НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

МАТЕРІАЛИ
ІІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ»

22 грудня 2021 року

Київ – 2021

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол №17 від 15 грудня 2021 р.)

Б-39 **Безпека енергетики** в епоху цифрової трансформації, ІІІ науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 22 грудня 2021 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2021. 140 с.

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ

ім. Г.Є. ПУХОВА НАН УКРАЇНИ

МАТЕРІАЛИ III НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

22 грудня 2021 року
м. Київ

2021

Вельмишановний учасник _____

_____

Запрошуємо Вас прийняти участь в роботі III науково-практичної конференції «Безпека енергетики в епоху цифрової трансформації», яка буде проходити 22 грудня 2021 року в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України (м. Київ).

СПІВОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

АСОЦІАЦІЯ «ІНФОРМАТІО-КОНСОРЦІУМ»

ТОВ «ІНФОРМАТІО»

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Артемчук Володимир Олександрович
доктор технічних наук, старший науковий співробітник

Чемерис Олександр Анатолійович
доктор технічних наук, старший науковий співробітник

Куцан Юлій Григорович
доктор технічних наук, заслужений енергетик України

Гончар Сергій Феодосійович
доктор технічних наук, старший дослідник

Гурєєв Віктор Олександрович
доктор технічних наук

Гільгурт Сергій Якович
доктор технічних наук, старший науковий співробітник

Богданов Олександр Михайлович
доктор технічних наук, професор

Борукаєв Зелімхан Харитонович
доктор технічних наук, старший науковий співробітник

Верлань Анатолій Федорович
доктор технічних наук, професор

Винничук Степан Дмитрович
доктор технічних наук, професор, старший науковий співробітник

Владимирський Олександр Альбертович
доктор технічних наук, старший науковий співробітник

Євдокимов Віктор Федорович
член-кореспондент НАН України, доктор технічних наук, професор, почесний директор Інституту

Самойлов Віктор Дмитрович
доктор технічних наук, професор

Саух Сергій Євгонович
член-кореспондент НАН України, доктор технічних наук, професор

Яцишин Андрій Володимирович
доктор технічних наук, старший науковий співробітник

Анфимова Галина Викторовна,
ННПМ НАН Украины,
научный сотрудник,
ИПМЭ им. Г.Е. Пухова НАН Украины,
инж. 1 кат,
anfimova77@ukr.net

О РИСК-ОРИЕНТИРОВАННОМ ПОДХОДЕ В ОБЕСПЕЧЕНИИ ЭКОЛОГИЧНОСТИ И КАЧЕСТВА ЭКСПЛУАТАЦИИ ТРУБОПРОВОДОВ ТЕПЛОСНАБЖЕНИЯ

Анотація. Наведено підхід до побудови системи збору даних та оцінки ризиків аварійних подій на трубопроводах теплових мереж на основі дистанційних засобів визначення корозійного стоншення стінок трубопроводу.

Abstract. An approach to the construction of a system for collecting data and assessing the risks of emergency events on pipelines of heating networks based on remote means for determining the corrosive thickness of the pipeline walls is presented.

В ИПМЭ им. Г.Е. Пухова НАН Украины проводятся исследования, направленные на создание проактивной системы управления рисками, связанной с безопасной эксплуатацией изношенных трубопроводов теплосетей урбанизированных территорий.

Известно, что большая часть системы теплоснабжения отечественных городов выработала свой ресурс и находится в крайне аварийном состоянии. Постоянные порывы подземных трубопроводов, большой объем оперативных диагностических и ремонтных работ по выявлению и устранению повреждений приводят к огромным финансовым затратам и экологическому ущербу. Аварийный режим работы стал повседневной практикой организаций, эксплуатирующих трубопроводы. Следует признать, что из-за отсутствия адекватной масштабной программы замены трубопроводов, тепловые сети превратились в достаточно опасный объект и инциденты с человеческими жертвами становятся все более вероятными.

В последние десятилетия в различных отраслях интенсивно внедряются и применяются подходы, связанные с понятием рисков [1]. Риск характеризуется как “сочетание вероятности события и его последствий”. В качестве примеров можно привести использование элементов риск-ориентированного подхода в системах управления промышленной безопасностью и охраной труда предприятий [2], в обеспечении экологических требований на объектах нефтехимии [3], в атомной энергетике [4] и в газотранспортных системах [5].

На основании опыта многолетних работ по диагностированию трубопроводов киевских тепловых сетей в ИПМЭ им. Г.Е. Пухова выработан

комплекс мер, направленных на повышение качества их эксплуатации [6]. При этом основой, необходимой для достоверной оценки рисков аварий на участках теплосетей, должны стать, в первую очередь, точные данные о текущем коррозионном износе подземных трубопроводов, получаемые с помощью оригинального специализированного дистанционного оборудования «РАСТР» [6], разработанного в ИПМЭ им. Г.Е. Пухова НАН Украины. Многолетний опыт свидетельствует о том, что тепловые сети имеют большой запас прочности и повреждения происходят практически исключительно в местах коррозионного утонения стенок трубопроводов. В качестве дополнительных факторов необходимо учитывать соотношение величины нормативного и фактического сроков эксплуатации трубопроводов, статистику повреждений и ремонтов на разных участках в последние годы, режимные параметры и прочие обстоятельства, повышающие риск масштабных аварий, например, высокий уровень грунтовых вод, заливание каналов теплосетей водой из систем водоснабжения и многое другое.

На основе ранжирования полученных рисков должны планироваться соответствующие организационно-технические мероприятия, в том числе, и прицельная перекладка небольших, наиболее корродированных участков трубопроводов до того момента, когда на них произойдет авария, создание локальных систем постоянного мониторинга наиболее ответственных участков и пр.

Построение предлагаемой системы сбора данных и оценки рисков позволит снизить влияние человеческого фактора, а также перейти на проактивное управление рисками при эксплуатации трубопроводов теплосетей урбанизированных территорий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Хенли Э.Д., Кумато Х. Надежность технических систем и оценка риска. М.: Машиностроение, 1979. 528 с.
2. Bulygin Yu. I., Tkacheva V. A., Lutkova E. M. Elements of risk-oriented approach in industrial safety and labor protection management systems of enterprises. *Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal)*, #11 (51), 2019. С. 35-40.
3. Фоменко Г.А., Комаров С.И., Фоменко М.А., Бородкин А.Е., Лузанова А.К. Риск-ориентированный подход к управлению экологической безопасностью нефтеперерабатывающего предприятия. *Стратегические решения и риск-менеджмент*. 2018;(2):102-109. https://doi.org/10.17747/2078-8886-2018-2-102-109
4. Комаров Ю.А. Развитие риск-ориентированных подходов для повышения безопасности и эффективности эксплуатации атомных электростанций: монография / Под ред. В. И. Скалозубова. Чернобыль: Ин-т проблем безопасности АЭС НАН Украины, 2014. 288 с.

5. Бородин В.И., Ляпичев Д.М., Шепелев Р.Е., Лопатин А.С., Никулина Д.П. Применение риск-ориентированного подхода к оценке необходимости и целесообразности установки систем мониторинга технического состояния газопроводов. https://neftegas.info/article/ primenenie-risk-orientirovannogo-podkhoda-k-otsenke-neobkhodimosti-i-tselesoobraznosti-ustanovki-sis/.

6. Владимирський О.А., Владимирський І.А. Шляхи підвищення якісних показників експлуатації зношених підземних трубопроводів теплових мереж. *Моделювання та інформаційні технології. Збірник наукових праць*. Вип. 88, Київ: Інститут проблем моделювання в енергетиці НАН України, 2019. С. 23-32. http://doi.org/10.5281/zenodo.3859671.

Артемчук Володимир Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з науково-організаційної роботи,
ak24avo@gmail.com

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ «ЗЕЛЕНИХ» СЕРТИФІКАТІВ ДЛЯ ПІДПРИЄМСТВ В УКРАЇНІ

Анотація. Глобальні кліматичні та екологічні проблеми спонукають багато компаній у всьому світі до переходу на відновлювальні джерела енергії (ВДЕ). В цьому контексті необхідно мати надійний спосіб відстеження генерування та споживання електроенергії з ВДЕ. Для вирішення цієї проблеми запропоновано використовувати електронні «зелені» сертифікати (також мають назву «гарантії походження» - GO в ЄС або «сертифікати на відновлювану енергію» - REC в США).

Abstract. Global climate and environmental challenges are prompting many companies around the world to switch to renewable energy sources (RES). In this context, it is necessary to have a reliable way to track the generation and consumption of electricity from RES. To solve this problem, it is proposed to use electronic "green" certificates (also called "guarantees of origin" - GO in the EU or "renewable energy certificates" - REC in the US).

Сертифікація енергії виробленої з ВДЕ - відносно тривала концепція, яка вже впроваджена в більшості країн ЄС шляхом запровадження системи видачі сертифікатів походження електричної енергії. Нормативно-правова основа системи GO - Директива 2009/28/ЄС Європейського парламенту та Ради про заохочення до використання енергії виробленої з ВДЕ, стаття 15 якої зобов'язує держави-члени ЄС видавати гарантії походження з метою підтвердження кінцевому споживачу відсотку чи кількості енергії, отриманої з ВДЕ. Така інформація повинна керувати поведінкою кінцевих споживачів, усуваючи «інформаційну асиметрію», коли кінцевий споживач не має цієї інформації. Водночас, сприяючи обміну GO в масштабі ЄС, Європейська Комісія мала на меті створення привабливого ринкового інструменту для виробників, трейдерів та постачальників. Основним припущенням було те, що GO стимулюватимуть нові інвестиції у ВДЕ. Минуло десять років з моменту введення GO, озираючись на які, європейський ринок GO навряд чи можна назвати великим успіхом. Незважаючи на те, що кількість виданих GO постійно збільшується, і спостерігається очевидне зростання споживання GO, розмір цього ринку, напевно, не такий великий, як планувалося спочатку. Що дуже важливо - і на цьому необхідно постійно та безперервно наголошувати - це поява функціонуючої та стандартизованої рамкової нормативної основи для GO. Гарантії походження видаються відповідно до правил Європейської системи енергетичних сертифікатів (EECS), які кожна держава-член транспонує у свій національний протокол домену. Правила, в

свою чергу, затверджуються Асоціацією органів видачі сертифікатів (AIB), яка управляє міжнародним реєстраційним хабом, який прямо підключений до кожного національного органу, що видає GO. Ця система дозволяє здійснювати безперебійну торгівлю GO в державах-членах ЄС, мінімізуючи трансакційні витрати та можливість шахрайства. Це важлива передумова для будь-якого подальшого розвитку і реформування системи [1].

Однак звичайні «зелені» сертифікати не прив'язують виробництво до фактичного споживання за часом. Облік зазвичай ведеться на річній основі. Водночас з'являються інструменти, що дозволяють споживачам відстежувати походження енергії в режимі близького до реального часу. Понад 100 корпорацій і організацій, серед яких Google, Microsoft, PwC, Vattenfall, Statkraft і Engie, підтримали проєкт EnergyTag, мета якого - підвищити прозорість ринку «зелених» сертифікатів. З використанням EnergyTag, ціни на сертифікати будуть рости в періоди, коли виробництво відновлюваних джерел енергії знаходиться на низькому рівні, «посилаючи ринковий сигнал для збільшення інвестицій в технології, які можуть генерувати електроенергію в ці години». Погодинне відстеження також дозволить споживачам більш точно розраховувати свої викиди в залежності від того, наскільки вуглеводною є мережа в певні години. EnergyTag стверджує, що ринок погодинних сертифікатів також буде стимулювати зростання гнучких технологій, таких як зберігання енергії або управління попитом. «Створюючи ринок для погодинних сертифікатів, EnergyTag буде ефективно винагороджувати чисту енергію, доступну при обмеженій пропозиції, забезпечуючи новий ціновий сигнал для стимулювання інвестицій в накопичення енергії й гнучкість» [2].

Україна взяла на себе зобов'язання з впровадження системи GO в 2012 році. Однак, як зазначається в останньому звіті Енергетичного Співтовариства (ЕС) у листопаді 2020 року про впровадження системи, Державному агентству з енергоефективності та енергозбереження як призначеному органу не вдалося впровадити електронну систему, сумісну з системою Європейських енергетичних сертифікатів. Крім того, в даному контексті необхідно забезпечити можливість достовірно довести всім сторонам, які беруть участь в аукціонах з GO, що видані, передані та скасовані сертифікати відповідають об'єктивній дійсності. Також було б неправильно надмірно покладатися на інноваційні рішення, такі як блокчейн, щоб гарантувати правильність даних, пов'язаних з GO. Блокчейн гарантує, що ніхто не заволодіє даними після їх введення в систему. Проте потрібно, щоб введені дані вже пройшли перевірку на відповідність і були перевірені. При цьому, централізований орган з чіткою відповідальністю та доступом до відповідних даних від операторів системи є більш вдалим для функціонуючої системи GO, ніж децентралізоване рішення. Тому, створення додаткової до поточної системи, що базується на EECS, якою керує AIB, може бути ризикованою справою. Поступове і безперервне зближення з EECS і, врешті-решт, повноцінне членство в AIB ЄС є, ймовірно, кращим підходом [3].

Одним з стимулів для прискорення впровадження «зелених» сертифікатів в Україні може стати механізм прикордонного вуглецевого коригування (CBAM), проєкт регламенту про встановлення якого опубліковано в липні 2021 року. CBAM – це кліматичний захід, який покликаний запобігти ризику витоку вуглецю та підтримати кліматичні амбіції ЄС. Спочатку цей інструмент застосовуватиметься до імпорту цементу, заліза та сталі, алюмінію, добрив, електроенергії. Починаючи з 2026 року імпортери ЄС, зокрема і українські імпортери, придбаватимуть вуглецеві сертифікати, що відповідатимуть ціні вуглецю, яка була б сплачена, якби товари були вироблені за правилами ціноутворення на вуглець, які діють в ЄС. У разі ухвалення акта по CBAM в нинішній редакції українські імпортери будуть сплачувати до бюджету ЄС до 396 млн євро щорічно [4].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Зелені» сертифікати в Європі; підсумок за останні десять років [Електронний ресурс] https://expro.com.ua/statti/zelen-sertifkati-v-vrop-pdsumok-za-ostann-desyat-rokv. Дата звернення: 10.12.2021.
2. Зелені сертифікати для підприємств [Електронний ресурс] https://energy365.com.ua/tpost/k27ixafkz1-zelen-sertifkati-dlya-pdprimstv. Дата звернення: 10.12.2021.
3. «Зелені» сертифікати в Україні; quo vadis? [Електронний ресурс] https://expro.com.ua/statti/zelen-sertifkati-v-ukran-quo-vadis-. Дата звернення: 10.12.2021.
4. Європейський зелений курс та Зелений перехід України: спільні цілі та трансформаційні виклики [Електронний ресурс] https://vkp.ua/about-us/news/ievropeyskiy-zeleniy-kurs-ta-zeleniy-perekhid-ukrayini-spilni-tsili-ta-transformatsiyni-vikliki. Дата звернення: 10.12.2021.

Владимирський Олександр Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
пров.н.с.,
av1000000@ukr.net

Владимирський Ігор Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
ст.н.с.,
av1000000@ukr.net

Куцан Юлій Григорович,
ІПМЕ ім. Г.Є. Пухова НАН України,
ст.н.с.,
kutsan.ug@ukr.net

Криворучко Ігор Петрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
uhmi_igorkr@ukr.net

Анфімова Галина Вікторівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
інж. 1 кат,
anfimova77@ukr.net

ПРО ПАРАМЕТРИЧНІ КОРЕЛЯЦІЙНІ МЕТОДИ ДИСТАНЦІЙНОГО ПАСИВНОГО ВИЗНАЧЕННЯ КООРДИНАТ ВИТОКІВ ТА СУПУТНІХ КОРОЗІЙНИХ ПОШКОДЖЕНЬ ТРУБОПРОВОДІВ

Анотація. Представлено вдосконалення методів параметричної кореляції в напрямку зручності аналізу недомінуючих спалахів взаємних кореляційних функцій. Новий метод дає змогу визначити координати менших витоків та корозійного витончення стінок трубопроводів, пов'язаних із витоками.

Abstract. The improvement of parametric correlation methods in the direction of the convenience of analyzing non-dominant bursts of cross correlation functions is presented. The new method makes it possible to determine the coordinates of smaller leaks and corrosive thinning of pipelines' walls associated with leaks.

Представлено результати досліджень та розробок з НДР «Монітор-2» та «Ресурс-3», які присвячено створенню параметричних методів діагностування підземних трубопроводів, які є розвитком відомого кореляційного методу визначення координат витоків у напрямку врахування

ускладнень, які вносять множинність типів хвиль та пошкоджень у сукупності зі сторонніми завадами.

Є спосіб частотного аналізу кореляційних функцій вібросигналів [1], згідно з яким, за допомогою високоякісних цифрових фільтрів виконують розкладання взаємної кореляційної функції на вузькосмугові складові. Для кожної частотної смуги визначають наступні параметри: затримка, при якій спостерігається максимум кореляції; якість максимуму кореляційної функції (виразність); потужність вузькосмугової складової. Саме ці параметри: затримка, якість та потужність відображають потрібні оператору якості частотної залежності домінуючого сплеску в оцінці ВКФ, яку він аналізує. Тому зазначений підхід параметричного подання ВКФ було прийнято за основу для подальшого розвитку.

Слід зауважити, що практикована деякими фахівцями перестановка датчиків і повторне визначення координати витоку з метою контролю повторюваності одержуваних координат витоків є корисною, однак в частині врахування впливу багатохвильового поширення вібросигналів, явищ інтерференції, її замало, оскільки при цьому потрібен критерій не повторюваності результатів, а правильності вибору конкретної позиції датчиків на трубопроводі для селекції необхідного типу акустичних хвиль, адекватних за швидкістю поширення величині швидкості, що використовується для забезпечення коректних результатів.

Розробка починається побудовою діагностичної моделі ділянки трубопроводу, яка моделює наявність на ньому пошкоджень як джерел стаціонарних акустичних шумів, багатохвильове поширення цих шумів до датчиків течешукача, а також наявність сторонніх, статистично не пов'язаних завад. Модель призначена для формалізації наявних ускладнень та побудови адекватних алгоритмів їх подолання. Формується перелік діагностичних параметрів, які в умовах інтерференційних спотворень за величиною характеризують якість селекції інформативної хвилі гідравлічного удару. Проаналізовано зв'язок ускладнень з цими параметрами. Показано зв'язок між моделлю, параметричним аналізом та визначенням координат витоків.

Представлено кореляційні параметричні просторовий та частотний методи [2, 3] визначення координат витоків. Ці методи можуть використовуватись незалежно один від одного. Просторовий метод націлено на подолання часово-частотних спотворень інформативної кореляції, а частотний – на подолання амплітудно-частотних завадових спотворень.

Розроблено параметричний автоматизований метод узгодженої просторово-частотної селекції координат пошкоджень трубопроводів. Метод базується на параметрах наступного рівня, а саме на параметрах просторового та частотного неузгодження параметрів потужності та якості (відношення сигнал-завада). Ці параметри дозволяють узгодити просторову та частотну селекцію інформативної кореляції, сформованої потужними хвилями гідравлічного удару, за допомогою оцінки кінцевої похибки цієї селекції.

Створено об'єкти інтелектуальної власності:

- Патент на корисну модель “Параметричний кореляційний спосіб визначення координат пошкоджень трубопроводів” [4].
- Науковий твір “Параметричний кореляційний течешукач К-10.5М3. Керівництво з експлуатації К105М3-1.00.04 КЕ” [5].
- Комп'ютерна програма “Параметричний кореляційний течешукач К-10.5М3”.

Нові параметричні методи реалізовані у складі нової версії кореляційного течешукача розробки ІПМЕ ім. Г.Є.Пухова НАН України К-10.5М3. Отримано експериментальне підтвердження ефективності запропонованих параметричних методів при діагностуванні теплової мережі.

Подальші дослідження будуть зосереджені на вдосконаленні активних методів низькочастотного акустичного діагностування, оскільки саме ці методи повинні стати основними при вирішенні наступного актуального завдання - розвитку та створенню системи корозійного дистанційного інструментального моніторингу підземних трубопроводів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Владимирский А.А., Владимирский И.А. Способ частотного анализа характеристик корреляционных функций вибросигналов. XX науково-технічна конференція "Моделювання": тези конференції 12-14 січня 2000 р. Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Київ, 2000. С. 23-24.
2. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів// Електрон. моделювання, 2021, 43, № 3, с. 3—17.
3. Владимирський О.А., Владимирський І.А. Просторовий і частотний кореляційні параметричні методи визначення координат витоків підземних трубопроводів // Електрон. моделювання, 2021, 43, № 4, с.22 —36.
4. Заявка на корисну модель № u 2021 04508; G01M 3/24, G01M 3/18, F17D. від 04.08.2021. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат пошкоджень трубопроводів. Заявник та власник патенту - ІПМЕ ім. Г.Є. Пухова НАН України. Рішення Укрпатенту № 14498/3У/21 про державну реєстрацію від 12.11.2021р.
5. Владимирський О.А., Владимирський І.А. Науковий твір “Параметричний кореляційний течешукач К-10.5М3. Керівництво з експлуатації К105М3-1.00.04 КЕ”. Заява про реєстрацію авторського права на службовий твір № С202108578 від 29.11.2021р. Заявник - ІПМЕ ім. Г.Є. Пухова НАН України.

Васильєв Олексій Всеволодович,
ІПМЕ ім. Г.Є. Пухова НАН України,
с.н.с.,
oleksii.vasyliev@gmail.com

Чьочь Вікторія Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
учений секретар Інституту,
Victoria.choch@gmail.com

МЕТОДИКА ПОРІВНЯННЯ ЗАКОНОДАВЧИХ ДОКУМЕНТІВ ТЕХНОЛОГІЧНОГО НАПРЯМУ

Анотація. В матеріалах доповіді представлена методика організації та аналізу порівняння законодавчих документів під час науково-методичних досліджень технологічного напряму. Використання такої методики дає можливість тривалого і систематичного вивчення законодавчих документів із визначенням їх рейтингової важливості для підготовки методичних документів науково-технічної сфери.

Abstract. The materials of the report present the methods of organization and analysis of the comparison of legislative documents during scientific and methodological research in the technological field. The use of such methodsprovides long-term and systematic study of legislative documents with the definition of their rating importance for the preparation of methodological documents in the scientific and technical sphere.

У структурі політики інформаційної безпеки необхідно виділити два основні напрями — державно-правовий та технологічний [1]. Найважливішим завданням держави в галузі інформаційної безпеки (в т.ч. кібербезпеки) є забезпечення гарантій конституційних прав і свобод людини та громадянина на доступ до інформації та забезпечення повноцінних можливостей для діяльності в інформаційній сфері.

Загальне законодавство в цілому визначає суспільні вимоги до кіберзахисту технічних та технологічних систем і може бути застосоване у правовій оцінці загроз при порушенні норм кібербезпеки, а в деяких випадках загальне законодавство включає прямі (безпосередні) норми кібербезпеки технічних систем.

Основні законодавчі документи провідних країн добре відомі фахівцям з питань кібербезпеки Тому метою інформаційного пошуку та порівняльного аналізу поставлено знаходження більш широкого кола законодавчих документів.

Існують два підходи досягнення поставленої мети. Перший – прямий пошук в законодавчих інформаційних масивах різних країн. Другий –

використання професійних (SCOPUS, WebofScience та ін.) та загальних (Scholar.Google.com та ін.) інформаційно-пошукових систем.

Загальним недоліком ефективності пошуку при першому підході є необхідність проведення пошуку мовою відповідної країни (колекції перекладів законодавчих документів англійською мовою дуже нечисленні), обмежені можливості організації пошуку в таких масивах (через переважне архівне призначення таких систем). Проте перший підхід необхідний для доступу до першоджерел, які необхідні для порівняльного аналізу законодавства.

Другий підхід надає доступ до вторинних документів – публікацій у спеціальній пресі (для професійних БД) або будь-яких публікацій для загальних пошукових систем, де обговорюються питання кібербезпеки із згадуванням законодавчих документів та норм. Результати такого пошуку дають реферативно-бібліографічний список публікацій, що задовольняють заданим критеріям пошуку (формулам пошуку), а також можливість виходу на повні тексти знайдених публікацій (може ускладнюватися необхідністю оплати доступу). Аналіз повних текстів публікацій, а інколи рефератів, може дати певні фактичні дані про законодавчий документ, його повну назву та інші атрибути законодавчого акту, іноді включаючи Інтернет-адресу першоджерела.

Загальна схема організації та обробки відомостей (включаючи зміст)публікацій та першоджерел представлена на Рис. 1.

