сигнали від контролера до серводвигуна візуально представлені на рисунку 4. Серводвигунові на вхід із приймача подається прямокутний імпульс, тривалість якого визначає кут повороту двигуна (рисунок 5). У дослідному зразку використовується серводвигун HXT900. Ширина імпульсу становить 450-2450 мкс. Період між імпульсами дорівнює 20 мс. Кут повороту - 90 °. При імпульсах тривалістю 450 мкс серводвигун встановлюється у положення 0°. При імпульсах тривалістю 2450 мкс серводвигун встановлюється у положення 90° [4, 5].

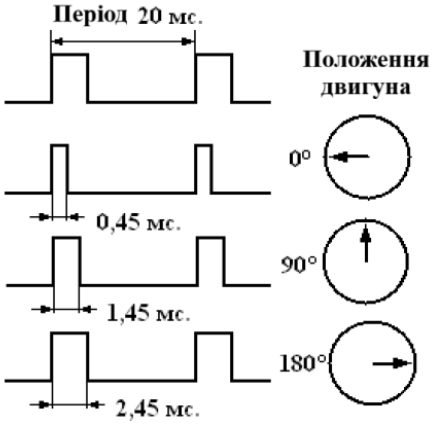


Рисунок 5 – Керуючі сигнали від контролера до серводвигуна

Команди подаються на контролер з комп'ютера. Структура команди від керуючої програми на контролер є наступною: <початок><номер двигуна><необхідне положення>. Початок – це один старт-байт у шістнадцятковій системі дорівнює FF, що позначає початок передачі. Номер двигуна набирає значення від 0 до 7. Система управління має можливість керувати становищем трохи більше 8 сервоприводів. Ця кількість є достатньою для абсолютної більшості пристроїв паралельної структури. Далі передаються дані про ширину імпульсу ШІМ-сигналу, за допомогою якого відбувається керування сервоприводами (таблиця 1). Потрібне положення задається одним байтом. Можливе збільшення кількості байтів для більшої точності.

Таблиця 1 - Передача інформації про поточне положення серводвигунів

Число в десятковій сист. числ.	Число в шістнадцятковій сист. числ.	Необхідна ширина імпульсу в мкс	Положення двигуна в град.
0	0	450	0
127	7F	1450	45
255	FF	2450	90

Величина помилки позиціонування двигуна, що виникає під час передачі інформації від ПК до МК, визначається виразом [6, 7]:

$$\Delta = \frac{\theta}{256^n},$$

де Θ - кут повороту сервопривода; n – число байт, з інформацією щодо положення приводу.

Якщо інформація про положення передається одним байтом, то похибка становить

$$\Delta = \frac{90^\circ}{256} = 0{,}352^\circ.$$

Якщо інформація про положення передається двома байтами, то похибка становить

$$\Delta = \frac{90^\circ}{256^2} = 0{,}001\,37^\circ.$$

Нище представлено приклади команд, що відправляються від керуючої програми до контролера [7]: FF 00 00 – означає перевести перший двигун у кут 0°; FF 01 7F – означає перевести другий двигун у кут 45°; FF 07 FF – означає перевести восьмий двигун у кут 90°.

Алгоритм керування серводвигунами є структурно упорядкований. Прийняті мікроконтролером з комп'ютера дані записуються в масив ServoState. За значеннями з цього масиву визначається тривалість імпульсу широтно-модульованого сигналу для кожного серводвигуна. З періодом 20 мс на кожний двигун надходить передній фронт імпульсу (рисунок 6).

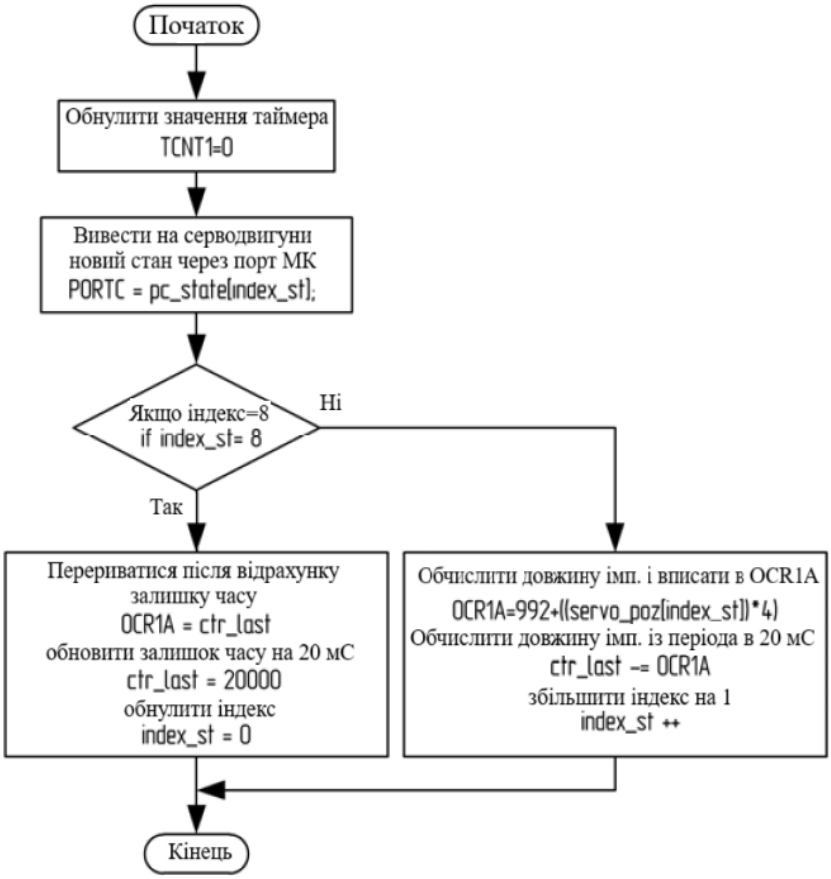


Рисунок 6 – Блок-схема алгоритму роботи таймера, що відповідає за формування переднього і заднього фронтів ШІМ – імпульсів

Задній фронт подається тоді, коли з переднього фронту пройшов час, що дорівнює необхідній ширині імпульсу для даного двигуна (від 450 до 2450 мкс).

Частота тактування мікроконтролера F_t обчислюється розподілом частоти роботи резонатора F_{res} на коефіцієнт дільника k_d :

$$F_t = \frac{F_{res}}{k_d}.$$

З використанням зовнішнього кварцового резонатора можна досягти частоти роботи мікроконтролера Atmega-16 до 16 МГц. У роботі використаний внутрішній генератор тактових імпульсів із частотою 1 МГц. Таймери мікроконтролера тактуються від генератора тактових імпульсів, частота якого поділена на коефіцієнт дільника, записаний у регістр TCCR1. Для зручності розрахунків коефіцієнт дільника дорівнює одиниці. Таким чином, частота тактування таймерів мікроконтролера дорівнює 1 МГц, а період тактування – 1 мкс. Період тактування – параметр, який використовується у таймерах мікроконтролера для формування широтно-модульованих імпульсів.

Час тривалості імпульсу, що подається на сервопривід, визначається кількістю тактів, що повинен зробити таймер до переривання. Необхідна кількість тактів таймера обчислюється за формулою

$$T = T_{\min} + Sp_i \cdot \frac{T_{\max} - T_{\min}}{256^n},$$

де T_{min} - мінімальне значення тривалості імпульсу, у вибраному серводвигуні, воно дорівнює 450 мкс; T_{max} – максимальне значення тривалості імпульса, у вибраному серводвигуні воно дорівнює 2450 мкс; Sp_i - значення позиції і сервоприводу з масиву станів сервоприводів srv_poz [i]; i – номер поточного сервоприводу змінюється від 0 до 7; n - число байт, з інформацією про положення приводу [8].

Приклад розрахунку кількості тактів таймера: середнє положення серводвигуна - 45 ° відповідає поданому з комп'ютера сигналу 127 (таблиця 1) кількість тактів таймера обчислюється за виразом

$$T = 450 + 127 \cdot \frac{2\,450 - 450}{255} = 1\,446.$$

Оскільки величина одного такту таймера дорівнює 1 мкс, кількість тактів дорівнює періоду імпульсу. Обчислена кількість тактів таймера записується в регістр мікроконтролера OCR1A. При кожному відліку таймера його значення збільшується на одиницю, а також порівнюється з регістром OCR1A. При збігу відбувається переривання роботи МК і формування заднього фронту імпульсу, тобто встановлюється нульовий потенціал усім серводвигунам.

3. Моделювання роботи контролера.

Контролер сервоприводів спроектований з урахуванням мікроконтролера Atmega-16. Керуючі ШІМ-сигнали на сервоприводи надходять із восьми виходів порту

з мікроконтролера. Для індикації робочих станів, а також помилок висновку PB0 підключений світлодіод. Прийом сигналів керування з комп'ютера здійснюється через порт COM1.

За допомогою програмного засобу Proteus створено електричну модель контролера сервоприводів (рисунок 7).

Порт COMPIM підключається до існуючого com-порт комп'ютера. При налагодженні цей порт підключається до віртуального com-порту, створеного

програмою Virtual Serial Ports Driver (як представлено на рисунку 3).

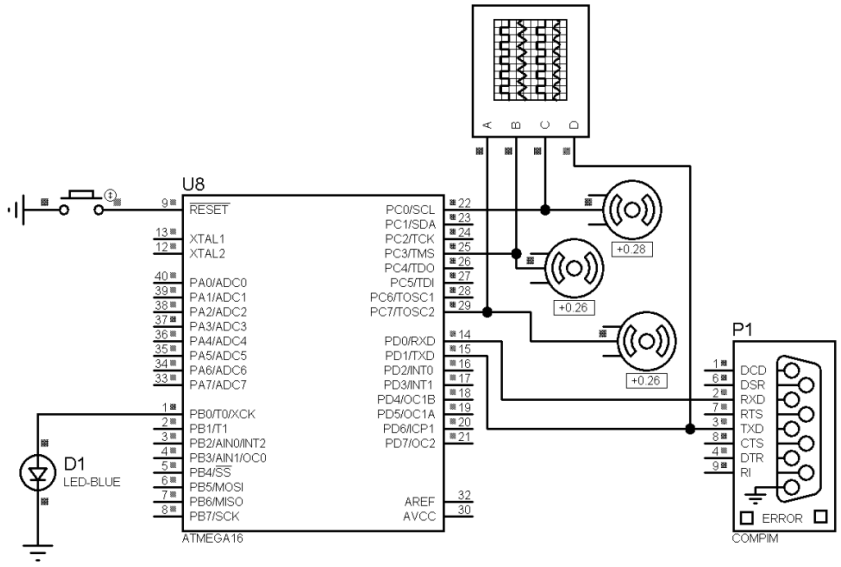


Рисунок 7 – Схема моделювання контролера в програмному комплексі Proteus

У середовищі налагодження VMLAB промодельовано роботу програми мікроконтролера. Використана можливість виконання інструкцій у покроковому режимі, а також наявність віртуального осцилографа та терміналу з'єднання RS-232. Виміряна ширина імпульса, що подається на перший двигун (рисунок 8), вона становить 2,2 мкс [9].

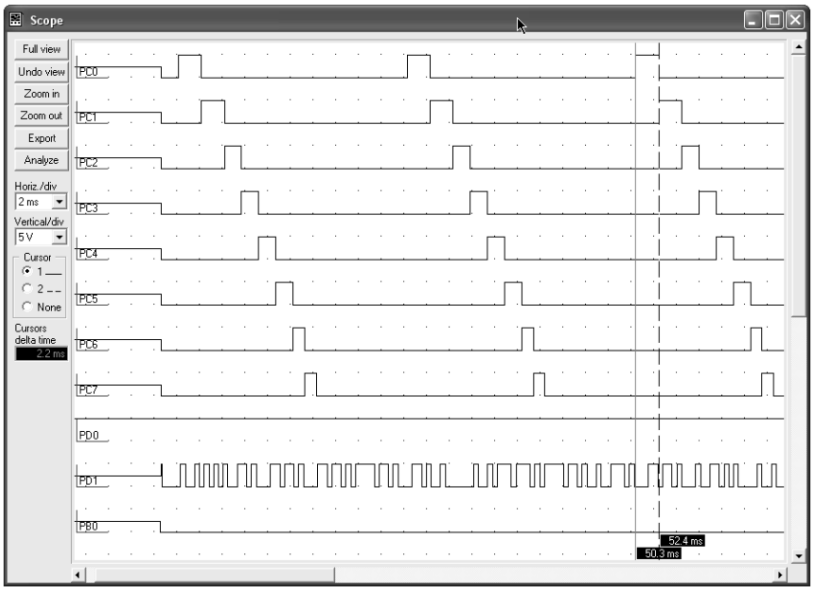


Рисунок 8 - Результати моделювання роботи мікроконтролера за програмою VMLAB (ШІМ-сигнали, що подаються на вісім двигунів)

Висновок. Ця система управління повністю промодельована на комп'ютері, перш ніж було створено прототип. Моделювання роботи системи керування виконується за допомогою трьох програм: Serial Port Monitor, Visual Serial Ports Driver, Proteus.

Автоматизація процесу керування виконавчими механізмами роботизованої платформи є ключовим етапом створення високоефективних кібер-фізичних систем,

здатних працювати автономно та виконувати складні технологічні операції. На основі аналізу сучасної літератури та технічних джерел встановлено, що розвиток робототехніки безпосередньо пов'язаний з удосконаленням методів регулювання руху, адаптивного керування та інтеграції інформаційних потоків між сенсорними й виконавчими підсистемами. Використання інтелектуальних алгоритмів керування, сучасних мікроконтролерних платформ та високоточних актуаторів дозволяє суттєво підвищити точність, швидкодію і стабільність роботизованих систем. Аналіз доступних джерел засвідчив, що тенденції індустріального розвитку, розвитку машинного навчання та мережевих технологій стають визначальними факторами модернізації виконавчих механізмів та їх автоматизованого керування. Роботизовані платформи переходять від простих механізмів до складних адаптивних систем, здатних до самодіагностики, оптимізації траєкторій і взаємодії з зовнішніми технологічними процесами. Таким чином, автоматизація керування виконавчими механізмами не лише забезпечує ефективність та надійність роботи роботів, але й створює передумови для їх інтеграції у сучасні виробничі та сервісні комплекси. Отримані теоретичні положення та огляд технічних рішень формують основу для подальших досліджень і практичної реалізації роботизованих систем нового покоління.

Перелік використаних джерел.

1. Грудська В.П. Електротехнічні пристрої систем автоматичного управління технологічними процесами: навчальний посібник/В.П.Грудська, В.І.Чибеліс/КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 107 с

2. Діордієв В. Т. Засоби автоматизації електротехнічних комплексів: навчальний посібник / В. Т. Діордієв, А. О. Кашкарьов, С. В. Дубініна, Г. В. Новіков. – Мелітополь: ФОП Однорог Т.В., 2020. – 220 с.

3. Чуклін Н.О., Ларченко Л.В. Огляд динаміки ринку МЕМС для сфер промисловості. / Н.О. Чуклін, Л.В. Ларченко // CXIII Міжнародна інтернет-конференція «Розвиток науки та техніки під час воєнного стану». – м. Херсон, 28 листопада, 2022.– С. 294-296.

4. Іванов Л.С. Конспект лекцій з дисципліни «Технічні засоби автоматизації» для студентів усіх форм навчання спеціальності 151 - Автоматизація та комп'ютерно-інтегровані технології, Частина 1 [Електронне видання] / Упоряд. Іванов Л.С. − Харків: ХНУРЕ, 2023. − 88 с.

5. Кабашкін І. В. Інтелектуальні транспортні системи: інтеграція глобальних технологій майбутнього / І. В. Кабашкін // Транспорт, 2019. – № 2 (27). – С. 34-38.

6. Гуртов В. А. Микроэлектромеханические системы / Гуртов В. А. – Петрозаводск : ПетрГУ, 2016. – 172 с.

7. Bielecki, Zbigniew & Stacewicz, Tadeusz & Wojtas, Jacek & Mikolajczyk, Janusz & Szabra, Dariusz & Prokopiuk, Artur. (2018). Selected optoelectronic sensors in medical applications. Opto-Electronics Review.

8. Трегуб В.Г. Проектування систем автоматизації / В.Г.Трегуб - Ліра-К, 2019. – 344с.

9. Гуржій А. М. Основи автоматики та робототехніки: Навчальний посібник/ А. М. Гуржій, А. Т. Нельга, В. М. Співак, О. С. Ітякін:–Дніпро:«Гарант СВ», 2021.- 243с.

УДК 681.32

Вадим БІЛЯВСЬКИЙ, Петро ГУМЕННИЙ

Західноукраїнський національний університет

КОМП'ЮТЕРНО-ІНТЕГРОВАНА ГРАФІЧНА МОДЕЛЬ АВТОМАТИЗАЦІЇ ОБЛІКУ ПРОДУКЦІЇ НА ПОЛІГРАФІЧНОМУ ВИРОБНИЧОМУ СКЛАДІ

Вступ. Сучасні поліграфічні підприємства функціонують в умовах високої конкуренції, зростання вимог до швидкості обробки замовлень та мінімізації виробничих витрат. Однією з критичних ланок, що прямо впливає на рентабельність виробництва, є процес складського обліку, зокрема точність списання матеріалів, облік напівфабрикатів і готової продукції, а також коректність реєстрації внутрішніх переміщень [1].

Традиційні ручні або частково автоматизовані системи складського контролю не забезпечують необхідної точності, призводять до помилок у документації, відхилень між фактичними та бухгалтерськими залишками, затримок у виробництві та непродуктивних втрат часу працівників. У цих умовах ефективність функціонування підприємства залежить від здатності інтегрувати автоматизовані засоби збору даних у єдине інформаційне середовище.

У роботі представлено комп'ютерно-інтегровану систему автоматизації обліку продукції, яка вирішує проблему неточності обліку та забезпечує оперативну взаємодію між складом, виробництвом і системами управління підприємства. Основні результати системи проявляються у зниженні витрат, прискоренні облікових процесів та мінімізації людського фактора.

Мета: Дослідження та розробка комп'ютерно-інтегрованої графічної системи автоматизації обліку продукції на виробничому складі.

Основна частина

Складський облік у поліграфічному виробництві має специфічні особливості: висока номенклатура матеріалів, залежність витрат від технологічних параметрів машин, швидкі цикли виконання замовлень, складність прогнозування витрат паперу й фарби. У багатьох підприємствах облік здійснюється вручну або за допомогою декількох розрізнених програмних засобів, що створює низку проблем:

- висока ймовірність помилок при ручному введенні даних;
- затримки в оновленні інформації, що унеможливлює оперативне управління виробництвом;
- невідповідність між фактичними та обліковими залишками, що призводить до перевитрат;
- обмежена аналітика, яка не дозволяє прогнозувати потреби виробництва;
- велика частка трудомістких операцій, що знижує продуктивність праці.

Аналіз сучасних технологічних рішень показує, що найбільш ефективними є системи, що поєднують автоматичний збір даних, сенсорні модулі, комп'ютерний аналіз та єдину базу даних, синхронізовану з виробничими процесами

На рисунку 1 представлено розробку та дослідження комп'ютерно-інтегрованої системи автоматизації обліку продукції на виробничому складі поліграфічного підприємства. Система забезпечує точний контроль руху матеріалів і готової продукції у режимі реального часу, інтегрує засоби автоматичного збору даних, оптичні сенсори, модулі статистичної аналітики, а також взаємодіє з центральною інформаційною базою підприємства. Запропоноване рішення дозволило зменшити витрати виробництва на 11% та скоротити час облікових операцій на 30%, що значно підвищило ефективність складської логістики. Представлено архітектуру системи, методи взаємодії апаратних і програмних модулів, результати випробувань та економічний ефект упровадження

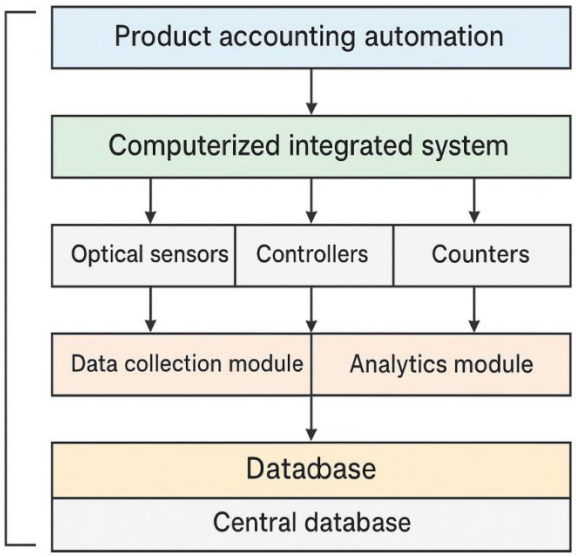


Рисунок 1 Схема ієрархічної роботи системи

Розроблена система включає такі основні компоненти:

Апаратний рівень:

- оптичні сенсори контролю руху матеріалів;
- лічильники витрати паперу та фарби;
- модулі контролю позиціювання та натягу рулону;
- промислові контролери, що обробляють первинні дані з датчиків.

Програмний рівень:

- модуль збору та класифікації даних;
- сервер обробки і збереження інформації;
- аналітичний модуль прогнозування витрат;
- веб-інтерфейс для операторів складу та адміністрації;
- база даних SQL, інтегрована з виробничими системами підприємства.

Передача даних здійснюється через промислові протоколи (Modbus, OPC-UA), що гарантує надійність та синхронізацію інформаційних потоків між складом і друкарським обладнанням.

Запропонована система працює за принципом автоматичного збору та синхронізації інформації. Оптичні сенсори фіксують усі переміщення матеріалів: від моменту подачі рулону на машину до отримання готової продукції. Дані передаються

на центральний сервер, де обробляються та записуються до бази даних. Оператори складу отримують доступ до інтерфейсу з оновленням даних кожні 0,5 секунди, що дає змогу контролювати стан запасів та уникати виробничих затримок[2].

На рисунку 2 зображено електричну принципову схему підключення та взаємодії елементів системи контролю використання матеріалів і обліку (tension control system), що застосовується у рулонних друкарських, офсетних ротаційних машинах[3]. Дана схема демонструє правильне підключення датчиків натягу (load cell tension detectors), тензодатчиків, оптичних датчиків, комунікаційних інтерфейсів, сигналів керування, виходів швидкості та аналогових каналів, які формують комплексну систему автоматизованого керування обліку і розмоткою або намотуванням рулону.