Позначення елементів на Рис. 1. наведені нижче:

Джерелами інформації для проведення інформаційного пошуку обрані наступні бази даних (БД):

БД1 – Інформаційно-пошукова система SCOPUS (ElsevierB.V.); Пропонує структурований інформаційний пошук та можливості бібліографічного експорту результатів пошуку. Надає URLпосилання на архіви видавця та забезпечує крос-лінк на повні тексти публікацій (у випадку їх статусу – «Вільний доступ»);

БД2 - Інформаційно-пошукова системаWebofScience (ClarivateAnalytics). Пропонує структурований інформаційний пошук та можливості бібліографічного експорту результатів пошуку. Надає URLпосилання на архіви видавця та забезпечує крос-лінк на повні тексти публікацій (у випадку їх статусу – «Вільний доступ»);

БД3 - Інформаційно-пошукова система EBSCO-Host/BusinessSearchPremier (EBSCO Information Service). Пропонує структурований інформаційний пошук та можливості бібліографічного експорту результатів пошуку. Надає URLпосилання на архіви видавця та забезпечує ліцензований доступ до (або крос-лінк на) повні тексти публікацій;

БД4 – Інформаційно-пошукова система EBSCO-Host/AcademicSearchPremier (EBSCO Information Service). Пропонує структурований інформаційний пошук та можливості бібліографічного

експорту результатів пошуку. Надає URLпосилання на архіви видавця та забезпечує ліцензований доступ до (або крос-лінк на) повні тексти публікацій;

БД5 Scholar Google (Alphabet Inc.). Відкрита пошукова система, яка надає вільний доступ до вторинних джерел інформації у повному тексті (при наявності вільного доступу). Пропонує слабоструктурований пошук. Доступ до документів здійснюється через отримання прямого URL – посилання на джерело. Можливостей надання бібліографічного опису документу та експорту через будь-які транспортні формати система не має. Інформація в робочу БД переноситься в ручному режимі. Система користується каталогами наукових видавництв (та інших відкритих Інтернет сайтів) для створення глобального пошукового індексу;

БД6 - СистемаLEX-EU.(Архів законодавчих документів Європейського союзу. Пропонує слабоструктурований пошук та доступ до HTML/ PDF формату текстів законодавчих документів. Можливостей надання бібліографічного опису документу та експорту через будь-які транспортні формати система не має. Інформація в робочу БД переноситься в ручному режимі;

БД7 – Пошукова система USCode (Довідкова система Кодексу законів США). Пропонує слабоструктурований пошук та доступ до HTML/ PDF формату текстів законодавчих документів. Можливостей надання бібліографічного опису документу та експорту через будь-які транспортні формати система не має. Інформація в робочу БД переноситься в ручному режимі;

У випадку отримання прямих URL- посилань для доступу до першоджерел використовувалися Інтернет- сайти інших організацій.

Інформаційний пошук наукових та бізнес документів проводився на основі застосування інформаційно-пошукових формул (наведений універсальний синтаксис, для конкретних пошукових систем він замінювався на аналогічні формули відповідно до пошукових стандартів цих систем). На схемі Рис.1 процес виконання відповідних пошукових формул, представлено інформаційними фільтрами:

Ф1 – Search ((cybersecurityand (legislationorlawor«Executiveorder» OR Directive))

Ф2 – Ф1 AND SCADA

Ф3 – Ф1 AND («Industrial Internet of things» OR IoT)

Ф4 - Ф1 AND «cloud based manufacturing»”

Ф5 – Ф1 AND « Cyber-Physical System»

Ф6 – Ф1 AND «Internet 4.0»

Ф7 – Ф1 AND «Industrial Control System»

Ф8* – група пошукових формул для вибірки першоджерел законодавчих документів (уточнюється для конкрентного законодавчого документу

Відповідні результати використання формул пошуку представлені у Таблиці 1.

В процесі інформаційного пошуку та обробки знайдених документів була створена робоча база даних реферативно-бібліографічних записів з метою формування бібліографічних списків літератури, приєднання повних текстів до знайдених документів, використання документального масиву для подальшої аналітичної роботі та порівняльного аналізу. Для цього була обрана технологічна платформа Zotero (www.zotero.org). Технологічною перевагою цієї платформи є наявність хмарної (з можливістю колективного доступу) та десктопної версій систем та функцій упорядкування створеного документального масиву. Результати пошуку у визначених БД імпортувалися до системи Zotero за допомогою транспортного інформаційного формату представлення записів БД – RIS. В деяких випадках реферативно-бібліографічна інформація вводилася у цю систему методом ручного вводу.

В процесі накопичення та попередньої обробки документального масиву у технологічній схемі передбачені наступні процеси:

- СЕЛЕКЦІЯ ІНФОРМАЦІЙНОГО ШУМУ (НЕРЕЛЕВАНТНИХ ПУБЛІКАЦІЙ) - Результати застосування пошукових формул у всіх обраних БД представлені у Таблиці 1. Характерною особливістю всіх пошукових формул даного дослідження є виключне використання ключових слів, як критеріїв пошуку, і, як результат, наявність помітного рівня інформаційного шуму (документів, що формально включають задані ключові слова, проте не відносяться до заданої теми пошуку). Експерти шляхом перегляду коротких відомостей про документ відкидали нерелевантні документи здійснююча селекцію;

- ВИДАЛЕННЯ ДУБЛІКАТІВ - Масив документів, які пройшли формальну селекцію, де-факто сформований з використанням БД1-БД5 і природньо на початку формування містить дублікати документів, які були отримані з різних БД. Процедура видалення дублікатів виконувалась періодично в напівавтоматичному режимі, що передбачений функціональною структурою інформаційно-пошукової системи Zotero;

- СЕЛЕКЦІЯ ПУБЛІКАЦІЙ – повторна процедура селекції, що виконується експертами на основі аналізу рефератів та повних текстів вторинних документів та першоджерел законодавчих актів;

- КОНТЕНТ-АНАЛІЗ РЕФЕРАТІВ / ПОВНИХ ТЕКСТІВ ПУБЛІКАЦІЙ – процес аналізу вторинних документів з метою виявлення згаданих у вторинних документів відомостей про згаданих авторами законодавчих документів, їх місцезнаходження та можливі аналітичні оцінки першоджерел. По результатах такого аналізу створюються відповідні пошукові формули типу Ф8*, в результаті яких отримуються повні тексти першоджерельних законодавчих документів;

- ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАКОНОДАВЧИХ ДОКУМЕНТІВ – знайдені законодавчі документи (першоджерела) підлягають порівняльному аналізу по обраній порівняльній схемі і доповненню інформацією, яка була отримана на етапі контент-аналізу. Результатом такого аналізу є Звіт про дослідження.

- Використання такої методики дає можливість тривалого і систематичного вивчення законодавчих документів із визначенням їх рейтингової важливості для підготовки методичних документів науково-технічної сфери.

Таблиця 1 – Результати застосування пошукових формул у всіх обраних БД

Статистичні результати пошуків по формулах Ф1-Ф5	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Ф7
БД1 (Scopus)	815 (184)	13 (0)	34 (7)	0	13 (5)	0	11 (2)
БД2 (Wos)	564 (132)	5 (0)	25 (3)	0	11 (4)	0	9 (2)
БД3 (BSP)	4971 (2860)	68 (37)	71 (19)	985 (348)	16 (4)	30 (17)	2 (1)
БД4 (ASP)	3004 (1328)	2 (1)	52 (16)	448 (190)	880 (381)	806 (348)	1 (0)
БД5 ScolarGoogle	20400 (-)	2350 (-)	4960 (-)	6 (4)	364 (-)	4 (2)	605 (-)

Формат: Кількість документів (Доступ до ПОВНОГО ТЕКСТУ), (-) – кількість повних текстів неможливо визначити, через неструктурований пошук)

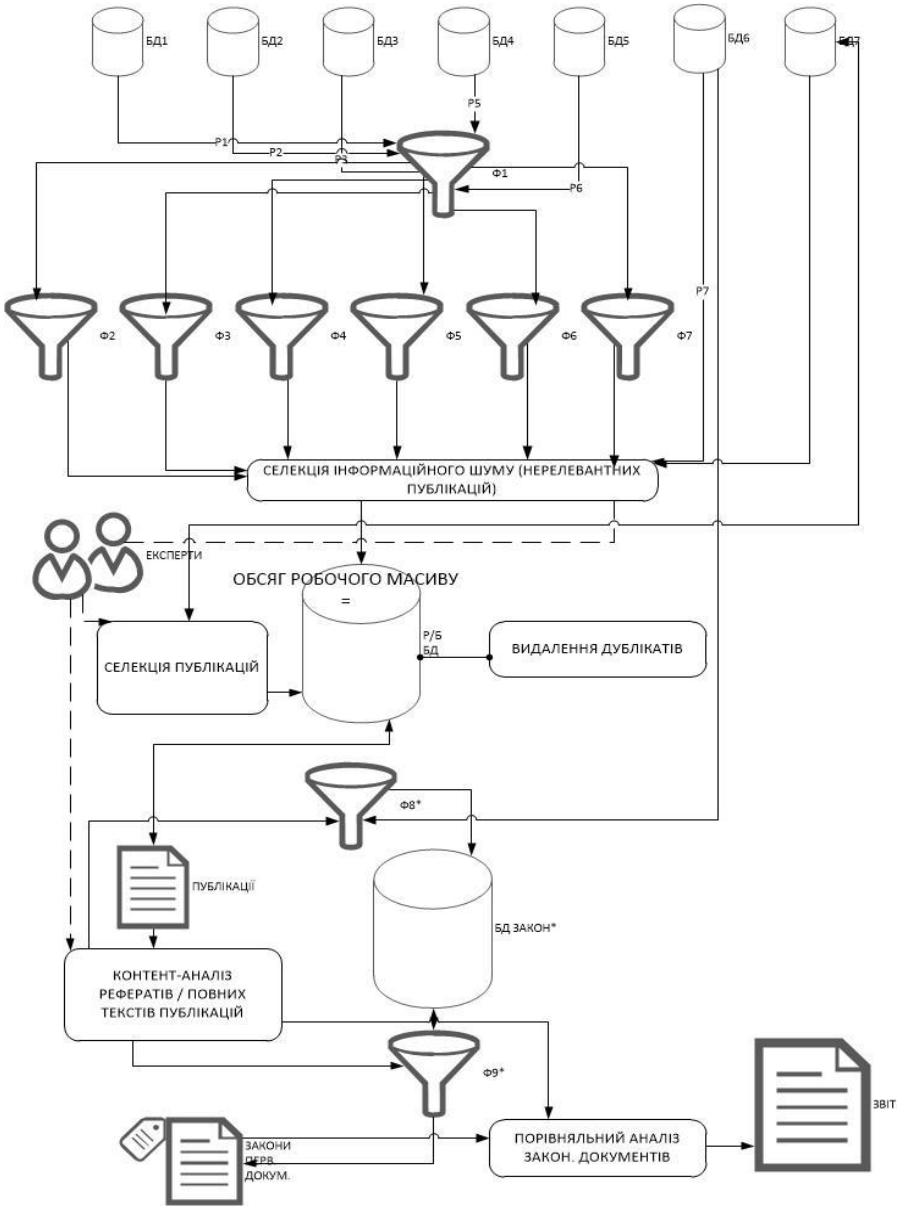


Рисунок 1 – Загальна схема організації та обробки відомостей (та змісту) публікацій та першоджерел

Однією з можливостей порівняльного законодавства є виявлення загальних закономірностей його розвитку в державах, що включені у порівняльну групу.

Показники (фактори) порівняльного аналізу:

- Оцінка синхронності розвитку законодавства
- Оцінка тенденції до зближення норм законодавства
- Паралельне викладення тексті вокремих норм законодавства
- Нормативне порівняння - При цьому передбачається, що інша порівнювана правова система користується такими ж термінами, поняттями, категоріями та правовими інститутами, а за подібною назвою ховається адекватний правовий зміст. Такий підхід був більш менш правомірним, коли порівнювалися правові системи континентальної Європи.
- Функціональне порівняння. Функціональне порівняння можна визначити як дослідження правових засобів та способів вирішення подібних чи однакових соціальних та правових проблем різними правовими системами.

Якщо звернутися до правових систем, які у законотворчому процесі використовують порівняльне право, то виявляються помітні відмінності у романо-німецькій та англосаксонській правових сім'ях.

Європейський законодавець при використанні порівняльних даних звертається як до права інших країн романо-німецькоїсім'ї, так і до англосаксонських джерел і найчастіше до права США.

Законодавець в англо-американських країнах звертається переважно до права інших англо-американських країн і досить нечасто – до континентальної системи. суперечать принципам повільної, поступової еволюції, властивої країнам загального права.

В цілому головною метою порівняльного правознавства є уніфікація права на міжнародномурівні.

В данному дослідженні буде у більшості випадків застосовуватися функціональні методи порівняльного законодавства.

Пропонується наступна схема порівняльного опису колекції законодавчих документів різних країн наведена у Таблиці 2.

Таблиця 2 – Порівняльний опис колекції законодавчих документів різних країн

№	Назва порівняльного елементу	Коротка назва	Примітка – опис елементу порівняння
1	Назва законодавчого документу	Назва документу	Робоча назва для нелатинських (кириличних) текстів
2	Країна	Країна	
3	Рік прийняття останньої	Рік	Рік або дата

	відомої редакції		затвердження
4	Наявність опублікованого англомовного тексту (крім національної мови)	Мови тексту	Мови публікації через кому
5	Зв'язок із відомим міжнародним законодавством	Міжнародна Асоціація	Законодавство ЕС (для європейських країн) та інші асоціації
6	Наявність норм щодо передачі даних	Передача даних	Значення: Так/Ні
7	Наявність норм щодо телекомунікації	Телекомунікація	Значення: Так/Ні
8	Наявність норм щодо хмарних обчислень	Хмарні технології	В даному випадку виключено інформацію про соціальні мережі
9	Наявність норм щодо авторизації віддаленого доступу	Віддалений доступ	Значення: Так/Ні
10	Наявність прямих норм по темі дослідження (об'єкти критичної інфраструтури, АСУ ТП, тощо	Норми АСУ ТП	Значення: Так/Ні. Зазначення контенту у розділі 2.4.
11	Наявність норм матеріальної відповідальності за порушення кібербезпеки	Матеріальна відповідальність	Значення: Так/Ні Коротко – штраф, блокування, вилучення
12	Наявність кримінальних норм відповідальності (або посилання на кримінальне законодавство)	Кримінальна відповідальність	Значення: Так/Ні
13	Інші норми законодавства, які мають відношення до теми дослідження	Інші норми	Короткі суттєві відомості

Результатом використання представленої вище методики для досліджень по темі «Кібербезпека у промислових системах управління» було знайдено більше 30 законодавчих документів технологічного напрямку, с також до 50 законодавчих норм Кодексу законів США.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дмитрієв А.І., Шепель А.О. Порівняльнеправознавство: Підручник / Відп. редактор В.Н.Денисов

Герасимов Ростислав Павлович,
ІПМЕ ім. Г.Є. Пухова НАН України,
наук. співроб.,
gerasimov.rostislav@gmail.com

Крук Ольга Миколаївна,
ІПМЕ ім. Г. Є. Пухова НАН України,
мол. наук. співроб.,
o.n.kruk@gmail.com

ЦурканОксана Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
мол. наук. співроб.,
otsurkan24@gmail.com

Яшенков Вадим Петрович,
ІЕ ім. Є.О. Патона НАН України,
наук. співроб.,
vadym.yashenkov@gmail.com

СПОСОБИ ПРЕДСТАВЛЕННЯ ВІДНОШЕНЬ МІЖ СОЦІАЛЬНИМ ІНЖЕНЕРОМ І КОРИСТУВАЧЕМ СОЦІОТЕХНІЧНОЇ СИСТЕМИ

Анотація. Досліджено вплив соціальної інженерії на користувачів соціотехнічних систем. Виокремлено способи представлення відношень між соціальним інженером і користувачем.

Abstract. The influence of social engineering on users of sociotechnical systems is investigated. The ways of representing the relationship between a social engineer and a user are singled out.

Відповідно до [1] передумовою аналізування уразливостей користувачів соціотехнічних систем до впливів соціальної інженерії є формування множини екторів. Вона задається об'єднанням, зокрема, користувачів, соціальних інженерів і форм маніпулятивного впливу. Тому представлення відношень між соціальним інженером і користувачем соціотехнічної системи є актуальним.

Серед способів представлення відношень між соціальним інженером і користувачем соціотехнічної системи виокремлено діади та тріади. Кожна з них відображається підграфом, вершинами якого визначаються соціальні інженери, користувачі, форми маніпулятивного впливу. Так, діадою представляється наявність або відсутність впливу соціальної інженерії на користувача соціотехнічної системи. Тоді як використання способу на основі тріад дозволяє врахувати особливості такого впливу, наприклад: безпосередній (на

користувача), опосередкований (з урахуванням форм маніпулятивного впливу [1, 2].

Отже, використання способів представлення відношень між соціальним інженером і користувачем соціотехнічної системиорієнтоване як на встановлення наявності/відсутності, так і врахування його особливостей.

1. Mokhor V., Tsurkan O., Herasymov R., Kruk O., PokrovskaV., “Model of vulnerabilities analysis of socio-technical systems to the social engineering influences”, Cybersecurity: Education, Science, Technique. 2020. Vol. 4,no. 8.P. 165-173. DOI: https://doi.org/ 10.28925/2663-4023.2020.8.165173.

2. Wasserman S., Faust K. Social Network Analysis: Methods and Applications. Cambridge, England: Cambridge University Press, 2012.DOI: https://doi.org/10.1017/CBO9780511815478.

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук. співроб.,
д-р техн. наук, старш. наук. співроб.,
hilgurt@ukr.net

Кіслов Олексій Геннадійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
kislov@ipme.kiev.ua

Попова Валентина Миколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
інженер першої категорії,
popovavn@ukr.net

ОЦІНКА КІЛЬКІСНИХ ХАРАКТЕРИСТИК СХЕМ ФІЛЬТРА БЛУМА ДЛЯ РЕКОНФІГУРОВНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. Розглянуто техніку прискореного обчислення функціональної залежності кількісних характеристик реконфігуровних засобів сигнатурного аналізу з використанням фільтра Блума на базі геш-функцій від властивостей набору патернів та апаратного прискорювача, яка дозволяє виконувати процедуру оптимізації за прийнятний час.

Abstract. The technique of accelerated calculation of functional dependence of quantitative characteristics of reconfigurable means of signature analysis using Bloom Filter based on hash-functions on the properties of a pattern set and hardware accelerator, which allows performing the optimization procedure in a reasonable time, is considered.

В проведеному дослідженні розглянуто техніку прискореного обчислення технічних параметрів реконфігуровної схеми розпізнавання, яка дозволяє виконувати процедуру пошуку оптимального рішення за прийнятний час. Наведений приклад побудови так званої функції оцінки (а саме – її ресурсної складової) для базової схеми розпізнавання патернів, побудованої у вигляді фільтра Блума на базі геш-функцій [1]. Отримано математичний запис залежності вихідного значення оцінки потрібних ресурсів ПЛІС від вхідних змінних, якими є параметри множини патернів, що мають розпізнаватися, низці констант, що є параметрами реконфігуровного прискорювача, який використовується та додаткових параметрів , що задає користувач. Отримана залежність не тільки дозволяє прискорити процедуру оптимізації, але також може бути окремо використана для попередньої оцінки ефективності реконфігуровних технічних рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bloom B.H. Space/Time Trade-offs in Hash Coding with Allowable Errors. Communications of the ACM, Article vol. 13, no. 7, 1970. P. 422–426, doi: 10.1145/362686.362692.

Голомолзін Ігор Валерійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
8799949@gmail.com

Дяченко Сергій Михайлович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
putechukraine@gmail.com

Давиденко Анатолій Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний наук. співроб., д-р техн. наук,
старш. наук. співроб.,
davidenkoan@gmail.com

Чьочь Вікторія Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
учений секретар, канд. техн. наук,
victoria.choch@gmail.com

МОДЕЛЮВАННЯ КОМПЛЕКСНОГО СОНОТРОДА, ПРИЗНАЧЕНОГО ДЛЯ УЛЬТРАЗВУКОВОГО ЗВАРЮВАННЯ ПОЛІМЕРІВ

Анотація. Розглянуто методику та результати моделювання комплексного сонотрода, призначеного для ультразвукового зварювання компонентів полімерних виробів.

Abstract. The method and results of modeling of the complex sonotrode for ultrasonic welding of polymeric products components are considered.

Застосування ультразвукового зварювання для з'єднання різних за властивостями термопластичних матеріалів дозволяє виключити використання клеїв, підвищити міцність з'єднань та якість продукції, а також спростити автоматизування технологічного процесу виготовлення полімерних виробів.

В даному дослідженні розглянуті питання моделювання пристроїв ультразвукового зварювання нетканих термопластичних матеріалів, які використовуються для виготовлення виробів, що складаються з окремих деталей, і можуть бути використані зокрема для виготовлення медичних масок, а саме для закріплення завушних гумок.

Одна з основних вимог, що висуваються до обладнання для ультразвукової обробки, є забезпечення умов повторюваності параметрів технологічного процесу від циклу до циклу. Складність виконання цієї

вимоги обумовлена тим, що процеси ультразвукової обробки дуже чутливі до впливу великої кількості різноманітних дестабілізуючих факторів [1]. Недоліками відомих пристроїв ультразвукового зварювання є невисока якість зварних з'єднань, внаслідок недостатньої стабільності температурного режиму зони зварювання від циклу до циклу, що пов'язано зі зміною температури зварювального інструменту [2]. Також, існуючим пристроям притаманний низький коефіцієнт корисної дії, що обумовлено надмірною енергією зварювання, яка надходить в зону зварювання при нагріванні хвилеводу-інструменту, тому що для приварювання вушних петель використовують два сонотроди (хвилеводи), кожний з який з’єднаний з окремим випромінювачем та окремим генератором ультразвуку, що потребує збільшених енерговитрат.

Сонотрод, що складається з базового сонотрода, форма якого наближена до прямокутного паралелепіпеда, і чотирьох робочих хвилеводів видовженої форми, закріплених на ньому (рис. 1), дає можливість здійснити операцію приєднання завушних гумок до заготовки захисної маски одночасно у чотирьох точках з’єднання з однаковою якістю зварних з’єднань.

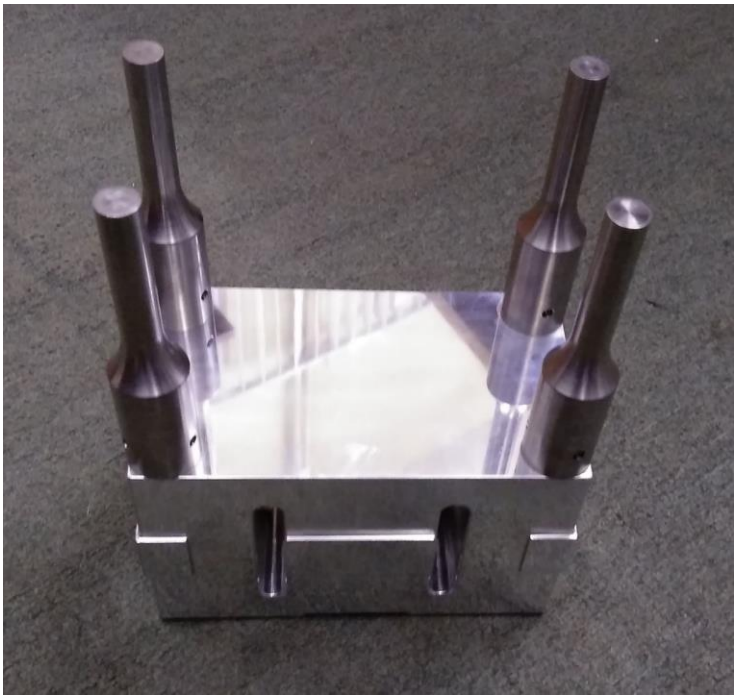


Рисунок 1 – Зовнішній вигляд комплексного сонотрода

Методологічною основою для проектування сонотродів є моделювання спектру резонансних частот прямокутної пластини постійної товщини. В обчислювальному сенсі найбільша складність моделювання сонотрода, поданого на рис. 1, полягає у необхідності варіювання геометричного положення щілин, висоти та розташування додаткових виступів та западин на гранях паралелепіпеда з метою досягнення максимальної однорідності на робочій грані сонотрода.

Для математичного моделювання характеру руху сонотрода застосовувалися чисельні методи розв'язання системи диференціальних рівнянь – завдання на власні значення. Для виконання моделювання були використані програмний пакет COMSOL Multiphysics та конструкторська програма SW.

Результати розрахунків моди коливань комбінованого сонотрода, отримані під час моделювання, подані на рис. 2.

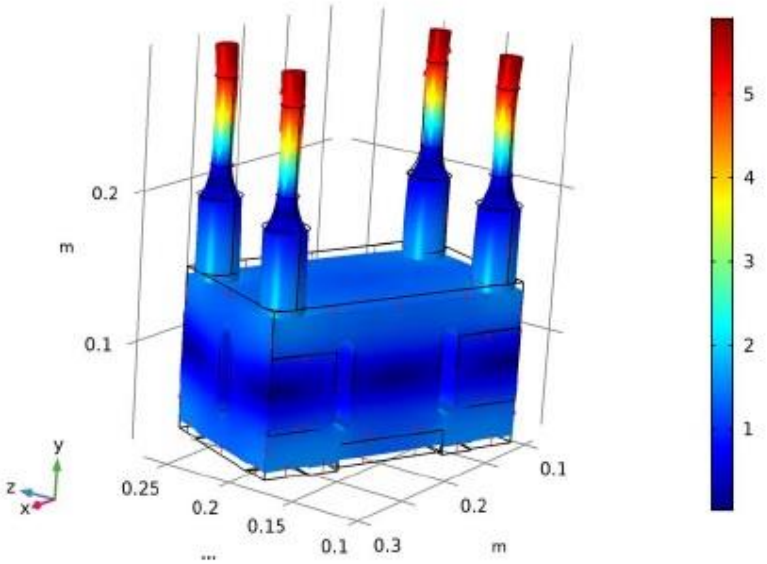


Рисунок 2 – Робоча мода коливань комплексного сонотрода

Після об’єднання результатів окремого моделювання базового та чотирьох робочих сонотродів, було отримано модель комплексного сонотрода з необхідними параметрами: робоча частота – 20 кГц; загальний коефіцієнт трансформації – 4,0; мода коливань задовольняє вимогам, що висувалися.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петушка І.В. Устаткування для ультразвукового зварювання. – СПб: «Андріївський видавничий дім», 2007. – С. 45–46.

2. Патент RU141451U1, B23K 20/10; Устройство ультразвуковой сварки (варианты) / Петушко И.В. (RU); Общество с ограниченной ответственностью "Ультразвуковые технологии и оборудование (RU). – Заяв. 30.12.2013, № 2013159031/02. – Опубл. 10.06.2014, Бюл. № 16.

Serhii Honchar,
PIMEE NAS of Ukraine,
deputy director,
sfgonchar@gmail.com

Maxim Komarov,
PIMEE NAS of Ukraine,
researcher,
maxkom@i.ua

Alla Onyskova,
PIMEE NAS of Ukraine,
junior researcher,
maxkom@i.ua

ABOUT CYBER RESILIENCE ASSESSMENT OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Анотація. показано, що забезпечення кіберстійкості критичної інформаційної інфраструктури, як стану критичної інформаційної інфраструктури, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз являється актуальною задачею. Необхідним є здійснення оцінки кіберстійкості, порівняння з допустимим значенням, аналіз достатності кіберстійкості. Окремі організації використовують різні підходи до оцінки кіберстійкості, при цьому відсутня єдина методологія її побудови та методика вимірювання для об'єктів критичної інформаційної інфраструктури

Abstract. It is shown that ensuring the cyber resilience of critical information infrastructure, as a state of critical information infrastructure, which ensures its ability to function reliably and provide basic services in cyber threats is an urgent task. It is necessary to assess cyber resilience, compare with the allowable value, analyze the adequacy of cyber resilience. Some organizations use different approaches to assessing cyber resilience, but there is no single methodology for building it and a method of measurement for critical information infrastructure.

In accordance with [1], in order to assess the state of cyber protection of critical information infrastructure, state information resources and information the requirement for protection of which is established by law, and the readiness of units of review subjects, whose powers include ensuring cyber protection of critical information infrastructure objects, protection of state information resources and information, the requirement for protection of which is established by law, to effective and prompt response to cyber threats, prevention, detection and protection from cyberattacks and cyber incidents, elimination of their consequences, restoration of critical information infrastructure objects, an

appropriate review is carried out. One of the tasks of the review is to analyze the cyber resilience of critical information infrastructure, as well as to plan measures to ensure cyber resilience of critical information infrastructure.

In view of the above, it is necessary to assess cyber resilience, compare with the allowable value, analysis of the adequacy of cyber resilience. At the same time, research shows that some organizations use different approaches to assessing cyber resilience, and there is no single methodology for its construction and measurement methods for critical information infrastructure objects. Thus, the approaches of some organizations in assessing cyber resilience focus on creating a cycle of cyber resilience, while others propose to build and improve cybersecurity risk management systems.

The most important factor in ensuring the cybersecurity of critical information infrastructure objects of the critical infrastructure objects is the creation of a cybersecurity management system, which should ensure the sustainable, durable and secure operation of critical infrastructure objects; environmental safety; protection of the interests of the individual, society and the state, as well as consumers of services [2, 3].

The goal of stakeholders is to ensure that the level of cybersecurity of critical information infrastructure objects of the critical infrastructure objects, where threats and risks are reduced to a minimum acceptable level. Management provides a targeted impact on the object to maintain its characteristics at a given level. Management requires constant monitoring of the parameters that characterize the managed object, i.e. the functioning of the established system of control, monitoring and rapid response to changes in these parameters.

As noted in [4], unpredictability, extreme uncertainty, and the rapid evolution of potential cyber threats make risk assessment efforts impossible to adequately address cybersecurity for critical infrastructure systems. For this reason, the traditional approach to strengthening cyber systems against identified threats has proved impossible.

Cyber resilience issues play a key role in addressing the risks of cybersecurity, cyber threats and uncertainties associated with cyber threats. The level of cyber resilience of an information system or organization is determined by its ability to maintain or restore its basic functionality after a cyber attack. An information system with a sufficient level of cyber resilience is capable of [5]:

- respond to regular and irregular cyber threats in a reliable, flexible (adaptive) way;
- track what is happening, including their own productivity;
- predict the risks of cybersecurity, cyber attacks, countermeasures;
- to carry out training on own experience.

By using a combination of continuous monitoring, early detection of cyberattacks and early and adequate response to them, failures can be avoided.

In [6], cyber resilience is defined as the ability of a process, business, organization to anticipate, withstand, recover and develop in conditions of destructive actions, cyber attacks on information resources that are critical to

functioning. The ability to detect cyber threats may also be included in this definition. These studies show that cyber resilience enables companies or information systems to be resilient to changes in the cyber threat scenario by having reliable and adapted ways to counter cyber threats. One of the basic principles of ensuring the cyber resilience of an organization is that this organization uses its assets (people, information, technology and equipment) to support specific operational missions or critical services [7]. The application of this principle makes it possible to understand the capabilities of the organization in the implementation, planning, management, measurement and definition of practices and behaviors of operational resilience by studying the following ten domains [7]:

- asset management;
- control management;
- configuration and change management;
- vulnerability management;
- incident management;
- continuity of service management;
- risk management;
- management of external dependence;
- training and awareness;
- situational awareness.

Studies show that it is possible to build an approach to cyber resilience using the full life cycle [8]:

- preparation - analysis of the impact on business, analysis of compliance with standards, risk assessment;
- identification - detection and assessment of vulnerabilities, analysis of the shortcomings of their business on IT requirements;
- protection - processing of cybersecurity risks, business continuity management;
- detection - detection of violations and their prevention in real time, incident management;
- analysis - analysis of cyber threats, determination of priorities in countermeasures;
- response - implementation of appropriate countermeasures, business resumption in accordance with the plan to ensure its continuity;
- restoration - establishment of the regular mode of work of the organization, collection of data on cyber incident, development of measures for improvement of cyber resilience.

Researchers note that cyber resilience is covered by the following international standards [8]:

- ISO 31000 - an international standard that defines the basics of risk management;
- ISO 27001 - an international standard that covers the information security management system;

- ISO 22301 - an international standard that covers the business continuity management system;

- ISO 22316 - international standard, new standard of "sustainability organization".

Studies show that cybersecurity includes technologies, processes and controls designed to protect organizations and / or information systems from cyber threats in the form of cyber attacks. Ensuring cybersecurity involves reducing the risk of cyberattacks or the consequences that would result from the implementation of these cyberattacks. However, it should be noted that cyber resilience is a broader approach that encompasses cybersecurity, business continuity management. Cyber resilience is aimed at protecting against potential cyberattacks and ensuring the functioning of the organization or information system in the normal mode after a cyberattack.

Thus, it is shown that ensuring the cyber resilience of critical information infrastructure, as a state of critical information infrastructure, which ensures its ability to function reliably and provide basic services in cyber threats is an urgent task. It is necessary to assess cyber resilience, compare with the allowable value, analyze the adequacy of cyber resilience. Some organizations use different approaches to assessing cyber resilience, but there is no single methodology for its construction and measurement methods for critical information infrastructure objects.

REFERENCES

[1] Cabinet of Ministers of Ukraine, Resolution of the Cabinet of Ministers of Ukraine "On approval of the Procedure for reviewing the state of cyber protection of critical information infrastructure, state information resources and information required for protection by law", № 1176, November, 11, 2020, [Online]. Available: ttps://zakon.rada.gov.ua/laws/show/1176-2020-п#Text.

[2] S.F. Honchar, “The concept of creating an automated cybersecurity management system for critical infrastructure facilities,” Modeling and Information Technology, №83, pp. 70-76, 2017.

[3] V. Mokhor, S. Gonchar, and O. Dybach, “Methods for assessing the total cybersecurity risk of critical infrastructure,” Nuclear and Radiation Safety, Vol. 82, Issue 2, pp. 4-8, 2019. https://doi.org/10.32918/nrs.2019.2(82).01.

[4] I. Linkov and A. Kott, Fundamental Concepts of Cyber Resilience: Introduction and Overview, Springer, 2018, [Online]. Available: https://arxiv.org/ ftp/arxiv/papers/1806/1806.02852.pdf

[5] T. Aven, “Risk assessment and risk management: Review of recent advances on their foundation,” European Journal of Operational Research, Vol. 253. pp. 1-13, 2016.

[6] Juan F. Carías, Saioa Arrizabalaga, Leire Labaka and Josune Hernantes, “Cyber Resilience Progression Model,” Applied Sciences, Vol. 21, Issue 10, pp. 73-93, 2020.

[7] Carnegie Mellon University, Cyber Resilience Review (CRR). Department of Homeland Security, 2016, [Online]. Available: https://www.us-cert.gov/ccubedvp/assessments (accessed on 7 March 2021).

[8] Cyber Resilience, EBRC, [Online]. Available: https://www.ebrc.com/en/company/cyber-resilience.

Давиденко Анатолій Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний наук. співроб., д-р техн. наук,
старш. наук. співроб.,
davidenkoan@gmail.com

Чьочь Вікторія Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
учений секретар, канд. техн. наук,
victoria.choch@gmail.com

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук. співроб., д-р техн. наук,
старш. наук. співроб.,
hilgurt@ukr.net

Голомолзін Ігор Валерійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
8799949@gmail.com

РИЗИК-ОРІЄНТОВНЕ КЕРУВАННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ ВИГОТОВЛЕННЯ ПОЛІМЕРНИХ ВИРОБІВ

Анотація. Розглянуто принципи створення апаратно-програмних комплексів контролю, оптимізації та управління технологічним процесом виготовленням полімерних виробів, які дозволяють враховувати можливі ризики та керувати ними.

Abstract. The principles of creation hardware/software complexes of control, optimization and management of technological process of polymeric products manufacturing which allow to consider possible risks and to manage them are considered.

Останніми роками завдяки науково-технічному прогресу отримано різноманітні синтетичні матеріали, таки як синтетичні тканини, полімери, термопласти, композиційні матеріали та вироби з них. Застосування полімерів в якості конструкційних матеріалів є економічно доцільним, але створення виробів з них вимагає або інтенсивного використання людського ресурсу, або автоматизації технологічного процесу. Але при використанні автоматизованих систем зростає залежність безпеки виробництва та якості отримуваної продукції від обраних технічних рішень та алгоритмів курування. Враховувати ці важливі моменти дозволяє оцінка ризиків конкретного технологічного процесу.

В даному досліджені розглянуті питання створення апаратно-програмних комплексів контролю, оптимізації та управління технологічним процесом ультразвукового зварювання полімерів при виготовленні критично-необхідних виробів з високими вимогами щодо якості, в яких існуючі ризики враховуються на всіх етапах технологічного процесу. При цьому врахування можливих ризиків та управління ними здійснюється через їх ідентифікацію, аналізування та потрібне наступне реагування. Підставою для отримання раціонального рішення при розробці комплексів контролю та управління технологічним процесом є наявність максимально повної та достовірної інформації щодо джерел потенційної небезпеки, а також – можливих наслідків її реалізації.

До основних ідей, що реалізовані в дослідженні, належать використання натурного та комп'ютерного моделювання, цільовий ризик-орієнтований аналіз процесів ультразвукової діагностики та зварювання полімерів. Контроль та управління в створюваних системах здійснюється шляхом ультразвукової діагностики властивостей матеріалу в різних технологічних ситуаціях (стискання матеріалу, його нагрів тощо) та зміни частоти резонансу у коливальному контурі за рахунок адитивного корегування. Завдяки цьому знижується вірогідність виникнення ризиків та забезпечується оптимізація системи за критеріями якості кінцевої продукції та безпеки її виробництва. Оптимізація та автоматизація розрахунку технологічних режимів також призводить до зниження кваліфікаційних вимог до оператора системи, що позитивно впливає на конкурентоспроможність продукції.

Одна з основних вимог, що висуваються до обладнання для ультразвукової обробки, у тому числі – зварювання, є забезпечення умов повторюваності параметрів технологічного процесу від циклу до циклу. Складність виконання цієї вимоги обумовлена тим, що процеси ультразвукової обробки дуже чутливі до впливу великої кількості різноманітних дестабілізуючих факторів [1]. Для вирішення цього завдання використовуються різні системи авторегулювання та стабілізації режимів зварювання.

Отримані в результати були апробовані шляхом розробки апаратно-програмного комплексу ризик-орієнтованого керування технологічним процесом ультразвукового зварювання полімерів, в якому використовувались також результати попередніх досліджень авторів [2]. Комплекс був впроваджений у технологічний процес з виготовлення захисних медичних масок. Тестування комплексу здійснювалося шляхом порівняння з відомими аналогами. Зібрана за 12-ти годинну робочу зміну статистика показала значення середнього відсотку браку за зміну на рівні 3 %, в той час як для існуючих аналогічних установок цей показник сягає значення у 15 %.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петушка І.В. Устаткування для ультразвукового зварювання. – СПб: «Андріївський видавничий дім», 2007. – С. 45–46.

2. Давиденко А.М., Політучий О.О. Визначення типу контролеру для побудови програмно-технічного комплексу керування технологічним процесом зневоднення бішофіту // Безпека енергетики в епоху цифрової трансформації: матеріали науково-практичної конференції Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, м. Київ, 20 грудня 2019. – К.: ІПМЕ ім. Г.Є. Пухова НАН України, 2019. – С. 11.

Давидюк Андрій Вікторович
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
andrey19941904@gmail.com

Сергеєв Сергій Миколайович
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант

Ткаченко Володимир Володимирович
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
v.v.tkachenko69@gmail.com

Ткаченко Анастасія Володимирівна
Національний технічний університет України «КПІ ім. Ігоря Сікорського»,
студентка фізико-математичного факультету,
912kiev.nt@gmail.com

ОСНОВНІ АСПЕКТИ АУДИТУУ СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

Анотація. У тезах проводиться аналіз нормативних документів, які регламентують проведення аудиту в сфері інформаційної безпеки України та забезпечення кібербезпеки на об'єктах критичної інфраструктури України.

Abstract. The report analyzes the normative documents governing the audit in the field of the information security of Ukraine and cybersecurity at the critical infrastructure of Ukraine.

У Законі України «Про основні засади забезпечення кібербезпеки України»[1] за текстом вживаються такі терміни, що стосуються поняття аудиту:

1) незалежний аудит діяльності основних суб'єктів національної кібербезпеки;

2) незалежний аудит інформаційної безпеки;

3) аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;

4) аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури.

Враховуючи різні назви та наведений в таблиці 1 розподіл відповідно до [1] завдань з аудиту у частині, що стосується Державної служби спеціального зв'язку та захисту України (далі - ДССЗЗІ), можна зробити висновок про те, що аудит інформаційної безпеки та стану кіберзахисту об'єктів критичної

інформаційної інфраструктури (далі - Аудит) є окремим видом аудиту, на який не розповсюджуються, розроблювані ДССЗЗІ вимоги до аудиторів інформаційної безпеки, порядок атестації (переатестації), що у свою чергу залишає процес проведення Аудиту та аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість без відповідного нормативного підґрунтя.

Таблиця 1 – Розподіл завдань з аудиту

ДССЗЗІ	забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість;
Державний центр кіберзахисту ДССЗЗІ	забезпечує аудит інформаційної безпеки та стану кіберзахисту об’єктів критичної інформаційної інфраструктури

Водночас Аудит можна розуміти як два різних аудити, зокрема як аудит інформаційної безпеки та аудит стану кіберзахисту об’єктів критичної інформаційної інфраструктури. У такому випадку вже є наявною кореляція понять аудиту інформаційної безпеки з вимогами до аудиторів інформаційної безпеки та порядком їх атестації (переатестації). Результатом такого тлумачення є відсутність нормативних підстав для проведення аудиту стану кіберзахисту об’єктів критичної інформаційної інфраструктури. Також виникає конфлікт інтересів при встановленні вимог та атестації (переатестації) ДССЗЗІ власних співробітників, що може ставити під сумнів як якість їх підготовки та компетенції, так і авторитет ДССЗЗІ, з точки зору незалежності такого аудиту, що є не припустим для державного органу виконавчої влади.

Варто зазначити, що у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [2] відсутнє поняття будь-якого аудиту. Як засіб підтвердження відповідності системи управління інформаційною безпекою є процедура з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка має проводитися органом оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної

організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності. Відповідно до національних стандартів (ДСТУ) такою процедурою з оцінки є аудит системи управління інформаційною безпекою, що відсутній у [1].

З чого виникає невизначеність в тому чи є необхідним аудит системи управління інформаційною безпекою за наявності інших аудитів вказаних у даному законі і навпаки.

Зокрема варто зазначити, що зі змісту Закону виникає питання різниці між аудитом захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість та заходами, що вже здійснюються Держспецзв'язку в рамках наказів Адміністрації Держспецзв'язку від 02.12.2014 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [3] та від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті» [4].

Стратегія кібербезпеки України безпечний кіберпростір – запорука успішного розвитку країни, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021 [5] передбачає лише один аудит інформаційної безпеки.

За результатами вищезазначеного поверхневого аналізу нормативних документів та наявного сприятливого законодавчого підґрунтя, що знаходиться у стані розвитку, в частині що стосуються аудиту, вважаємо що доцільним є:

- визначити аудит інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури як єдиний вид аудиту, що може здійснюватися ДССЗЗІ;
- розробити нові та/або актуалізувати існуючі нормативно-правові акти Адміністрації Держспецзв'язку (проєкти), в частині, що стосується аудиту та оцінки стану захищеності державних інформаційних ресурсів(далі – ДІР) в інформаційно-телекомунікаційних системах (далі - ІТС) та сканування на предмет вразливості ДІР, розміщених в Інтернеті передбачивши заходи з оцінки стану захищеності ДІР в ІТС та сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті як можливі складові аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури. Вимоги до аудиторів інформаційної безпеки та порядку їх атестації (переатестації) викласти з урахуванням існуючої системи оцінки якості персоналу органами з оцінки якості персоналу, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з

акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

На нашу думку, таким чином вдасться уникнути існуючих правових колізій, та невизначеності при впровадженні системи аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, ефективно та швидко її впровадити, зосередивши робочий потенціал на якості розроблюваних процедур, пов'язаних з Аудитом та мінімізувавши можливий негативний вплив на господарчу діяльність, як державних так і приватних організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України». [чинний, редакція від 01.08.2021].
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [чинний, редакція від 04.07.2020].
3. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», від 02.12.2014 № 660 [чинний, редакція від 02.12.2014].
4. Наказ Адміністрації Держспецзв'язку «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», 15.01.2016 № 20, [чинний, редакція від 15.01.2016].
5. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/202 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"», [чинний, редакція від 26.08.2021].

Джигун Олена Миколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук. співроб., канд. техн. наук ,
elromanenko@gmail.com

Ониськова Алла Вікторівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодш. наук. співроб.,
alla.oniskova@ukr.net

СУЧАСНИЙ СТАН РОЗВИТКУ ВІДНОВЛЮВАНИХ ДЖЕРЕЛ ЕНЕРГІЇ

Анотація. Критеріями необхідності використання відновлювальних джерел енергії в сучасному світі є підтримання рівня енергетичної безпеки для промислово-розвинених країн, що залежить від імпорту паливно-енергетичних ресурсів, постійного зростання цін на первинні енергоресурси, підтримання рівня екологічної безпеки та збереження навколишнього середовища.

Abstract. Criteria for the need to use renewable energy sources in the modern world are to maintain the level of energy security for industrialized countries, which depends on the import of fuel and energy resources, the constant rise in prices for primary energy resources, maintaining environmental security and preserving the environment.

Сьогодні важливою особливістю розвитку світового господарства є вирішення питань енергобезпеки та енергоефективності, в зв'язку з чим, особливі надії покладаються на виробництво енергії за допомогою відновлюваних природних джерел — сонячного світла, вітру, води, теплової енергії земних надр. Постійна загроза виникнення кризи з поставками нафти, ризики, пов'язані з розвитком ядерної енергетики і заклопотаність сучасного суспільства проблемами навколишнього середовища і, відповідно, кліматичними питаннями, зумовили виникнення сучасної енергетичної політики, яка націлена на те, щоб протягом декількох наступних десятиліть була сформована відновлювальна енергетична система, що базується на відновлюваних джерелах енергії (ВДЕ), без викидів парникових газів в атмосферу. Практично у всіх розвинених країнах формуються і реалізуються програми розвитку ВДЕ.

Національний план дій України з відновлюваної енергетики на період до 2020 року, затверджений Розпорядженням Кабінету Міністрів України від 1 жовтня 2014 року № 902-р, передбачав в період 2014-2020 років збільшення потужності вітроенергетики з 497 МВт до 2280 МВт, а сонячної енергетики — з 819 МВт до 2300 МВт [1].

Впродовж минулих чотирьох років потужності сонячної та вітрової електроенергії (СЕС та ВЕС) у складі ВДЕ в Україні постійно зростали. Станом на середину 2021 року в структурі встановлених потужностей установок, що виробляють електроенергію з різних ВДЕ, сумарна частка ВЕС та СЕС склала понад 97% (рис. 1).

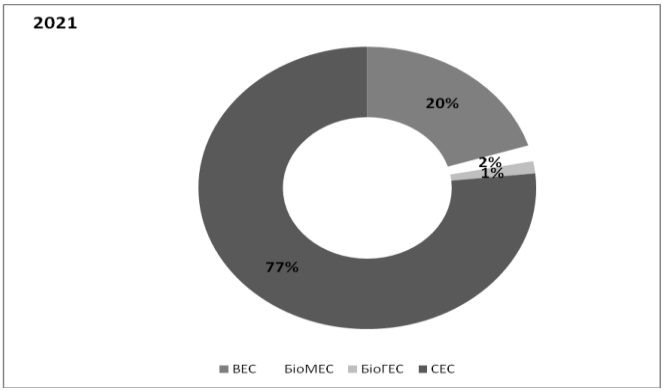


Рисунок 1 – Встановлена потужність ВДЕ у 2021 р.: виробники електричної енергії з вітру (ВЕС); біогазу (БіоГЕС); біомаси (БіоМЕС); сонця (СЕС).

Суттєво зросли обсяги виробництва електроенергії ВЕС та СЕС (рис. 2). Їх частка у загальному обсязі виробництва електроенергії в Україні у 2020 році досягла 7,0% порівняно з 0,8% у 2017 році [2, 3].

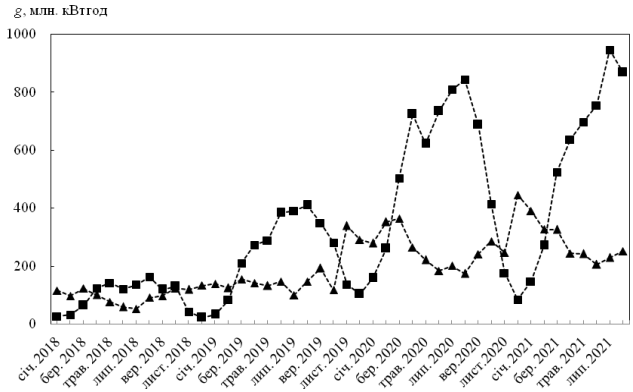


Рисунок 2 – Обсяги виробництва електроенергії (g, млн. кВт год) ВЕС та СЕС у 2018-2021 рр.: ▲— ВЕС; ■ — СЕС.

Невирішеність цілого ряду методологічних питань щодо впровадження ВДЕ, відсутність належного досвіду, недостатня розвиненість законодавчої і нормативної бази на всіх рівнях стримують впровадження ВДЕ, що обумовлює актуальність дослідження даної проблематики. Розвиток відновлюваної енергетики поступово переходить з розряду експериментальної діяльності в комерційну область.