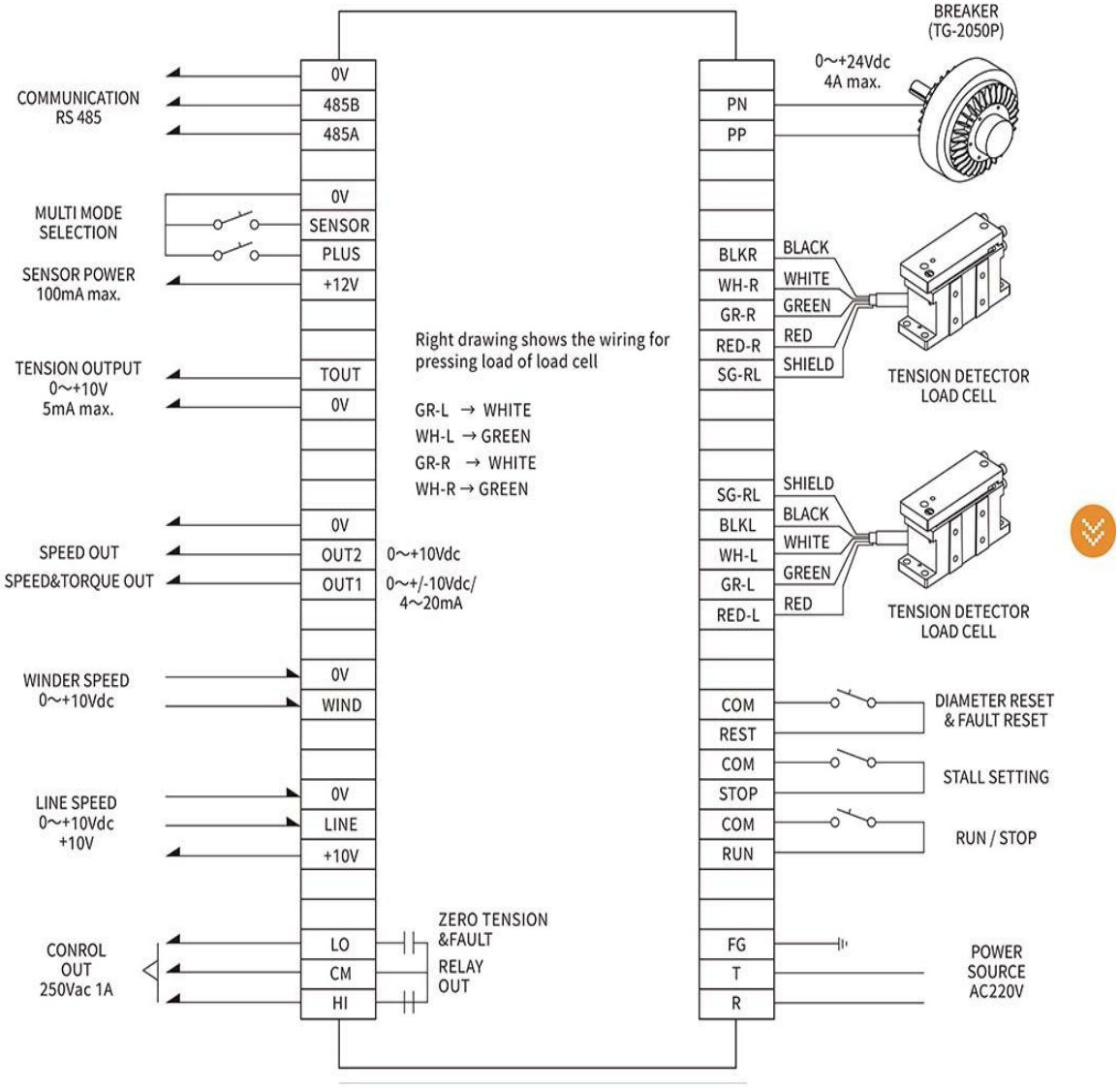


Рисунок 2 - Електрична принципова схема підключення та взаємодії елементів

У центрі схеми знаходиться контролер, що виконує такі ключові функції:

- прийом сигналів з тензодатчиків;
- перетворення даних у цифрову форму;
- формування керуючих сигналів для приводу розмотки/намотки;
- передача даних у систему керування через RS-485;

- забезпечення живлення датчиків;
- реалізація логіки "RUN/STOP", "RESET", "STALL" та релейних виходів.

Контролер включає набір клем, які групуються за функціональними зонами.

Зліва схеми розташовано клеми: 485A, 485B, 0V. Ці лінії забезпечують обмін даними з PLC, HMI або іншим промисловим контролером через протокол Modbus RTU, що дозволяє керуватипараметрами натягом, швидкістю, діаметром рулону, станом датчиків.

Контролер забезпечує: +12V постійного струму, максимальний струм до 100 mA. Це живлення використовується для оптичних датчиків, інкодерів або тензодатчиків, що потребують зовнішнього живлення

Канал TENSION OUTPUT це аналоговий вихід 0–10V, максимум 5 mA. Він формує сигнал керування на привід натягування паперового полотна. Значення напруги відповідає реальному або заданому натягу, 0 V - відсутність натягу, 10 V - максимальний натяг рулону.

Відповідає швидкості лінії: 0-10V вхід; +10V живлення для датчика. OUT1 / OUT2 формують команду швидкості і крутного моменту. Це критично для систем автоматичної компенсації діаметра рулону. У правій частині схеми знаходяться два тензодатчики. BLACK (BK) - живлення або негативний сигнал, WHITE (WH) - позитивний сигнал, GREEN (GR) - негативний зворотний сигнал, RED (RD) - живлення або компенсуючий сигнал, SHIELD (SG) - екран для захисту від завад. Тензодатчики вимірюють вагу рулону та механічну силу натягу полотна. Контролер отримує аналоговий сигнал, перетворює його у цифрове значення натягу й використовується у регулюванні швидкості.

Праворуч під контролером підключені інтерфейсні кнопки: RUN / STOP - керують запуском та зупинкою процесу. STALL SETTING - встановлює межі аварійних режимів. FAULT & DIAMETER RESET - скидання аварій та обнулення діаметра рулону, якщо рулон був знятий, якщо рулон був замінений датчик виміряє і зафіксує новий діаметр. Кожна кнопка має вхід COM - загальна шина, вхід для сигналу. Оператор може керувати системою безпосередньо з панелі контролера.

Нижня частина схеми R, S, T - трифазне або однофазне підключення до мережі AC220V, FG - заземлення. Живлення необхідне для роботи всього контролера та підключених пристроїв.

Релейний контакт HI-CM-LO спрацьовує при аварії, сигналізує про втрату натягу полотна і може керувати зовнішньою сиреною, лампою або зупиняти привід.

На рисунку 3 представлено графічну залежність різних технологічних параметрів друкарського процесу від номеру вибірки (Sample number). Даний графік використовується для аналізу стабільності роботи друкарської машини, а також для контролю якості нанесення фарби під час офсетного друку.

На діаграмі відображено чотири ключові показники, кожен з яких представлений окремою кривою. Рожева крива демонструє коливання фактичної подачі пурпурової фарби під час друку. Оскільки маджента є однією з основних фарб у моделі CMYK, її рівномірне нанесення критично важливе для відтворення точних кольорів на відбитку.

На графіку видно, що подача фарби зазнає невеликих флуктуацій, що пояснюється зміною в'язкості фарби. Динамічним режимом роботи зволожувального апарату, мікроколиваннями у відкритті фарбових зон (Ink key opening) та зміною температури. Такі природні варіації є нормальними, але їх надмірне збільшення може сигналізувати про необхідність корекції друкарських налаштувань

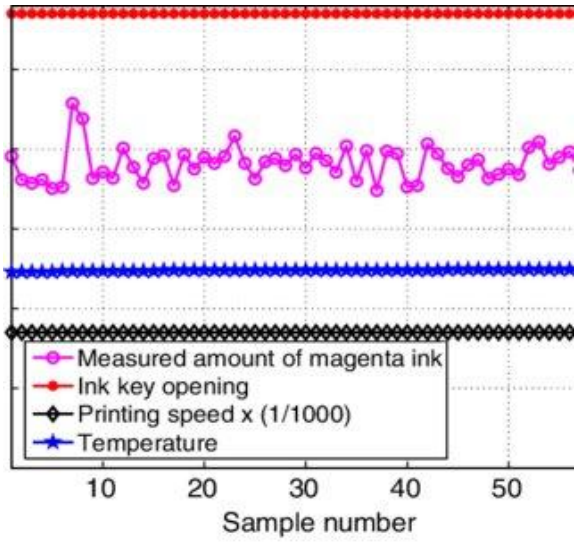


Рисунок 3 – Графік залежності технологічних параметрів друкарського процесу

Ступінь відкриття фарбового ключа це параметр позначений червоною лінією, який визначає наскільки відкрита фарбова зона на друкарській секції. Фарбові ключі регулюють товщину шару фарби, що подається на форму. На графіку червона лінія практично горизонтальна, що означає, стабільне механічне положення фарбових зон. Також відсутність корекцій у налаштуваннях під час вибірки, автоматична система дозування не вносила змін. Це свідчить про стабільність процесу та відсутність потреби у втручанні оператора під час досліджуваного періоду.

Чорна лінія це швидкість друку подана у відносному масштабі (позначено x (1/1000)). Лінія є абсолютно рівною, що означає, стабільний режим роботи друкарської машини, відсутність розгону або уповільнення і контрольовані умови експерименту. Швидкість є важливим фактором, оскільки при її зміні змінюється товщина нанесеної фарби, ефективність переносу фарби з форми на офсетне полотно та поведінка паперу у друкарському тракті.

Температура в зоні друку позначена синьою лінією. Цей параметр відповідає за контроль в'язкості фарби, роботу зволожувального розчину і стабільність кольору. Графік показує, що температура залишається майже незмінною протягом усього періоду відбору даних. Така стабільність є позитивною, оскільки різкі зміни температури можуть спричинити коливання у подачі фарби, зміни в балансі «фарба–вода», також появу дефектів на відбитках.

На рисунку 4 представлено залежність швидкості обертання фарбових валів друкарської машини від продуктивності друку, що виражена кількістю відбитків на годину. Графік демонструє, як збільшується відносна швидкість обертання для кожної з фарбових секцій - Cyan (блакитна), Magenta (червона), Yellow (жовта) та Black (чорна) - при нарощуванні швидкості роботи друкарського агрегату[4].

CMYK (Cyan, Magenta, Yellow, Key/Black) є розширеною версією моделі CMY, оскільки включає не три, а чотири канали. Чорний пігмент додається через те, що в реальних умовах суміш блакитної, пурпурової та жовтої фарб не здатна створити чистий, насичений чорний колір. На це впливають домішки, оптичні властивості та хімічний склад друкарських фарб. Використання окремого чорного шару дозволяє отримати глибокі тіні, підвищити різкість шрифтів і водночас зменшити витрату кольорових фарб.

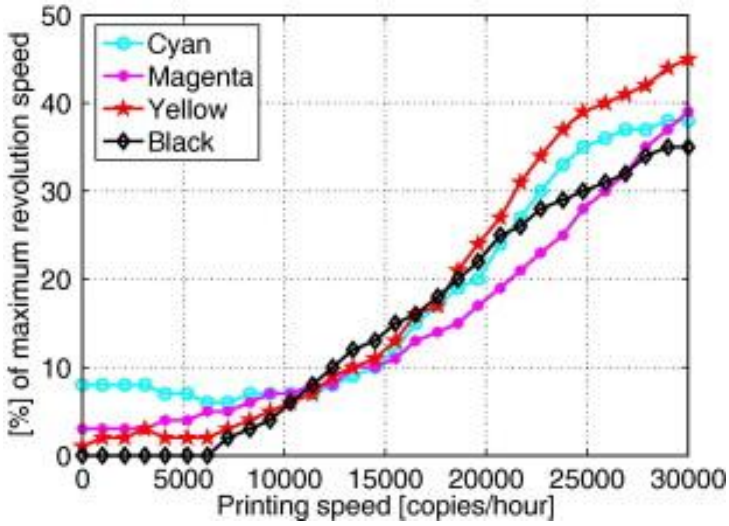


Рисунок 4 - графік накладання фарб за моделлю CMYK

По осі X задано швидкість друку в одиницях відбитків/годину - від 0 до 30 000 копій. По осі Y відображено відсотковий рівень обертів фарбових циліндрів відносно їх максимальної можливої швидкості. Графік дозволяє оцінити, як кожний кольоровий канал реагує на збільшення продуктивності, а також визначити нелінійні ділянки, де змінюється характер росту швидкості обертання

Cyan (блакитна крива). У початковому діапазоні до ~8000 коп./год значення стабільні і знаходяться близько 10%. Після 10 000 відбитків спостерігається поступове зростання швидкості. На максимальному режимі (≈ 30 000 коп./год) крива сягає близько 35% максимальної швидкості.

Magenta (червона крива). Спочатку демонструє дещо нижчі значення, ніж Cyan - на рівні 5-7%. Після 10 000 відбитків зростає швидше. Досягає приблизно 30–32% при максимальній швидкості друку.

Yellow (жовта крива). Має найбільш стрімке зростання серед усіх кривих. У діапазоні 20 000-25 000 коп./год відбувається різкий приріст обертів. У кінцевій точці (30 000 коп./год) значення сягають понад 45%, що є максимальним серед усіх фарбових каналів. Це свідчить про більшу чутливість жовтої фарби до зміни швидкості друку або про її фізичні властивості, які потребують більш інтенсивного накату фарби.

Black (чорна крива). Початкова швидкість найменша серед усіх (≈ 2-3%). Повільно наростає до рівня Cyan і Magenta. При максимальних швидкостях наближається до 30-33%.

На всіх кривих простежується різке зростання після досягнення швидкості ~10 000 коп./год. Це пояснюється особливостями фарбопередачі та потребою компенсувати інерційні втрати при високих передачах. Графік демонструє

коректну роботу системи управління: при збільшенні продуктивності друкарська машина автоматично підвищує подачу фарби відповідно до потреб технологічного процесу.

Проаналізовані випробування підтверджують, що основним фактором підвищення ефективності є комплексність підходу: поєднання апаратних сенсорів, програмних модулів і централізованої бази даних. Система забезпечує прозорість виробничих процесів, створює умови для оптимізації планування та дозволяє прогнозувати потреби виробництва з високою точністю.

Завдяки архітектурі система може масштабуватися, розширюватися шляхом підключення додаткових сенсорів, інтеграції з ERP-рішеннями або впровадження модулів контролю якості продукції. Це робить її перспективною платформою для цифрової трансформації поліграфічного підприємства.

Висновок. У ході дослідження було розроблено та впроваджено комп'ютерно-інтегровану систему автоматизації обліку продукції для виробничого складу поліграфічного підприємства. Запропоноване рішення поєднує апаратні сенсори, промислові контролери, програмні модулі аналізу та єдину базу даних, що забезпечує точний контроль руху матеріалів і готової продукції в режимі реального часу. Система продемонструвала високу ефективність: зменшення виробничих витрат на 11%, скорочення часу облікових операцій на 30% і суттєве зниження впливу людського фактора. Вона забезпечує прозорість виробничих процесів, стабільність технологічних параметрів друку та підвищує якість управління ресурсами. Завдяки модульній архітектурі розроблене рішення є масштабованим і може легко інтегруватися з сучасними ERP-системами, що відкриває перспективи подальшого розвитку та цифрової трансформації підприємства

Перелік використаних джерел.

1. Биков В. Ю., Спірін О. М., Шишкіна М. П. Інформаційно-комунікаційні технології в сучасному виробництві: методологія, інструменти, застосування. – Київ: Логос, 2020. – 284 с.

2. Клепіков В. О., Костенко В. Г. Автоматизовані системи управління технологічними процесами: навчальний посібник. – Харків: ХНУРЕ, 2019. – 312 с

3. Зоренко О. В., Соловей В. П. Технології поліграфічного виробництва та автоматизація контролю якості друку. – Львів: Українська академія друкарства, 2021. – 228 с.

4. Скляр В. М., Кривенко С. П. Комп'ютерно-інтегровані системи обліку та моніторингу у промислових підприємствах. – Київ: КНУТД, 2022. – 196 с.

УДК 66.078.2

Мукомела Р.В, Жовток В.В., Біловус Д.П.

Західноукраїнський національний університет

АВТОМАТИЗОВАНА СИСТЕМА КЕРУВАННЯ КОМПРЕСОРНИМ АГРЕГАТОМ

Вступ. У сучасних умовах інтенсивного розвитку промисловості та енергетики особливе значення набуває ефективне використання технічних ресурсів і впровадження автоматизованих систем керування. Компресорні агрегати часто є невід'ємною частиною більшості технологічних процесів – вони забезпечують подачу стисненого повітря, газу або іншого робочого середовища для приводу пневматичного обладнання, транспортування матеріалів, охолодження, вентиляції тощо. Їхня безперервна і надійна робота визначає стабільність функціонування всього виробництва [1-3].

Проте в більшості підприємств досі експлуатуються застарілі системи керування компресорними установками, які мають низький рівень автоматизації, не дозволяють ефективно регулювати робочі параметри, не враховують зміни навантаження та зовнішніх умов. У результаті це призводить до перевитрати електроенергії, частих аварійних зупинок, підвищеного зносу механічних вузлів і погіршення загальної економічної ефективності виробництва.

Проблема енергозбереження та підвищення ефективності роботи компресорних систем є особливо актуальною в умовах постійного зростання вартості електроенергії та необхідності зниження собівартості промислової продукції [4-6]. Одним із найбільш перспективних шляхів вирішення цих завдань є розроблення та впровадження автоматизованих систем керування, які забезпечують інтелектуальне регулювання роботи компресорних агрегатів, контроль їх технічного стану та адаптацію до змінних режимів експлуатації.

Автоматизована система керування компресорним агрегатом дозволяє не лише оптимізувати технологічні параметри – тиск, температуру, витрату повітря чи газу, – але й реалізувати моніторинг стану обладнання в реальному часі, виявлення несправностей, прогнозування технічного обслуговування та інтеграцію у загальну виробничу інформаційну систему підприємства. Це сприяє підвищенню рівня цифровізації виробництва, переходу до концепції «розумного заводу» (Smart Factory) та забезпечує досягнення високих показників надійності й енергоефективності.

Таким чином, актуальність теми зумовлена необхідністю розроблення сучасних автоматизованих систем керування компресорними агрегатами, які відповідають вимогам промисловості до енергозбереження, гнучкості, надійності та інтеграції з комп'ютерно-інтегрованими технологіями [7].

Мета: дослідження автоматизована система керування компресорним агрегатом.

1 Склад та призначення окремих вузлів компресорної установки

До складу стаціонарної компресорної установки входять: поршневий крейцкопфний компресор, електродвигун, а також системи охолодження, змащування, автоматичного керування та захист [1].

Поршневий компресор крейцкопфний з оппозитним чи кутовим розташуванням циліндрів. Конструкції компресорів побудовані на основі прийнятих на заводі-виробнику нормальних параметричних рядів діаметрів циліндрів. Основою параметричних рядів є оппозитна база 4М та кутові бази 5П та 2П, проте зустрічаються і спеціально розроблені системи для орієнтованого виробництва типу 5ГЦ, 5РЦ.

Компресор включає такі основні вузли: базу, циліндри, систему охолодження та привід.

База складається з уніфікованих вузлів кривошипно-шатунного механізму (колінчастого валу, шатуна та крейцкопфа), рами, блоку змащення механізму руху та багатоплунжерного насоса (для змащення циліндрів та ущільнювальних пристроїв штоків). У компресорах без змащування багатоплунжерний насос (мастильна станція) відсутній.

Рама виготовлена з чавунна методом лиття, уформі коробки з внутрішніми ребрами жорсткості. У верхній частині рами передбачені люки, що щільно закриваються кришками, які забезпечують доступ до деталей механізму руху. Нижня частина рами служить резервуаром для масла. На верхній частині рами встановлено покажчик рівня масла. Для кріплення циліндрів компресора до рами є спеціальні наплави. В отворах поперечних ребер рами встановлені крейцкопфні чавунні гільзи, що є направляючими для крейцкопфів. При зношенні гільзи можуть бути повернуті на певний кут або замінені новими.

Сталевий колінчастий вал – штампований, з кривошипами для встановлення шатунів, спирається на роликові підшипники (для кутових баз колінчастий вал виконується однокривошипним, для врівноваження на вал встановлюються противаги). На одному кінці колінчастого валу встановлений ротор електродвигуна (з'єднання шпонкове), а в закріпленому на торці валу фланці виконано квадратний отвір для забезпечення провертання валу компресора за допомогою рукоятки перед запуском. (Рукоятка входить до комплекту ЗІП). На іншому кінці валу кріпиться шестерня передачі обертання валу масляного насоса блоку змащування.

Крейцкопфи виготовляються разом з повзунами з чавуна або алюмінію методом лиття або штампування. Крейцкопф з'єднаний із штоком гайкою та контргайкою, законтреними стопорними болтами. З шатуном крейцкопф з'єднується за допомогою пальця. Пальці крейцкопфів – сталеві, при складанні запресовуються в крейцкопф і стопоряться пружинними кільцями.

Шатуни виготовлені штампуванням зі сталі двотаврового перерізу. Шатун має кривошипну головку з відокремленою кришкою та нероз'ємну крейцкопфну головку. Рознімні вкладиші кривошипної головки з антифрикційним шаром із алюмінієвого сплаву. У крейцкопфну голівку запресовано бронзову втулку. Змащування пальця крейцкопфа здійснюється через отвір шатуна.

Кришка кривошипної головки шатуна з'єднується із стрижнем шатуна, двома шатунними болтами з легованої сталі та гайками. На головці кожного шатунного болта вказується початкова довжина, необхідна для оцінки залишкового подовження болта за час експлуатації.

Одноступінчасті компресори мають циліндри подвійної дії однакового діаметра. У двоступінчастих компресорах встановлені циліндри подвійної дії різного діаметра.

У триступінчастих – циліндр першого ступеня подвійної дії, циліндри другого і третього ступенів об'єднані в одному блоці, з диференціальним поршнем і з вирівнюючою порожниною між ступенями.