Критеріями необхідності використання ВДЕ в сучасному світі є:

підтримка рівня енергетичної безпеки для промислово-розвинених країн, що залежать від імпорту паливно-енергетичних ресурсів;

постійне зростання цін на первинні енергоресурси;

підтримка рівня екологічної безпеки та збереження навколишнього середовища, пов'язані зі зменшенням шкідливого впливу енергетики на навколишнє середовище, в тому числі, необхідність дотримання угод Кіотського протоколу щодо зниження викидів парникових газів;

завоювання світових ринків збуту обладнання відновлюваної енергетики, особливо в країнах, що розвиваються;

збереження запасів власних енергетичних ресурсів для майбутніх поколінь для промислово-розвинених країн, багатих енергоресурсами;

забезпечення диверсифікації діяльності підприємств, що діють на енергетичних ринках;

збільшення споживання сировини для неенергетичного використання палива.

Головний недолік альтернативної енергетики в Україні та світі є її висока вартість в порівнянні з традиційними джерелами. Однак з кожним роком відміну в собівартості 1 кВт год, отриманого від ВДЕ і традиційних джерел, зменшується завдяки інноваційним технологіям і постійного подорожчання останніх. Відновлювана енергетика створює надмірне фінансове навантаження на ринок електроенергії України, тому Урядом України прийнято Документ, згідно якому виробники ВДЕ приймають умови добровільної реструктуризації «зелених» тарифів, що передбачає їх зменшення [4, 5].

Прогрес в «зеленій» енергетиці неможливий без поєднання винахідливості вчених, щедрого фінансування розробок і політичної волі. Можна виділити чотири основні напрями того, куди далі можуть піти інновації в енергетичній галузі для досягнення стійкого, екологічно безпечного розвитку світової економіки:

1. Удосконалення сонячних і вітрових установок. Поступове впровадження в галузі нових технологій, які в найближчі роки забезпечать їй подальше зростання. Наприклад, у випадку з вітряками, мова йде про застосування штучного інтелекту і про більш точний прогноз погоди і напряму вітру. Для сонячних батарей розробляються технології, що дозволяють отримувати набагато більше енергії з кожного квадратного сантиметра панелі.

2. Розвиток електромереж. Можна скільки завгодно мріяти про повний перехід на енергію сонця і вітру, але в похмурі безвітряні дні користі від неї буде небагато. Тому треба мати потужну накопичувальну систему з високорозвиненою електромережею, споруда Енергоміст (потужних силових кабелів) між регіональними мережами. Існує безліч інноваційних методів того, як поліпшити процес накопичення енергії.

3. АЕС нового покоління. Атомна енергетика є потужним і екологічно чистим джерелом електрики, але дорожнеча АЕС і міркування безпеки привели до відмови від неї в ряді західних країн. Оживити галузь можуть два підходи, які зараз знаходяться на стадії розробки. По-перше, це створення міні-реакторів, які обслуговують конкретну фабрику або район. Такі АЕС виробляють менше ядерних відходів і не вимагають невпинного висококласного обслуговування. Друга розробка, ще на стадії ідеї, — це плани використовувати для вивільнення енергії при розщепленні атомного ядра, а з'єднання ядер.

4. Перетворити викиди CO2 на благо. Одна з основних причин катастрофічної зміни клімату — викиди вуглекислоти, з чим і намагаються боротися через впровадження ВДЕ. Але можна зайти і з іншого боку: виловлювати парникові гази, звільняти від них атмосферу. Циклічне використання CO2 дозволить зменшити шкоду навколишньому середовищу, не змінюючи стилю життя людства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про внесення змін до статті 9-1 Закону України «Про альтернативні джерела енергії» щодо врегулювання питання генерації електричної енергії приватними домогосподарствами. Закон України. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2755-19#Text
2. НКРЕКП. [URL:http://www.nerc.gov.ua/data/filearch/elektro/energo.
3. https://ua.energy/zagalni-novyny/u-2020-rotsi-vstanovlena-potuzhnist-ves-ta-ses-zrosla-na-41-a-yihnya-chastka-u-strukturi-vyrobnytstva-elektroenergiyi-vdvichi/
4. «Про встановлення «зелених» тарифів на електричну енергію для суб'єктів господарювання та надбавки до «зелених» тарифів за дотримання рівня використання обладнання українського виробництва» / Постанова Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг від 16.03.2017, №278. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/rada/show/v2380874-16.
5. Меморандум про взаєморозуміння щодо врегулювання проблемних питань у сфері відновлюваної енергетики. [Електронний ресурс]. URL: https://www.kmu.gov.ua/news/uryad-pidpisav-memorandum-z-virobnikami-zelenoyi-elektroenergiyi.

Дімітрієва Дар'я Олександрівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
da_dimitrieva@sstc.ua

Шкарупило Вадим Вікторович,
ІПМЕ ім. Г.Є. Пухова НАН України,
с.н.с., доцент, канд. техн. наук,
shkarupylo.vadym@gmail.com

ДОСЛІДЖЕННЯ СПЕЦИФІКИ ЗАСТОСУВАННЯ ФОРМАЛЬНИХ МЕТОДІВ ПІД ЧАС РОЗРОБЛЕННЯ СИСТЕМ КРИТИЧНОГО ПРИЗНАЧЕННЯ

Анотація. Працю присвячено огляду та класифікації методів формальної верифікації артефактів процесу розроблення програмної складової систем критичного призначення. Проаналізовано специфіку прикладного застосування названих методів.

Abstract. Work is devoted to the review and classification of formal verification methods to be applied with respect to the artifacts of engineering process of software plane of safety-critical systems. The specifics of named methods application has been analyzed.

У наш час застосування формальних методів стає все більш поширеним явищем у різноманітних предметних областях. Шляхи їх використання охоплюють сценарії як комерційного, так і некомерційного характерів. Особливої уваги при цьому заслуговують системи критичного призначення (СКП) – системи, відмови або збої в роботі яких можуть призвести до критичних наслідків. Традиційні методи аналізу програмної складової таких систем полягають у доведенні вірної працездатності програм (верифікація програм). Початок цьому напрямку було покладено роботами П. Наура і Р. Флойда, в яких сформульована ідея приписування точці програми так званого «індуктивного» – проміжного – затвердження, і зазначена можливість доказу часткової правильності програми (тобто відповідності один одному її передумови і постумови), побудованого на встановленні узгодженості індуктивних тверджень [1].

Під верифікацією, як правило, розуміють здійснення перевірки відповідності результатів, отриманих на окремих етапах процесу розроблення вимогам та обмеженням, встановленим для них на попередніх етапах. На початковому етапі перевіряють, чи результати відповідають вихідним вимогам (технічному завданню). У контексті даної праці під верифікацією розуміємо формальну верифікацію (ФВ) – коли перевірка тих чи інших артефактів процесу розроблення здійснюється не безпосередньо, а

на основі відповідних формалізованих подань – формальних специфікацій (ФС).

Мета здійснення верифікації – контроль артефактів процесу розроблення СКП.

Один із перспективних підходів до верифікації програмної складової – гарантуваннябезпечності програмного коду вже за його створення, або «закладання фундаменту» для спрощення майбутньої верифікації. Інший підхід до здійснення ФВ коду під час його створення – використання парадигми контрактного програмування. Зокрема, можна досліджувати характер зміни вихідних значень програми, кількість операцій під час виконання програми, наявність зациклення, а також незадіяних ділянок програмного коду [2].

Формальні методи верифікації програмного забезпечення (ПЗ) використовують формальні моделі вимог – ФС, поведінки і оточення ПЗ для аналізу його властивостей. Такі моделі є або логіко-алгебраїчними, або виконуваними, або проміжними, що мають риси і логіко-алгебраїчних, і виконуваних моделей.

Перший тип – логіко-алгебраїчні моделі (property-basedmodels), вони ж – логічні або алгебраїчні обчислення [3]. Під час моделювання ПЗ модель такого типу описує деякий набір його властивостей, але не дає точного уявлення про те, за рахунок чого змінюються ці властивості.

Другий тип – виконувані моделі (операційні, executablemodels) характеризуються тим, що їх можна якимось чином виконати, щоб простежити зміну властивостей ПЗ, що моделюються [3]. Кожна реалізація моделі є, по суті, програмною реалізацією для деякої досить строго визначеної віртуальної машини [4]. Виконувані моделі можна вважати розширенням і узагальненням кінцевих автоматів.

Ще один тип – модель проміжного типу мають риси як логіко-алгебраїчних, так і виконуваних [5]. Варто зазначити, що частина перерахованих вище прикладів може бути, за деякими причинами, віднесена до обох цих класів. Наприклад, алгебри процесів мають точний виконуваний аналог – розмічені системи переходів, а машини абстрактних станів визначаються як деяке сімейство універсальних алгебр. Є, однак, види моделей в яких логіко-алгебраїчні і виконуючі елементи поєднуються [6].

Як узагальнення вищесказаному – формальні методи верифікації програмної складової полягають у перевірці математичної моделі програми, а не програми безпосередньо [7].

Можна виокремити два основних підходи до верифікації. Перший підхід будується на методах доказів, тобто перевірка відповідності отримуваних рішень вимогам та проектним рішенням ґрунтується на теоретичному доказі. Згідно цього підходу, ФС складається з набору декларативних операторів або декларативних пропозицій де,як правило, визначаються властивості реальних сутностей, їх поведінка та взаємодія.

Другий підхід будується на залученні представників сімейства методів перевірки на моделі – теоретико-модельний підхід. Згідно цього підходу, система є операторною моделлю, яка, зазвичай, відображає поведінки системи.У якості моделі – системи переходів, як правило, використовується структура Кріпке [5].При цьому кожен стан системи визначається логічним виразом, тобто система перебуває у тому чи іншому стані тоді, і тільки тоді, коли названий вираз набуває істинного значення.

Верифікація шляхом перевірки на моделі починається з вихідного стану системи та, застосовуючи операції, генерує наступні стани.При цьомудосліджувані властивості або обмеження перевіряються для кожного із синтезованих станів. Перевага такого підходу – можливість автоматизації процесу верифікації [6]. Специфіка – для побудови математичної моделі (системи переходів) потрібен кваліфікований фахівець. Успішність застосування названого підходу безпосередньо залежить від адекватності створеної ФС.

Класичні оптимізаційні моделі прийняття рішень побудовані таким чином, щоб можна було використовувати математичний алгоритм та отримати оптимальну практичну рекомендацію. Їх недоліки полягають у вимушеному спрощенні дійсності, оскільки визначення параметрів моделі має бути орієнтоване на забезпечення можливості вироблення рішень. Отримані в такий спосіб рекомендації часто втрачають практичну цінність. Водночас, оптимізаційні моделі мають і значні переваги:

- не допускають логічних помилок;
- не містять нічого зайвого та зводять проблему до її суті;
- сприяють вираженню основних взаємозв'язків.

Будь-яка названа модель характеризується такими основними елементами:

- є кінцева мета функціонування системи;
- існують кілька способів досягнення мети, що допускають кількісне зіставлення результатів;
- ресурси, необхідні для функціонування системи, кінцеві в кожен момент часу, а ефективність їх використання за напрямками різна;
- функціонування системи можливе за різних комбінацій ресурсів;
- існує критерій оцінки можливих шляхів досягнення цілей.

У якості суттєвого недоліку методів перевірки на моделі можна вказати залежність результатів ФВ від адекватності ФС, але, водночас,названі методи дають гарні результати при їх застосуванні у промислових проектах [8]. Для створення ФС, як правило, залучають певну темпоральну логіку [9].

Вагомою перевагою методів перевірки на моделі є можливість автоматизації процесу ФВ.

Під час використання формальних методів процес розроблення програмної складової СКП може виявитися повільним та трудомістким, проте, отримуваний результат буде містити менше помилок завдяки

математичній строгості ФС, що можуть залучатися на всіх етапах процесу розроблення, починаючи зі складання вимог. У контексті розроблення СКП, формальні методи дозволяють підтвердити (на основі ФС) відповідність досліджуваних показників артефактів процесу розроблення заданим вимогам. Більше того, вони можуть розглядатися як засоби, що доповнюють та сприяють поліпшенню процесу тестування [10].

Таким чином, методи перевірки на моделі відрізняються трудомістким процесом побудови ФС, застосовуваних у якості вихідних даних, але при цьому вони забезпечують придатність процедури ФВдо автоматизації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Karpov Yu.G. Model checking. Verifikatsiya parallel'nykhi raspredelennykh programmnykh sistem [Model checking. Verification of parallel and distributed software systems]. St. Petersburg, BKhV-PeterburgPubl., 2010. 560 p. (inRussian).
2. Boyer R.S., Elspas B., Levitt K.N. SELECT a formal system for testing and debugging programs bysymbolic execution. Proceeding softheInternational Conference on Reliable Software, LosAngeles, California, 1975. ACM NewYork, NY, USA, 1975, pp. 234-254. DOI: 10.1145/800027.808445
3. Lamport L. Specifying systems: The TLA+ language and tools forhard ware and software engineers. Boston: Addison-Wesley, 2002. 382 p.
4. Kuliamin V.V. Metody verifikatsii programmnogo obespecheniia [Method sofsoftware verification]. 2008. 117 p. Single Window Access toInformation Resources: internet portal. Availableat: http://window.edu.ru/resource/168/56168, accessed 01.09.2015. (inRussian).
5. Кларк Е.М., Верифікація моделей програм: Modelchecking: перев. з англ. під. ред. Р. Смілянського. Москва: МЦНМО, 2002. 416 с.
6. Конорєв Б.М. Інваріантно-орієнтована оцінка якості програмного забезпечення космічних систем: Державний центр регулювання якості поставок та послуг, Національний аерокосмічний університет ім. Н.Є. Жуковського «ХАІ», 2009. 224 с.
7. Майер Б. Програмна інженерія як предмет навчання. Відкриті системи. Липень-серпень, 2001. С.80-86.
8. Омельчук Л.Л. Формальні методи специфікації програм: навч. посібник. Київ: УкрІНТЕІ, 2010. 78 с.
9. Орлов С.А. Технології розробки програмного забезпечення. Підручник для Вузів. Пітер. 2002. 463с.
10. Харченко В.С. Аналіз проблем ІТ-інженерії безпеки: проект TEMPUS-SAFEGUARD. Радіоелектронні і комп'ютерні системи. 2010. No 7 (48). С. 297-300.

Євдокимов Віктор Федорович,
ІПМЕ ім. Г.Є. Пухова НАН України,
головний науковий співробітник,
д-р техн. наук, професор, чл.-кор. НАН України,
evdokimovvf@gmail.com

Давиденко Анатолій Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний наук. співроб., д-р техн. наук,
старш. наук. співроб.,
davidenkoan@gmail.com

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук. співроб., д-р техн. наук,
старш. наук. співроб.,
hilgurt@ukr.net

СЕРВІС ЦЕНТРАЛІЗОВАНОГО СИНТЕЗУ АПАРАТНИХ ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В КІБЕРФІЗИЧНИХ СИСТЕМАХ

Анотація. Розглянуто техніку прискореного обчислення функціональної залежності кількісних характеристик реконфігуровних засобів сигнатурного аналізу з використанням фільтра Блума на базі геш-функцій від властивостей набору патернів та апаратного прискорювача, яка дозволяє виконувати процедуру оптимізації за прийнятний час.

Abstract. The technique of accelerated calculation of functional dependence of quantitative characteristics of reconfigurable means of signature analysis using Bloom Filter based on hash-functions on the properties of a pattern set and hardware accelerator, which allows performing the optimization procedure in a reasonable time, is considered.

Кіберфізичні системи (КФС), під якими розуміють широкий спектр складних, багатодисциплінарних, інженерних систем наступного покоління, інтегрують вбудовані обчислювальні технології (кіберчастину) у фізичний світ [1]. У таких системах високосинхронізована інформація передається між фізичним обладнанням і віртуальним обчислювальним простором, що призводить до нового рівня контролю, ефективності, прозорості та спостереження технологічних процесів. Тому проблема забезпечення цілісності інформації, що передається в каналах обміну даними між компонентами кіберфізичних систем, є дуже важливою, особливо у випадку використання КФС у критичній інфраструктурі, зокрема, в енергетичній галузі.

Найвідомішим шляхом боротьби з помилками, що виникають внаслідок впливу завад, є використання спеціальних коригуючих кодів, здатних виправляти помилки [2]. Ефективність такого підходу безпосередньо залежить від якості коду, що використовується, яка повністю визначається його породжувальною матрицею. Пошук найкращих кодів, які відповідали б вимогам, що висуваються до комунікаційних засобів КФС, не є тривіальною задачею. Один з підходів до пошуку таких кодів полягає у переборі можливих комбінацій рядків, що складають їх породжувальні матриці. У зв'язку з тим, що повний перебір всіх можливих варіантів є NP-повною задачею, безпосередня реалізація такого підходу потребує неприйнятно багато часу. Але комбінування певних методів та технік у поєднанні з використанням високопродуктивної обчислювальної техніки дозволяють за певних умов здобути непогані результати при помірних часових витратах [3].

В даній роботі розпочато низку досліджень, спрямованих на використання високопродуктивних обчислювальних ресурсів для побудови засобів забезпечення цілісності інформації в КФС, що базуються на лінійних блокових коригуючих кодах. На першому етапі розроблено методику централізованої побудови додаткових модулів забезпечення цілісності інформації, що передається в каналах обміну даними між компонентами кіберфізичних систем, з використанням грід-ресурсів [4]. Створено грід-сервіс для пошуку та дослідження породжувальних матриць лінійних блокових коригуючих кодів.

Створений сервіс дозволяє за наданими параметри здійснювати пошук правильних породжувальних матриць та відповідних значень мінімальної кодової відстані для лінійних блокових кодів. Сервіс складається з інтерфейсу користувача, бази даних та серверних компонент. Розрахунок породжувальних матриць та мінімальної кодової відстані виконується з використанням обчислювальних потужностей Українського національного гріду. При цьому максимально використовуються результати попередніх розрахунків, які зберігаються в базі даних породжувальних матриць.

Запропоновані в роботі методика та сервіс синтезу додаткових модулів забезпечення цілісності інформації, що передається в КФС, дозволяє досліджувати властивості лінійних блокових коригуючих кодів та їх породжувальних матриць, а також оцінювати залежності часових витрат на пошук породжувальних матриць від розмінностей відповідних кодів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gunes V., Peter S., Givargis T., Vahid F. A survey on concepts, applications, challenges in cyber-physical systems. KSII Trans. Internet Inf. Syst., 2015. P. 4242–4268. doi: 10.3837/tiis.2014.12.001.

2. Блейхут. Р. Теория и практика кодов, контролирующих ошибки. Пер. с англ., М.: Мир, 1986. 576 с.

3. Винничук С.Д., Давиденко А.Н., Гильгурт С.Я., Потенко А.С. Нижняя оценка максимального кодового расстояния для линейных блоковых кодов (n, k) над полем GF(2). Тез. доп. Міжнар. наук.-техн. конф. «Моделювання-2012», Київ, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2012. – С. 150–153.

4. Винничук С.Д., Давиденко А.Н., Гильгурт С.Я., Потенко А.С. Применение грид-системы при исследовании линейных блоковых кодов. Системи обробки інформації: Збірник наукових праць, Харків, Харківський університет Повітряних Сил ім. Івана Кожедуба, 2013. Вип. 7 (114). С. 1–64.

Євдокімов Володимир Анатолійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
пров. наук.співроб., канд. наук з держ. упр.
ievdokimov40@gmail.com

Остапченко Костянтін Борисович
НТУУ «Київський політехнічний інститут
імені Ігоря Сікорського»
доцент, канд.техн.наук
okb2003@ukr.net

Борукаєв Зелімхан Харитонович,
ІПМЕ ім. Г.Є. Пухова НАН України,
зав.лабораторією., д-р техн. наук
zelimh1948@gmail.com

КІБЕРБЕЗПЕКАОРГАНІЗАЦІЙНИХ І ОРГАНІЗАЦІЙНО-ТЕХНІЧНИХ СИСТЕМ В ЕНЕРГЕТИЦІ УКРАЇНИ

Анотація. У роботі проведено стислий аналіз причин виникнення загроз длякібербезпеки в організаційних та організаційно-технічних системах управління в енергетиці. Наведено приклади застосування сучасних систем кібербезпеки.

Abstract. The paper provides a brief analysis of the causes of threats to cybersecurity in organizational and organizational-technical control systems in the energy sector. Examples of the use of modern cybersecurity systems are given.

Створення комп'ютерних засобів автоматичного та автоматизованого управління в енергетиці протягом багатьох років є однією з актуальних проблем моделювання процесів оперативно-технологічного, організаційного управління та інформаційного забезпечення. Ще в 60-х-70-х рр. минулого століття була поставлена задача створення інтегрованої галузевої АСУ енергетики СРСР «Енергія», основні науково-технічні вимоги до якої знайшли відображення в [1]. З того часу її вирішенню, розробці теоретичних та інформаційних аспектів присвячено чимало робіт, їх аналізу та узагальненню цілий ряд монографій.

В той же час почалося активне впровадження автоматичних систем диспетчерського управління (АСДУ) в енергосистеми та формування ієрархічних телеінформаційних мереж, що забезпечують передачу телеметричної інформації від енергооб'єктівдо диспетчерських пунктів енергосистем. Основною метою виконання цих робіт було підвищення надійності електропостачання до господарського комплексу країни шляхом підвищення ефективності вирішення двох найважливіших та взаємопов'язаних проблем розвитку електроенергетичного виробництва:

керованості об'єктів електроенергетики об'єднаної електроенергетичної системи (ОЕС); спостережливості стану ОЕС на всіх етапах виробництва, передачі та розподілу електричної енергії.

З початку 2000 років електроенергетична галузь України вступила на новий етап розвитку, який мав на увазі інтеграцію автоматичних і автоматизованих систем, що застосовуються в оперативно-технологічному диспетчерському управління режимами енергосистем (ЕС): системи SCADA (SupervisoryControlAndDataAcquisition); системи WAMC (WideAreaMeasurement Systems) для вирішення завдань спостереження і оцінки стану ОЕС, яка використовує пристрої синхронізованих вимірювань векторів напруги PMU (PhasorMeasurementUnit). Аналогом системи WAMC, яка застосовується в ОЕС України є система моніторингу, яка створена на базі високоточного електровимірювального реєструючого приладу (ЕВРП) «Регіна-Ч», якій розроблено в Інституті електродинаміки НАН України [9]. Він забезпечує: реєстрацію миттєвих значень струмів і напруги, збереження та обробку результатів вимірювань; їх відображення у вигляді найбільш інформативному для персоналу (текстові повідомлення, графіки, таблиці, осцилограми та ін.); передачу інформації набудь-який рівень ієрархії керування з її прив'язкою до сигналів точного часу [2]. Система моніторингу перехідних режимів є глобальною для території України, охоплює ключові вузли ОЕС України і здійснює синхронізований моніторинг та реєстрацію системних параметрів, а саме нормальних (сталих) і аварійних (перехідних) режимів роботиЕС. Така інтеграція надавала нові можливості для розв'язання низки завдань АСДУ та автоматичного керування ЕС. В цей же час, у зв'язку зі створенням оптового ринку електроенергії України почався і процес розробки та інтеграції автоматизованої системи комерційного обліку електричної енергії (АСКУЕ) із зазначеними вище апаратно-програмними системами. Всі системи зараз інтегровані на рівні формування вихідних даних та використовують для вирішення функціональних завдань одну й ту ж саму систему оперативно-вимірювальних комплексів, які розташовані практично по всій території України.

Протягом останніх 10 років інтерес кіберзлочинців до промислових підприємств електроенергетичної галузі зростає. Що призводить до кібератак, які можуть завдати шкоди як регіональним структурним елементам енергосистеми, так і ОЕС в цілому шляхом створення аварійних ситуацій, аж до каскадного розвитку аварії, яка характеризується послідовним відключенням дією релейного захисту або протиаварійної автоматики електромережевого і / або станційного обладнання, викликаним виникненням неприпустимого для цього обладнання режиму. На тлі цих атак, які уже мали місце на енергосистемах багатьох країн світу, кібербезпекаелекроенергетичного виробництва стала предметом наукових досліджень і прикладних розробок по всьому світу. В результаті все більше організацій веде розробку масштабних проектів з метою запобігання новим кіберзагрозам.

Можна з упевненістю сказати, що при проектуванні і побудові більшості із зазначених вище систем, які знайшли широке застосування в багатьох енергосистемах світу, при оцінці їх чутливості до змін у вхідної інформації, на помилки моделювання процесів функціонування або варіацій параметрів режиму, не враховували питання, пов'язані з їх вразливістю до різного роду кібератак.

Згідно з даними, наведеними в роботі [3], в ОЕС України використовуються різноманітні прикладні розробки в усіх напрямках технологічної і комерційної діяльності. Це: оперативно-інформаційні комплекси; обчислювально-технологічні комплекси, які вирішують завдання розрахунку усталених режимів, статичної та динамічної стійкості; завдання, які пов'язані з аналізом і перспективним плануванням режимів роботи ЕС; локальні і регіональні автоматизовані системи обліку електроенергії; автоматизовані системи збору інформації від приладів цифрового релейного захисту та автоматики і т.ін. Кожен з наведених додатків має свою унікальну прикладну модель інформаційної бази даних зі своїми структурами і описом взаємозв'язків між ними, свої інтерфейси доступу та обміну даними.

Очевидно, що з розвитком ОЕС, зростанням потужності генеруючих об'єктів та їх кількості, в тому числі і за рахунок розподіленої генерації, особливо це стосується розвитку відновлювальних джерел енергії (ВДЕ), ліній електропередач зростає число взаємозв'язків між АСДУ різних рівнів, автоматизованих систем управління технологічними процесами (АСУ ТП) об'єктів,управління, спостереження (моніторингу) і контролю, засобів управління в нормальних і аварійних режимах, автоматичних систем протиаварійного та релейного захисту і т.ін. Очевидно, що в цих умовах значно ускладнюються процеси функціонування енергосистем, а разом з цим і рішення задач управління їх режимами та спостереженнями [4].

Тому в Україні, як і у США, а потім у Європейському союзі, КНР та інших країнах прийнято новий напрямок розвитку електроенергетики на базі концепції SmartGrids, в основі інформаційно-технологічної ідеології якої лежить цифрова трансформація всіх процесів збору, накопичення і передачі інформації в автоматичних і автоматизованих системах управління виробництвом, передачею та розподілом електроенергії, див., наприклад, [5,6]. У цих роботах поряд з аналізом проблем, які пов'язані з розвитком електроенергетики в зазначеному напрямку визначені основні технологічні і технічні складові реалізації, як складові майбутньої концепції розвитку SmartGrids в Україні.

Очевидно, що не менш важливою складовою такої концепції є інформаційна кібербезпека. Тому ця обставина обумовлює необхідність вивчення, дослідження проблем та врахування сучасного стану кібербезпеки електроенергетичного господарства ОЕС, як одного з найважливіших об'єктів критичної інфраструктури.

Однією з таких проблем є проблема дослідження чутливості засобів автоматичного та автоматизованого управління, які забезпечують вирішення

перелічених вище завдань управління ОЕС на верхньому ієрархічному рівні, яка більшою мірою визначається вразливістю програмного забезпечення систем управління від кібератак.

Томупостає необхідність розробки методичних засад забезпечення кібернетичної безпеки функціонування ОЕСУкраїни до кібернетичних впливів, на підставі застосування підходів, прийнятих в міжнародних нормативно-правових актах і стандартах, відомих з теорії безпеки інформації, теорії поводження з інформаційними ризиками.

Більшість великих системних аварій, які сталися протягом останніх років, є наслідком виникнення, посилення та поширення в енергосистемі низькочастотних (до 1 гц) електромеханічних коливань (нчк). якщо обмежитися випадками виникнення нчк в енергосистемах лише у 21-му столітті, то їхня «географія» (за країнами виникнення) матиме такий вигляд (в хронологічній послідовності): КНР (6.03.2003 р.); США – Канада (14.08.2003 р.); Італія (28.09.2003 р.); Тайвань (24.01. 2004 р.).

Цей перелік далеко не повний, зокрема не згадано про виникнення НЧК в ОЕС України – 16.03.2016 р., 21.03.2016 р. та 18.02.2017 р. Наведені факти стосуються аварій які сталися з технологічних причин неприпустимої зміни тільки одного з параметрів управління режимом енергосистем - частоти. Але, вочевидь, достатньо і наведених фактів для того, щоб зрозуміти до яких тяжких наслідків може призвести проникнення кіберзлочинців в систему спостереження і оцінки стану енергосистем або АСДУ. Спотворення даних оцінки стану енергосистеми може привести до прийняття неправильних рішень в АСДУ, помилок при проведенні розрахунків платежів суб'єктів ринку електричної енергії на основі даних АСКОЕ. А спотворення даних диспетчерських команд від АСДУ вже на рівні виробництва і передачі електроенергії може призвести до виникнення аварійних ситуацій.

Агресивні кібератаки спрямовані в основному на зрив технологічнихопераційв енергосистемі і можуть привести до руйнування системної інфраструктури, травм і загибелі людей, завдати шкоди виробництвам промислової і сільськогосподарської продукції, транспорту, житлово-комунального господарства, навколишньому середовищу, викликати економічні і фінансові збої.

Як приклад реалізованої кібератаки на ОЕС України, можна навести інцидент, що стався в грудні 2015 року в декількох областях України, де понад 220 000 споживачів протягом майже 6 годин залишилися без електрики через кібератаки організовані на енергокомпанії. Ця атака включала до себе етапи: розвідки та збору даних, що передують атаці (в тому числі з використанням троянаBlackEnergy); безпосередньо захоплення управління промисловим обладнанням; відключення споживачів в декількох місцях одночасно, що супроводжувалося шквалом помилкових телефонних дзвінків на телефонні лінії енергокомпаній; приховування слідів і створення перешкод до відновлення (відключення систем безперебійного живлення, видалення всієї інформації з жорстких дисків, пошкодження конвертерів

послідовних інтерфейсів). Атака стали можливою в тому числі через відсутність на промислових об'єктах надійних механізмів моніторингу і запобігання кіберзагрозам та управління доступом.

Як вже зазначалося вище, при проектуванні, створенні та експлуатації існуючих в ОЕС АСДУ, систем спостереження та оцінки стану, при аналізі їх чутливості до можливих змін спостережуваних параметрів режимів не розглядалися проблеми, пов'язані з несанкціонованим зовнішнім впливом як на окремі елементи, так і на системи захисту і управління ними. Сучасний стан енергетичної галузі в цілому, розвиток систем розподіленої генерації, ВДЕ і пов'язаної з ними інфраструктури призвело до необхідності отримання достовірної і, по можливості, максимально повної інформації про режими і їх параметри в реальному часу. Модернізація існуючих мереж за рахунок введення мікропроцесорних систем захисту, контролю стану і параметрів, управлення і зв'язку сприяє переходу на рівень інтелектуальних електричних систем, які відповідають сучасним вимогам економічності, надійності, безперебійності і живучості із забезпеченням активного управління електроспоживанням.

Відомо, що між інтегрованими автоматизованими і автоматичними системами постійно і безперервно йде інформаційний обмін даними між різнотипним обладнанням мережевого комплексу, генеруючими компаніями, постачальниками електричної енергії. Він включає не тільки передачу даних, а й команди, що дозволяють дистанційно впливати на мережеву структуру (вмикати та вимикати обладнання) та режими, які пов'язані з управлінням процесом балансування виробництвом і споживанням електроенергії. В ОЕС, особливо з інтегрованими в них системами розподіленої генерації, включаючи і альтернативними джерела енергії, велика кількість яких може істотно впливати на режим роботи «основної» мережі, актуальними стають питання достовірності інформації та її захисту від несанкціонованого доступу, її спотворення, крадіжок або знищення. Природно, що при цьому зростає ймовірність реалізації кіберзагроз, які пов'язані з широкомасштабним впровадженням інформаційно-комунікаційних компьютерних технологій управління параметрами і режимами ОЕС.

Так, за даними Державного підприємства «Гарантований покупець», що розміщено на його офіційному сайті, загальна кількість об’єктів відновлювальної енергетики, які продають свою електроенергію до Оптового ринку складає 926 (станом на 17 вересня 2021 року). Але, цей показник кожен місяць змінюється у зв’язку із активним розвитком та введенням нових об’єктів відновлювальної енергетики [7].

Високий рівень кібербезпеки може бути досягнуто за допомогою низки заходів, наприклад таких, як закриття вразливості каналів доступу, впровадження адекватних процедур і процесів інформаційної безпеки, а також шляхом застосування спеціальних технічних рішень на основі брандмауерів (так званий мережевий екран).

Прикладами вразливостей також можуть бути:

- необачність персоналу (користувачі зберігають свої паролі в доступних місцях);

- відсутність контролю доступу (при виникненні загрози несанкціонованого доступу можлива втрата активів);

- ігнорування систем захисту (користувачі відключають засоби захисту);

- недисциплінованість (користувачі не змінюють паролі, використовують один і той же пароль для доступу до різних ресурсів на підстанції).

Прикладом запровадження заходів кібербезпеки є НЕК Укренерго (оператор системи передачі та є диспетчерським центром) та ДП Оператор ринку (оператор відповідних сегментів ринків, що здійснює погодинне формування ціни на електричну енергію), які розпочали реальні дії по впровадженню системи захисту управління ОЕС України та комерційними даними.

З метою автоматизації контролю та своєчасного виявлення змін та порушень роботи усіх систем інформаційної інфраструктури в НЕК "Укренерго" впроваджується централізована система управління подіями та інцидентами інформаційної безпеки (SIEM система), яка виконує функції збору та аналізу журналів подій із усіх систем забезпечення захищеної інфраструктури, включаючи мережеве обладнання, сервери та робочі станції, системи автентифікації, та інше.

ДП Оператор ринку здійснив відповідні заходи кібербезпеки, згідно до вимог міжнародному сертифікату ISO/IEC 27001, якій створює на підприємстві системи управління безпекою та визначає необхідні методи захисту [8].

Таким чином, система кібербезпеки в енергетиці є пріоритетною для держави з точки зору безпеки об'єктів критичної інфраструктури. Вона повинна мати динамічний прогрес, із використанням новітніх передових технологій та обміну даними між основними суб'єктами, які здійснюють моніторинг таких загроз, а також повинні виділятися необхідні кошти для проведення аудиту захищеності даних, збереження конфіденційності, цілісності й доступності усіх фізичних та інформаційних активів, доступність та надійність інформаційної інфраструктури та інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Основные научно–технические требования к созданию интегрированной отраслевой автоматизированной системы управления Минэнерго СССР (ИОАСУ Энергия). – Режим доступа :www.lawru/dok/1989/05/25/п1179110.htm. - Дата последнего посещения: 14.01.17

2. Стогній Б.С. Організація моніторингу режимів енергооб'єднанняУкраїни та нові можливості розв'язання задач диспетчерського керування / Б.С. Стогній, О.В. Кириленко, О.Ф. Буткевич, М.Ф. Сопель, В.М. Авраменко, В.Л. Прихно, П.О. Черненко // Наука та інновації.- 2009.- Т. 5, № 6.- С. 25—35.

3.ОсновополагающиепринципыинтеграцииАСКУЄ в НЭК «Укрэнерго» / К. В. Ущаповский, Г. И. Гримуд, П. А. Сергиенко, В. И. Васильченко, ГП «НЭК «Укрэнерго»,А. В. Гинайло, П. С. Лукьянчук, И. Н. Блощаневич, В. А. Гинайло, А. С. Яндульский. [Електронний ресурс] : [сайт] : Режим доступу : www.eknis.net/uploads. - (Дата звернення: 10.10.19). 28 с.

4. Гамм А.З. Наблюдаемостьэлектроэнергетических систем / А.З. Гамм, И.И. Голуб.- М.: Наука,1990. – 200 с.

5. Стогній Б.С. Інтелектульні електричні мережі електроенергетичних систем та їхне технологічне забезпечення / Б. С. Стогній, О.В. Кириленко, С.П. Денисюк // Техн. електродинаміка. – 2010.- №6.- С. 44-50.

6.Интеллектуальныеэлектроэнергетическиесистемы: элементы и режимы: Подобщ. ред. акад. НАН Украины А.В. Кириленко / Институтэлектроди-намики НАН Украины. – К.: Ин-т электродинамики НАН Украины, 2014. – 408 с.

7. Сайт ДП «Гарантований покупець» - https://www.gpee.com.ua

8. Сайт ДП «Оператор ринку» - https://www.oree.com.ua/index.php/web/300003.

Євдокимов Віктор Федорович,
Заслужений діяч науки і техніки України,
почесний директор ІПМЕ ім. Г.Є. Пухова НАНУ

Огір Олена Олександрівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
наук. співроб.,
lenaogir@gmail.com

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ РЕКОНСТРУКЦІЇ ДІАГНОСТИЧНИХ ЗОБРАЖЕНЬ

Анотація. В практиці застосування комп'ютерних методів реконструкції діагностичних зображень відомі дві класичні схеми, що мають декілька модифікацій. До першої групи відомих методів можуть бути віднесені: т. зв. метод оберненого хвильового фронту і його модифікації типу методу звернених проекцій. Фазове відтворення в значній мірі зберігає кореляцію між сигналами, із цього можливо зробити висновок про те, що в зображенні і об'єкті – точки, лінії повинні зберігати своє місцеположення. Фаза в значній мірі відображає взаємне геометричне положення деталей в об'єкті і зображенні ніж амплітуда. Наприклад, зміщення (в часі або просторі) сигнала не впливає на амплітуду перетворення Фур'є (Френеля), а впливає тільки на фазу, призводячи до появи лінійного фазового члена.

Abstract. In the practice of computer methods of reconstruction of diagnostic images, two classical schemes are known, which have several modifications. The first known methods include groups: the so-called. the method of the inverse wavefront and its modification of the type of the method of inverted projects. Phase reproduction largely preserves the correlation between signals, from which it can be concluded that in images and objects - points that must maintain their location. Phase reflects the relative geometric position of details in objects and images rather than amplitude. For example, the shift (in time or space) of a signal does not affect the Fourier (Fresnel) amplitude transformation, and it only affects the phase, resulting in a linear phase term.

Процес реконструкції та виводу діагностичних зображень включає наступні типи операцій:

- Опромінення об'єкта контролю.
- Реєстрація розсіяних ехосигналів.
- Обробка ехосигналів з метою фокусування зображень.
- Знаходження зображення, відповідного об'єкту сканування шару.
- Виконання обчислювальної процедури фільтрації від сигналів-завад.
- Проведення аналізу отриманого зображення.

Зменшення масштаба відтвореного Фур'є-перетворенням зображення також пов'язано з адекватним масштабуванням фази голограмного опису. [1,2,3].

На користь ефективності фазової інформації при відтворенні сигналів зображень в системах дефектоскопії голографічного типу говорить і той факт, що амплітуди спектральних складових на високих частотах мають тенденцію до спаду, в той час як короткотривалі деталі об'єктів, зображень відображаються більш високими просторовими частотами, безпосередньо пов'язаними із зміною фазової інформації.

Уявлення формування фазового сигнала з присвоєнням одиничної амплітуди можливо інтерпретувати як процес спектрального відбілювання сигналів звукової голограми об'єкта контролю. [4]

Сутність методу оберненого хвильового фронту полягає у вирішенні зворотного завдання хвильового поля: по відомому, що реєструється в площині голограми розподілу комплексних амплітуд когерентного поля $U(x_0, y_0, z)$ визначити хвильове поле об'єкта, що складається з точкових джерел сферичних хвиль, що інтерферують у вільному просторі і створюють, власне, реєстроване хвильове поле в площині голограми, розташованої на відстані z від об'єктної площини.

Відомо, що рівняння хвильового поля в площині голограми може бути записано у вигляді інтегрального перетворення об'єктної функції $U(x_0, y_0, z=0)$:

$$U(x_0,y_0,z) = \int\int_{-\infty}^{+\infty} \frac{\omega \cdot Cos(\overline{n},\overline{r}) \cdot l^{\frac{j\omega|\overline{r}|}{c}}}{j2\pi c|\overline{r}|} \cdot U(x_1,y_1,z=0)dx_1dy_1 \qquad (1)$$

де ω - частота коливань;

$\overline{n}$ - вектор нормалі до фронту падаючої хвилі в точці x_0, y_0, z;

$\overline{r}$ - вектор поширення хвилі від точки $x_1, y_1, z=0$ до точки x_0, y_0, z;

c – швидкість поширення хвилі;

x_1, y_1 – площина голографуючого об'єкта;

x_0, y_0 – площина голограми;

$U(x_1, y_1, z=0)$ – об'єктна функція хвильового поля в площині об'єкта;

$U(x_0, y_0, z)$ – розподіл комплексних амплітуд хвильового поля в площині голограми.

Метод базується на поданні дифракційного інтеграла у вигляді інтеграла згортання функції $U(x_1, y_1, 0)$ і передавальної функції вільного простору $h(x_0-x_1, y_0-y_1, z)$:

$$U(x_0,y_0,z) = h(x_0-x_1,y_0-y_1,z) \times U(x_1,y_1,z=0) \qquad (2)$$

або $U(x_0,y_0,z) = h(x_0-x_1,y_0-y_1,z) \times U(x_1,y_1,z=0)$

$$h(x_0 - x_1, y_0 - y_1, z) = \frac{\omega \cdot Cos(\overline{n,r}) \cdot 1^{j\omega|\overline{r}|}}{j2\pi c|\overline{r}|}$$

Використовуючи відомі апроксимації Френеля щодо вимог до взаємної геометрії розташування об'єктної площини та площини голограми, вибору моделей падаючої і відбитої хвиль, їх когерентності і розглядом тільки хвилі, що розповсюджується без загасання.

Виконавши операцію зворотного перетворення Фур'є отримуємо оцінку для функції розподілу поля на об'єкті.

Таким чином, алгоритм реконструкції зображення об'єкта по його голограмі на основі методу ОХФ наступний:

– а) виконати пряме перетворення виміряної голограмної функції $U(x_0, y_0, z)$;

– б) визначити Фур'є-перетворення h-функції;

– в) помножити $U_0(f_x, f_y, z)$ на $H^{-1}(f_x, f_y, z)$;

– г) виконати зворотне перетворення Фур'є добутку функцій, отриманого згідно в).

Отримана в результаті виконання зворотного перетворення функція є відновлене зображення об'єкта.

До переваг методу слід віднести прийнятний обсяг обчислень, відсутність складних інтерактивних процедур, що призводять при великих масивах вхідних найчастіше до нестійкості обчислювальних процедур, можливість реалізації в спеціалізованих обчислювальних структурах

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Евдокимов В.Ф. Огир А.С. О дискретной математической модели звуковой голограммы / Электронное моделирование. – 2000. № 1. – С.3 – 8.
2. Євдокимов В. Ф. Огір О.С., Огір О. О. Дослідження характеристик якості УЗ зображень та алгоритмів їх обробки / Моделювання та інформаційні технології: зб. наук. праць. – К.: ІПМЕ ім. Г. Є. Пухова НАНУ, 2017. Вип. 80. – С. 3 – 11.
3. Кравченко В. Ф. Цифровая обработка сигналов и изображений /М. : Физматлит, 2007. – 552 с.
4. Огир А. С. Тарапата В. В., Огир Е. А. О голографической системе визуализации медицинского назначения / Інформаційні технології: зб. наук. праць. – К. : ІПМЕ ім. Г. Є. Пухова НАНУ, 2006. – Вип. 37. – С. 3 – 6.

Зубок Віталій Юрійович,
ІПМЕ ім. Г.Є.Пухова НАН України,
ст.наук.співр.,
vitaly.zubok@gmail.com

Давидюк Андрій Вікторович,
ІПМЕ ім. Г.Є.Пухова НАН України,
аспірант,
andrey19941904@gmail.com

ФУНКЦІОНАЛЬНА СКЛАДОВА БЕЗПЕКИ АСУ ТП ЗА NIST SP 800-82

Анотація. У тезах доповіді представлено аналіз функціональної складової безпеки АСУ ТП за NIST SP 800-82, зображено відношення між складовими АСУ ТП. Додатково здійснено огляд нормативних документів України щодо безпеки АСУ ТП. Визначено проблеми захисту АСУ ТП. Акцентовано увагу на вразливостях АСУ ТП та уніфікації підходів до їх класифікації за NIST SP 800-82.

Abstract. The abstracts of the report present an analysis of the functional component of the safety of ICS according to NIST SP 800-82, showing the relationship between the components of ICS. Additionally, the review of the Ukrainian normative documents on the ICS security. The ICS protection problems are defined. Emphasis is placed on the ICS vulnerabilities and unification of approaches to their classification according to NIST SP 800-82.

Пунктом 20 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» [1] (далі - Закон) визначено термін «система управління технологічними процесами» (за текстом Закону використовується скорочення - технологічна система), а саме – автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних. У викладенні результатів дослідження буде використовуватися саме це визначення цього терміну (далі - АСУ ТП).

Сучасні АСУ ТП властиві різноманітні загрози з боку внутрішніх та зовнішніх зловмисників (терористичні, екстремістські та вороже налаштовані групи тощо), що мають на меті порушити стале функціонування системи. Варто зазначити, що самі виробники та користувачі не завжди забезпечують належний рівень захисту таких систем безпеку, маючи у пріоритеті виконання бажаних вункцій, при нехтуючи необхідними вимогами до безпеки власних систем. Із-за необхідності безперервної роботи

технологічних процесів базові компоненти АСУ ТП (індустріальні протоколи, операційні системи, системи управління базами даних) не мають можливості регулярного оновлення. Крім цього до джерел вразливостей можна віднести використання широко розповсюджених технологій (операційні системи – Windows, WinCE, Linux тощо, застосунки – системи управління базами даних, вебсервери тощо, протоколи – HTTP, RPC, FTP, DCOM, XML, SNMP тошо), з метою підвищення ефективності управління організацією з використанням віддаленого доступу мають місце випадки підключення АСУ ТП до корпоративних мереж. Усе вищезазначене призводить до появи вразливостей у системі, з викристанням яких реалізуються нові загрози (атаки).

Сьогодні для АСУ ТП найбільш актуальними є загрози збою, відмов та порушення режиму роботи, поширення шкідливого програмного забезпечення. Реалізація цих загроз безпосередньо пов'язана з помилковими діями користувачів, випадковим доступом сторонніх осіб до систем, несанкціонованим підключенням пристроїв до автоматизованих робочих місць користувачів, а також до Інтернету. Вирішення цих проблем зводиться до комплексу заходів із забезпечення інформаційної безпеки з урахуванням специфіки побудови та функціонування АСУ ТП та їх системи електронних комунікацій.

Проте, на даний час в існуючій нормативно-правовій базі України необхідні механізми для впровадження таких заходів відсутні у явному вигляді.

Адміністрацією Держспецзв’язку видано Наказ [2], яким затвердила Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури (далі - Рекомендації). У рекомендаціях зазначено, що їх розроблено «за мотивами» широко відомого NIST Cyber Security Framework [3] (далі – CSF). І, хоча Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання, їх затвердження є важливим і вагомим кроком з імплементації кращих практик і стандартів з кіберзахисту промислових інформаційних систем, зокрема, АСУ ТП. Варто зазначити, що Рекомендації запозичують з CSF таксономію і структуру кіберзахисту АСУ ТП.

Серед документів Національного інституту стандартизації США (NIST) є інше керівництво (NIST SP 800-82 «Керівництво з промислових систем керування») зі специфічним напрямком, в якому основну увагу надано захисту виробничих систем [4].

Даний документ визначає промислові системи керування (ICS), або автоматизовані системи управління (керування) технологічними процесами – як комплекс програмних і технічних засобів, призначений для вироблення та реалізації керувальної дії на технологічний об'єкт управління відповідно до прийнятих критеріїв керування [4].

У англомовних джерелах такі системи детерміновані більш чітко завдяки розподілу на промислові керуючі системи (industrial control systems, ICS), системи диспетчерського контролю та збору даних (Supervisory Control And Data Acquisition, SCADA), розподілені системи керування (Distributed Control System, DCS), та більш дрібні компоненти чи підсистеми, наприклад виробничий майданчик (site), мережа на виробництві (field network), контролер з програмованою логікою (PLC), датчик (sensor), виконавчий пристрій (actuator), архіватор даних (data historian) і таке інше. Надбудовою над ICS є операційні технології, або OT (Див. рис.1).

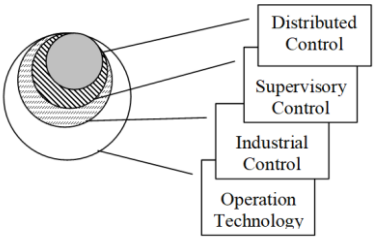


Рисунок 1 – Співвідношення між OT, ICS, SCADA та іншими компонентами промислових систем

Для ліпшого розуміння важливості вищенаведених компонентів варто розглянути їх місце у загальній структурі типової промислової системи (Див. рис. 2).

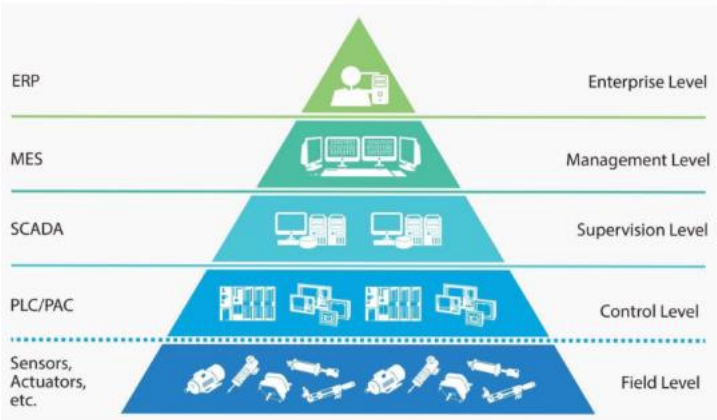


Рисунок 2 – Місце компонентів АСУ ТП у загальній структурі типової промислової системи [5]

Сучасні АСУ ТП безпосередньо керують складними та критичними технологічними процесами. Аварії викликані вразливостями АСУ ТП у енергетичній, хімічній, транспортній та інших галузях можуть призвести до величезних збитків не тільки в бізнесі, а й до важких екологічних наслідків, у тому числі й негативно вплинути на здоров'я та життя людей.