У чотириступінчастих застосовуються два циліндри з диференціальним поршнем з вирівнюючою порожниною. У п'ятиступінчастих в одному ряду встановлений циліндр з двома, а в іншому з трьома ступенями стиснення, при цьому поршень першого ступеня подвійної дії.

Циліндри наступних степенів багатоступінчастих компресорів виготовлені з різних матеріалів залежно від робочого газу та кінцевого тиску, більшість мають змінні робочі гільзи із спеціального зносостійкого чавуну, що ущільнюються по діаметру гумовими кільцями, а по торцю паронітовими прокладками. Клапани (всмоктувальні та нагнітальні) – пластинчасті кільцеві, прямоточні та стрічкові закріплюються в гніздах натискним стаканом та опорними болтами або натискними шпильками з ковпачковими гайками. У ступенях високого тиску встановлюються комбіновані клапани, що складаються з всмоктувальних та нагнітальних клапанів.

Ущільнення циліндрів, люків, клапанних кришок та фланцевих з'єднань забезпечується застосуванням паронітових прокладок, а на ступенях високого тиску встановлюються прокладки з м'якої міді.

Поршні виготовляються з чавуну, алюмінію або сталі. На одно- і двоступінчастих компресорах - дискові, подвійної дії, на багатоступінчастих диференціальні.

Поршневі кільця як правило – чавунні. У компресорах без мастила циліндрів застосовуються кільця з композиційних матеріалів, що самозмащуються. Штоки виготовлені із вуглецевої сталі з поверхневим ущільненням. Узагальнену схему виконання поршневого компресора представлено на рисунку 1.

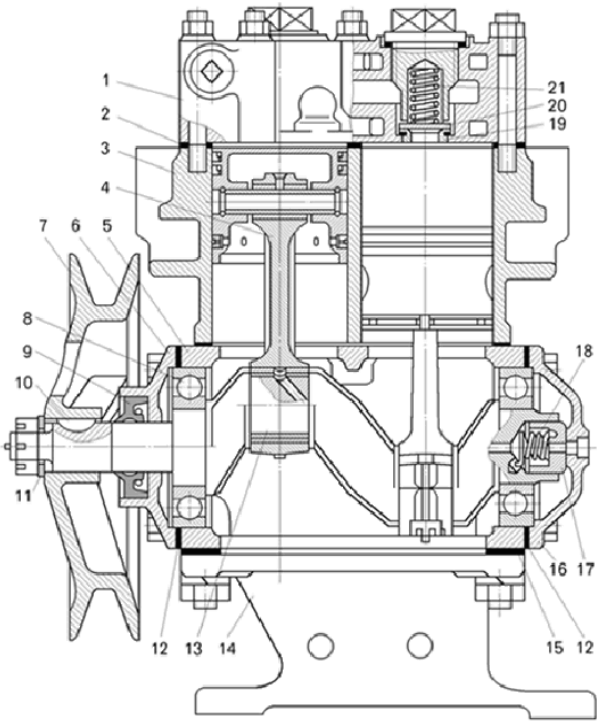


Рисунок 1 – Узагальнена схема стандартного виконання поршневого компресора

На рисунку 1 позначено: 1 – головка блоку циліндрів; 2 – прокладка головки блоку; 3 – блок циліндрів; 4 – шатун; 5 – картер; 6 – передня кришка; 7 – шків; 8 – шарикопідшипник; 9 – ущільнювальна манжета; 10 – шпонка; 11 – шайба; 12, 15 – прокладки; 13 – колінчастий вал; 14 – нижня кришка картера; 16 – задня кришка; 17 – ущільнювач; 18 – пружина ущільнювача; 19 – сідло;20 – нагнітальний клапан; 21 – пружина клапана.

2. Загальна структура та функціонування системи автоматизованого управління компресорною установкою

Найбільш сучасним є регулювання за допомогою перетворювачів частоти, які дозволяють плавно регулювати частоту обертання електродвигуна компресора і підтримувати тиск в системі при різних витратах газу, що перекачується. При малих витратах газу двигун компресора обертається з малою швидкістю, необхідної лише підтримки номінального тиску, і витрачає зайвої енергії. При збільшенні витрати газу перетворювач збільшує частоту обертання електродвигуна, підвищуючи продуктивність компресора за збереження заданого тиску.

На рисунку 2 показано функціональну схему регулювання електродвигуна компресора з використанням перетворювача частоти Micromaster440 фірми «Siemens».

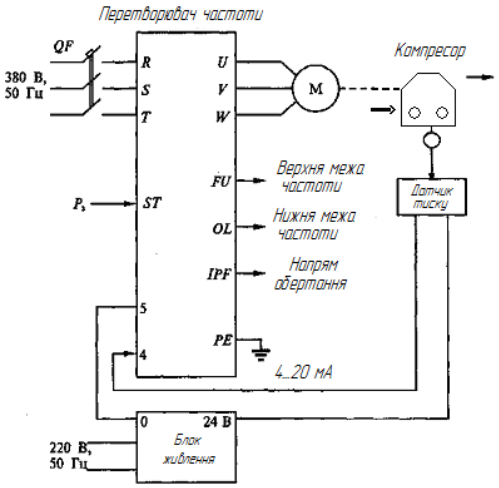


Рисунок 2 – Функціональна схема регулювання електродвигуна компресора з використанням перетворювача частоти

На вхід системи подаються сигнали завдання тиску та сигнал реального тиску, що отримується з датчика тиску, встановленого в ланцюзі зворотного зв'язку. Відхилення між реальним та заданим значеннями тиску перетворюється ПІД-регулятором на сигнал завдання частоти для перетворювача. Під впливом сигналу завдання перетворювач змінює частоту обертання електродвигуна компресора та прагне привести різницю між заданим та реальним значеннями до нуля.

Ця схема є модульною і застосовна до створення проекту, у якому буде реалізований алгоритм управління.

Сучасні перетворювачі частоти дозволяють створювати системи управління (СУ) без додаткових апаратних засобів, оскільки мають вбудовані програмні функції, що дозволяють реалізовувати порівняльний вузол і ПІД-регулятор [7]. Однак у складних системах регулювання тиску в системі з використанням простих

засобів реєстрації не дає бажаного ефекту. Тому даний спосіб регулювання поєднують з мікропроцесорною системою управління [8].

Система управління (рисунок 3) включає мікропроцесорну систему і перетворювач частоти, що дозволяє регулювати подачу компресора зміною його частоти обертання.

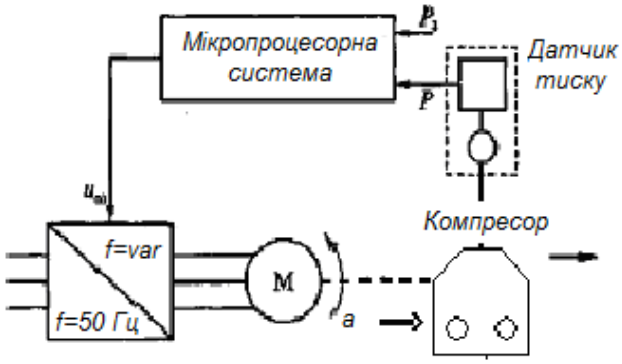


Рисунок 3 – Мікропроцесорна система управління

Функції залежності вхідних та вихідних сигналів, правила прийняття рішень формуються на основі програми, «зашитої» в контролер даної системи, що стежить за перебігом технологічного процесу.

3. Апаратна реалізація системи управління компресорною установкою.

Для ефективного управління компресорною установкою використаємо платформу DeltaV. Системи DeltaV ефективно використовуються управління мережами різних розмірів. Система DeltaV має можливості гнучкого планування та моделювання розмірів мережі таким чином, щоб система найбільш повно відповідала вимогам управління процесом. Мінімальний набір компонентів для системи DeltaV представлений на рисунку 4, де показано кількість робочих станцій та контролерів з усім необхідним обладнанням, яке має бути включене до системи.

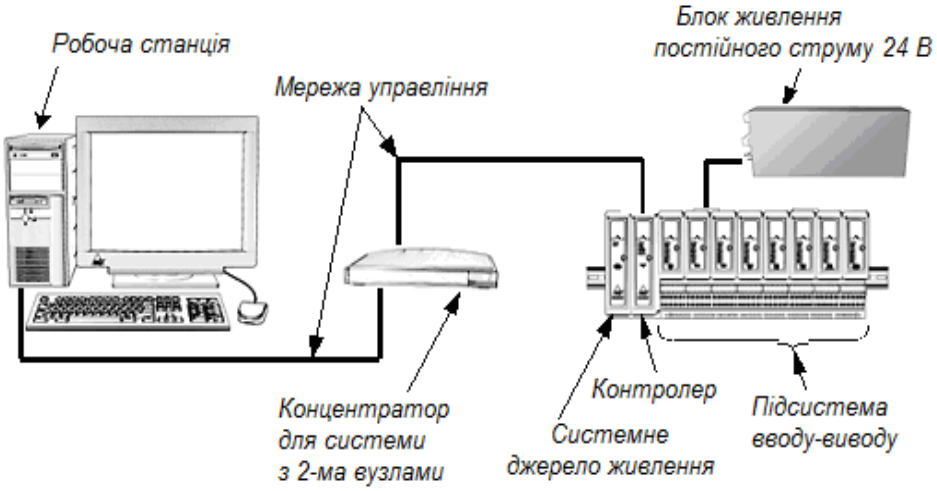


Рисунок 4 – Мінімальний комплект системи DeltaV

Система DeltaV підтримує уніфіковані аналогові сигнали 4-20 мА, 1-5 В, мілівольтні, омічні сигнали, стандартні вхідні сигнали термопари та термоопір. Це найбільш підходящий стандарт підключення блоків, т.к. більшість аналогових сенсорів

працює саме у такому режимі (4-20 мА).

Кожна плата послідовного інтерфейсу має 2 порти. Кожен порт підтримує до 16 наборів даних. Набір даних є безперервною областю до 100 регістрів/реле в ПЛК. Якщо порт налаштований як RS-485, можна використовувати шлейфове підключення пристроїв. 16 наборів даних можуть бути розподілені за будь-якою кількістю пристроїв від 1 до 16, залежно від обсягу та структури даних. У разі порт необхідний зчитування інформації що зберігається в ПЛК, і навіть організації місцевого пульта спостереження, реалізує функції тестування.

Інтелектуальна панель H1 – це 2-слотова панель, що встановлюється поруч із польовими пристроями. Панель, що несе, з платою дискретного входу і дискретного виходу забезпечує перетворення звичайних дискретних сигналів у сигнал польової шини FOUNDATION. Завдяки цьому можлива передача дискретних сигналів у тому ж сегменті польової шини, де передаються аналогові сигнали, що сприяє скороченню сегментів, що купуються, а це економія в споживаній потужності.

Панель H1, що несе, стикується з сегментом польової шини, як будь-який інший пристрій польової шини. Живлення до несучої панелі та встановлених плат дискретного введення-виведення підводиться від додаткового зовнішнього джерела. Панель, що несе, кріпиться на рейці DIN (можлива установка тільки на Т-рейку), стіні або панелі

Плати H1 польової шини FOUNDATION встановлюються на стандартній 8-слотовій панелі DeltaV, що несе. Кожен модуль Fieldbus H1 дозволяє підключити два сегменти польової шини. На кожному сегменті H1 система підтримує до 16 пристроїв. У загальному випадку система набуде вигляду, представленого на рисунку 5.

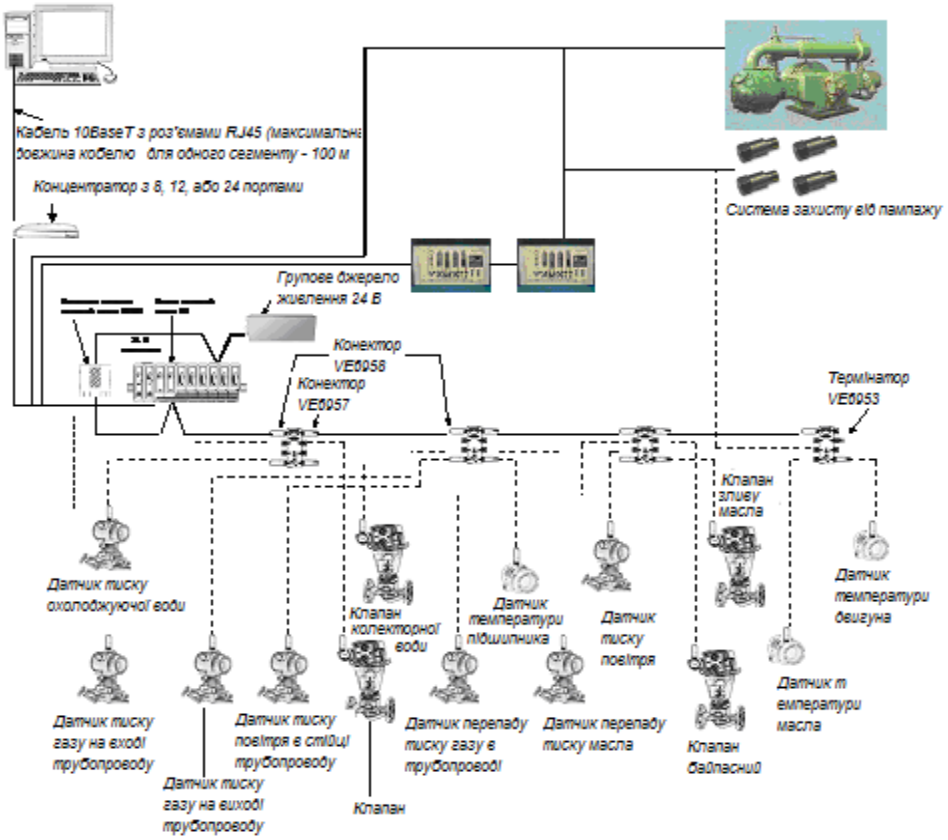


Рисунок 5 – Структурна схема САУ компресора

Висновок. Запропонована система автоматизованого управління на базі DeltaV дозволить підвищити ефективність функціонування комплексу гідроочищення за рахунок оптимального режиму роботи компресорної установки, підвищення продуктивності обладнання та оперативності управління технологічним процесом, зниження споживання енергоресурсів, а також знизити аварійність та збільшити термін служби обладнання, зменшити вплив людського фактора у виробничому процесі та експлуатації

Впровадження такої САУ надає широкі можливості щодо інтеграції її з іншими існуючими або новоствореними системами і, при необхідності, без значних витрат , може розширити свої функціональні можливості і нарощувати кількість каналів обробки сигналів. В подальшому система відкрита до впровадження нейронних мереж для підвищення її можливостей та ефективності [10]/

Перелік використаних джерел.

1. US Department of Energy. Improving compressed system performance: a sourcebook for industry. –Washington : U.S. Department of EERE,2003. – 128 c

2. Brian S. Elliott. (2006) Compressed Air Operations Manual. - McGraw-Hill Education – 2006,407 p.ISBN: 978-0-07-149184-6 MHID: 0-07-149184-8.

3. Neil Mehltretter(2012), “Proper Application of Variable Speed Compressors”. World Energy Engineering Congress,2012 ,999-1015 p.

4. Radgen P. (2006). Mission 6.2: Energy Efficiency, Режим доступу: http://okolje.arso.gov.si/ippc/uploads/File/ Compressed_air_en.pdf :[13.04.2019]

5. Don van Ormer (2017). [Електронний ресурс]. Режим доступу: https://www.airbestpractices.com/ system-assessments/compressor-controls/central-monitoring-and-control-multiple-air-compressors

6. Energy Efficiency of Compressed Air Systems/ Smaeil Mousavi,Sami Kara, Bernard Kornfeld// 21 st CIRP Conference on Life Cycle Engineering/ Procedia CIRP,2014. – 313-318p.

7. Chunyue PAN(2017) Air Compressor Pressure Control System Based On Gearshift Integral PID Controller. MATEC Web of Conferences 139, 00199 (2017) ICMITE 2017 DOI: 10.1051/matecconf/201713900199. [Електронний ресурс]. Режим доступу: https://www.matec-conferences.org/articles/matecconf/pdf/2017 /53/matecconf_icmite2017_00199.pdf.

8. Chris Schmidt, Kelly Kissock (2005) Modeling and Simulation of Air Compressor Energy Use. ACEEE Summer Study on Energy Efficiency in Industry,July 19-22, 131 – 142p. [Електронний ресурс]. Режим доступу: https://aceee.org/files/proceedings/2005/data/index.htm.

9. Офіційний сайт Компанії Emerson. [Електронний ресурс]. Режим доступу: https://www.emerson.com/ru-am/automation/deltav

10. J. Javadi Moghaddam, M. Madani (2010) A decoupled adaptive neuro-fuzzy sliding mode control system to control rotating stall and surge in axial compressors Expert Systems with Applications Volume 38, Issue 4, April 2011, Pages 4490-449 https://doi.org/10.1016/j.eswa.2010.09.122 .

УДК 004

Остап ЛУКАШ

Західноукраїнський національний університет

АНАЛІЗ ВРАЗЛИВОСТЕЙ ТА КЛАСИЧНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СМАРТ-КОНТРАКТІВ

Вступ. З розвитком технологій блокчейн смарт-контракти стали ключовим елементом децентралізованих систем. Смарт-контракти - це цифрові угоди, які автоматично виконують транзакції при настанні певних умов. Вони працюють на платформах, таких як Ethereum Virtual Machine (EVM), і дозволяють виконувати процеси без посередників. Однак їхня незмінність гарантує, що після впровадження код не може бути змінений, що робить питання безпеки критичним.

Мета. Метою роботи є класифікація основних вразливостей смарт-контрактів та порівняльний аналіз існуючих методів виявлення дефектів коду, таких як статичний аналіз, фаззінг та формальна верифікація.

1. Класифікація критичних вразливостей.

Безпека смарт-контрактів має першочергове значення через незворотний характер транзакцій. Один-єдиний недолік може призвести до значних фінансових втрат, як це сталося під час атак на DAO та Parity Wallet [1]. Основні типи вразливостей виникають через логічні помилки або особливості середовища виконання:

- Reentrancy: Використання функції зовнішнього виклику, що дозволяє повторювати виклики до завершення початкової функції. Саме ця вразливість дозволила зловмисникам викрасти кошти з DAO.
- Integer Overflow/Underflow: Результати арифметичних операцій, які перевищують ємність пам'яті типу даних.
- Front-Running: Використання часового проміжку між трансляцією транзакції та її включенням до блокчейну.
- Access Control: Дозвіл неавторизованим користувачам отримувати доступ до критичних функцій, наприклад, initWallet у випадку Parity Wallet.

2. Огляд методів аналізу безпеки.

Для виявлення зазначених вразливостей використовуються три основні підходи. Статичний аналіз коду. Інструменти статичного аналізу перевіряють код без його виконання. До найпоширеніших належать:

- Mythril: Використовує символьне виконання та аналіз забруднення для виявлення переповнень та інших дефектів [2].
- Securify: Розроблений Ethereum Foundation, аналізує байт-код EVM для визначення семантичних фактів та відповідності шаблонам вразливостей [3].
- Slither: Будує граф потоку управління та діаграми успадкування, дозволяючи швидко знаходити вразливості та оптимізувати код [4].

Динамічний аналіз та фаззінг. Fuzzing - це метод динамічного аналізу, при якому інтерфейс програми отримує неправильно сформовані вхідні дані для виявлення

аномальної поведінки. Це економічно ефективний спосіб знаходження невідомих помилок ("black box" тестування), який не вимагає знання вихідного коду.

Формальна верифікація. Це сувора техніка, що використовує математичні докази для гарантування правильності системи. Вона забезпечує всебічне дослідження шляхів виконання, усуваючи певні класи помилок. Проте цей метод є складним у впровадженні та погано масштабується для великих проектів.

У Таблиці 1 наведено порівняння основних вразливостей, які виявляються цими методами.

Таблиця 1 – Основні компоненти системи безпеки Kubernetes

Вразливість	Опис
Reentrancy	Використовує функцію зовнішнього виклику контракту, що дозволяє повторювати виклики до завершення початкової функції.
Integer Overflow/Underflow	Результати арифметичних операцій, які перевищують ємність пам'яті типу даних.
Improper Access Control	Дозволити неавторизованим користувачам отримувати доступ до даних або функцій контракту (наприклад, незахищене зняття коштів) або змінювати їх через недостатні обмеження доступу.
Front-Running	Використовує часовий проміжок між трансляцією транзакції та її включенням до блокчейну

Висновок. Традиційні методи аналізу, такі як статичні аналізатори, базуються на фіксованих правилах, що призводить до високого рівня хибно-позитивних спрацювань. Динамічний аналіз та фаззінг вимагають значних ресурсів і не завжди покривають всі шляхи виконання. Для підвищення надійності смарт-контрактів необхідно застосовувати комбінований підхід, що поєднує інструменти на кшталт Slither та Mythril із методами формальної верифікації для критичних ділянок коду.

Перелік використаних джерел.

1. Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack. [Електронний ресурс]. Режим доступу: https://www.semanticscholar.org/paper/Understanding-a-Revolutionary-and-Flawed-Grand-in-Mehar-Shier/e40e6ca0778a1bdf04cc99a318b220c2ff40e889

2. Mythril: Security analysis tool for Ethereum smart contracts. [Електронний ресурс]. Режим доступу: https://github.com/ConsenSys/mythril

3. Securify: Practical Security Analysis of Smart Contracts. [Електронний ресурс]. Режим доступу: https://files.sri.inf.ethz.ch/website/papers/ccs18-securify.pdf

4. Slither – a Solidity static analysis framework. [Електронний ресурс]. Режим доступу: https://blog.trailofbits.com/2018/10/19/slither-a-solidity-static-analysis-framework/

УДК 681.32

Ілля Довгалюк, Олег ЗАСТАВНИЙ

Західноукраїнський національний університет

ПІДВИЩЕННЯ ЕНЕРГОЕФЕКТИВНОСТІ ПРОЦЕСУ ПЕРІОДИЧНОЇ РЕКТИФІКАЦІЇ ШЛЯХОМ ВПРОВАДЖЕННЯ СИСТЕМИ МОДЕЛЬНО-ПРОГНОЗУЮЧОГО КЕРУВАННЯ

Вступ: у сучасній харчовій та хімічній промисловості процес ректифікації залишається одним із найбільш енергоємних технологічних етапів. Для підприємств малої та середньої потужності, що спеціалізуються на виробництві високоякісних спиртів та дистилятів, критично важливими є питання стабільності якості продукції та мінімізації виробничих витрат. Специфікою таких виробництв є використання установок періодичної дії (batch distillation), які функціонують в умовах нестаціонарності: склад кубової рідини та температури кипіння суміші безперервно змінюються в часі [1].