Такі наслідки можна розділити на фізичні - визначають інженерну взаємозалежність між об'єктами, інформаційні - залежність від інформаційного обміну (потоку інформації) між об'єктами, геопросторові– виникають в результаті спільного розташування компонентів інфраструктури на місцевості, процедурні (політичні) – виникають при будь-якій зміні (події) в одному з компонентів сектора інфраструктури і тягне за собою вплив на об'єкти інших секторів, соціальні - виражається через соціальні чинники: громадська думка, суспільна довіра, страх та ін. Наявність такого розподілу наслідків викликана наступною моделлю зв’язків об’єктів критичної інформаційної інфраструктури (ОКІІ) (Див. рис. 3).

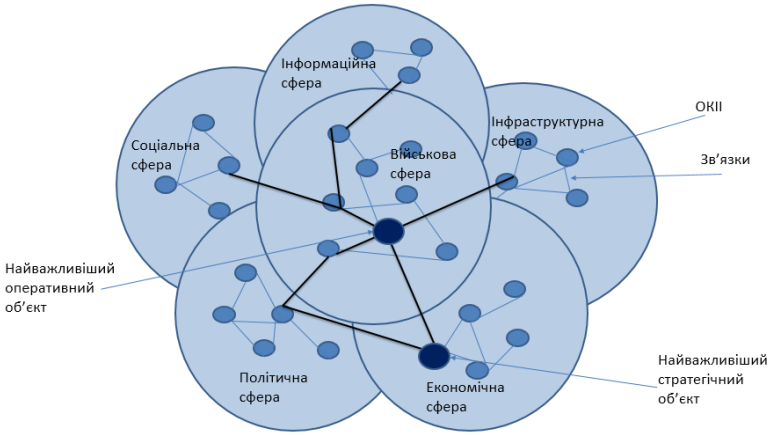


Рисунок 3 – Модель зв’язків наслідків за сферами впливу

Ризик техногенних катастроф визначається як надійністю системи, так і її безпекою. Безпека пов’язана з наявністю вразливостей – властивостей системи, використання яких зловмисником може призвести до негативних наслідків. Розробляючи атаку, зловмисник використовує будь-яку вразливість системи, а отже, для надійного захисту системи слід знайти та усунути якнайбільше критичних вразливостей. Документ [4] наводить класифікацію типових та найнебезпечніших вразливостей та причини їх виникнення, а також рекомендації щодо усунення цих вразливостей на основі аналізу архітектури АСУ ТП, а також етапів її життєвого циклу. Додатково розглядаються різні аспекти проєктування та функціонування АСУ ТП: розробка системи, налаштування, обслуговування, мережеві з'єднання та інші. Кожному аспекту притаманні власні типові вразливості. Їх

аналіз дозволяє співвіднести вимоги та рекомендації національних стандартів та вітчизняної нормативної бази з міжнародним досвідом.

NIST SP 800-82 є комплексним посібником з безпеки АСУ ТП в якому у вигляді настанов надано рекомендації для забезпечення повного циклу розробки системи захисту АСУ ТП. Рекомендації охоплюють всі кроки від постановки завдання до впровадження системи безпеки АСУ ТП та її безпечної експлуатації. На даний момент чинною є друга ревізія цього документа (NIST SP 800-82 Rev.2). Порівняно з початковою версією в ній оновлено загрози та вразливості АСУ ТП, процедури управління ризиками, рекомендовані практики та архітектури, інструменти безпеки в АСУ ТП, а також додано порівняння з іншими стандартами та настановами з інформаційної безпеки АСУ ТП.

Згідно з настановами вразливості в АСУ ТП можна класифікувати таким чином:

− вразливості у політиці безпеки, заходах щодо її реалізації;
− вразливості у розробці та архітектурі системи;
− вразливості у налаштуванні та обслуговуванні;
− вразливості фізичного характеру;
− вразливості у розробці програмного забезпечення;
− вразливості в телекомунікаціях та налаштуванні мережі.

Мережа АСУ ТП складається з багатьох взаємозалежних компонентів. Вразливості можуть виникнути на будь-якій складовій архітектури АСУ ТП, при чому не є неможливо відмовитись від якоїсь компоненти задля зменшення ризику використання вразливості зловмисником та забезпечення більшої стійкої роботи АСУ ТП. Крім того, в деяких випадках мережа АСУ ТП може бути з'єднана із зовнішньою мережею для організації обслуговування та можливості надати керуючий вплив у разі екстреної ситуації. Таким чином, разом із складністю зростає кількість вразливостей, що вимагає відповідних заходів захисту. Класифікація вразливостей NIST SP 800-82 стосується ключових компонентів і етапів життєвого циклу АСУ ТП, що дає можливість зменшити ризики порушення функціонування.

З огляду на вищезазначене можемо констатувати, що еволюція АСУ ТП дозволяє широко впроваджувати їх в існуючі фізичні системи замість ручних засобів керування. Масштабність впроваджень таких технологій можна спостерігати завдяки розповсюдженню префіксу smart («розумний») стосовно енергетичних мереж, будівль, транспортних систем. Цифровізація все нових і нових сфер з одного боку підвищує взаємозв’язок між ними і їхню критичність, а з іншого – підвищує вимоги до конфіденційності, цілісності, доступності та інших важливих властивостей АСУ ТП.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про основні засади забезпечення кібербезпеки України" [Електронний ресурс] // Верховна Рада України. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 601 [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-06-zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi.

3. Framework for Improving Critical Infrastructure Cybersecurity [Електронний ресурс] // NIST. – 2018. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

4. NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security / K.Stouffer, V. Pillitteri, M. Abrams, A. Hahn. // NIST. – 2015. – №2. – С. 1–247.

5. COLLINS D. What is Single Pair Ethernet (SPE) and how is it used in industrial applications? [Електронний ресурс] / DANIELLE COLLINS // Motion ControlTips. – 2021. – Режим доступу до ресурсу: https://www.motioncontroltips.com/what-is-single-pair-ethernet-how-is-it-used-in-industrial-applications/.

Каменева Ірина Петрівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
ст. н. сп.,
kamenevaip@gmail.com

ВІЗУАЛЬНИЙ ПІДХІД ДО ВИЯВЛЕННЯ АДАПТИВНИХ РЕСУРСІВ НА ПРИКЛАДІ ГРУПИ РИЗИКУ

Анотація. Розглядається імовірнісне уявлення про норму і патологію, одержане за допомогою імовірнісного розподілу окремих показників. В рамках запропонованого підходу на основі експериментальних даних (показників крові обстежених) виділено різні типи адаптивних реакцій, які характеризують адаптивний потенціал в групі ризику.

Abstract. The probabilistic idea of the norm and pathology, obtained using the probabilistic distribution of individual indicators, is considered. In the framework of the proposed approach, on the basis of experimental data (blood parameters of the subjects), different types of adaptive reactions characterizing the adaptive potential of the risk group are identified**.**

Багаторічні дослідження показують, що адаптивний потенціал довкілля (зокрема, організму людини) можна вважати основним джерелом, яке забезпечує життєздатність суспільства протягом тривалого часу, а також розкриває нові можливості для його розвитку [1].

Процес адаптації можна визначити як механізм налаштування, або пристосування, що забезпечує екологічній системі певну стабільність при кліматичних та екологічних змінах, які відбуваються в навколишньому середовищі. Прогнозуючи окремі характеристики природного середовища, можна завчасно передбачити певні тенденції в зміні основних параметрів досліджуваної системи.

Адаптація екологічної системи до нових умов визначається в рамках значень певних параметрів, що характеризують розміри максимальних навантажень на дану систему. Можливості успішної адаптації до граничних навантажень характеризують «адаптивний потенціал» екологічної системи, тобто індивідуальну здатність до адаптації в умовах безперервних змін навколишнього середовища [2].

Для більш глибокого дослідження процесів адаптації пропонується розглянути імовірнісне представлення норми, яке можна застосувати як для оцінки стану екосистеми в цілому, так і для окремого організму.

При нормальному стані система підтримує оптимальний рівень своїх адаптивних ресурсів та їх мобільність по відношенню до зовнішніх несприятливих подій. Захворювання можна розглядати як особливу форму адаптації (можливо, не зовсім вдалу), спрямовану на зменшення впливу особливо небезпечних для життя зовнішніх і внутрішніх факторів з метою відновлення стабільного стану організму [2, 3].

Норма в даному контексті відображає певний діапазон зміни якості (стану, співвідношень) та властивих йому кількісних значень в межах допустимих коливань, що не порушують даної якості. У зазначеному сенсі норма виступає як *міра здоров'я,* будучи не просто характеристикою кількості й якості, а мірою їх взаємозв'язку і відповідності певним станам.

Імовірнісне визначення норми (візуальна інтерпретація).

Нехай деяка змінна x набуває певних значень *F(x)* на відрізку $[a, b]$. Припустимо, що спостереження за значеннями x дозволили побудувати гістограму, показану на рис.1. Тоді *нормі* будуть відповідати ті значення x, які зустрічаються найбільш часто. Зазвичай виділяють певний інтервал значень, всередині якого окремі значення вважаються *нормальними*. Якщо значення x лежать зліва від інтервалу норми, то вони менше норми. Коли значення x знаходяться справа від цього інтервалу, вони інтерпретуються як перевищення норми. Отже, можна оперувати з деякою (досить суб'єктивною) шкалою, де поняття норми займає центральне положення, яке відповідає стабільному стану досліджуваної системи.

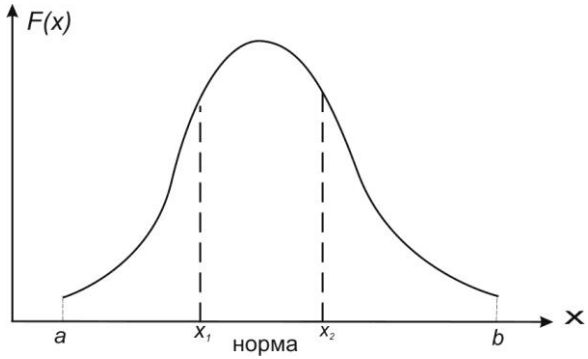


Рисунок 1 – Графічне представлення норми

Таким чином уявлення про норму і патологію можна отримати за допомогою імовірнісного розподілу ряду окремих показників. В термінах математичної статистики таке уявлення про норму формально відображує *нормальний закон розподілу* певної випадкової величини.

Для двох показників аналогічним чином можна описати двовимірний імовірнісний розподіл значень цих показників, або систему двох випадкових величин, яка підпорядковується нормальному закону розподілу.

Якщо дві випадкові величини *(X, Y)* враховуються одночасно, то вони утворюють систему випадкових величин, яка відображується на площині як випадкова точка з координатами *(X, Y)* або випадковий вектор, спрямований

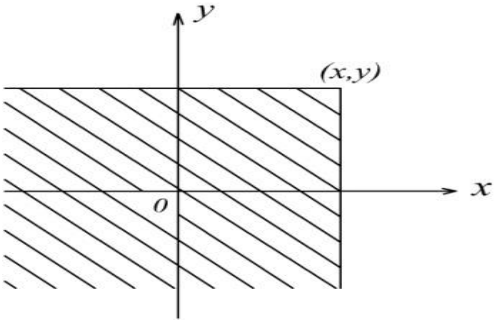
із початку координат в точку *(X, Y)*. Систему n випадкових величин також можна представити як випадкову точку (випадковий вектор) в просторі n вимірювань (імовірнісному фазовому просторі).

Якщо *X* і *Y* - дві випадкові величини (незалежні чи ні), то вони породжують відображення $Z(\omega) = (X(\omega), Y(\omega))$ простору Ω в R^2. Це відображення визначає міру $P_{X,Y}$ на σ- полі плоских борелевських множин, яка представляє спільний розподіл *X* і *Y*, де вираз

$$F_{X,Y}(x, y) = P(\{\omega: X(\omega) \le x, Y(\omega) \le y\})$$

визначає спільну функцію розподілу двох величин.

Геометрично така функція інтерпретується як імовірність попадання випадкової точки *(X, Y)* в заштриховану область, показану на рис. 2. Це визначення автоматично переносимо на випадок *n* вимірювань, де функція розподілу може інтерпретуватися як імовірність попадання випадкової точки в обмежену зверху по кожній координаті область *n*-вимірного простору.



Рисинук 2 – Геометрична інтерпретація розподілу двох величин

Нагадаємо також формулу, що визначає щільність розподілу $f(x, y)$ для системи двох випадкових величин (X, Y), яку можна записати через їх функцію розподілу наступним чином:

$$f(x, y) = (\partial^{\uparrow}2\, F(x, y))/\partial x \partial y = F_{\downarrow}xy^{\uparrow}{}_{\blacksquare}(x, y)$$

В системі двох випадкових величин виділяється елементарна величина *f(x,y)dxdy*, яка наближено відображує ймовірність попадання випадкової точки *(X, Y)* в елементарний прямокутник зі сторонами dx, dy, що примикає до точки (x, y).

Імовірність попадання випадкової точки (X, Y) в довільну область *D* визначається за формулою

$$P\big((X,Y)\epsilon D\big) = \iint_{(D)} f(x,y)dxdy .$$

Формули, наведені для системи двох випадкових величин, можна узагальнити для системи n випадкових величин. Однак надалі для наочного представлення медичних даних обрано відображення в систему випадкових величин, що має розмірність не більше трьох, яку зручно аналізувати і модифікувати засобами сучасної комп'ютерної графіки.

Зокрема, для двох незалежних випадкових величин нормальний закон розподілу набуває канонічного вигляду:

$$f(x,y) = \frac{1}{2\pi\sigma_x\sigma_y} e^{-\frac{x^2}{2\sigma_x^2}-\frac{y^2}{2\sigma_y^2}} .$$

В межах прийнятої гіпотези про нормальний розподіл щодо обраних показників можна одержати візуальне уявлення про стан обстежуваних осіб, яке в даному випадку визначається рядом медичних показників.

Візуальне уявлення про стан здоров'я

В якості кількісних показників психофізіологічного стану організму (параметрів) систематизовано різні групи фізіологічних характеристик, вимірюваних при обстеженні. Такі параметри можуть характеризувати склад крові (на основі результатів аналізів), стан системи дихання (за даними спірографії), особливості серцевого ритму (за даними кардіографії) та інші фізіологічні характеристики групи обстежуваних осіб.

Психофізіологічний стан, або стан здоров'я індивіда розглянемо як образ (точку певної розмірності) в m – вимірному просторі параметрів

$$x = \{x_1, x_2, \dots, x_m\}.$$

В процесі аналізу використовувалась відома гіпотеза компактності, яка передбачає деяку просторову впорядкованість досліджуваних образів: окремим групам точок в багатовимірному просторі відповідають певні варіанти адаптаційних можливостей.

Щоб отримати досить адекватне уявлення про структуру та взаємне розташування цих образів, на основі методів багатовимірного аналізу даних побудовано відображення φ: $X \to R^2$, яке забезпечує наочну інтерпретацію багатовимірної статистичної інформації у площині двох узагальнених координат [4, 5]. В максимально спрощеному вигляді одержані результати можна проілюструвати за допомогою рис.3.

Нехай A відповідає певному стану обстежуваного, A_1 - стану, що виник в результаті певного навантаження (впливу подразника). Тоді для кількісної оцінки зміни досить визначити величину зміщення від стану A в стан A_1. Використовуючи візуальне уявлення багатовимірної інформації, можна визначити допустимі межі зміни (норму) як область 1 і критичні межі зміни (стрес) як область 2. За межами цієї області знаходиться область патологічних змін 3.

Різниця між гранично допустимим і фактичним станом характеризує наявні психофізіологічні ресурси організму (або адаптивний потенціал обстеженого індивіда), що на рис. 3 умовно характеризує відстань від точки A до меж норми – овалу, позначеному (1).

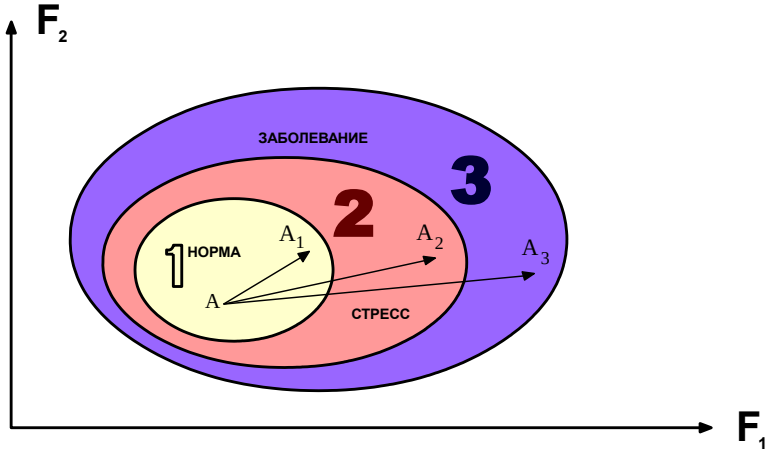


Рисунок 3 – Візуальне уявлення про норму і захворювання

Тоді величину збитку, заподіяного здоров'ю цього індивіда в результаті навантаження, можна охарактеризувати довжиною відрізка вектора AA_3, який потрапив в зону патологічних змін (3).

Далі розглянемо приклад, де в якості показників стану здоров'я, що відображають процес адаптації в умовах радіаційного та техногенного забруднення, виступають показники периферичної крові. Для спрощення обрано два показника, які виявилися найбільш інформативними для дослідження відомих адаптивних реакцій та визначення адаптивного потенціалу обстежуваних осіб. Приклад побудовано на основі статистичної інформації за результатами обстеження, проведеного для окремих категорій населення, пов'язаних з ліквідацією наслідків аварії на ЧАЕС [6].

Виявлення адаптивних реакцій на основі показників крові

Різні типи адаптивних реакцій можна однозначно визначити за співвідношенням між показниками периферичної крові. Виявлено також кореляцій між показниками крові та суб'єктивними станами індивідуума (настроєм, активністю, адаптивним потенціалом).

На основі досліджень, наведених в [3], виділено три типи адаптивних реакцій: реакція тренування, реакція активації і реакція стресу.

На експериментальному рівні встановлено, що тип реакції можна визначити по лейкоцитарній формулі крові пацієнта. Так, для реакції тренування число лімфоцитів становить 21-28%, а число сегментоядерних нейтрофілів - 55-65%. Для реакції активації можна виділити дві окремі зони: зону спокійної активації (лімфоцити - 28-33%, сегментоядерні нейтрофіли - 47-50%) і зону підвищеної активації (лімфоцити - 33-45%, сегментоядерні - менше 47%).

У стадії гострого стресу кількість лейкоцитів перевищує 9000, еозинофілів - 0, лімфоцитів - менше 20%, сегментоядерних нейтрофілів - більше 65%. При хронічному стресі кількість лейкоцитів і еозинофілів може бути довільною, а кількісне співвідношення лімфоцитів та сегментоядерних нейтрофілів таке ж, як і при гострому стресі.

Експериментальні дослідження підтвердили, що роль ключових факторів при виявленні типу адаптивної реакції грає чисельне співвідношення *лімфоцитів* і *сегментоядерних нейтрофілів*, максимальне для зони підвищеної активації і мінімальне при стресі.

На основі аналізу експериментальних даних [3, 4] побудовано двовимірний розподіл параметрів, який визначає співвідношення між значеннями показників крові та рівнем адаптивних ресурсів (рис. 4). Окремі області представленого розподілу відповідають різним рівням адаптивного потенціалу організму, тобто отримано графічне представлення наявних знань про адаптивні можливості організму людини.

На рис. 4 для виділених класів (або рівнів) адаптивних реакцій використовувались наступні позначення: Т – зона тренування, СА – зона спокійної активації, ПА – зона підвищеної активації.

Області тренування та активації описують сукупність адаптивних реакцій, які розглядаються як успішні способи адаптації організму до несприятливих умов. Області стресу та лімфоцитозу вже знаходяться за межами норми, тобто вказують на підвищену ймовірність захворювання при зазначених навантаженнях.

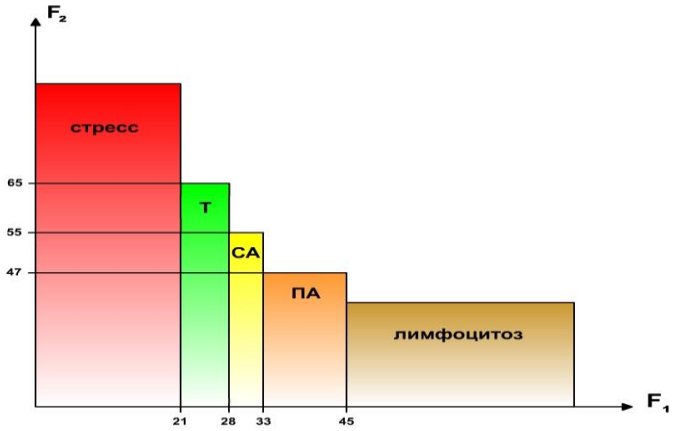


Рисунок 4 – Візуальне представлення адаптивних реакцій.

Розподіл за типами реакцій, наведений на рис. 4, запропоновано розглядати як двовимірну еталонну шкалу для діагностики обстежуваних осіб на основі окремих показників крові. Кожному індивіду з групи ризику відповідає певна точка в просторі станів, яка визначає його адаптивний потенціал в умовах підвищеного ризику.

Для аналізу експериментальних даних за результатами обстеження використовувались засоби інтегрованої системи STATISTICA, розроблена для вирішення прикладних задач статистичного аналізу даних в середовищі Windows, що включає широкий спектр методів візуалізації даних [7].

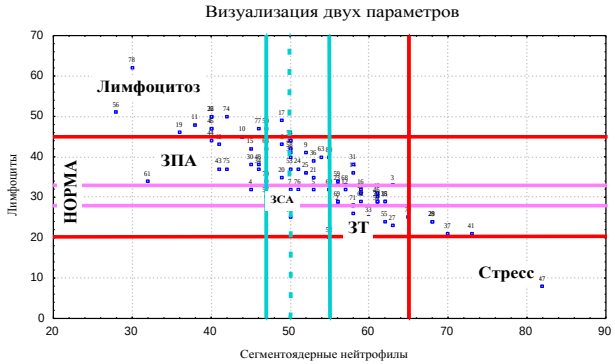


Рисунок 5 – Приклад діаграми розсіювання для групи ризику

На окремих етапах аналізу експериментальної інформації передбачено можливості для візуальної інтерпретації чисельної інформації за допомогою різних типів графіків. Наприклад, графічна візуалізація чисельних значень окремих показників у вигляді діаграм розсіювання дозволяє швидко оцінити співвідношення між основними показниками в фазовому просторі двох або трьох координатних осей.

На рис. 5 показано приклад діаграми розсіювання, побудованої за значеннями двох показників периферичної крові, що грають ключову роль в процесі визначення адаптивних реакцій. Приклад побудовано на основі показників крові представників групи ризику, що включила 80 осіб, які проживали в Овруцькому районі Житомирської області [4, 6].

Вздовж горизонтальної осі показано чисельні значення (у відсотках) для сегментоядерних нейтрофілів, а по вертикалі – щодо кількості лімфоцитів.

Поглиблене вивчення реакцій на різні подразники показало, що сприйнятливість (реактивність) індивіда залежить від загального стану організму. Зокрема, виявилося, що діапазони реактивності для різних рівнів енергетичних ресурсів можуть відрізнятися. При занадто інтенсивному для даного рівня навантаженні спостерігається відключення цього діапазону і включення наступного. Тобто при поступовому збільшенні навантаження адаптивні можливості організму можна істотно розширити.

Висновки

Запропоновано візуальний підхід до визначення норми і патології, яке можна формалізувати на основі імовірнісного розподілу окремих показників стану здоров'я. В рамках даного підходу на основі експериментальних даних (показників стану крові) визначено різні рівні адаптивних реакцій, що характеризують адаптивний потенціал групи ризику. Кожній особі з групи ризику ставиться у відповідність певне значення в просторі станів, яке визначає його адаптивний потенціал в умовах високого ризику.

Візуальний підхід надає можливість компактно відобразити великі обсяги інформації, накопичені в результаті обстеження. Кожна така діаграма може розглядатися як інформаційний портрет групи ризику, де у стислому вигляді міститься основна інформація про наявні адаптивні ресурси.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Экология. Справочник. [Электронный ресурс] – Режим доступа: https://ru-ecology.info/term/48659/ – Загл. с экрана.

2. Дичев Т. Адаптация и здоровье, выживание и экология человека. М.: «Витязь», 1994. С. 324.

3. Гаркави Л. Х., Квакина Е. Б., Уколова М. Ф. Адаптационные реакции и резистентность организма. Изд-во Ростовского университета, 1979. С. 125.

4. Сердюцкая, Л.Ф. Системный анализ и математическое моделирование медико-экологических последствий аварии на ЧАЭС и

других техногенных воздействий. [Текст] / Л.Ф. Сердюцкая, И.П.Каменева. – К.: «Медэкол» МНИЦ БИО-ЭКОС, МЧС и НАН Украины , 2000. – 173 с.

5. Каменева И.П. Вероятностные модели репрезентации знаний в интеллектуальных системах принятия решений / И.П. Каменева // Искусственный интеллект. – 2005. – № 3. – С. 399-409.

6. Клименко В.И., Дягиль И.С. Система кровотворения / Медицинские проблемы производственного объединения «Чернобыльская атомная станция» и объекта «Укрытие». К., 1996. С. 40–49.

7. Боровиков В.П. STATISTIKA. Искусство анализа данных на компьютере. 2-е изд. (+CD). – СПб.: Питер, 2003. – С. 688.

Комаров Максим Юрійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
науковий співробітник,
maxkom@i.ua

Гончар Сергій Феодосійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заст. директора,
sfgonchar@gmail.com

АКТУАЛЬНІСТЬ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ ЕНЕРГЕТИКИ

На сьогоднішній день не можна гарантувати повну захищеність будь-якої інформаційної системи, у тому числі інформаційної системи об'єкта енергетики [1-3]. Якщо раніше метою кібербезпеки об'єктів енергетики були заходи щодо запобігання кібервторгненням, то поступово вона трансформується у виявлення кібератак, адекватне та негайне реагування на них і ліквідація наслідків реалізації цих кібератак. Виникають задачі мінімізації часу відновлення функціонування інформаційної системи в штатному режимі, забезпечуючи захист життєво важливих компонентів для її функціонування шляхом резервування, дублювання тощо. Це, особливо актуально для об'єктів критичної інфраструктури енергетичного сектора.

Таким чином, актуальною задачею являється забезпечення кіберстійкості інформаційних систем об'єктів енергетики, як стану таких об'єктів, за якого забезпечується її спроможність надійно функціонувати та надавати основні послуги в умовах кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Комаров М.Ю., Гончар С.Ф. Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури. Моделювання та інформаційні технології, 2017. №81. С. 12-19.

2. Komarov M., Davydiuk A., Onyskova A., Tkachenko V., Honchar S. (2021) Requirements for a Taxonomy of Cyber Threats of Critical Infrastructure Facilities and an Analysis of Existing Approaches. In: Zaporozhets A., Artemchuk V. (eds) Systems, Decision and Control in Energy II. Studies in Systems, Decision and Control, vol 346. Springer, Cham. 22 March 2021.

3. Комаров М.Ю., Гончар С.Ф., Дімітрієва Д.О. Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 2021. С. 59-66.

Криворучко Ігор Петрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
uhmi_igorkr@ukr.net

КУСКОВО-ЛІНІЙНА АПРОКСИМАЦІЯ СИНУСОЇДАЛЬНОГО РУХУ КАРЕТКИ ВІБРОКАЛІБРУВАЛЬНОГО КОМПЛЕКСУ

Анотація. Для спрощення реалізації руху каретки віброкалібрувального комплексу пропонується апроксимація синусоїди кусково-лінійною функцією. Розроблена програма для розрахунку необхідних параметрів: частоти слідування імпульсів, величин інтервалів, числа імпульсів в залежності від заданих частоти коливань, амплітуди та рівня нелінійностей.

Abstract. To simplify the realization of the carriage motion of the vibro-calibration complex, an approximation of the sine wave by a piecewise linear function is proposed. The program for calculation of necessary parameters: frequency of following of impulses, sizes of intervals, number of impulses depending on the set frequency of oscillations, amplitude and level of nonlinearities is developed.

Апаратно-програмний віброкалібрувальний комплекс складається із системи приводу руху каретки з датчиками параметрів руху (акселерометри) та вимірювального блоку [1]. Відповідно до ТЗ потрібно забезпечити періодичний рух каретки з досить високими показниками якості руху. Використовуваний у якості приводу кроковий двигун (КД) має, як і всі КД, ступінчастий характер обертання якоря. Обертальний рух якоря за допомогою спеціального пристрою - актуатора перетворюється на послідовне ступінчасте переміщення каретки. Величина кроку визначається як параметрами актуатора так і обраним режимом роботи КД. Залежно від КД і обраного режиму роботи драйвера величина кроку КД може змінюватися від 1,8 кут. град. до 1/512 цієї величини у режимі "мікрокроку". Можна оцінити величину основного кроку в мм.

$$l_{\text{ш}} = \frac{2\pi * \mathbf{R}}{\mathbf{200}} \simeq \mathbf{0.5\,мм}, \qquad (1)$$

де $l_{\text{ш}}$ - величина основного кроку, R – радіус шестерні актуатора КД.

Кількість кроків необхідна для переміщення каретки на відстань 0,5 метра (від центрального положення до крайнього положення) можна розрахувати так:

$$N = \frac{\mathbf{A}}{l_{\text{ш}}} \simeq \mathbf{10000} \quad (2)$$

де А – амплітуда коливання.

Одним із основних типів коливань каретки – синусоїдальний рух. Реалізація синусоїдального руху каретки вимагає розрахунку моментів здійснення чергового кроку згідно з формулою наведеною в [2]. Для зберігання, оперативного зчитування без затримок та передачі контролеру значень інтервалів між кроками потрібна наявність оперативної або іншої пам'яті, що швидко зчитується, від 100 кБайт і більше для ¼ періоду коливань. Іншим варіантом реалізації синусоїдального руху можливо представлення його кінцевим числом послідовно з'єднаних прямолінійних відрізків. Перевага такого представлення - рівність часових інтервалів кожного кроку межах окремого відрізка. У такому разі розмір пам'яті для зберігання величин інтервалів зменшується у сотні разів. Заміна руху по синусоїді рухом по ламаною полілінії супроводжуватиметься збільшенням нелінійних спотворень у порівнянні з еталонним. Очевидно, що зі збільшенням числа відрізків, що використовуються для представлення синусоїди, зменшується ступінь відмінності двох графіків. Для оцінювання рівня відмінності можна використовувати кілька оцінок: коефіцієнт кореляції, Евклідова відстань, різницю площ двох графіків, сума квадратів відхилень у заданих точках (квадратичне наближення), а також максимум модуля різниці та ін. Однак для нашої задачі доцільно використовувати коефіцієнт нелінійних спотворень (Кн), оскільки у вимірювальному блоці комплексу передбачено вимірювання параметрів датчиків, що тестуються на частоті коливань каретки з датчиками. Тому оцінка Кн, отже, і величини гармонійних складових дуже важлива. Для оцінки величини відхилень двох графіків розроблено алгоритм і реалізовано програму розрахунку точок перелому (точки на синусоїді, в яких закінчується попередній відрізок і починається наступний), числа кроків для кожного кутового інтервалу, частоти кроків в залежності від заданої частоти коливань каретки та амплітуди коливань (максимального відхилення каретки від положення рівноваги). В результаті роботи програми будуються обидва графіки (рис. 1). По осі абсцис - кут відхилення каретки з кроком 0,17578125 град.

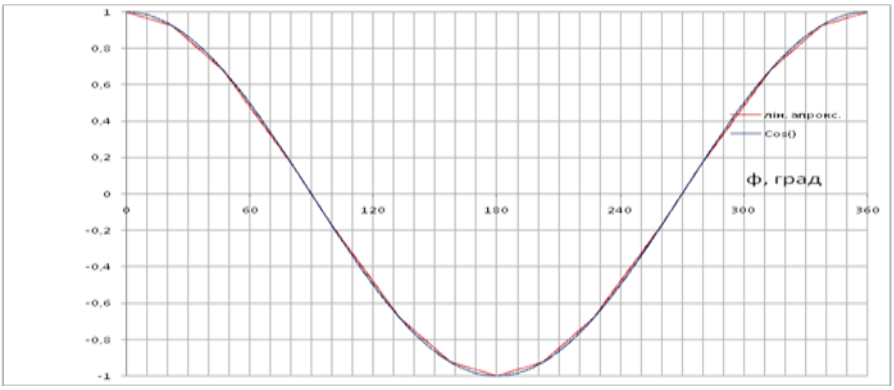


Рисунок 1 – Кусково-лінійна апроксимація y=cos(φ) чотирма відрізками (на ¼ періоду)

Куту 90 град. відповідає максимальне відхилення від положення рівноваги незалежно від періоду коливань. Для спрощення сприйняття амплітуда коливання на графіку дорівнює одиниці.

Ступінь відмінності двох графіків визначається параметром d1, що використовується в програмі, який задає максимальне допустиме відхилення ординат двох графіків.

На рис. 2 представлений аналогічний графік, але кількість прямолінійних відрізків становить 10.

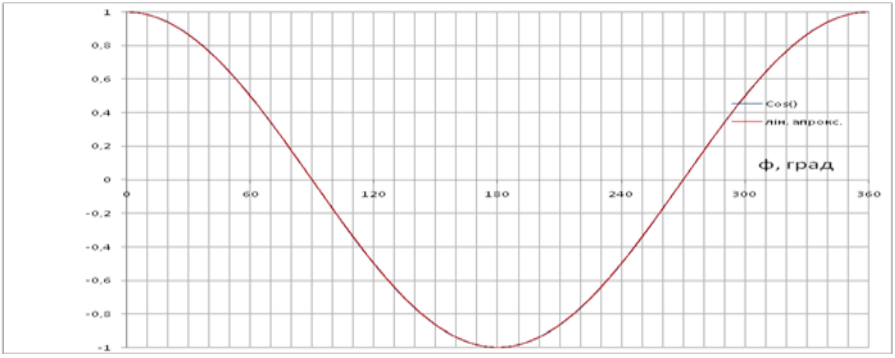


Рисунок 2 – Кусково-лінійна апроксимація y=cos(φ) 10-ма відрізками (на ¼ періоду)

З малюнка видно, що збільшення кількості відрізків призводить до значного покращення «якості» графіка. Узагальнені результати вимірювань деяких оцінок міри близькості для ряду значень параметра d1 наведено на рис.3.

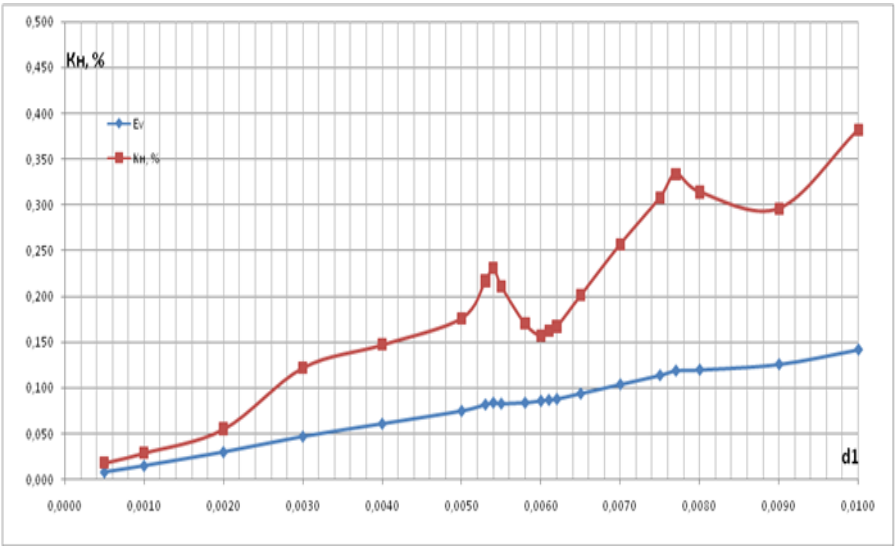


Рисунок 3 – Залежність Кн та Ev від максимального модуля різниці d1.

Евклідова відстань (Ev) є найбільш зрозумілою та інтерпретованою мірою відмінності або близькості об'єктів і є геометричною відстанню в багатовимірному просторі. Воно обчислюється за теоремою Піфагора. У нашому випадку Ev обчислюється як квадратний корінь від суми квадратів різниці ординат на кожному кроці (512 точок). Кн дорівнює відношенню середньоквадратичного значення всіх вищих гармонік сигналу до напруги першої гармоніки.

Задання величини d1 впливає як на оцінні параметри схожості графіків так і на число прямих відрізків і відстань точок перелому від початку відліку в кутових одиницях. Тому для певних значень d1 можуть виникнути ситуації, коли відстань між точками перелому (найбільших неоднорідностей графіка) може становити точну частину від періоду коливань, а значить може розглядатися як додаткова гармонійна складова результуючого сигналу. Це підтверджується графіком залежності Кн від d1. Наприклад, для d1=0,0054 7-а гармоніка у спектрі сигналу збільшена більш ніж у 22 рази порівняно з величиною цієї гармоніки для значення d1=0,006. Цьому випадку відповідає відстань між першою та четвертою точками перелому рівна 49,5 град. і між 4-ою та 2-ою (у наступному квадранті) 52 град. Це можна розглядати як додатковий сигнал, що заважає, на частоті близької до 7-ї гармоніки. Коректним вибором d1 можна мінімізувати Кн кусково-лінійної функції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. О.А.Владимирський, І.А.Владимирський, А.П.Іващенко, І.П.Криворучко Розробка структури низькочастотної автоматизованої вібро-калібрувальної установки НАВКУ-3. Моделюваннята інформаційні тех-нології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 89, Київ, 2019р.-с.45-49.

2. І.П. Криворучко. Методика розрахунку параметрів управління крокових двигунів для моделювання руху довільного характеру, Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці НАН України. Вип. 91, Київ, 2020 р.

Лєпатьєв Антон Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
antonlepatiev@gmail.com

Самойлов Віктор Дмитрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
доктор технічних наук, старший науковий співробітник,
samoylov.vd@gmail.com

ТРЕНАЖЕРНА ПІДГОТОВКА ПЕРСОНАЛУ ТА ГАЛУЗЕВА КОМП'ЮТЕРНА ТЕХНОЛОГІЯ ПОБУДОВИ ЗАНЯТЬ

Анотація. Описаний процес підготовки персоналу. Розглянуто роль комп'ютерних технологій у створені тренажерних занять. Описано запропонований імітаційно – технологічного методу підготовку персоналу. Проведено порівняння ручного методу вводу параметрів і автоматичного методу вводу параметрів.

Abstract. The process of personnel training is described. The role of computer technologies in the development of training problems is considered. The proposed imitation-technological method of personnel training is described. A comparison of the manual method of entering parameters and the automatic method of entering parameters has been made.

Важливою задачеюгалузі електроенергетики України є забезпечення і підтримка компетентності експлуатаційного і оперативно-диспетчерського персоналу теплових і атомних станцій, мережевих підприємств. Результативне досягнення цієї мети неможливо без комп'ютерних засобів підготовки і контролю знань та навиків управління, і зокрема тренажерів, які орієнтовані на імітацію і контроль робочої діяльності персоналу.

На рис. 1 показано порядок підготовки та підтримки рівня компетентності персоналу, що включає базову освіту, навчання і тренаж навиків по управлінню об'єктом.

У галузеві підприємства персонал приходить після закінчення вищого навчального закладу (ВНЗ), де отримує базову підготовку до майбутньої спеціальності. На останніх курсах студенти можуть отримати вузьку профільну інформацію та можливість профільної практики. При прийомі на роботу новий персонал проходить вхідний контроль знань, котрий допомагає визначити професійні навички і знання майбутнього персоналу. Після вхідного контролю формується індивідуальна програма підготовки на посаду на основі посадової інструкції(ПІ) або робочої інструкції(РІ). Ця програма включає теоретичну та практичну підготовку на тренажерах для набуття персоналом навиків. Після проходження програми підготовки та вхідного контролю приймається рішення про допуск персоналу до самостійної роботи.

Для прийняття такого рішення рекомендовано здійснити також психофізіологічне тестування(ПФ) персоналу. При навчанні для перевірки знань використовуються системи дистанційного навчання. Таким чином, при підготовці нових спеціалістів і для підтримки потрібного рівня компетентності наявного персоналу значну роль відіграє тренажерна практика[1].

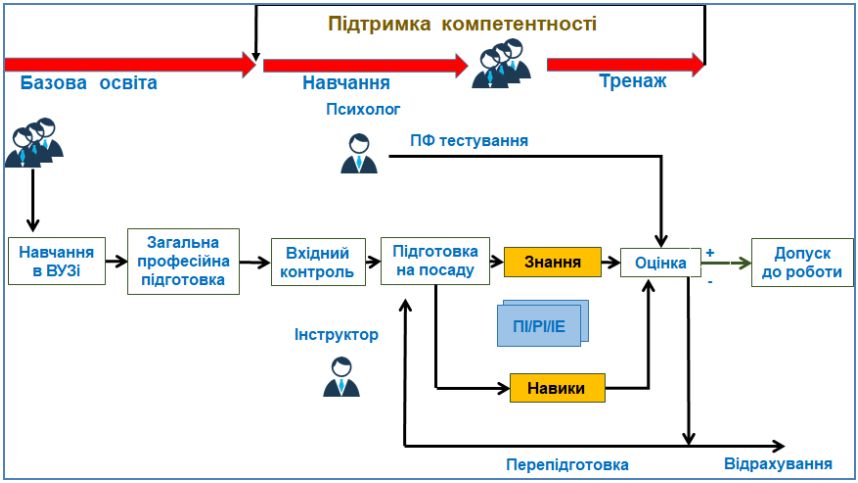


Рисунок 1 – Порядок підготовки персоналу

Тренажер – це набір тренажернихзанять(ТрЗ), котрий визначається вимогами навчального процесу до рівня компетенції персоналу.

Системи підготовки спеціалістів – це структури сценарного типу, орієнтовані на процеси взаємодії учасників один з одним і з об'єктом управління.

Тренажери бувають ситуаційними і динамічними. Ситуаційні тренажери не потребують наявності в моделі часової залежності від дій користувача. Моделі динамічних тренажерів повинні відображати залежні від часу процеси об'єкта управління.

Комп'ютерні технології для розробки програм дорого коштують та потребують значних зусиль всіх розробників для їх реалізації. Зазвичай реалізація повномасштабної моделі після її створення потребує подальшої корекції програмістами за результатами висновків технологів (досвідчених операторів, диспетчерів). Для розробки моделей використовують мови програмування, складні і дорогі спеціально розроблені або універсальні редактори, що зумовлює залучення до процесу проектування висококваліфікованих спеціалістів-програмістів. Після створення і налагодження математичної моделі об'єкта для неї створюються сценарії

тренажерних занять, навчально-педагогічне супроводження. Цю роботу на ПМТ блоків АЕС виконує інструктор[2].

Розглянемо запропонований новий підхід до розробки комп'ютерних засобів підтримки компетентності персоналу і комп'ютерної інформаційної технології розробки комп'ютерних тренажерів , орієнтованих на спеціалістів галузі. Основа запропонованого підходу — відмова від інформаційних технологій, базованих на створенні єдиної математичної моделі об'єкта, орієнтованої на всі заплановані тренажерні заняття тренажера, і подальшого налаштування до такої моделі всіх тренажерних занять. При реалізації нового підходу використовується не загальна математична модель об'єкта, а модель управління об'єктом для кожного тренажерного заняття. Цей метод названо імітаційно-технологічним.

На рис. 2 схематично показано процес створення та використання тренажерних занять тренажерів на основі імітаційно-технологічних моделей управління об'єктом. Для наочності і легкості порозуміння між усіма учасниками проекту, а також для своєчасного забезпечення в подальшому функціонування та підтримки актуального стану створеної сценарно-моделюючої сценарно-моделюючої структури(СМС)тренажерного заняття бажана наявність графічної специфікації усіх складових розробки (робочих процесів діяльності при управлінні, сценарно-моделюючої структури тренажерного заняття, моделі оцінювання, моделі інструктора та інших). Для кожного тренажерного заняття проектується локальна модель або набір моделей відображення діяльності з управління об'єктом в ситуаціях, що визначаються сценарієм тренажерного завдання, котрий включає також навчально-педагогічне супроводження процесу підготовки.

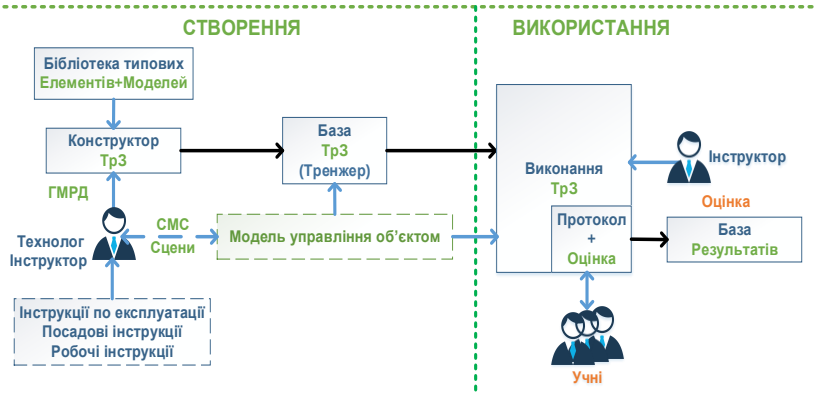


Рисунок 2 – Структурна схема імітаційно-технологічного методу

Імітаційно-технологічний метод засновано на використанні моделі управління об'єктом та експлуатаційних інструкцій(ІЕ) по управлінню. Розробниками тренажерних занять є галузеві спеціалісти. На відміну від об'єктно-математичного методу імітаційно-технологічний не потребує знань в області математики та програмування, менш складний, тому що базується на застосуванні доступних стандартних пакетів як редакторів. Імітаційно-технологічний метод орієнтований на дистанційне використання і може працювати на стандартних офісних комп'ютерах з забезпеченням комфортного часу відгуку моделей тренажерних завдань. Оцінка може формуватися автоматично за допомогою сценарно-імітаційних моделей. У випадку відсутності деяких учнів в групових тренуваннях у цьому методі передбачено сценарну імітацію діяльності відсутніх учнів[3].

На даний час для відносно нечисленного оперативно-диспетчерського персоналу блочних щитів управління атомна електростанція (АЕС) або теплова електростанція(ТЕС) створені та використовуються такі тренажери, не зважаючи на високу ціну розробки. Але їх немає (або дуже мало) для професій рівня диспетчерського і експлуатаційного персоналу розподільчих мереж, ремонтного та допоміжного персоналу розподільчих мереж, ремонтного і експлуатаційного персоналу ТЕС та АЕС.

Для складання набору тренажерних занять необхідно вивчити галузеві регламентуючі документи по організації навчального процесу, які використовуються на підприємстві. Формування набору тренажерних занять проводиться спільно технологами, інструкторами, педагогами. Для кожного тренажерного заняття на основі регламентуючих документів (інструкцій по експлуатації, бланків перемикань, описів діяльності при аваріях, планових ремонтах та ін.) визначаються початкові умови тренування, мета та кінцева ціль тренажерного заняття.

Існуючі технології побудови тренажерів оперативних перемикань припускають виконання розробки мнемосхеми у вигляді малюнка як складової робочого місця диспетчера і окремо підготовку даних для налаштування моделі об'єкта управління. Доцільно поєднати ці два процеси. Розглянуто варіант ручного налаштування введення даних такої моделі в процесі побудови мнемосхеми з бібліотечних компонентів.

Одним з етапів при побудові моделі мнемосхеми є введення розробником структурних параметрів (індекси гілок, трансформаторів, вимикачів, роз'єднувачів, елементів виводу напруг та струмів). Номери вузлів і індекси компонентів заносяться у налаштовану мнемосхему. У ручному варіанті введення данихкожен структурний параметр записується непрограмуючим спеціалістом і під час їх заповнення можна допустити помилку. Помилка під час заповнення структурних параметрів призводить до того що модель не працює. Так як зазвичай моделі мнемосхем мають велику кількість активних компонентів, виникає проблема знаходження екземпляру з невірно записаним структурним параметром. Тому необхідно розробити метод підготовки даних, котрий нівелює фактор людської помилки. Таким

методом є автоматична підготовка даних. У автоматичній підготовці даних структурні параметри вводяться не непрограмуючим спеціалістом, а за допомогою програмного коду, відповідно помилок з заповненням структурних параметрів не виникає.

Запропоновані технології дозволять підвищити ефективність процесу проектування тренажерів, скоротити час проектування і зможуть забезпечити широке впровадження тренажерів на енергетичних підприємствах за допомогою Інтернет-ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамович Р.П., Самойлов В.Д., Лєпатьєв А.О. Комп'ютерні технології розробкитренажерних систем для енергетичної галузі. "Електронне моделювання" Том 42, № 3 (2020 рр.) 89- 97
2. Р.П. Абрамович, А.О. Бальва, В.Д. Самойлов. Інтегрована технологія проектування комп'ютерних засобів сценарного типу підготовки фахівців для енергопідприємств. Журнал Електронне моделювання. 2018. Т. 40. №2
3. А.О. Бальва, ,Р.П. Абрамович, В.Д. Самойлов. До вибору графічної специфікації діяльності персоналу енергопідприємств.