Традиційні системи автоматизації, що базуються на каскадних схемах з використанням незалежних пропорційно-інтегрально-диференціальних (ПІД) регуляторів, часто виявляються недостатньо ефективними для керування такими об'єктами. Це обумовлено наявністю значних транспортних запізнень, інерційністю теплових процесів та, що найважливіше, сильним взаємним впливом (coupling) між каналами регулювання нагріву та охолодження. Неузгодженість дії контурів призводить до виникнення автоколивань та непродуктивних витрат енергії.

У роботі вирішується актуальна науково-технічна задача автоматизації процесу періодичної ректифікації спирту на установках гібридного типу. Проведено аналіз динамічних характеристик об'єкта та обґрунтовано необхідність модернізації виконавчої підсистеми шляхом заміни газового нагріву на електричний для забезпечення лінійності каналу керування. Розроблено математичну модель процесу у просторі станів та здійснено синтез багатозв'язкового MPC-регулятора з урахуванням технологічних обмежень. За результатами симуляційного моделювання встановлено, що запропонований підхід дозволяє знизити енергоспоживання на 10,2% та зменшити дисперсію температури на контрольній тарілці в 1,8 рази порівняно з традиційним ПІД-регулюванням.

Мета: підвищення енергетичної ефективності та якості керування процесом періодичної ректифікації шляхом розробки та впровадження системи модельно-прогнозуючого керування (Model Predictive Control - MPC), адаптованої до модернізованої апаратної частини установки.

1. Аналіз об'єкта керування та обґрунтування модернізації

Об'єктом дослідження є гібридна ректифікаційна установка лабораторного типу з робочим об'ємом куба 120 л. Конструкція колони поєднує в собі чотири ситчасті тарілки у нижній частині та насадкову царгу з мідним наповнювачем у верхній частині. Така конфігурація дозволяє досягти високого ступеня розділення та зберегти органолептичні властивості продукту, проте створює складну гідродинамічну

картину процесу [2].

З точки зору теорії автоматичного керування, установка класифікується як багатовимірний об'єкт (MIMO - Multiple Input Multiple Output) з розподіленими параметрами. Аналіз вихідного проекту прототипу виявив критичний недолік у виконавчій підсистемі - використання газового пальника як джерела тепла. Газовий нагрів характеризується високою інерційністю, нелінійною залежністю теплового потоку від положення клапана та залежністю від тиску в магістралі. Це унеможливлює побудову точної математичної моделі, що є необхідною умовою для роботи MPC.

У зв'язку з цим, в рамках роботи запропоновано та обґрунтовано модернізацію системи шляхом переходу на високоточний електричний нагрів (ТЕН) з тиристорним керуванням. Це дозволяє:

- Лінеаризувати статичну характеристику каналу «сигнал керування – теплова потужність».
- Зменшити постійну часу нагріву за рахунок виключення проміжних теплоносіїв.
- Забезпечити точне дозування енергії, що є критичним для алгоритмів оптимізації.

В якості керованих змінних (inputs) обрано електричну потужність ТЕНу (P_{heat}) та витрату охолоджуючої води в дефлегматор (F_{cool}). Регульованими змінними (outputs) є температура на контрольній (третій) тарілці колони та температура в кубі.

2. Розробка математичної моделі та синтез MPC-регулятора

Для синтезу системи керування було застосовано підхід, що базується на моделі («Model-Based Design»). На першому етапі розроблено нелінійну динамічну модель установки ("Digital Twin"), яка складається з системи диференціальних рівнянь матеріального та теплового балансу для кожного елемента установки (куба, тарілок, дефлегматора). Модель враховує фазову рівновагу бінарної суміші етанол-вода та гідродинаміку рідини на тарілках.

Для використання в алгоритмі лінійного MPC модель було лінеаризовано в околі робочої точки ($T_{set} = 78.1^{\circ}C$) та приведено до канонічної форми простору станів:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \end{cases},$$

де x(t) - вектор змінних стану (температури та концентрації по висоті колони),

$u(t)$ - вектор керування, y(t) - вектор вимірюваних виходів.

Синтез контролера полягав у формулюванні задачі квадратичної оптимізації, яка розв'язується на кожному кроці дискретизації. Цільова функція (Cost Function) J має вигляд:

$$J = \sum_{k=1}^{N_p} \left(w_y \left(y_{ref}(k) - y(k) \right)^2 \right) + \sum_{k=1}^{N_c} \left(w_u \left(\Delta u(k) \right)^2 \right) \rightarrow min,$$

де перший доданок відповідає за мінімізацію помилки регулювання (якість продукту), а другий - штрафує систему за агресивні зміни керуючих впливів, що забезпечує плавність роботи та економію ресурсу виконавчих механізмів.

Вагові коефіцієнти w_y та w_u налаштовано таким чином, щоб пріоритетом була стабілізація температури при мінімально необхідній потужності нагріву. Також в

алгоритм інтегровано жорсткі обмеження (constraints) на фізичні межі виконавчих механізмів ($0 \le P_{heat} \le P_{max}$), що гарантує безпеку процесу [3].

3. Результати симуляційного моделювання та аналіз ефективності

Верифікація розробленої системи проводилася шляхом порівняльного моделювання в середовищі MATLAB/Simulink. Було створено два віртуальні стенди: «Базова система» (класичний ПІД-регулятор) та «Нова система» (синтезований МРС). Сценарій експерименту передбачав стабілізацію температури в умовах дії зовнішніх збурень (імітація зміни параметрів охолодження).

Аналіз отриманих перехідних процесів (рисунок 1) показав суттєву перевагу МРС-підходу.

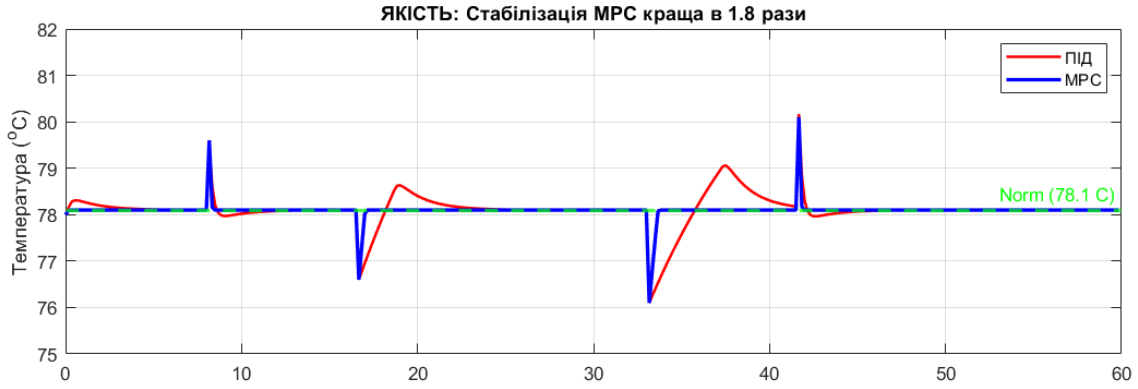


Рисунок 1 - Графіки перехідних процесів температури на контрольній тарілці

Система з ПІД-регулятором демонструє характерну коливальну поведінку з перерегулюванням, оскільки реагує на збурення із запізненням. МРС-контролер, використовуючи прогнозну модель, компенсує збурення на ранній стадії. Розрахунок середньоквадратичного відхилення показав, що дисперсія температури для МРС зменшилася в 1,8 рази ($0{,}21 \le P_{heat} \le P_{max}$), що свідчить про значно вищу стабільність складу дистиляту.

Найвагомішим результатом є підвищення енергоефективності. Як видно з діаграми споживання потужності (рисунок 2), ПІД-регулятор реалізує енергетично невигідну стратегію: підтримує завищену потужність нагріву для гарантії кипіння, компенсуючи надлишок тепла збільшеною подачею флегми («газ і гальмо»).

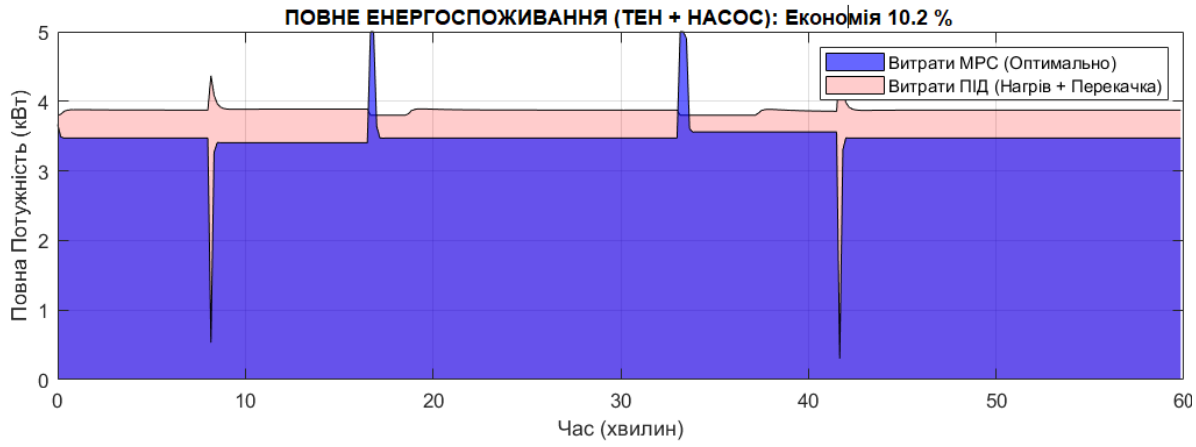


Рисунок 2 - Порівняльна діаграма споживання повної потужності (нагрів + перекачка)

MPC-алгоритм автоматично знаходить точку енергетичного оптимуму, знижуючи потужність нагріву до мінімально необхідного рівня. Інтегральна оцінка енергоспоживання за цикл показала економію електроенергії на рівні 10,2%. Крім того, плавність керування сприяє подовженню ресурсу ТЕНів та клапанів.

Висновок. У роботі вирішено актуальну науково-технічну задачу підвищення ефективності процесу періодичної ректифікації спирту шляхом комплексної модернізації системи керування. Проведений аналіз динамічних характеристик об'єкта підтвердив, що традиційні схеми автоматизації на базі ПІД-регуляторів є субоптимальними для керування даним багатовимірним процесом через його інерційність та наявність сильних перехресних зв'язків.

Обґрунтовано та запропоновано модернізацію виконавчої підсистеми шляхом заміни газового нагріву на електричний, що забезпечило лінійність каналу керування та стало необхідною передумовою для впровадження прецизійних алгоритмів. Розроблено математичну модель установки та синтезовано систему модельно-прогнозуючого керування (MPC), яка враховує технологічні обмеження та критерії енергоефективності.

Результати порівняльного симуляційного моделювання переконливо довели переваги запропонованого підходу: система з MPC забезпечила зменшення дисперсії температури на контрольній тарілці в 1,8 рази та зниження питомих енерговитрат на 10,2% порівняно з класичною системою. Це підтверджує перспективність впровадження MPC-алгоритмів для оптимізації роботи ректифікаційних установок періодичної дії.

Перелік використаних джерел.

1. Skogestad S. Control of distillation columns // Process Control. Springer, 2007. P. 359–408.

2. Довгалюк І. Р. Автоматизація процесу ректифікації спирту : Дипломна робота бакалавра. Тернопіль : ЗУНУ, 2024.

3. Qin S. J., Badgwell T. A. A survey of industrial model predictive control technology // Control Engineering Practice. 2003. Vol. 11. No. 7. P. 733–764.

4. Seborg D. E. et al. Process Dynamics and Control. 4th ed. Wiley, 2016.

УДК 004.891.3; 004.93.11

Сегін А.І., Рибін А.С., Мукомела Р.В.

АВТОМАТИЗОВАНА СИСТЕМА ДІАГНОСТИКИ ЧАСТОТНО-РЕГУЛЮВАЛЬНОГО АСИНХРОННОГО ЕЛЕКТРОПРИВОДУ

Вступ. Асинхронний електропривод є найбільш поширеним типом електроприводу, що широко використовується для приведення в рух і керування масовими механізмами. Найчастіше для живлення та керування асинхронним електродвигуном (АД) використовується дволанковий перетворювач частоти (ПЧ).

Сучасні промислові підприємства дедалі частіше застосовують частотно-регульовані асинхронні електроприводи завдяки їхній енергоефективності, гнучкості керування та високій надійності. Водночас зростає потреба у своєчасній та достовірній діагностиці їхнього технічного стану, оскільки навіть незначні несправності можуть призвести до зупинки виробничого процесу, фінансових втрат або аварій.

Традиційні методи діагностики, що базуються на візуальному огляді чи періодичному технічному обслуговуванні, є недостатньо ефективними в умовах інтенсивної експлуатації обладнання. У зв’язку з цим актуальним є впровадження автоматизованих систем моніторингу та діагностики, що забезпечують безперервний контроль за станом електроприводів у режимі реального часу [1-5].

Одним з перспективних підходів до підвищення ефективності діагностики є застосування спектрального аналізу електричних сигналів [3, 6-7], який дозволяє виявляти характерні ознаки пошкоджень на ранніх етапах розвитку несправностей. Це відкриває можливості для прогнозного технічного обслуговування та зниження витрат на ремонт.

Огляд літератури в галузі передиктивного аналізу стану електротехнічного обладнання показав, що на сьогоднішній момент актуальне завдання створення оптимальної ієрархічної системи збору та аналізу даних як для конкретного промислового об'єкта, так і створення універсального методу моніторингу та контролю стану електротехнічного обладнання реальному часі без виведення з експлуатації його елементів.

Таким чином, розробка автоматизованої системи діагностики частотно-регульованого асинхронного електроприводу з використанням спектрального аналізу є актуальним завданням, що відповідає сучасним тенденціям розвитку електроприводної техніки, цифровізації та промислової автоматизації.

Мета: дослідження автоматизована система діагностики частотно-регулювального асинхронного електроприводу

1. Теоретичне дослідження системи асинхронного електроприводу

Для дослідження системи перетворювача частоти асинхронного двигуна зі скалярним керуванням розглянуто функціональну електричну схему представлену на рисунку 1.

На рисунку 1.1 представлена схема дволанкового перетворювача частоти. Силова частина включає трифазний нерегульований випрямляч, автономний інвертор напруги, ланку постійного струму та гальмівний модуль.

Інвертор реалізований на шести транзисторах IGBT і працює в режимі широтно-імпульсної модуляції і перетворює нерегульовану напругу на виході випрямляча в регульовану за частотою і амплітудою першої гармоніки напругу на статорі асинхронного електродвигуна. Для здійснення гальмівних режимів паралельно конденсатору, підключений гальмівний ланцюжок із послідовно з'єднаного транзистора та резистора.

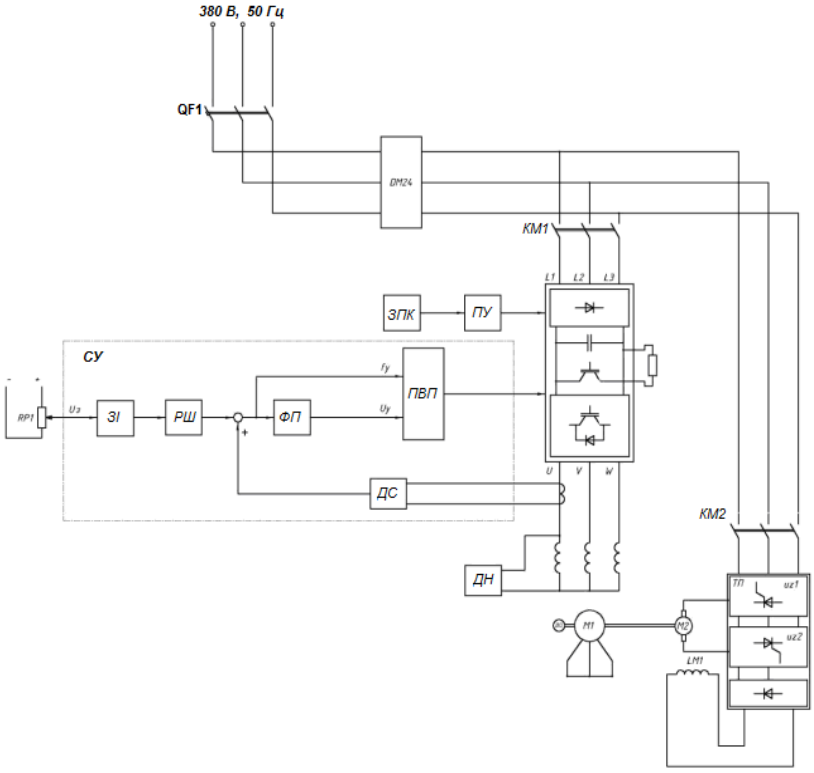


Рисунок 1 – Функціональна електрична схема перетворювача частоти

Основою системи керування електроприводом є програмований контролер, за допомогою якого здійснюється керуванням перетворювачем частоти. Управління інвертором здійснюється двома каналами: сигналом пропорційним заданій частоті і сигналом пропорційним заданій величині напруги.

Схема управління, представлена на рисунку 1, є розімкнутою скалярною схемою управління. На ній зображено регулятори, реалізовані у вигляді окремих блоків програми.

У даній роботі було застосовано метод половинного розбиття без урахування ймовірності виходу з ладу. В даному методі ймовірності технічних станів та ваги перевірок всіх логічних елементів рівні, тому першим перевіряється той, елементарна перевірка якого ділить навпіл всю множину логічних елементів по справних та несправних станах.

Відповідно, граф пошуку несправності об'єкта, що діагностується, за заданим методом пошуку несправності буде мати вигляд представлений на рисунку 2.

В результаті розроблено функціональну схеми системи, структуру логічної моделі, сформовано таблицю функцій несправності та побудовано граф пошуку несправності, шляхом половинного розбиття.

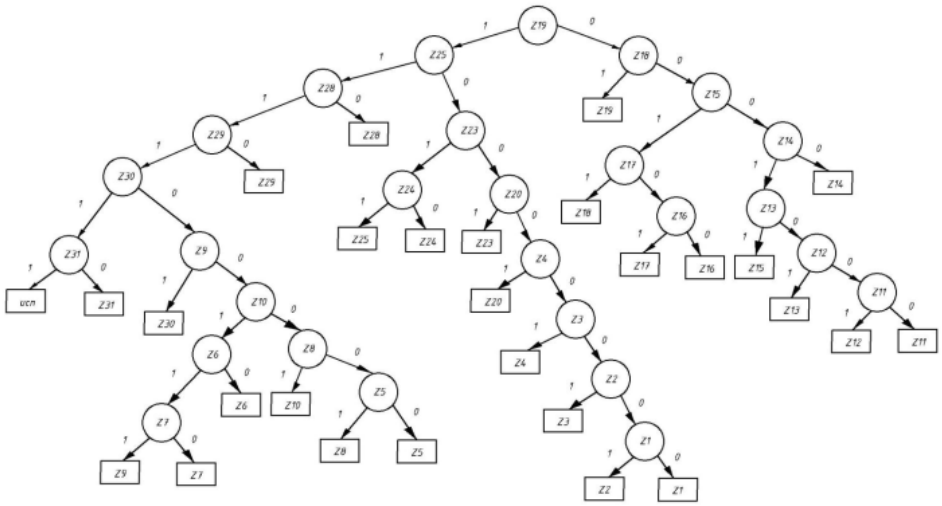


Рисунок 2 – Граф пошуку несправності

2. Аналіз несправностей асинхронного електродвигуна та їх типів

Поділяють внутрішні та зовнішні причини несправностей двигуна.

Внутрішні дефекти поділяються на механічні (ушкодження підшипників, і т. д.) та електричні (пробою ізоляції, пошкодження магнітного контуру, і т. д.). Зовнішні дефекти можуть бути механічними (поганий монтаж, пульсуючий навантаження, перевантаження), електричні (такі як коливання напруги), на рисунку 3 показана ймовірність появи різних дефектів в АТ:

Рисунок 3 – Ймовірність несправностей у АТ

Дефекти підшипників можуть бути поділені як розподілені або локальні. Розподілені дефекти включають хвилястість, шорсткість поверхні і елементи кочення без зміни. Локалізовані дефекти включають відскоки, ями та тріщини на поверхні кочення. Ці локалізовані дефекти створюють серію ударних вібрацій у той момент, коли рухливий валик проходить поверхнею дефекту, період та амплітуда якого знаходяться за положенням, швидкістю та наявного дефекту. Несправними підшипниками генеруються механічні коливання (вібрації). Ці збурення визначаються швидкості обертання кожного елемента. Габарити підшипника та швидкість обертання двигуна потрібні для визначення відповідних частот, пов'язаних з інтервалами кочення, а також кулями або роликами. Стан підшипник знаходиться шляхом аналізу цих частот. Ця проблема вирішується за допомогою методів механічного вібраційного аналізу.

Дефекти в обмотці статора, такі як коротке міжвиткове замикання, обрив ланцюга, міжфазне замикання і замикання фази із землею, є одними з найчастіших і отже – руйнівних несправностей. Якщо вони не ідентифіковані, тоді це може бути

причиною глобальної поломки двигуна, і як наслідок, повного виходу його з ладу. Дефекти ротора можуть бути викликані електричними несправностями, такими як обрив стрижня або механічні збої, такі як неспіввісність ротора. Перший дефект виникає через термічні дії, гарячі точки або перенапруги під час перехідних процесів, таких операцій як пуск, особливо в великогабаритних машинах. Обламаний стрижень ротора значно змінює момент і стає небезпечним для електричного двигуна. Другий вид дефекту ротора безпосередньо пов'язаний із нерівномірністю повітряного зазору. Ця проблема є загальним дефектом, пов'язаним із рядом механічних несправностей у машинах змінного струму, таких як дисбаланс навантаження або неспіввісність валу.

Неспіввісність валу означає горизонтальне, вертикальне або радіальне зміщення між валом та його зчепленим навантаженням. При неспіввісності валу ротор буде зміщений зі свого нормального положення через постійну радіальну силу.

Стандартна система діагностики, представлена рисунку 4, складається з вузла датчиків, який подає сигнал несправності блок обробки сигналів, який далі відправляє його результат для аналізу експертними системами, де в кінцевому підсумку виявляється відповідна несправність.

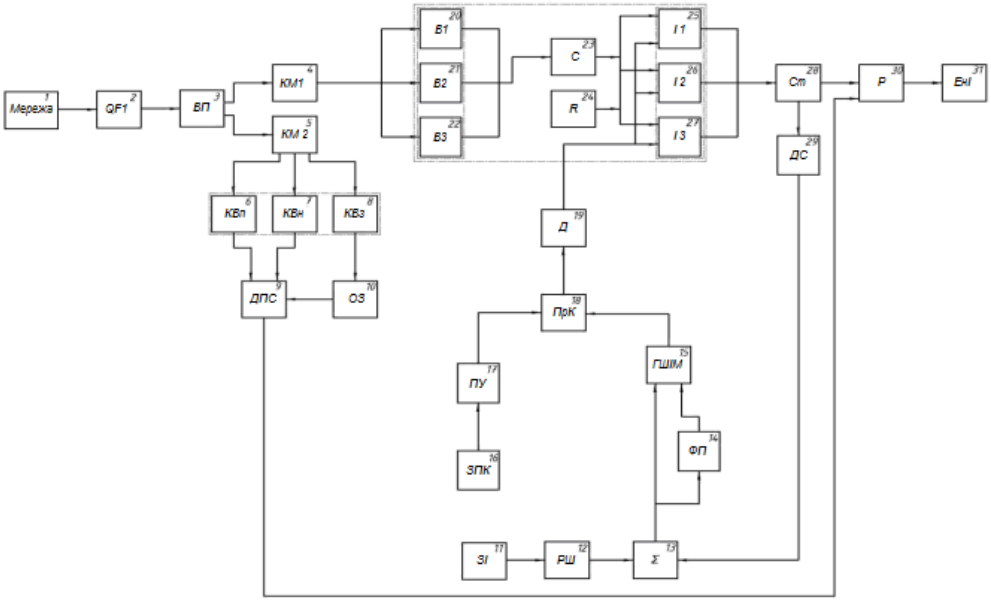


Рисунок 4 – Логічна модель системи пошуку несправностей електродвигуна

Сучасний метод діагностування електричних машин повинен відповідати наступним пунктам, наведеним нижче:

- висока достовірність та точність виявлення дефектів та несправностей електромашини;
- можливість виявлення всіх або більшої частини електричних та механічних дефектів електромашини та пов'язаних з нею пристроїв;
- проведення діагностичних вимірювань віддалено, що необхідно у тих ситуаціях, коли важко звернеться до обладнання безпосередньо;
- мала трудомісткість та простота проведення діагностичних вимірювань;
- можливість проведення обробки отриманих результатів вимірювань за короткий час, із застосуванням програмних засобів.

3. Діагностика несправностей асинхронних електродвигунів на основі спектрального аналізу струмів

У разі пошкодження стрижня очікуються бічні смуги навколо частоти живлення в спектрі потужності фазного струму. Внаслідок цього бічні гармоніки першого порядку (*k=1*) мають колосальне значення знаходження дефектів несправного стрижня. Ліва бічна смуга $f_s(1-2k_s)$ обумовлюється електричною або магнітною асиметрією ротора, спричинена дефектами роторних стрижнів, тоді як поява правої смуги $f_s(1+2k_s)$ обумовлюється наявністю пульсацією швидкості або вібрацією.

Амплітуди та присутність бічних смуг безпосередньо залежать від положення у просторі несправних стрижнів ротора, швидкості та навантаження. Розташування бічних смуг зміщуватиметься назовні, якщо швидкість і навантаження будуть збільшуватися. Було визначено, що бічні смуги можуть виявлятися, коли електромашина не має дефектних стрижнів ротора. Це викликано тим, що еліптичність ротора та неспіввісність валу можуть певною мірою викликати асиметрію ротора. Але все одно, амплітуди бічних смуг, що вийшли в цих ситуаціях, набагато менші в порівнянні з іншими, які виявляються при дефектних роторних стрижнях. У роботі [6] використовувалися два несправні двигуни, один з одним зламаним стрижнем ротора, інший двигун – з двома зламаними стрижнями. Ротори цих двигунів були просвердлені та використані у випробуваннях для імітації пошкоджень стрижнів ротора, а потім порівнювалися зі справним двигуном.

Різниця амплітуд лівих пелюсток спектральних характеристик у випадку справного ротора і ротора з двома пошкодженими стрижнями дорівнює 14 дБ при 75% від повного навантаження двигуна. Зрозуміло, що амплітуда бокового діапазону буде збільшуватися по мірі збільшення навантаження і степені серйозності пошкодження при чому цей дефект краще може бути виявлений при більш високих навантаженнях.

На рисунку 5 показані спектри струму, справного и пошкодженого електродвигуна при різних навантаженнях. Амплітуди бокових пелюсток справного двигуна рівні -27 дБ (зліва) і -34 дБ (справа), тоді як вони складають -16 дБ (зліва) і -19 дБ (справа) у випадку одного дефектного стрижня і -13 дБ (зліва) і -14 дБ (справа) у випадку двох дефектних стрижнів. Діючим є метод, базується на аналіз вібрації двигуна [6, 7, 9]. Використовуючи спектр вібрації електродвигуна, можна отримати більш точну швидкість та частоту мережі, а також частоти, пов'язані з дефектами. Завжди притаманний дисбаланс маси ротора та неспіввісність валу, що призводить до пікових компонентів у частоті обертання двигуна та до виникнення гармонік у його вібраційному спектрі. Як згадувалося раніше, у разі пошкодження стрижня ротора відбувається коливання швидкості із частотою $2sf_s$. Це коливання діє як частотна модуляція на частоті обертання і двох частотах бічних смуг $(f_r - 2sf_r)$ і $(f_r + 2sf_r)$ (fr + 2sfr), які виявляють f_r у спектрі вібрації. Коли дисбаланс ланцюга ротора збільшується, величина коливання швидкості, і навіть величини частоти бічної лінії теж збільшуються. Отже, величини $(f_r \pm 2sf_r)$ можуть бути добре виміряні у разі виявлення пошкоджень стрижня. У роботі [6] наведено результат проведення цього методу виявлення пошкодженого стрижня з використанням вібрації.

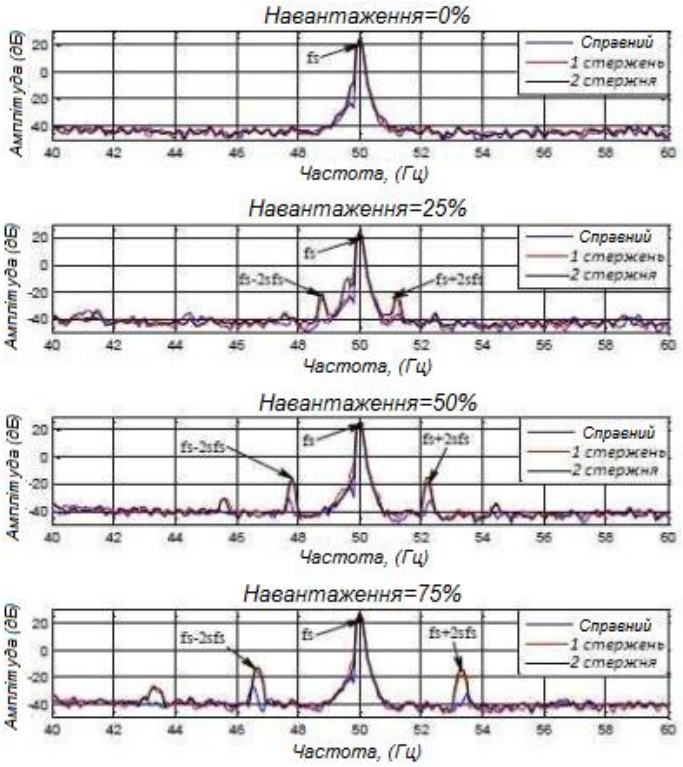


Рисунок 5 – Спектри струму асинхронного двигуна при різних навантаженнях

4. Використання нейронних мереж для автоматичної діагностики асинхронних електродвигунів

Нейронна мережа може бути використана, щоб виявити власну асиметрію та негативну частоту [8]. На рисунку 6 представлено схему нейронних мереж для моніторингу стану асинхронного електродвигуна.

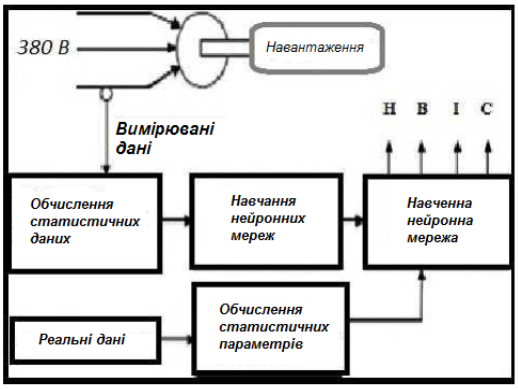


Рисунок 6 – Система діагностики АД з нейронною мережею

Метод ґрунтується на стандартній моделі аналізу спектральної характеристики струму статора (рисунок 5). На підставі досліджень, можна зробити висновок, що частота дискретизації вимірювального каналу повинна знаходитися в межах від 1,5 кГц до 3 кГц.

Висновок. Проведено моделювання електромагнітних процесів у різних режимах роботи двигуна - холостому ході, під навантаженням і при перевантаженні. Застосування спектрального методу діагностики дозволило визначити частотні

складові, що відповідають різним видам дефектів, таким як пошкодження стрижнів ротора, порушення симетрії фаз або міжвиткові замикання. Порівняння спектрів показало, що даний метод забезпечує найвищу точність і чутливість порівняно з іншими існуючими підходами.

Отримані результати свідчать, що спектральний аналіз може бути ефективно використаний як основа для побудови автоматизованої системи діагностики асинхронних електроприводів. Така система здатна виявляти ранні ознаки несправностей, здійснювати прогнозування стану двигуна та запобігати аварійним ситуаціям.

Перелік використаних джеоел.

1. Губаревич О.В. Надійність і діагностика електрообладнання: Підручник / О.В. Губаревич. – Сєвєродонецьк: вид-во СНУ ім. В. Даля, 2016. – 248 с.

2. Губаревич О.В., Голубєва С.М. Систематизація дефектів і вибір методів діагностики технічного стану ізоляції асинхронних двигунів: Тези доповідей III Міжнародної науково-практичної конференції «Мехатронні системи: інновації та інжиніринг», 10 жовтня 2019 р. / відп. за вип. М. А. Зенкін. – Київ: КНУТД, 2019. – 176 с. С.65-67.

3. Худий Є.Г. Сучасні методи діагностики стану ізоляції електричних машин /Є.Г. Худий, І.І. Пельтек//Сб. научн. трудов "Вестник НТУ "ХПИ": Проблеми автоматизованого електроприводу. Теорія і практика. №28 - Вестник НТУ "ХПИ", 2010. С.549-550..

4. 1. Шавкун, В. М. Методи моніторингу параметрів тягових електричних двигунів в процесі експлуатації рухомого складу міського електротранспорту [Текст] / В. М. Шавкун, В. М. Бушма // Комунальне господарство міст: наук.-техн. зб. – ХНАМГ.: технічні науки і архітектура, 2011. – Вип. 97. – С. 272-278.

5. Яцун, М. А. Експлуатація та діагностування електричних машин і апаратів [Текст] / М. А. Яцун, А. М. Яцун. – Львів.: «Львівська політехніка», 2010. – 228 с. 3. Шавкун, В. М. Вплив періодичності діагностування на показники надійності тягових електродвигунів рухомого складу електротранспорту [Текст] / В. М. Шавкун, С. П. Шацький // Комунальне господарство міст: наук.-техн. зб. – ХНАМГ.: технічні науки і архітектура, 2011. – Вип. 101. – С.265-269.

6. Кузнєцов Д.І. Експертна система розпізнавання дефектів електрообладнання / Д.І. Кузнєцов, А.І. Купін // Інформаційні управляючі системи та комп'ютерний моніторинг. – 2012. – С.185–187.

7. Khadim Moin Siddiqui. Fault diagnosis in induction motors by motor current signal analysis / Khadim Moin Siddiqui, V.K. Giri // International Journal of Electronics & Communication Technology. – 2011.– vol 2.– pp 114 – 119.

8. Кузнєцов Д.І. Моніторинг використання електроенергії електроустаткуванням засобами нейромереж / Д.І. Кузнєцов, А.І. Купін // Системні технології. – 2011.– №26.– С. 78–85.

9. Standard. ISO 20958:2013. Condition monitoring and diagnostics of machine systems – Electrical signature analysis of three-phase induction motors. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/39839.html

УДК 681.5:621.9

Юрій БОЙКО, Віталій ГОВЕНКО, Олександр ЦИКВАС, Владислав ПІДГАНЮК

Західноукраїнський національний університет

ОБҐРУНТУВАННЯ ВИБОРУ ТЕХНІЧНИХ ЗАСОБІВ АВТОМАТИЗАЦІЇ ДЛЯ ЛІНІЇ НАНЕСЕННЯ ПОРОШКОВОГО ПОКРИТТЯ

Вступ. Підвищення якості технологічних процесів нанесення порошкового покриття на вироби значною мірою залежить від рівня автоматизації виробничої лінії. Внаслідок високої температури процесу полімеризації, складності підтримання стабільних параметрів середовища та підвищених вимог до охорони праці, виникає необхідність у використанні надійних технічних засобів автоматизації (ТЗА) [1].

Автоматизація забезпечує точне регулювання температури полімерної печі, контроль витрати повітря та рідин, моніторинг стану вентиляційної системи, а також підвищення енергоефективності процесу. Актуальність проблеми обґрунтування вибору ТЗА полягає у потребі забезпечити сумісність, надійність, метрологічну точність і відповідність умовам експлуатації в агресивному технологічному середовищі.

У статті розглянуто підходи до обґрунтування вибору технічних засобів автоматизації для автоматизованої лінії підготовки та нанесення порошкового покриття на вироби. Проведено аналіз технологічного процесу, визначено ключові параметри, що підлягають контролю та регулюванню. Обґрунтовано вибір датчиків, виконавчих механізмів, модулів вводу-виводу та програмованого логічного контролера. Окрему увагу приділено енергетичній ефективності, якості регулювання температури полімерної печі та економічній доцільності модернізації.

Об’єктом дослідження є є автоматизована система керування технологічним процесом нанесення порошкового покриття, що включає комплекс датчиків, виконавчих механізмів, модулів вводу-виводу та програмований логічний контролер, призначені для забезпечення стабільного функціонування виробничої лінії.

Метою дослідження є наукове обґрунтування вибору технічних засобів автоматизації для системи підготовки та нанесення порошкового покриття на вироби, що забезпечують підвищення точності контролю параметрів технологічного процесу, покращення якості регулювання температури полімерної печі, зменшення енергетичних витрат та підвищення загальної ефективності роботи виробничої лінії..

1. Аналіз технологічного процесу нанесення порошкового покриття

Технологічна лінія нанесення порошкового покриття включає етапи підготовки поверхні, нанесення порошкової фарби електростатичним способом та полімеризації в печі. Основними параметрами, що істотно впливають на якість покриття, є [2]:

- температура гарячого повітря в полімерній печі;
- температура виробу;
- витрата повітря та водних розчинів;
- рівень рідини в резервуарах підготовчої лінії;

- стан вентиляційної системи та концентрація шкідливих речовин.

Автоматизація цих параметрів дозволяє стабілізувати технологічний процес та зменшити ручне втручання (рисунок 1).

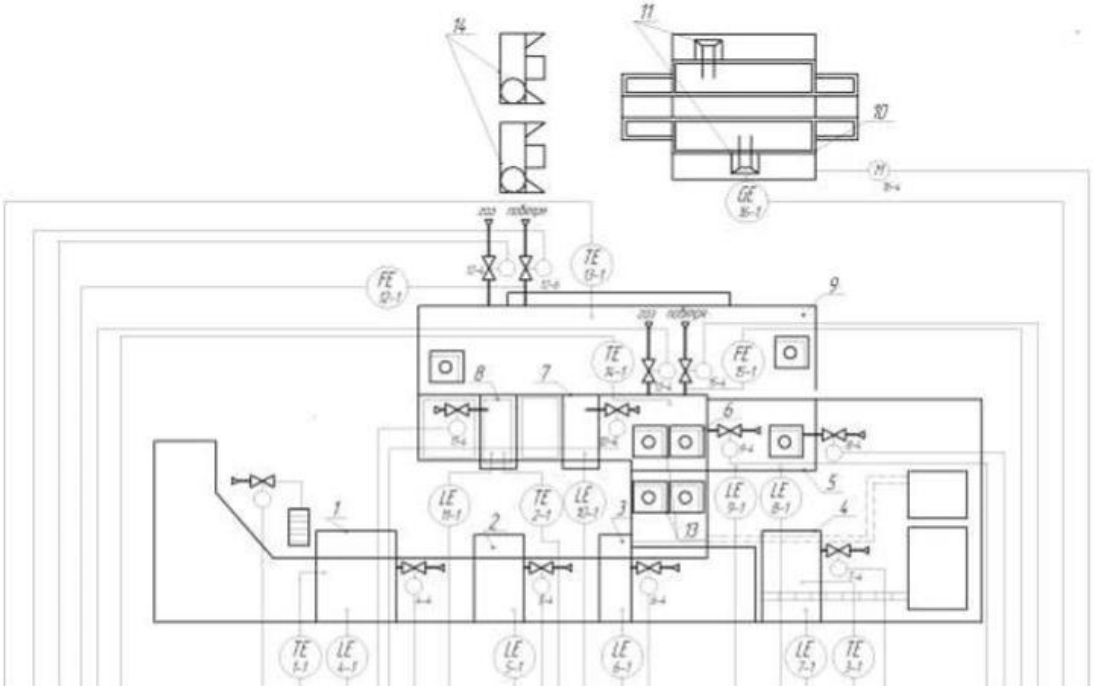


Рисунок 1 - Функціональна схема автоматизації

2. Методологія вибору технічних засобів автоматизації

Вибір ТЗА здійснювався на основі таких критеріїв:

- стійкість до високих температур та агресивних середовищ;
- відповідність метрологічним характеристикам;
- сумісність із PLC та мережевими інтерфейсами;
- вартість володіння та легкість інтеграції;
- надійність та ремонтопридатність.

Для контролю параметрів технологічного процесу було обрано компонентну базу [3], що включає датчики рівня NivoPress, датчики температури TM65, датчики витрати SV7504, датчики переміщення IFM, електричні приводи ML7421 та модулі вводу-виводу I-87017RW і I-87024W. Усі ТЗА об'єднані в єдину систему управління на базі програмованого логічного контролера LX-8x3x.

Кількість підібраних ТЗА для спроектованої системи нанесення порошкового покриття приведена в таблиці 1.

Вибір датчиків базувався на аналізі експлуатаційних умов: підвищена вологість, наявність розчинів, висока температура та необхідність швидкого реагування.

Датчики рівня NivoPress забезпечують точний контроль рівня рідини в резервуарах підготовчої лінії. Вони стійкі до хімічно активних розчинів та мають високу надійність.

Датчики температури TM65 застосовані для контролю температурного поля у полімерній печі. Їх робочий діапазон відповідає температурі полімеризації (190–220 °C), а конструкція забезпечує низьку похибку вимірювання.

Датчики витрати SV7504 забезпечують вимірювання витрати повітря та парів у системі вентиляції та подачі теплоносія.

Електричні приводи ML7421 використовуються для позиціонування регулюючих заслінок та вентилів, що дозволяє реалізувати пропорційне управляюче регулювання температури та тиску.

Таблиця 1 - Кількість ТЗА для спроектованої системи

Найменування ТЗА	**К-ть**
Давач рівня рідини NivoPress типу D	8
Давач температури TM65	5
Давач витрати SV7504	2
Давач переміщення IFM	1
Електричний привід ML7421	16
8-канальний модуль вводу I87017RW	2
4-канальний модуль виводу I87024W	4
Програмований логічний контролер LX-8x3x	1

3. Якість регулювання

Аналіз спроєктованої систем показує зменшення витрат електроенергії на:

- підігрів виробу;
- підігрів камери згорання;
- підігрів повітря;
- тепловтрати через стінки печі.

Регулювання температури полімерної печі здійснюється ПІ-регулятором, параметри якого оптимізовані методом моделювання. Моделювання показало зменшення перерегулювання та стабільність підтримання температури в межах допустимого діапазону, що напряму впливає на якість полімерного покриття.

В автоматизації виділяють три основні типи процесів для налаштування регулятора: технологічний процес з приблизно 20% перерегулюванням, аперіодичний процес з мінімальним часом регулювання та процес, що забезпечує мінімальну інтегральну оцінку якості.

Для нашого об’єкта, полімерної печі, налаштування ПІ-регулятора визначимо за формулами для аперіодичного процесу:

$$K_p = \frac{0.6 \cdot T}{K \cdot t} = \frac{0.6 \cdot 460}{2.325 \cdot 150} = 0{,}79; \quad (1)$$

$$K_i = \frac{1}{K \cdot \tau} = \frac{1}{2{,}325 \cdot 150} = 0{,}0029 \quad (2)$$

За допомого середовища Simulink та отриманих даних з формул 1 і 2 підставимо в ПІ-регулятор та змоделюємо нашу систему (рисунок 2).

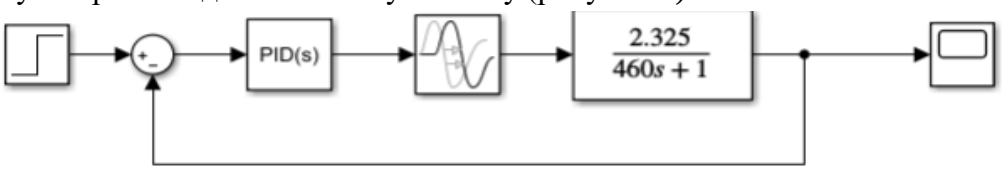


Рисунок 2 - Структурна схема в середовищі Simulink

Змоделювавши, отримано наступну перехідну характеристику, наведену на рисунку 3.

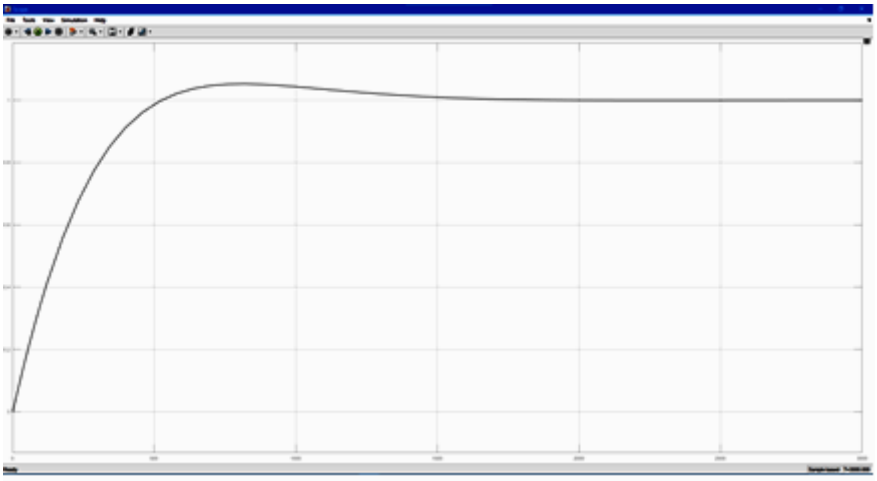


Рисунок 3 - Перехідна характеристика процесу регулювання

З рисунку 3 отримали показники якості (таблиця 2).

Таблиця 2 - Якісні показники системи з ПІ-регулятором

$h_{уст}$*0,95	0,95
t_p	888
Перерегулювання	5.2
ε(∞)	0
Ψ	0

Висновок. На основі проведеного аналізу обґрунтовано вибір технічних засобів автоматизації для лінії нанесення порошкового покриття на вироби. Підібрані ТЗА забезпечують підвищення надійності та точності вимірювання ключових параметрів; покращення якості регулювання температури полімерної печі; зменшення енергетичних витрат; підвищення продуктивності та якості готової продукції; значну економію за рахунок зниження експлуатаційних витрат.

Перелік використаних джерел

1. Бобров В. Т., Сидоренко О. П. Автоматизація технологічних процесів хімічного виробництва. - К.: Наука і техніка, 2017. - 380 с.

2. Качан В. В., Пилипенко А. Ю. Системи автоматизації промислових процесів. - К.: Ліра-К, 2020. - 412 с.

3. Костенко А. О., Лисенко В. М. Технічні засоби автоматизації: датчики, виконавчі механізми, контролери. - К.: НТУУ «КПІ», 2021. - 276 с.

УДК 629.423.14

Біловус Д. П, Жовток В.В. Рибін А.С.

Західноукраїнський національний університет

МОДЕЛЬ СИСТЕМИ ОБЛІКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ НА ЕЛЕКТРОВОЗАХ ЗМІННОГО СТРУМУ

Вступ. Сучасний контроль споживання електроенергії залізничними споживачами в системі тягового електропостачання не відповідає вимогам точності, які прийняті для енергопостачальних комплексів промислових підприємств і комунального господарства [1-2]. У тяговій мережі виникає проблема так званих «умовних» втрат електроенергії. Розбіжності між показаннями лічильників на тягових підстанціях та електровозах неможливо пояснити лише втратами в контактній мережі. Одним із чинників значних «умовних» втрат є недосконаліть самої системи тягового електропостачання щодо організації комерційного обліку на тягових підстанціях. Іншою причиною виступає недостатня точність вимірювальних комплексів, що фіксують витрату електроенергії на електровозах змінного струму.

Для того щоб оцінити ефективність впровадження енергозберігаючих технологій, необхідно застосовувати такі засоби вимірювань, які базуються на фіксації миттєвих значень електричних величин, що характеризують роботу електровоза, з подальшим їх числовим опрацюванням [3]. Цим вимогам відповідають прилади, побудовані на мікропроцесорних технологіях. Вони мають електронні носії пам'яті, дисплей для демонстрації результатів, можливість одночасного визначення споживання та повернення енергії, що дає змогу зменшити кількість лічильників на електровозах, обладнаних рекуперативним гальмуванням.

Мета: дослідження та розробка моделі системи обліку електричної енергії на електровозах змінного струму.

1 Математична модель системи обліку електричної енергії

У системі системи обліку електричної енергії застосована математична модель вимірювання активної електричної потужності, побудована відповідно до нормативної та методичної бази щодо вимірювання, комерційного й технічного обліку електроенергії й потужності [4-5]. Вона відображає середнє за інтервал часу T значення швидкості перетворення енергії електромагнітного поля в інші види енергії, зокрема механічну енергію руху електровоза з поїздом, незалежно від форми кривих струму та напруги:

$$P = \frac{1}{T}\int_0^T u(t)i(t)dt \approx \frac{1}{m}\sum_{j=1}^{m} u_j\, i_j\,, \qquad (1)$$

де u_j, i_j – миттєві значення напруги та струму будь-якої форми,

а N – кількість вимірювань за часовий інтервал T, кратний періоду напруги живлення.

Під час цифрової обробки масивів миттєвих значень струму й напруги величина потужності усереднюється за кількома періодами промислової частоти. Приріст

активної електроенергії протягом обраного проміжку часу визначається методом числового інтегрування активної потужності в цьому проміжку.

Через нелінійний характер навантаження електровоза форми кривих струму та напруги в контактній мережі відрізняються від синусоїдальних, що свідчить про наявність вищих гармонічних складових. У такому разі струм і напруга можуть бути представлені у вигляді ряду Фур'є. Графічно-аналітичний метод розкладання періодичних функцій довільної форми полягає в заміні визначеного інтеграла сумою скінченної кількості членів. Для цього період функції, рівний *T*, поділяють на *m* рівних частин *Δt*, після чого інтеграли замінюють сумами. Криву напруги довільної несинусоїдальної форми можна подати через ряд Фур'є:

$$f(x) = U_0 + \sum_{n=1}^{\infty} \left(U'_{(n)} \sin nx + U''_{(n)} \cos nx \right). \quad (2)$$

Постійна складова визначається виразом:

$$U_0 = \frac{1}{2\pi} \int_0^{2\pi} f(x) dx \approx \frac{1}{2\pi} \sum_{p=1}^{p=m} f_p(x) \Delta x = \frac{1}{2\pi} \sum_{p=1}^{m} f_p(x) \frac{2\pi}{n},$$

або

$$U_0 = \frac{1}{m} \sum_{p=1}^{m} f_p(x), \quad (3)$$

де $p = \overline{1, m}$ – поточний індекс; $f_p(x)$ – значення функції $f(x)$ при $x = (p - 0{,}5)\Delta x$, тобто в середині p -го інтервалу.

u_i – значення функції в середині *i* (і)-го інтервалу.

Амплітуди *n*-ої синусної гармоніки визначається формулами:

$$U'_{(n)} = \frac{1}{\pi} \int_0^{2\pi} f(x) \sin nx dx \approx 2 \cdot \frac{1}{2\pi} \sum_{p=1}^{m} f_p(x) \frac{2\pi}{m} \sin_p nx,$$

або

$$U'_{(n)} = \frac{2}{m} \sum_{p=1}^{m} f_p(x) \sin_p nx. \quad (4)$$

Амплітуди *n*-ої косинусної гармоніки визначаються формулами:

$$U'_{(n)} = \frac{1}{\pi} \int_0^{2\pi} f(x) \cos nx dx \approx 2 \cdot \frac{1}{2\pi} \sum_{p=1}^{m} f_p(x) \frac{2\pi}{m} \cos_p nx,$$

або

$$U''_{(n)} = \frac{2}{m} \sum_{p=1}^{m} f_p(x) \cos_p nx. \quad (5)$$

$\sin_p nx$ і $\cos_p nx$ – відповідні значення функцій $\sin nx$ і $\cos nx$ при $x = (p - 0{,}5)\Delta x$, тобто в середині p -го інтервалу.

Амплітуда кожної гармоніки обчислюється за формулою:

$$U_{(n)} = \sqrt{\left(U'_{(n)}\right)^2 + \left(U''_{(n)}\right)^2}. \quad (4.6)$$

Зміщення початкової фази гармоніки – тангенс кута $\psi(n)$ по відношенню до початкової фази $f(x)$, знаходять як:

$$tg\psi_{(n)} = \frac{U''_{(n)}}{U'_{(n)}}, \text{ звідки} \qquad \psi_{(n)} = arctg\left(\frac{U''_{(n)}}{U'_{(n)}}\right). \qquad (7)$$

2. Алгоритм розкладу кривих напруги та струму в ряд Фур'є

У моделі системи обліку електроенергії алгоритм розкладу кривих напруги та струму в ряд Фур'є реалізовано в середовищі OrCAD 9.2. Для виконання цього застосовано модель блока, зображену на рисунку 1, у якій використано ключі, керовані напругою (Sbreak), інтегратор (INTEG), імпульсне джерело (VPULSE), множник (MULT), блоки сумування (SUM) та віднімання (DIFF), степеневі функції (PWR), стандартні тригонометричні функції (SIN, COS, ARCTAN), операцію квадратного кореня (SQRT) та інші допоміжні елементи.

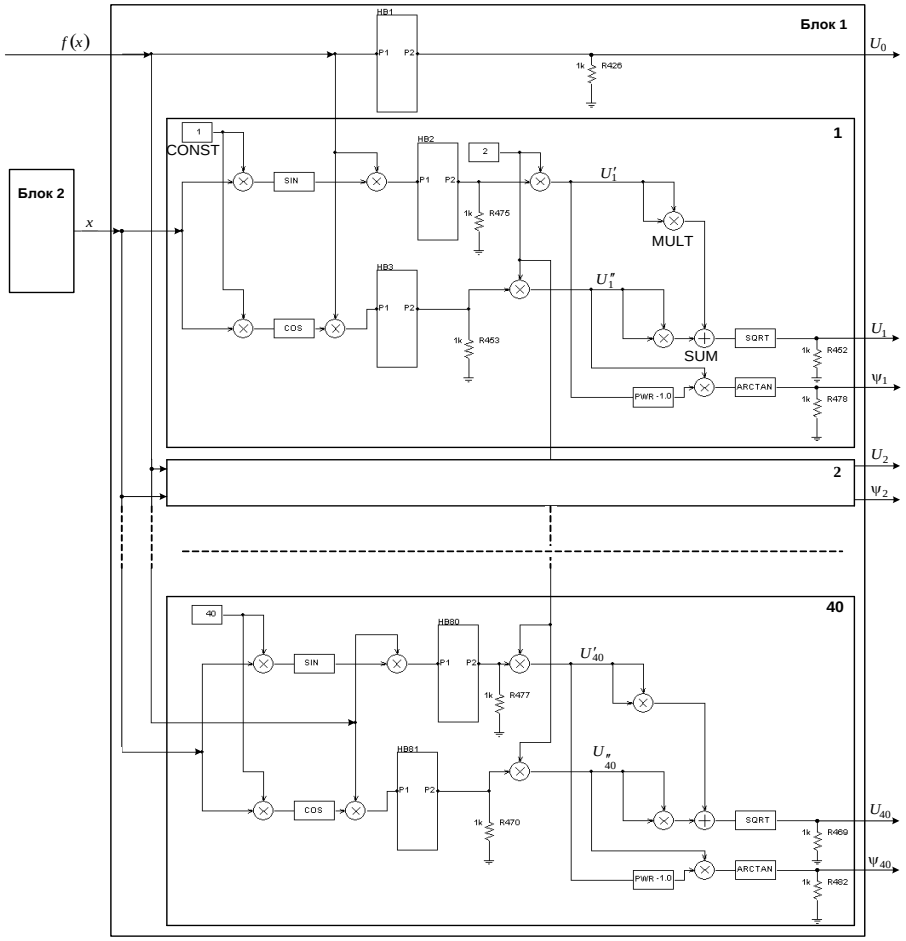


Рисунок 1 – Схема моделі блока реалізації алгоритму швидкого перетворення Фур'є в програмі OrCAD 9.2 (Блок 1)

Структура моделі дає змогу сформувати постійну складову ряду, визначити амплітуди синусної та косинусної компонент k-ої гармоніки, а також амплітуди та початкові фази всіх гармонічних складових періодичного несинусоїдального сигналу струму або напруги. У першому блоці на основі ієрархічних структур реалізовано модуль HB (Hierarchy Block), який забезпечує визначення інтеграла функції за періодом

частоти мережі за допомогою інтегратора INTEG. Розгорнута схема цього блока показана на рисунку 2.

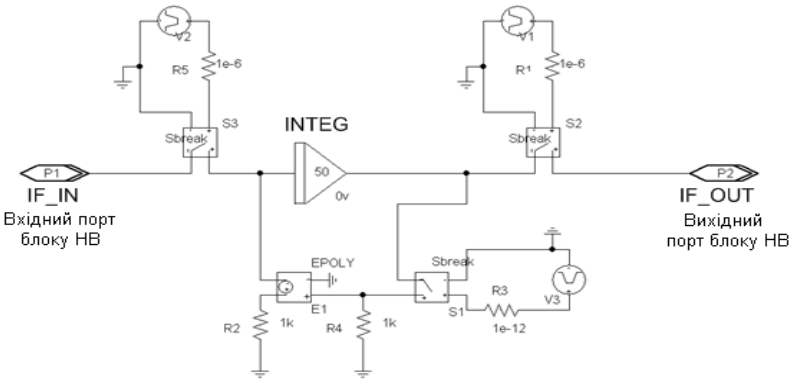


Рисунок 2 – Схема моделі блока реалізації способу визначення інтегралу функції за період

За допомогою керованих ключів S2 і S3, встановлених відповідно на вході та виході інтегратора, забезпечується обмеження інтервалу інтегрування. Після завершення інтегрування за один період ключ S1 разом із функцією EPOLY забезпечує скидання інтегратора до початкового стану, після чого відкривається ключ S3 і починається інтегрування за наступний період, що завершується спрацьовуванням ключа S2.

Застосування ієрархічних блоків НВ, блоків CONST з номерами гармонік від 1-ї до 40-ї, тригонометричних функцій SIN і COS та множників MULT дає змогу виконати обчислення амплітуд синусних і косинусних складових відповідно до формул (4) та (5). На виході першого блока отримуються значення постійної складової, амплітуди та початкової фази кожної гармоніки відповідно до формул (3), (6) та (7) з використанням множників, степеневих функцій, блоків сумування, квадратного кореня та арктангенса.

Другий блок моделі, схема якого подана на рисунку 3, забезпечує визначення поточного значення кута зсуву початкових фаз першої та *n*-ої гармонік. Синусоїдальні джерела формують функцію тангенса цього кута, а його числове значення визначається за допомогою функції арктангенса.

Після виконання відповідних математичних перетворень вираз (1) набуває такого вигляду:

$$P = P_0 + \sum_{n=1}^{k} P_{(n)} = U_0 I_0 + \sum_{n=1}^{k} U_{(n)} I_{(n)} \cos\varphi_{(n)}, \qquad (8)$$

де $P_{(n)}$ – активна потужність n-ї гармонічної складової ($n = 0 \div k$);

$U_{(n)}$ і $I_{(n)}$ – діючі значення напруги та струму для n-ї гармоніки;

$\varphi_{(n)}$ – кут зсуву фаз між напругою $U_{(n)}$ і струмом $I_{(n)}$.

Сформована математична модель електромагнітних процесів у системі «контактна мережа – електровоз», що дає можливість визначати витрати електричної енергії на електровозах змінного струму, забезпечує проведення досліджень як усталених, так і перехідних режимів роботи електрорухомого складу. Модель обліку споживання електроенергії ґрунтується на застосуванні розкладання кривих струму та напруги у гармонійний ряд Фур'є, що підвищує достовірність результатів вимірювань.

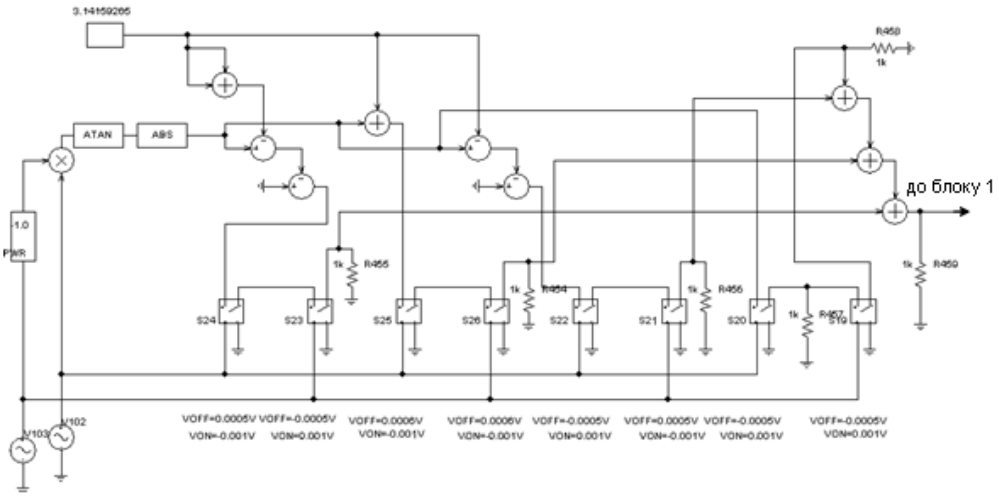


Рисунок 3 – Схема моделі блоку реалізації алгоритму швидкого перетворення Фур'є в програмі OrCAD 9.2 (Блок 2)

Подана методика математичного опису динамічних перехідних процесів у силових колах електровоза, а також програмна реалізація інтегрованої моделі «контактна мережа – електровоз», використовується у навчальному процесі на кафедрі «Електротехніка, електроніка та електромеханіка» Далекосхідного державного університету шляхів сполучення.

3 Результати експериментальних досліджень і математичного моделювання за показниками споживання електричної енергії електровозом

Через неможливість здійснити пряме вимірювання напруги на струмоприймачі електровоза, спричинену відсутністю вимірювального трансформатора напруги на високовольтній стороні його тягового трансформатора, реєстрація напруги проводилася з обмотки збудження тягового трансформатора. Саме ця обмотка живить випрямну установку збудження (ВУВ). Такий спосіб підключення мінімізує додаткові спотворення форми напруги, оскільки в режимі тяги обмотка збудження не навантажена, на відміну від обмотки власних потреб, що працює у всіх режимах та забезпечує живленням кола напруги лічильників електроенергії.

З метою перевірки відповідності створеної узагальненої математичної моделі системи «контактна мережа – електровоз» реальним процесам було виконано моделювання тягового режиму, адекватного роботі справжнього електровоза. Досліджено залежності напруги та струму в первинній обмотці тягового трансформатора, отримані під час експерименту та моделювання в режимі тяги за фазового кута 110 електричних градусів на четвертій зоні регулювання.

У якості критерію порівняння електромагнітних процесів у моделі і реальному силовому колі було обрано коефіцієнт несинусоїдальності напруги, який характеризує форму періодично змінюваних сигналів. За експериментальними даними значення цього коефіцієнта дорівнювало 5,64 %, а за результатами моделювання – 6,20 %. Визначений за іншою експериментальною кривою коефіцієнт становив 5,48 %, тоді як модель дала результат 5,97 %.

Отримані дані підтверджують достатній рівень відповідності показників

моделювання електромагнітним процесам реального електровоза. Відносні похибки 9,1 % і 8,6 % не перевищують допустимого значення для математичного моделювання, що становить 10 %. Це свідчить про придатність представленої моделі як інструмента аналізу процесів у силових колах електровоза змінного струму.

Запропоновані інженерні рішення та створений віртуальний вимірювальний пристрій для автоматизованої системи контролю споживання електричної енергії електровозами змінного струму забезпечують безперервне визначення як витрат електроенергії, так і коефіцієнта несинусоїдальності напруги без застосування проміжних вузлів обробки сигналу, що усуває вплив людського чинника.

Порівняння даних системи із записами у маршрутному листі машиніста показало, що відносна похибка вимірювання становить 8,5 %. Отже, результати експерименту підтверджують відповідність процесів у моделі реальним електромагнітним явищам у силових колах електровоза, що засвідчує можливість використання розробленої моделі для дослідження роботи електровоза у різних режимах.

Висновок. Створена математична модель підсистеми обліку електроенергії, яка є частиною узагальненої математичної моделі комплексу «контактна мережа – електровоз», а також розроблений алгоритм реалізації процесів її функціонування забезпечують можливість визначити реальні витрати електроенергії, яку електровози споживають під час тяги поїздів. Таким чином, підвищується точність обліку витрати електроенергії, розвантажуються обов’язки машиніста рухомого складу та підвищується обробка даних.

Перелік використаних джерел.

1. Христян Є.В., Арєстов О.П., Івін В.Ф., Михайлов В.С., Цап В.С. Нові заходи до зниження витрат енергії в енергетичному господарстві вагонного депо. // Енергозбереження на залізничному транспорті та в промисловості: Матеріали IV. Міжнародної науково-практичної конференції – Д.:ДНУЖТ, 2013.С. 83-84.

2. Концепція розвитку електричного транспорту та його систем : матеріали Всеукр. наук.-практ. конф., Харків, 7 – 9 квітня 2020 р. / Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова та ін. – Харків : ХНУМГ ім. О. М. Бекетова, 2020. – 116 с.

3. Системи електропостачання електричного рухомого складу залізниць і метрополітенів: підручник / С. В. Панченко, В. С. Блиндюк, М. М. Бабаєв та ін. – Харків: УкрДУЗТ, 2018. – 308 с.

4. Сухоніс, Т.Ю. Моделювання позаштатних режимів роботи системи інвертор – асинхронний двигун тягового електротехнічного комплексу двосистемного електровоза / Т.Ю. Сухоніс, Ю.О. Миколаєнко, О.В. Бялобржеський // Гірнича електромеханіка та автоматика. – 2013. – Вип. 91. – С. 89-94.

5. Крупінський О.М. Концепція побудови верхнього рівня системи АСКОЕ в умовах реформування залізничної галузі України. // Енергозбереження на залізничному транспорті та в промисловості: Матеріали IV. Міжнародної науково-практичної конференції – Д.:ДНУЖТ, 2013.С. 50-51

УДК 681

Валерій МАЛИЙ

Західноукраїнський національний університет

КОМП'ЮТЕРНО-ІНТЕГРОВАНА СИСТЕМА КОНТРОЛЮ БАЗОВИХ ПАРАМЕТРІВ НА ЦУКРОВОМУ ЗАВОДІ

Вступ. Сучасне цукрове виробництво є складним багатостадійним технологічним процесом, ефективність якого визначається стабільністю та точністю контролю ключових параметрів - температури, тиску, концентрації сухих речовин, витрат сировини та енергоносіїв. На роботу основних технологічних вузлів істотно впливають:

- варіації якості бурякової сировини,
- коливання характеристик теплоносіїв,
- нестаціонарність процесів випаровування та кристалізації,
- зовнішні збурення, притаманні сезонному виробництву.

Сукупність цих факторів робить технологічний процес цукроваріння складним для стабільного керування та потребує впровадження сучасних комп'ютерно-інтегрованих систем контролю. Такі системи забезпечують оперативний моніторинг параметрів, підвищують точність регулювання, мінімізують втрати та сприяють енергоефективності й конкурентоспроможності виробництва.

Мета: Метою роботи є технічна реалізація системи контролю базових параметрів на Збаразькому цукровому заводі із використанням сучасних підходів. Це дозволить ефективніше використовувати ресурси та регулювати технологічні процеси виробництва, підвищуючи якість продукції та забезпечуючи безпеку праці.

1. Дослідження технологічного процесу виробництва цукру та вимоги до контролю його основних параметрів

Задля збільшення виходу чистого продукту цукрові заводи проходять постійну модернізацію з метою оптимізації виробництва і покращення технологічного процесу. Це дає можливість витягнути максимум із наявної продукції і запобігти непотрібним виробничим втратам.

Для кращого розуміння підрозділів підприємства і виконуваних ним основних функцій необхідно зрозуміти саму суть переробки цукрового буряку і процесу виробництва цукру, описати технологічну схему і розглянути всі операції на кожному етапі.

Отож, щоб отримати цукор-пісок необхідно виконати такі операції [1]:

1. Прийняти сировину (цукровий буряк)
2. Очистити буряки від бруду та інших домішок.
3. Подрібнити їх до отримання стружки необхідної фракції.
4. Отримати сік методом дифузії.
5. Очистити отриманий сік.
6. Провести процедуру випарювання соку.
7. Очистити і уварити сироп.

8. Отримати утфель (кристалізувати).
9. Центрифугувати і вибілити.
10. Просушити цукор-пісок.

На рисунку 1 наведено технологічну схему виробництва цукру з буряку

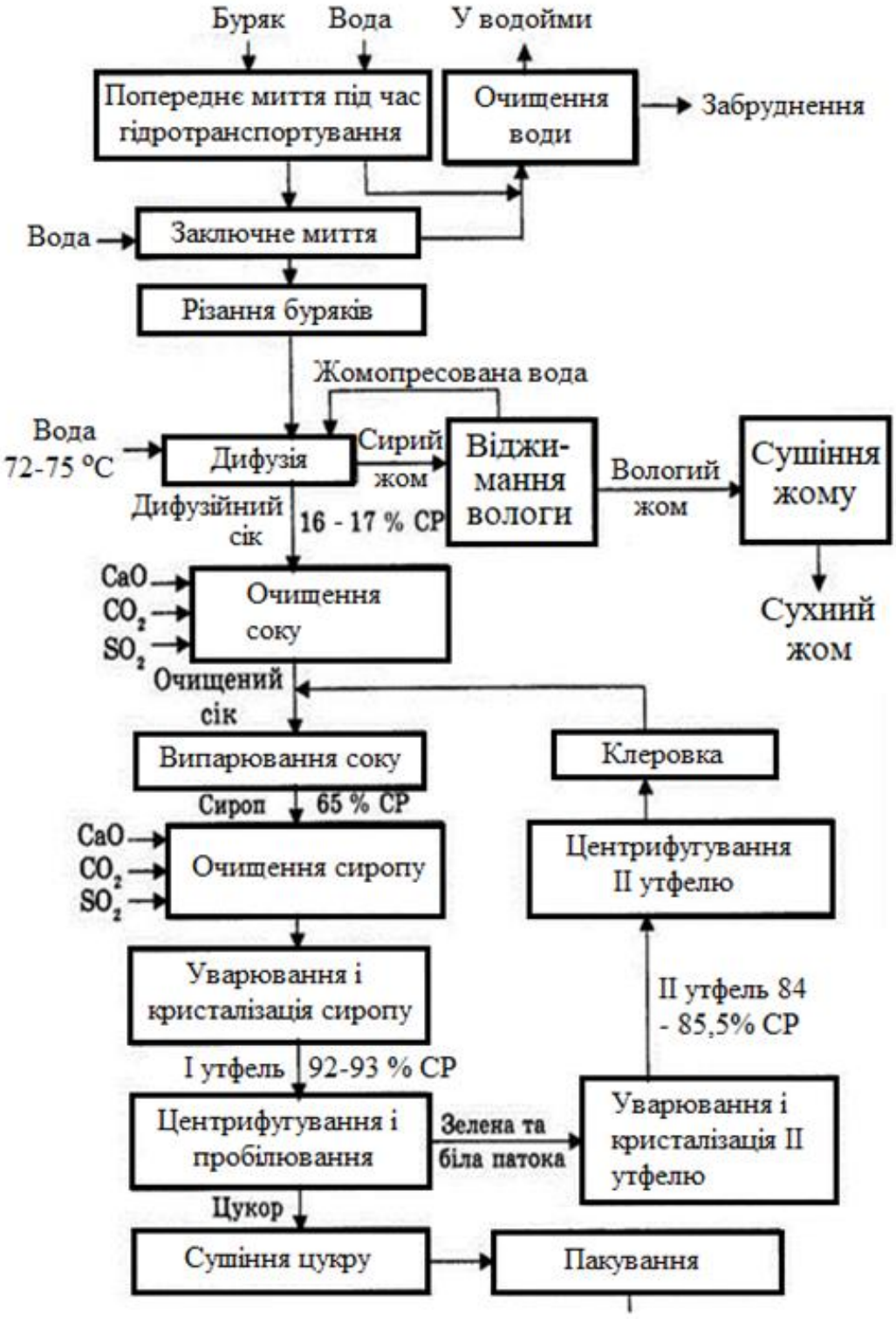


Рисунок 1 - Принципова технологічна схема виробництва цукру з буряку

На досліджуваному об’єкті для оптимізації управління використана модульна система управління. Архітектура мережі цукрового заводу наведена на рисунку 2.

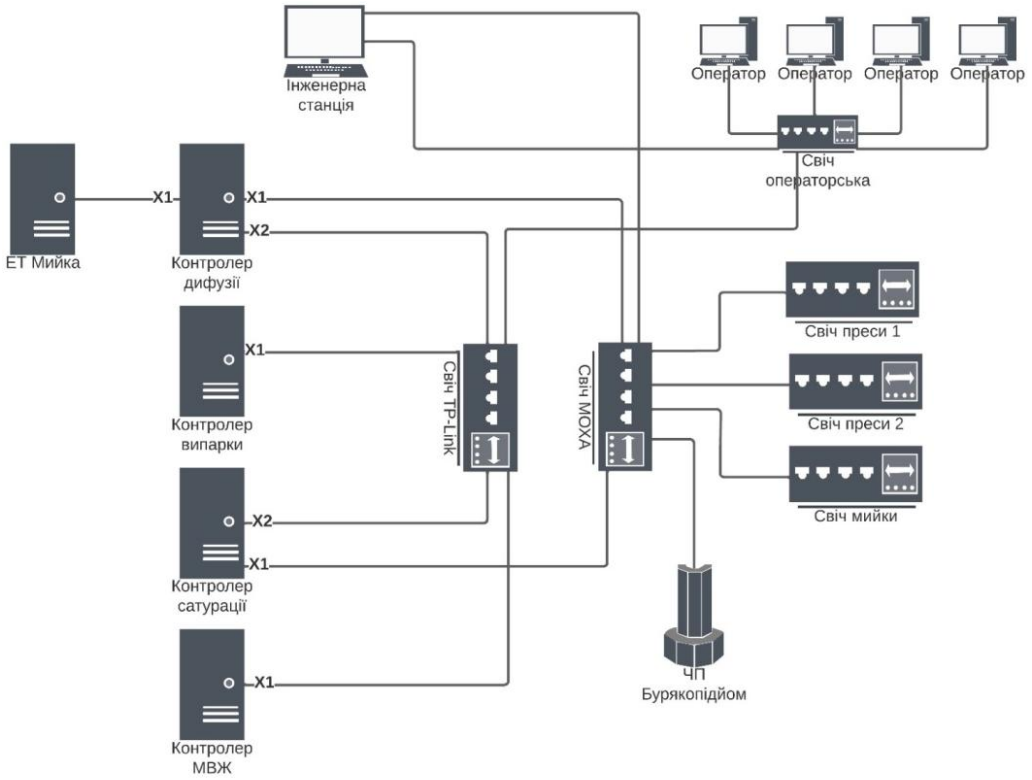


Рисунок 2 - Архітектура мережі цукрового заводу

Комп'ютерно-інтегрована система контролю параметрів на промисловому підприємстві – це складна система, що поєднує програмне забезпечення, апаратну частину, таку як сенсори і виконавчі механізми і мережеві технології [2].

Дані з різних відділів збираються в операторській станції, де відбувається автоматичний моніторинг, аналіз та управління базовими параметрами виробничого процесу цукрового заводу [3].

2. Оцінка алгоритмічних і апаратних рішень задач контролю технологічного процесу на досліджуваному об'єкті

Оцінка алгоритмічних і апаратних рішень є важливим аспектом автоматизації технологічного процесу на цукровому заводі. Оскільки це ключовий показник підвищення ефективності виробництва, зменшення витрат і покращення якості кінцевої продукції, варто провести аналіз і теоретичне обґрунтування існуючих методів розв'язку задач [4].

Крім блок-схем, одним з базових математичних методів є метод прогнозування, а саме – часові ряди. Це послідовність значень, які можуть змінюватися у часі.

До основних характеристик ЧР відносять:

- тренд – загальна тенденція зміни значень (зростання, спадання);
- сезонність – періодичні коливання, що повторюються через певні інтервали часу;
- циклічність – довгострокові коливання, які не мають фіксованого періоду і не залежать від сезонних змін;
- шум – випадкові коливання, які не мають закономірності та не піддаються аналізу.

Ознакою високоякісної комп'ютерно-інтегрованої системи є чітко виражена сезонність часових рядів і мінімальні або й повністю відсутні впливи шуму[5].

На рисунку 3 представлено приклад часового ряду з вираженими випадковими та регулярними коливаннями. Помаранчева лінія відображає вихідні спостереження, які характеризуються значною варіативністю та наявністю шумових компонент. Синя лінія демонструє згладжену версію ряду, що дає змогу виявити базові тенденції зміни даних у часі. На графіку простежується загальний тренд із чергуванням періодів підвищення та зниження, а також елементи сезонності, які проявляються у повторюваних коливаннях протягом кількох років.

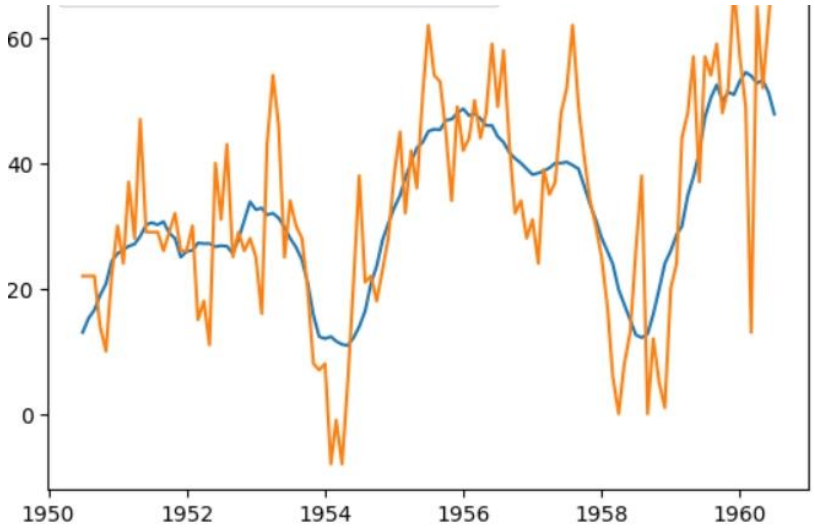


Рисунок 3 – Приклад часового ряду

Проте в сучасних ПЛК використовуються значно складніші схеми управління технологічним процесом. Крім того, програмовані логічні контролери не розуміють блок-схем, а програмувати їх потрібно мовою StructuredText або LadderLogic.

Приклад програми, реалізований на мові ST:

```
IF Start AND NOT Stop AND NOT LS2 THEN
        MotorFwd := TRUE;
ELSE
MotorFwd := FALSE;
END_IF;
IF LS1 AND NOT Stop THEN
        MotorRev := TRUE;
ELSE
        MotorRev := FALSE;
END_IF;
```

Утриманням параметрів в робочій зоні керує ПІД-регулятор. Обчислення зміни керуючого сигналу ПІД-регулятора здійснюється за формулою:

$$u(t) = Kp * e(t) + Ki * \int e(t)dt + Kd * de(t)/dt,$$

На рисунку 4 наведегно приклад діаграми стабілізації ПІД-системи.

Рисунок 4 - Приклад діаграми стабілізації ПІД-системи

Графік затухання коливань вихідного сигналу ПІД-системи після збурення. Крива демонструє характерну перехідну реакцію із початковим різким відхиленням, подальшими коливаннями та поступовим зменшенням їх амплітуди. Протягом часу амплітуда коливань зменшується до майже нульового рівня, що свідчить про стабілізацію системи та встановлення стаціонарного режиму. Така форма графіка підтверджує коректно налаштовані параметри ПІД-регулятора, які забезпечують затухаючий тип перехідного процесу без самозбудження.

3. Програмно-технічна реалізація елементів комп'ютерно-інтегрованої системи та оцінка перехідних процесів виробництва

Для повноцінного функціонування цукрового заводу потрібно розробити систему SCADA, яка керуючись запрограмованими алгоритмами, збирає параметри з кожного етапу виробництва. До таких належать: дифузія, мийка, градирня, випарна, жомопреска, сульфітація, конденсат, та інші [6].

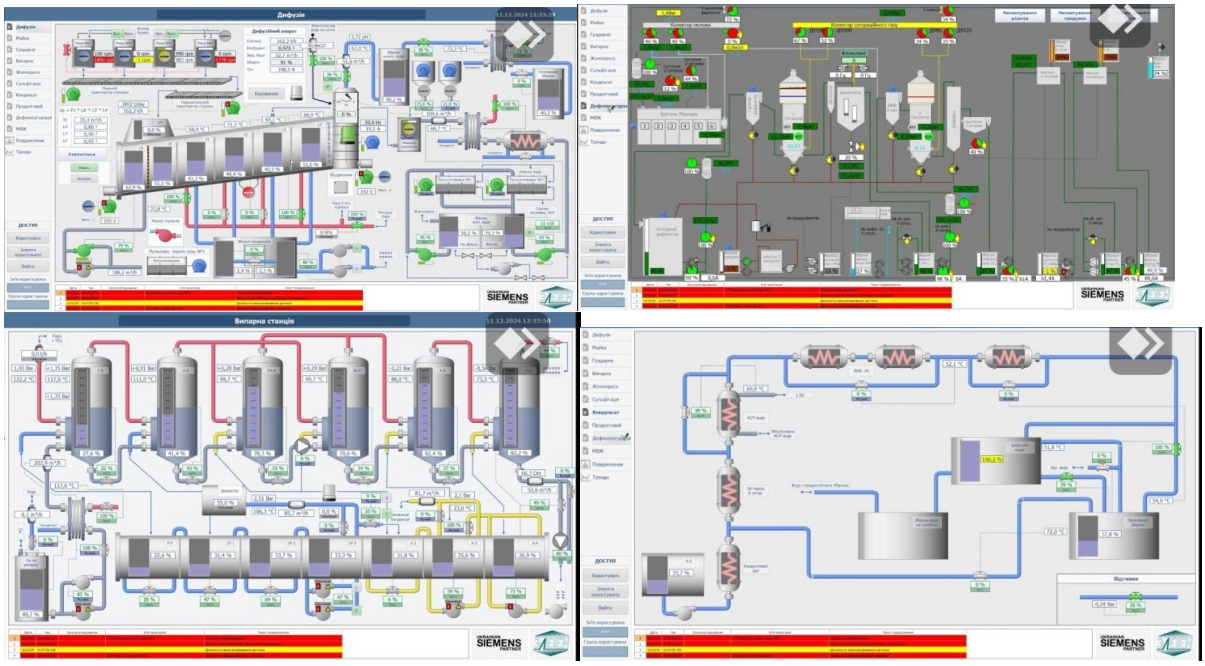


Рисунок 5 – SCADA схеми в режимі реального часу

Висновок. В ході виконання дипломної роботи було відвідано Збаразький цукровий завод та ознайомлено зі структурою підприємства. Досліджено технологічного процесу виробництва цукру та аналіз вимог до контролю його основних параметрів. Визначено основні характеристики досліджуваного об'єкта.

Проаналізовано існуючі архітектурні рішення вирішення задач контролю базових параметрів на підприємстві, а також визначено їхні переваги та недоліки. Оцінено алгоритмічні та апаратні рішення задач контролю технологічного процесу на досліджуваному об'єкті. Доведене теоретичне обґрунтування методів розв'язку задач. Описано роботу моделей формування базових показників в режимі реального часу. Описано існуючі та перспективні методи контролю стану обладнання виробничих процесів та чинники, що впливають на їх стан. Також проведений детальний аналіз програмно-технічної реалізації елементів комп'ютерно-інтегрованої системи, в тому числі, із запропонованою схемою контролю.

Досліджено базові методи застосування інформаційних систем та функції, які вони повинні виконувати. Досліджено програмні засоби реалізації, зокрема ПЗ контролерів Siemens та інтерфейси людино-машинної взаємодії. Побудовано системи контролю параметрів виробництва в SCADA для ключових відділів. Створено імітаційну модель та наведені основні робочі показники зняті в конкретний момент часу з реально працюючого обладнання.

Запропоновано модульну систему підтримки прийняття рішень виробничих процесів. Доведено ефективність та переваги даного методу контролю базових показників цукрового заводу. Реалізовано повний цикл такої комп'ютерно-інтегрованої системи контролю параметрів, що дозволяє розпізнавати відхилення і оперативно реагувати на них відповідно до заданого алгоритму роботи.

Перелік використаних джерел.

1. На Гнідавському цукровому заводі розповіли – [Електронний ресурс] –Режим доступу: https://business.rayon.in.ua/news/93732-na-gnidavskomu-zavodi-rozpovili-iak-pererobliaiut-buriaki-na-tsukor.

2. Технологія виробництва цукру – [Електронний ресурс] – Режим доступу: https://naurok.com.ua/tehnologiya-virobnictva-cukru-z-cukrovogo-buryaku-251777.

3. Промислові комутатори MOXA – [Електронний ресурс] –Режим доступу: https://www.moxa.com.ua/industrialethernet/products.

4. Слабоспицька О.О. Технологічна модель процесу автоматизованого виробництва сімейств програмних систем: Проблеми програмування, науковий журнал №1 – 2011.- С. 39-48.

5. Дорошенко А.Ю., Ігнатенко О.П., Іваненко П.А. Про одну модель оптимального розподілу ресурсів у багаторівневих середовищах: Проблеми програмування, науковий журнал №1 – 2011.- С. 29-38.

6. Аксьонова Т.В. Програмна технологія для проведення імітаційних експериментів з математичними моделями фізіологічних систем: Проблеми програмування, науковий журнал №1 – 2012.- С. 110-120.

УДК 681.32

Стасишин О.В., Носанчук О.О.[1] Заставний О.М.

[1]Західноукраїнський національний університет

ЕНЕРГОЕФЕКТИВНИЙ ЗБІР ДАНИХ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ БПЛА НА ОСНОВІ ПРОГРАМНО-ВИЗНАЧЕНОЇ АРХІТЕКТУРИ

Вступ. Сучасний розвиток технологій Інтернету речей та розширення сфер застосування бездротових сенсорних мереж (БСМ) формують потребу у більш ефективних методах збору даних з великих та розподілених територій. Традиційні підходи до організації БСМ обмежуються низькою енергоефективністю, нерівномірним навантаженням на вузли та складністю забезпечення надійного зв'язку, особливо у складних або важкодоступних умовах.

Використання безпілотних літальних апаратів (БПЛА) як мобільних колекторів даних відкриває нові можливості для підвищення продуктивності та адаптивності сенсорних мереж. Завдяки мобільності та автономності БПЛА здатні зменшувати енергоспоживання сенсорних вузлів, покращувати якість зв'язку та забезпечувати доступ до територій, де традиційні методи збору даних малоефективні або неможливі.

Особливо перспективним є підхід програмно-визначених сенсорних мереж (SDWSN), що дозволяє динамічно змінювати структуру мережі та ролі її вузлів залежно від умов завдання. Поєднання SDWSN із плануванням траєкторій БПЛА та моделями збору даних формує основу для створення енергоефективних, надійних і гнучких систем моніторингу.

Мета: Метою роботи є дослідження методів і алгоритмів енергоефективного збору даних у бездротових сенсорних мережах із використанням безпілотних літальних апаратів, що забезпечують підвищення продуктивності мережі, оптимізацію траєкторії польоту БПЛА та вдосконалення процесів динамічної оркестрації топології в межах програмно-визначеної сенсорної мережі.

1. Сучасний стан бездротових сенсорних мереж

Розвиток сучасних технологій Інтернету речей, збільшення масштабів розподілених систем моніторингу та необхідність оперативного збору достовірних даних зумовлюють актуальність дослідження нових підходів до організації бездротових сенсорних мереж (БСМ). Традиційні методи збору інформації в таких мережах мають суттєві обмеження, пов'язані з обмеженим енергетичним ресурсом сенсорних вузлів, нерівномірним навантаженням, складністю забезпечення надійного зв'язку та недостатньою масштабованістю. Особливої уваги потребують питання підвищення енергоефективності, надійності передачі даних та адаптивності мереж до змін структури або умов експлуатації.

Одним із перспективних напрямів розвитку є використання безпілотних літальних апаратів (БПЛА) як мобільних колекторів даних у бездротових сенсорних мережах [1].

Завдяки мобільності, автономності та здатності швидко охоплювати великі

території дрони дають змогу суттєво зменшити енергоспоживання вузлів БСМ, підвищити ефективність збору інформації та мінімізувати проблеми, пов'язані з багатохоповою маршрутизацією.

Сучасні БСМ складаються з автономних сенсорних вузлів, що вимірюють параметри середовища, виконують попередню обробку даних та забезпечують передачу інформації до центральних вузлів чи агрегаторів. Складні умови експлуатації - нерівномірний рельєф, перешкоди, обмеження пропускної здатності - спричиняють втрати пакетів, повторні передачі та передчасне виснаження енергоресурсів вузлів. В умовах багатохопових топологій вузли, розташовані ближче до точки збору, працюють із підвищеним навантаженням, що призводить до їх швидкого виходу з ладу та появи енергетичних «дірок», які порушують цілісність мережі [2].

Застосування БПЛА у ролі мобільного елемента збору даних дозволяє принципово змінити архітектуру передачі інформації. Дрон, рухаючись за заздалегідь спланованою або адаптивною траєкторією, здійснює безпосередній збір пакетів зі шлюзових вузлів, що зменшує енергетичний тиск на сенсорні мережі та усуває потребу в частій ретрансляції даних. Це підвищує загальний термін служби мережі, забезпечує стабільність зв'язку та дозволяє працювати в умовах, де традиційні схеми маршрутизації малоефективні або недоцільні.

У рамках сучасних досліджень активно розвивається модель SDWSN - програмно-визначена бездротова сенсорна мережа, у якій ключові параметри її архітектури формуються динамічно за участю хмарних серверів та мобільного БПЛА. Такий підхід дає можливість оркеструвати (тобто перебудовувати) топологію залежно від умов конкретної місії, розподілу сенсорних вузлів та вимог до швидкості чи енергоефективності. БПЛА виконує не лише функцію колектора, а й координує процес оновлення ролей наземних вузлів - кінцевих, маршрутизаторів або шлюзів. Це дозволяє створювати гнучкі топології, які самостійно адаптуються до розподілу вузлів, зміни щільності мережі та доступності ліній зв'язку.

2. Методи підвищення ефективності роботи БСМ

Ключовою концепцією є «нечіткий маршрут польоту» БПЛА[1], що означає можливість вибору траєкторії у певному діапазоні замість жорстко визначеного шляху. Така гнучкість дозволяє оптимізувати маршрут з урахуванням енергоспоживання, уникати різких змін прискорення й швидкості та мінімізувати витрати енергії двигуна. Використання кривих Без'є та напівкруглих сегментів дає змогу формувати плавні траєкторії, що знижують коливання швидкості та підвищують загальну енергоефективність польоту.

Принцип нечіткого маршруту є лише однією з низки методик, спрямованих на підвищення ефективності роботи БСМ у поєднанні з БПЛА. Важливим аспектом є також адаптивний вибір шлюзових вузлів та динамічне формування кластерів, які дозволяють рівномірно розподіляти навантаження між сенсорними елементами та запобігати передчасному виснаженню окремих ділянок мережі. Формування кластерів із часовою ротацією ролей значно подовжує термін роботи мережі, адже кожен вузол виконує енергозатратні функції лише у визначені інтервали часу.

Ще одним важливим напрямом підвищення ефективності є оптимізація процесів зв'язку «повітря–земля». Вибір частоти обміну, параметрів модуляції, потужності передавача та часу активності модулів бездротового зв'язку безпосередньо впливають на величину затримок і втрат пакетів. Застосування алгоритмів адаптивного керування MAC-рівнем дає змогу зменшити кількість колізій, оптимізувати графіки пробудження вузлів і скоротити тривалість їх перебування в енергозатратних режимах.

Суттєвого покращення енергоефективності вдається досягти також за допомогою прогнозних моделей маршрутизації та планування польоту. За рахунок аналізу просторової щільності вузлів, рівня їх залишкової енергії та обсягів накопичених даних БПЛА може обирати оптимальні точки збору, мінімізуючи довжину маршруту та скорочуючи тривалість простою. Це дозволяє не лише знизити витрати енергії самого БПЛА, а й зменшити затримки передачі даних у мережі.

Крім того, застосування програмно-визначеної архітектури SDWSN дає змогу централізовано керувати параметрами всієї мережі в реальному часі. Контролер у хмарному середовищі аналізує стан мережі й передає БПЛА рішення щодо вибору оптимальної конфігурації: ролей вузлів, маршрутів доставки пакетів, обмежень на обмін даними та пріоритетів передачі. Така централізована оркестрація забезпечує стабільну роботу навіть у динамічних або непередбачуваних умовах, де класичні децентралізовані підходи можуть бути малоефективними.

Висновки. У роботі розглянуто методи підвищення ефективності збору даних у бездротових сенсорних мережах із використанням БПЛА та програмно-визначеної архітектури (SDWSN). Проаналізовано обмеження традиційних БСМ, зумовлені високим енергоспоживанням вузлів, нестабільністю зв'язку та низькою масштабованістю, і показано, що використання БПЛА як мобільних колекторів суттєво покращує продуктивність мережі, зменшує кількість ретрансляцій та забезпечує доступ до віддалених зон.

Нечіткий маршрут польоту, адаптивне кластерування, вибір шлюзових вузлів, оптимізація радіоканалу та централізована оркестрація - спрямовані на зниження енергоспоживання і підвищення надійності передачі даних. Плавні траєкторії руху БПЛА, побудовані на основі кривих Без'є, додатково підвищують енергоефективність і якість зв'язку «повітря–земля».

Використання SDWSN забезпечує динамічне конфігурування мережі відповідно до умов місії, дозволяє змінювати ролі вузлів і структуру топології, підвищуючи адаптивність та стійкість системи. Поєднання БПЛА та програмно-визначеної архітектури створює основу для побудови інтелектуальних автономних систем моніторингу.

Перелік використаних джерел.

1. KAREGAR, Pejman A.; AL-ANBUKY, Adnan. UAV-assisted data gathering from a sparse wireless sensor adaptive networks. Wireless Networks, 2023, 29.3: 1367-1384.

2. GHORBANI DEHKORDI, Elham; BARATI, Hamid. Cluster based routing method using mobile sinks in wireless sensor network. International Journal of Electronics, 2023, 110.2: 360-372.

УДК 681.32

Карпюк І.О., Волянюк Т.Ф. Дорошенко О.В.

Західноукраїнський національний університет

ІНТЕГРАЦІЯ ЦИФРОВИХ ПРИЛАДІВ В АВТОМАТИЗОВАНІ СИСТЕМИ ВИМІРЮВАННЯ ТА МОНІТОРИНГУ

У сучасних умовах розвитку промислових, енергетичних та інформаційно-керуючих систем зростає потреба у високоточних, надійних і автоматизованих засобах вимірювання та моніторингу параметрів технологічних процесів. Інтеграція цифрових приладів передбачає їх об'єднання за допомогою інтерфейсів.

Функції інтерфейсів включають:

- передачу результатів вимірювань у цифровому вигляді для подальшої обробки або збереження;
- прийом команд керування від зовнішніх програмних або апаратних засобів (наприклад, запуск вимірювань, зміна режиму, калібрування);
- синхронізацію дій у складі багатоканальних або мультисенсорних систем;
- обмін діагностичною та службовою інформацією, наприклад, про стан приладу, помилки або статус підключення.

Інтерфейси цифрових приладів можна класифікувати за такими ознаками:

За типом з'єднання:

- провідні (дротові): USB, RS-232, GPIB (IEEE-488), LAN (Ethernet).
- бездротові: Wi-Fi, Bluetooth.

За способом передачі даних:

- серійні інтерфейси (RS-232, USB, GPIB) - передають дані послідовно, один біт за раз.
- паралельні інтерфейси - зустрічаються рідко, зазвичай у старих або спеціалізованих пристроях.

За призначенням:

- локальні інтерфейси (USB, RS-232) - для підключення до одного ПК або контролера на невеликій відстані.
- мережеві інтерфейси (LAN, Wi-Fi) - для підключення до локальної мережі або хмари, що дозволяє розміщення приладів у розподілених системах.

За рівнем підтримки стандартизованих протоколів:

- інтерфейси з підтримкою SCPI-протоколу (наприклад, USB, GPIB, LAN) - дозволяють використовувати прилад у складі стандартних програмно-апаратних рішень.
- інтерфейси з власними протоколами - характерні для дешевших або спеціалізованих приладів.

Таким чином, інтерфейси цифрових мультиметрів є критично важливою частиною їхньої функціональності в сучасних умовах, де все більшу роль відіграє автоматизація вимірювань, віддалений моніторинг, контроль та інтеграція в цифрові системи. Для реалізації системи вибрана централізована архітектура, яка передбачає наявність одного центрального вузла - сервера або головного контролера, до якого

підключаються цифрові прилади. Уся обробка інформації, прийняття рішень і керування процесами вимірювань, збору та обробки інформації відбуваються саме в цьому центрі. Завдяки такій простій структурі значно спрощується процес розробки системи, її впровадження та технічне обслуговування. Вартість такої системи порівняно невисока, адже периферійні пристрої можуть бути простими і не потребують власної обчислювальної потужності. Програмне забезпечення розміщується на одному сервері, що полегшує його оновлення та централізоване адміністрування. Математичні моделі, включаючи фільтрацію, діагностику та прогнозування, також реалізуються на центральному рівні, що дає змогу використовувати потужні аналітичні засоби. Особливою перевагою є простота масштабування системи, яка дозволяє без особливих труднощів інтегрувати додаткові пристрої (рисунок 1).

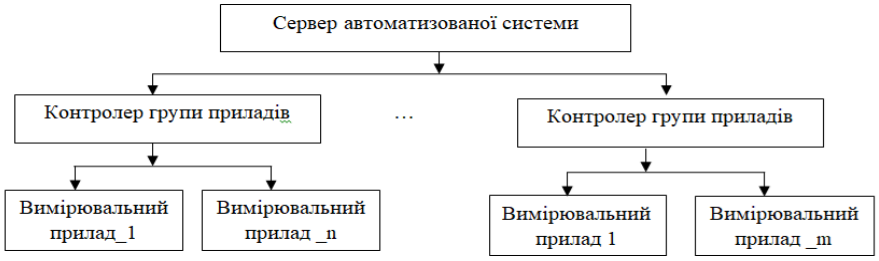


Рисунок 1 – Структурна схема автоматизованої системи вимірювання та контролю

Особливістю централізованої архітектури автоматизованої системи інтеграції цифрових приладів є використання в ролі проміжної ланки мікроконтролера ESP32. Він виконує функції контролера групи цифрових приладів, що розміщені просторово поряд. Зв'язок між ESP32 та цими вимірювальними приладами пропонується здійснюється через дротові інтерфейси, що забезпечує надійність обміну даними, мінімальні затримки та стійкість до зовнішніх завад. Вибір дротового інтерфейсу для передачі вимірювальних даних від приладів до ESP32 ґрунтується на трьох головних потребах автоматизованої системи: гарантії стабільності зв’язку, високій пропускній здатності та передбачуваності затримок при обміні даними.

Загальна структура функціонування системи виглядає наступним чином – рисунок 2.

```
ПК (SCPI-команди по Wi-Fi)
        ⇅
  Wi-Fi (TCP-сервер на ESP32)
        ⇅
ESP32 (обробка SCPI)
        ⇅
UART (RS-232 через MAX232)
        ⇅
Мультиметр SIGLENT SDM3045X
```

Рисунок 2 - Структура функціонування системи вимірювання та контролю

Тобто, контролер ESP32 приймає SCPI-команди через Wi-Fi, розпізнає тип вимірювання та канал, пересилає відповідну команду до цифрового приладу та приймає результати вимірювання по UART.

Перелік використаних джерел.

1. Володарський Є.Т., Кухарчук В.В., Поджаренко В.О., Сердюк Г.Б. В 68 Метрологічне забезпечення вимірювань і контролю. Навчальний посібник. -Вінниця: ВДТУ, 2001. –219с.

УДК 681.32

Возьний А.О., Луцак А.Р., Луцак Б.Р.

Західноукраїнський національний університет

МЕТОДИ КАЛІБРУВАННЯ СЕНСОРІВ ПРИ ВИМІРЮВАННІ ФІЗИЧНИХ ПАРАМЕТРІВ

Вступ. У сучасній метрологічній практиці поняття невизначеності вимірювань є фундаментальним для забезпечення достовірності результатів. На відміну від класичного уявлення про похибку як відхилення від істинного значення, яке, як правило, залишається невідомим, невизначеність дозволяє кількісно оцінити довіру до результату вимірювання.

Такий підхід ґрунтується на методології, викладеній у Міжнародному керівництві з вираження невизначеності вимірювань (GUM), що має статус стандарту ISO/IEC Guide 98-3:2008. Цей документ набув чинності також в Україні у вигляді ДСТУ ISO/IEC Guide 98-3:2009 і є базовим при аналізі точності вимірювань у технічних і наукових дослідженнях.

Виклад основного матеріалу.

Згідно з GUM, результат вимірювання слід подавати у вигляді оцінки значення величини разом з невизначеністю, яка охоплює діапазон можливих істинних значень. Центральним поняттям є стандартна невизначеність, яка може бути визначена на основі статистичного аналізу або із застосуванням апріорної інформації.

У першому випадку йдеться про невизначеність типу А, що базується на серії повторних вимірювань та характеризується дисперсією спостережуваних значень. Тип А базується на статистичному аналізі результатів серії вимірювань.

У другому - про невизначеність типу В, яка відображає наше знання про можливий діапазон значення величини на основі технічної документації, результатів калібрування, специфікацій виробника, досвіду або інших обґрунтованих джерел. Невизначеність типу В оцінюється на основі апріорної інформації, що не має статистичної природи: паспортні их характеристик засобів вимірювальної техніки; результатів калібрування; специфікації виробника; допусків; наукових публікацій; експертної оцінки.

Важливо розуміти, що невизначеність типу В не є менш надійною, ніж типу А - вона лише спирається на інші методи оцінювання.

Сучасні сенсорні технології розвиваються в умовах інтенсивної глобальної конкуренції, коли від якості, надійності та доступності сенсорної продукції залежить ефективність побудови вимірювальних систем у різних галузях - від побутових до промислових. Провідні світові компанії формують ринок сенсорів, орієнтуючись на мініатюризацію, енергоефективність, точність вимірювань і здатність до роботи в розподілених середовищах з мінімальним втручанням людини – таблиця 1.

Більшість сенсорів калібруються при виготовленні, проте з часом їх характеристики можуть змінюватись внаслідок старіння, дрейфу або механічного впливу.

Таблиця 1 - Порівняльна таблиця основних характеристик продукції провідних виробників

Виробник	Основна спеціалізація	Типи сенсорів	Типові інтерфейси	Визначальні особливості
Bosch Sensortec	MEMS для споживчої електроніки	Температура, тиск, газ, IMU	I²C, SPI	Інтегровані модулі, низьке споживання
Analog Devices	Промислові сенсори	Температура, струм, вібрації	SPI, UART	Висока точність, внутрішнє калібрування
Honeywell	Промисловість, транспорт	Тиск, температура, положення	Analog, I²C	Висока надійність, розширені діапазони
TE Connectivity	Автомобільна та військова сфера	Волога, температура, тиск	Analog, I²C, CAN	Захист IP67/68, ударостійкість
Sensirion	Smart Home, HVAC	Вологість, CO_2, леткі гази	I²C, UART	Картриджі з калібруванням, точність
Murata	Високочастотна електроніка	Акселерометри, гіроскопи	I²C, SPI	Компактність, низький рівень шуму

Для промислових рішень застосовують регулярне метрологічне обслуговування з використанням еталонного обладнання.

Нижче наведено таблицю 2 для орієнтації щодо діапазону умов експлуатації та потреби в калібруванні сенсорів температури

Таблиця 2 – Орієнтовна потреба в каліюрування

Сенсор	Робочий діапазон (°C)	Захист IP	Час служби (типовий)	Потреба в калібруванні
BME280 (Bosch)	-40...+85	IP20	до 5 років	бажано щороку
HIH6130 (Honeywell)	-25...+85	IP65	5–8 років	періодично
SCD30 (Sensirion)	0...+50	IP30	3–5 років	рекомендовано щопівроку
D6T-44L (Omron)	0...+80	IP20	до 3 років	обов'язково

Деградація сенсорів - це сукупність процесів, що з часом змінюють їх метрологічні властивості. Це є старіння матеріалів, яке відбувається через тривалі температурні та механічні цикли, що викликають окислення металевих компонентів, втрату еластичності полімерів та зміну електричних характеристик чутливих елементів. Ці процеси супроводжуються дрейфом сигналу, коли вихідний сигнал сенсора відхиляється від калібрувального рівня – таблиця 3.

Таблиця 3 - Основні фактори деградації та їх вплив на характеристики сенсорів

Фактор впливу	Вплив на сенсор	Наслідки для точності	Методи мінімізації
Температурні коливання	Механічні напруження в матеріалах	Дрейф, зміщення базового сигналу	Використання стабілізаторів температури, вибір сенсорів з широким діапазоном
Волога і корозія	Руйнування контактів і корпусу	Несправності, зростання шуму	Герметизація, IP-класифікація
Механічні удари і вібрації	Зсув калібрування, пошкодження	Зниження чутливості, втрата сигналу	Віброізоляція, міцні корпуси
Електромагнітні завади	Спотворення сигналів	Похибки, збільшення шумів	Екранування, використання диференціальних схем

Для забезпечення надійності і тривалості роботи сенсорів у складних умовах застосовують комплексні заходи. Серед них можна виділити регулярні повірку та калібрування за допомогою еталонних приладів, що допомагає відновити точність показань. Повірка і калібрування, хоча і тісно пов’язані між собою, мають принципові відмінності. Повірка - це офіційна процедура, що здійснюється відповідно до нормативних документів і передбачає перевірку відповідності приладу встановленим стандартам і технічним вимогам. Результатом повірки є підтвердження або відмова у відповідності, часто із внесенням запису до державного реєстру, що дає підставу для використання приладу в офіційних та юридично значущих процесах. В Україні ця діяльність регламентується, зокрема, ДСТУ ISO/IEC 17025, ДСТУ 8.584 та іншими документами, що встановлюють правила та порядок проведення метрологічних перевірок. Калібрування, у свою чергу, є процедурою встановлення або відновлення зв’язку між показаннями сенсора і еталонним значенням. Воно передбачає визначення похибок приладу та, за необхідності, їх корекцію або врахування при обробці результатів вимірювань. Калібрування не має юридичного статусу підтвердження відповідності, але є ключовим елементом у забезпеченні якості вимірювань і підтриманні метрологічної надійності. В рамках калібрування можуть використовуватися різні методи і підходи, залежно від типу сенсора, умов експлуатації та вимог до точності.

У практиці калібрування сенсорів широко застосовують кілька основних методів. Перший - це статичне калібрування, коли сенсор піддається тестуванню у фіксованих умовах, зокрема за визначених температур, вологості або інших параметрів, що мають суттєвий вплив на його роботу. Це дозволяє створити таблиці або функції корекції, які потім застосовуються під час реальних вимірювань. Другий підхід - динамічне калібрування, яке враховує змінні умови експлуатації та поведінку сенсора у реальному часі. Воно особливо важливе для IoT-систем, які працюють у непередбачуваних середовищах, де вплив зовнішніх факторів постійно змінюється. Для цього можуть використовуватися моделі, що адаптуються, або алгоритми машинного

навчання, які коригують показання автоматично. Третій напрям - калібрування на основі порівняння в мережі. У великих мережах дані з численних сенсорів порівнюють між собою для виявлення аномалій і оцінки точності, що дозволяє здійснювати непряму калібрувальну корекцію без необхідності фізичного доступу до кожного пристрою. При цьому важливо враховувати, що вибір методу калібрування залежить від типу сенсора, його призначення, умов експлуатації, а також вимог до точності і частоти оновлення даних. Відповідно, розробка ефективної стратегії калібрування сенсорів потребує комплексного підходу, що поєднує стандартизовані метрологічні процедури із сучасними цифровими технологіями.

З метою забезпечення достовірності вимірювань температури та виявлення деградації характеристик сенсора у складі вимірювальної системи запропоновано методику його повірки. Для повірки температурного сенсора на базі MAX31855 з термопарою типу K було обрано калібратор температури Fluke 714B Thermocouple Calibrator, що відповідає вимогам до точності, сумісності з термопарами та простоти інтеграції в лабораторний стенд – таблиця 4.

Таблиця 4 - Вимоги до точності, сумісності з термопарами

Параметр	Значення
Підтримка термопар	Типи J, K, T, E, R, S, B, N
Діапазон імітації температур (тип K)	від –270 °C до +1372 °C
Похибка імітації (тип K)	±0.5 °C при 0 °C; ±0.9 °C при 1000 °C
Інтерфейс	Ручне введення значень, калібрування в режимі джерела
Живлення	Батарейне
Сертифікація	NIST traceable calibration certificate

Калібратор дозволяє формувати точне значення температури у вигляді електричної напруги, що імітує сигнал термопари, забезпечуючи умови для безконтактного тестування MAX31855 без необхідності створення реального температурного середовища – рисунок 1.

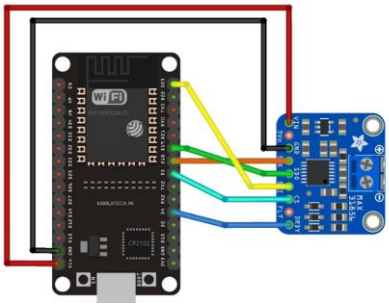


Рисунок 1 – Типова схема підключення MAX31855 до мікроконтролера

Завдяки такому підходу програмний код не лише реалізує зчитування, а й забезпечує адаптивне підвищення точності вимірювання, включаючи облік процесів старіння сенсора.

Перелік використаних джерел.

1. Основи метрології та вимірювальної техніки / Лис, О.М., Якименко, М.В., Шинкаренко [та ін.]. - Львів: Видавництво Львівської політехніки, 2021. – 424 с.