Мохор Володимир Володимирович,
ІПМЕ ім. Г.Є. Пухова НАН України,
член-кореспондент НАН України, доктор технічних наук, професор,
v.mokhor@gmail.com

Міснік Олексій Ігоревич,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
alexmisnik91@gmail.com

ДОСВІД УЧАСТІ ІНСТИТУТУ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г. Є. ПУХОВА НАН УКРАЇНИ В КІБЕРНАВЧАННЯХ

Анотація. Досліджено актуальність проведення кібернавчань фахівців з безпеки об'єктів критичної енергетичної інфраструктури. Як тенденцію виокремлено створеннягалузевого центру кібербезпеки паливно-енергетичного комплексу. Акцентовано увагу на отриманні практичного досвіду участі команди Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України в кібернавчаннях.

Abstract. The relevance of cybersecurity training for security specialists of critical energy infrastructure has been studied. The government has plan for create cybersecurity center of the energy complex. Emphasis is placed on gaining practical team experience participation for G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine.

Відповідно до Стратегії енергетичної безпекиоднією з основних її загроз є кібератаки. Насамперед це обумовлено такими їх негативними проявами як BlackEnergy, NotPetya. Запобігання даним кібератакам досягається забезпеченням кібербезпеки об'єктів критичної інфраструктури, зокрема, й сфери енергетики. Водночас це підтверджується тенденцією створення галузевого центру кібербезпеки паливно-енергетичного комплексу. Тоді як дієвість таких заходів досягається завдяки кібернавчанням [1, 2].

Характерною особливістю кібернавчань забезпеченню безпеки об'єктів критичної енергетичної інфраструктури є формулювання легенди. За нею організація енергетичної сфери володіє, керує активами виробництва, передавання та розподілення електроенергії. У своїй діяльності вона дотримується стандартів забезпечення безпеки, обмінюється інформацією з партнерами, надає енергетичні послуги зацікавленим сторонам. Однак, це супроводжується негативними проявами кібератак, що можуть призводити до настання ризиків як функціональної, так й інформаційної безпеки. Тому виникає потреба в гарантуванні зацікавленим сторонам безпечності діяльності та надання послуг об'єктами критичної енергетичної інфраструктури. Це досягається

підвищенням обізнаності як працівників, так і фахівців з безпекишляхом їх кібернавчання [3, 4]. Насамперед вони об'єднуються у відповідні фахово орієнтовані команди зі забезпечення безпеки діяльності об'єктів критичної енергетичної інфраструктури. Така фахово орієнтована команда створена й в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України.

Кібернавчання команд фахівців з безпеки здійснюється на основі отримання легенди. При цьому її формулюваннявизначається різновидом завдань, наприклад: дослідження архітектури мережі, реалізування віддаленого доступу, аналізування журналів подій, можливих скомпрометованих хостів і, як наслідок, прагнення впливати на надання енергетичних послуг. Крім того, можливе тестування способів реалізування загроз безпеціоб'єктів критичної енергетичної інфраструктури, дослідження дій зловмисників в операційному середовищі.

Так, протягом грудня команда Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України залучалася до проведення кібернавчань Grid NetWars [3] та «Використання засобів OSINT та OT для забезпечення кібербезпеки та протидії дезінформації» [4]. У межах обохзаходіввирішувалися завдання забезпечення безпеки об'єктів критичноїенергетичної інфраструктури. Для цього створювалися екстремальні умови за аналогією з реальними ситуаціями здійснення кібератак. Насамперед дані кібернавчання орієнтовані на отримання практичних умінь і навиків оброблення інцидентів як інформаційної безпеки, так і кібербезпеки зокрема. До того ж окремою метою кібернавчання є підвищення згуртованості, взаємодії між членами команд фахівців з безпеки, а також командами з різних організацій-об'єктів критичної енергетичної інфраструктури. Завдяки участі в таких заходах команда Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України накопичує практичний досвід оброблення інцидентів забезпечення інформаційної безпеки та кібербезпеки зокрема. Наприклад [4], за результатами кібернавчаньу форматі змагань CTF здобуто перше місце.

Отже, діяльність команди фахівців з безпеки в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України є одним з перспективних напрямів. Тоді як підвищення практичного досвіду її учасників досягається за результатами участі в кібернавчаннях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В Україні планують створити центр захисту енергетичної інфраструктури від кібератак. URL: https://www.ukrinform.ua/rubric-economy/3338873-v-ukraini-planuut-stvoriti-centr-zahistu-energeticnoi-infrastrukturi-vid-kiberatak.html (accessed on: 10.12.2021).

2. Mokhor V., Tsurkan V., Pokrovska V. Analysis of Cyber Exercises Approaches. *Information Technologies and Security* : selected papers of the XX international scientific and practical conference (Kyiv, 01 December 2020). Vol. 2859. Aachen, Germany : CEUR Workshop Proceedings, 2021. P. 61-70. URL:

http://ceur-ws.org/Vol-2859/paper6.pdf. E-ISSN 1613-0073.(accessed on:10.12.2021).

3. Кібернавчання «National Cybersecurity Preparedness: Grid NetWars». URL:https://www.rnbo.gov.ua/ua/Diialnist/5170.html. (дата звернення: 10.12.2021).

4. Онлайн-тренінг «Використання засобів OSINT та ОТ для забезпечення кібербезпеки та протидії дезінформації». URL: https://www.rnbo.gov.ua/ua/Diialnist/5188.html.(дата звернення: 10.12.2021).

Потенко Євген Сергійович,
Проектна організація UDEC,
студент
potenko94@gmail.com

СИСТЕМА КОНТРОЛЮ ЯКОСТІ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ НА ФАБРИЦІ ОГРУДКУВАННЯ

Анотація. Розглянуто проблеми якості електричної енергії на металургійному підприємстві. Запропоновано централізовану систему контролю та управління на промисловому підприємстві.

Abstract. Problems of quality of electric energy at the metallurgical enterprise are considered. A centralized system of control and management at an industrial enterprise is proposed.

Актуальність

На промислових підприємствах зниження напруги порушує нормальну роботу електроприймачів. Знижується частота обертання електродвигунів, що призводить до зниження продуктивності робочих машин, зменшується продуктивність електричних печей, погіршується якість зварювання, знижується світловий потік ламп, зменшується пропускна здатність заводських електричних мереж, а як наслідок - погіршується якість продукції[1].

На фабриціогрудування в м. Кривий Ріг основним навантаженням є вентиляційні установки станції обжигу, що керуються через частотні перетворювачі. Таке обладнання генерує в електричну мережу реактивну потужність та спотворює криву синусоїди напруги.

Асинхронні двигуни навантажуюсь електромережу реактивної потужністю(РП), що призводить до перегріву струмопровідних частин в електроустановках та їх передчасного зносу. Компенсувавши надлишок РП у вузлах мереж можна досягти підвищення ефективності роботи електричних мереж та об'єднаної енергосистеми України в цілому.

Постановка задачі

Для підвищенняякостіелектричноїенергіїнеобхідно створити структуру електричної мережі, параметри якої будуть коригуватись системою контролю та управління згідно діючих норм [2,3]. Для цього на підприємстві створена автоматизована система управляння технологічним процесом (АСУ ТП) на базі транформаторної підстанції ГПП-4 в яку необхідно інтегрувати ряд підсистем нижчого рівня, що будуть моніторити та контролювати параметри електричної мережі.

Вирішення задачі

Для створення системи контролю та управління у вузлах електричної мережі (ЕМ), що заштриховані зеленим кольором змонтовані регулятори реактивної потужності на напрузі 0.4 кВ. Вони передають інформацію про

стан електромережі в диспетчерський пункт ДПУ та в ручному або автоматичному режимі по заданому алгоритму вмикають секції конденсаторних батарей. Підключення можливо по провідному інтерфейсу RS-485, по бездротовому інтерфейсу через модеми GSM, що дозволить об'єднати в єдину централізовану систему на базі microSCADA.При цьому оператору доступні всі функції місцевого управління.

Рисунок 1 – Частина генерального плану фабрики огрудкування в м. Кривий Ріг

АСУ ТП ПС 150/6 кВ ГПП-4 має багаторівневу структуру.

Нижній рівень:

– мікропроцесорні пристрої релейного захисту і автоматики та системи керування схемами підстанції;

– вимірювальні регулятори (вимірювання наступних параметрів: напруга, струм, частота, активна та реактивна потужність);

– сигнальні контакти та виконавчі механізми.

Середній рівень:

– сервер збору даних та керування ПС 150/6 кВ;

– комунікаційне обладнання.

Верхній рівень:

– основний та резервний сервери АСУ ТП ГПП-4»;

- АРМ Диспетчера.

АСУ ТП ГПП-4 виконує наступні функції:

– Середній рівень

1 Опрацювання інформації від нижнього рівня;

2 Видача команд на нижній рівень;

3 Передача інформації на верхній рівень.

4 Збір інформації з суміжних систем (РАП, АСКОЕ та інше).

5 Отримання команд керування та передача інформації на головну диспетчерську ЦСП ГД.

– Верхній рівень

1 Опрацювання інформації від середнього рівня.

2 Забезпечення інформаційної безпеки.

3 Зберігання інформації.

4 Забезпечення відображення технологічної інформації.

Для відображення інформації та керування передбачений АРМ Диспетчера АСУ.

АСУ ТП підстанції має модульну структуру і є відкритою системою, що має спроможність розширення при збільшенні кількості приєднань та підключення нових об'єктів керування.

Розрахунок економічної доцільності компенсації реактивної потужності.

Доцільність впровадження засобів компенсації реактивної потужності можна розрахувати за формулою (1).

$$П = (WQp + K * WQg) * D * T \quad (1)$$

де П - основна плата за споживання і генерацію реактивної потужності;

WQp - спожита реактивна потужності за розрахунковий період, кВАр*годину;

К - к-т 3;

WQg - згенерована реактивна потужність;

D - Економічний еквівалент реактивної потужності;

Т- тариф, грн./кВт*година.

Сумарна потужність конденсаторних установок на підприємстві 1.4 МВАр. При тарифі в 2 грн/кВт*годину (значення тарифу округлено для спрощення розрахунку) економічний ефект від компенсації реактивної потужності становитиме 547 тис. грн в рік.

Висновки

Для вирішення проблем якості електричної енергії на металургійному підприємстві, запропонована багаторівнева система контролю та управління з застосуванням мікропроцесорної техніки та програмного забезпечення.Пакет програмногозабезпечення має бути універсальним та враховувати перспективу інтеграції нових, сучасних пристроїв в централізовану систему управління технологічного процесу підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ю. С. Железко. Компенсацияреактивноймощности в сложных электрических системах – М.: Энергоиздат, 1981. – 200 с

2. Закон України про енергозбереження № 74 / 94 – ВР : Редакція від 23.07.2017. // Верховна Рада України. – 1994р., ст.283.

3. Характеристики напруги електропостачання в електричних мережах загальної призначеності:ДСТУ EN 50160:2014.

Супруненко Оксана Олександрівна,
Черкаський національний університет ім. Б. Хмельницького,
доцент,
ra-oks@i.ua

Аль-Савах Маяда Мохаммедівна,
Черкаський національний університет ім. Б. Хмельницького,
магістрантка

МОДЕЛЮВАННЯ ТА АНАЛІЗ ДИНАМІЧНИХ ВЛАСТИВОСТЕЙ ПРОГРАМНИХ СЕРВІСІВ ТА ЇХ КОМПОНЕНТІВ

Анотація. У роботі описано експериментальне застосування комбінованого підходу до моделювання програмних систем з паралелізмом. Він застосований до побудови та вивчення динамічних властивостей програмного сервісу, який складається з двох компонент. Показано, що якщо моделі компонент відлагоджені, то при їх лінійному компонуванні у збірну модель відлагоджені динамічні властивості зберігаються.

Abstract. The paper describes the experimental application of a combined approach to modelling software systems with parallelism. It is used to build and study the dynamic properties of a software service that consists of two components. It is shown that if the component models are debugged, then when they are linearly assembled into a prefabricated model, the debugged dynamic properties are preserved.

При проектуванні та розробці програмних систем розробники часто працюють над реалізацією функціоналу, який утворює паралельні та конкуруючі процеси. Ці процеси при функціонування програмного засобу можуть приводити до непередбачуваної поведінки системи, але вони проявляються рідко, тобто переважно є прихованими. Тому виявити вади у поведінці програмного засобу лише тестуванням не вдається [1]. Для забезпечення передбачуваного функціонування програмних засобів пропонується проведення глибокого аналізу динамічних властивостей програмних засобів, для якого розроблено багато підходів та методів, які основуються на аналітичних та графоаналітичних інструментальних засобах, наприклад, таких, як числення взаємодіючих систем, π-числення [2], алгебра процесів [1-2], теорія мереж Петрі (PN) [3]. Кожен з інструментальних засобів має свою сферу застосування, яка залежить від предметної області та особливостей формування моделі.

Для побудови та аналізу моделі програмної системи важливо дотримуватись принципів структурної подібності, структурної безконфліктності, послідовної редукції часткових моделей [4], які найповніше забезпечуються засобами теорії мереж Петрі [5]. Тому у даній роботі застосований комбінований підхід до моделювання програмних

систем з паралелізмом [4], в якому будуються імітаційні моделі з використанням графових засобів PN, які також дозволяють однозначно аналітично описати модель для проведення дослідження її динамічних властивостей [6].

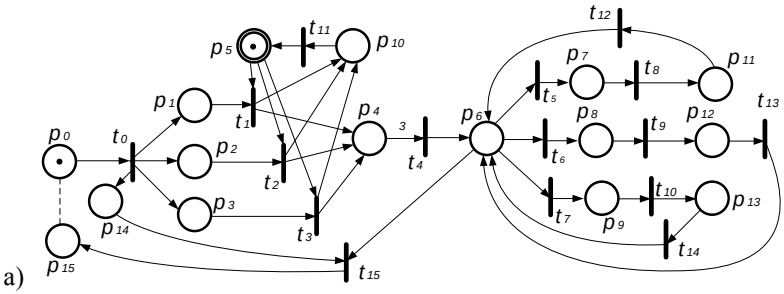
Аналіз моделей програмного забезпечення може проводитись при проектуванні програмних засобів, а також при перевірці властивостей вже розроблених програмних додатків. Проілюструємо застосування комбінованого підходу до моделювання систем з паралелізмом [4] для аналізу моделі програмного сервісу, який складається з кількох компонентів.

Для проведення аналізу побудована модель мобільного сервісу MMg, який призначений для перегляду зупинок міського транспорту, найближчих до місця перебування користувача та надання інформації про рух маршруток в околі цих зупинок. У сервісі визначаються три найближчі зупинку в околі 700 метрів, якщо такі не знаходяться, окіл пошуку розширюють до 1 та до 3 км. У моделі MMg (рис. 1, а) відображений пошук трьох найближчих зупинок міського транспорту від місця перебування користувача (у гілках від вершин p_1, p_2, p_3), запис їх характеристик (t_{11}), а також надання інформації про рух маршруток в околі визначених зупинок (t_4) для подальшого відображення на карті маршруток певного маршруту (у гілках від вершин p_7, або від p_8, або від p_9) для кожної вибраної користувачем зупинки.

Для моделі MMg-1 розраховані T- та P-інваріанти, елементи яких повністю покриті ненульовими значеннями:

$$T_1 = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 3 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]^T,$$
$$T_2 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2]^T$$

$$P_1 = [108 \quad 36 \quad 36 \quad 36 \quad 36 \quad 0 \quad 0 \quad 108 \quad 54 \quad 54 \quad 0 \quad 54 \quad 54 \quad 0 \quad 54]$$
$$P_2 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0].$$
$$P_3 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0]$$
$$P_4 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0]$$



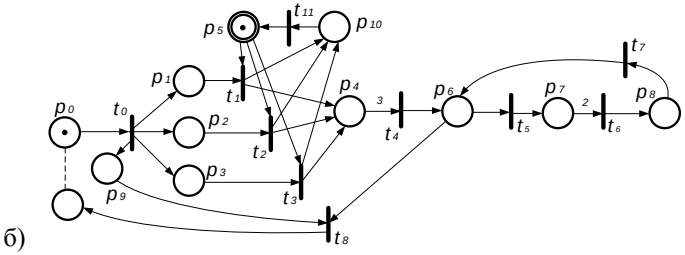


Рисунок 1 – Модель MMg сервісу «МараMagic»:
а) початкова модель, б) скорегована модель MMg*

При розрахунку інваріантів моделі MMg отримані наступні результати:

$$T_1 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0]^T$$
$$T_2 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0]^T$$
$$T_3 = [3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 9\ \ 0\ \ 0\ \ 3\ \ 0]^T$$
$$T_4 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1]^T$$

$$P_1 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0]$$
$$P_2 = [1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0]$$
$$P_3 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1]$$
$$P_4 = [3\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0\ \ 3\ \ 3\ \ 3\ \ 3\ \ 0\ \ 3\ \ 3\ \ 3\ \ 0\ \ 0]$$

Аналіз T- та P-інваріантів показав, що всі їх елементи покриті ненульовими значеннями, що підтверджує дотримання властивостей живості, повторюваності, обмеженості та збережуваності [6].

Ранг матриці інцидентності:

$$rang(W_{MMg}) = 13 < \min(|T_{MMg}|, |P_{MMg}|) = 16,$$

що говорить про неповну керованість моделі MMg. Такий результат пояснюється наявністю у моделі трьох замкнутих гілок від вершини переходу p_6, не всі з цих гілок можуть не використовуватись під час певної сесії роботи з додатком. Наприклад, коли користувач переглянув інформацію про найближчі зупинки і вийшов з додатку. Також в будь-якій з цих гілок мітка може нескінченне число разів проходити за замкнутою послідовністю вершин, наприклад, $t_5 - p_7 - t_8 - p_{11} - t_{12} - p_6$, якщо користувач вибирає перегляд одного і того ж маршруту багаторазово. Оскільки замкнуті гілки однакові за структурою і можуть використовуватись лише почергово, то доцільно відобразити їх однією гілкою (рис. 1, б).

У вершині місця p_7 (рис. 1, б), яка відображає рух маршруток в околі зупинки побудована конкретизуюча субмодель Mt на основі патерну 39 «Критичний розділ» [7], яким описано почергову передачу на карту координат маршруток для відображення. Субмодель Mt для двох маршруток представлена на рис. 2. При її аналізі визначено, що елементи Т- та Р-інваріантів повністю покриті ненульовими значеннями:

$$T_1 = [2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2]^T, \qquad \begin{matrix} P_1 = [2 & 1 & 1 & 0 & 1 & 1 & 1 & 0] \\ P_2 = [0 & 0 & 0 & 1 & 1 & 1 & 0 & 0] \\ P_3 = [0 & 1 & 1 & 0 & 1 & 1 & 0 & 1] \end{matrix}.$$

Для субмоделі Mt ранг матриці інцидентності $rang(W_{Mt}) = 6$, що відповідає мінімальному значенню потужності однієї з множин вершин (множини вершин переходів): $\min(|T_{Mt}|, |P_{Mt}|) = 6$. Таким чином, субмодель Mt є повністю керованою. Сформуємо гіпотезу за якою припустимо, що субмодель Mt може бути вбудована у інші моделі, наприклад, у модель MMg* (у вершину перходу p_7 з рис. 1, б), що не погіршить динамічних властивостей основної моделі.

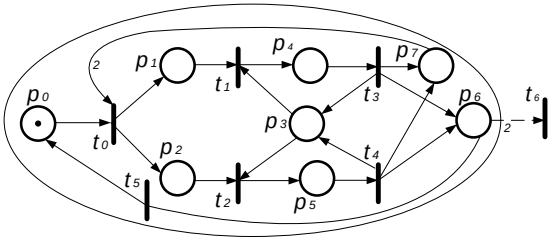


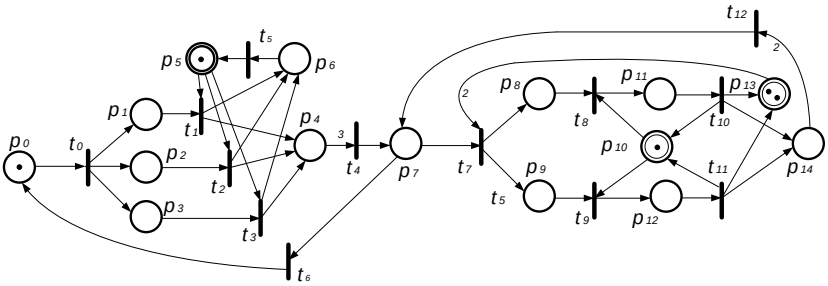
Рисунок 2 – Субмодель Mt сервісу MMg

Збірна моделі MMg-1, яка побудована шляхом доповнення моделі MMg у вершині перходу p_7 (рис. 1, б) субмоделлю Mt, відображена на рис. 3, а.

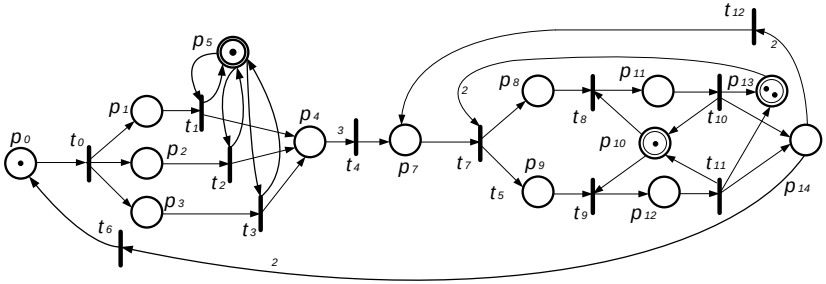
Для моделі MMg-1 розраховані T- та P-інваріанти, елементи яких повністю покриті ненульовими значеннями:

$$T_1 = [1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 3 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0]^T,$$
$$T_2 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2 \quad 2]^T$$

$$P_1 = [108 \quad 36 \quad 36 \quad 36 \quad 36 \quad 0 \quad 0 \quad 108 \quad 54 \quad 54 \quad 0 \quad 54 \quad 54 \quad 0 \quad 54]$$
$$P_2 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0].$$
$$P_3 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0]$$
$$P_4 = [0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0]$$



а)



б)

Рисунок 3 – Модель сервісу MMg: а) збірна модель MMg-1, б) скорегована модель MMg-1*

При розрахунку рангу матриці інцидентності отриманий результат, який вказує на неповну керованість моделі:

$$rang(W_{MMg-1}) = 12 < \min(|T_{MMg-1}|, |P_{MMg-1}|) = 13$$

Такий результат обумовлений наявністю у моделі замкнутої циклічної конструкції ($p_7 - t_7 - ... - p_{14} - t_{12} - p_7$), яка може використовуватись нескінченно довго, або не використовуватись взагалі у поточному сеансі роботи з додатком. Гілка $p_7 - t_6 - p_0$ є послідовною, у вершині місця p_7 відбувається вибір продовження перегляду на карті руху маршруток, чи вихід з режиму перегляду карти. Оскільки перехід на карту для перегляду маршрутів за проектом буде відбуватися відразу після отримання характеристик зупинок, ця гілка має бути замінена на гілку $p_{14} - t_6 - p_0$. При аналізі скорегованої моделі MMg-2-1* (рис. 3, б) отримані наступні результати:

$$T_1 = [3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 3\ \ 0\ \ 3]^T$$
$$T_2 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0]^T$$
$$P_1 = [6\ \ 2\ \ 2\ \ 2\ \ 2\ \ 0\ \ 6\ \ 3\ \ 3\ \ 0\ \ 3\ \ 3\ \ 0\ \ 3]$$
$$P_2 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0],$$
$$P_3 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0]$$
$$P_4 = [0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0]$$
$$rang(W_{MMg\,2-1^*}) = 12 < \min(|T_{MMg\,2-1^*}|, |P_{MMg\,2-1^*}|) = 12 \cdot$$

За даними результатами модель MMg-2-1* відповідає властивостям живості, повторюваності, обмеженості, збережуваності, а також повної керованості.

Таким чином, на розглянутому прикладі було показано, якщо у лінійну ділянку відлагодженої збірної моделі включається відлагоджена субмодель, для якої виконуються умови покриття Т- та Р-інваріантів ненульовими елементами (покриття визначається для кожної вершини моделі) та ранг матриці інцидентності *W* дорівнює мінімальній потужності множини вершин місць чи множини вершин переходів моделі, то збірна модель зберігає динамічні властивості живості, повторюваності, обмеженості, збережуваності та керованості моделей, з яких вона збирається. Тобто для побудови моделей інших систем коректно використовувати раніше видлагоджені моделі, якщо ділянки паралельних чи конкуруючих процесів не перекриваються.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Карпов Ю.Г. Model Checking. Верификация параллельных и распределённых программных систем. СПб, БХВ-Петербург, 2010. 560 с.

2. Андреев А.М., Можаров Г.П., Сюзев В.В. Многопроцессорные вычислительные системы. Теоретический анализ, математические модели и применение: учеб. пособ. для студ. вузов. М., Изд-во МГТУ им. Н.Э. Баумана, 2011. 332 с.

3. Murata T. Petri Nets: Properties, Analysis and Applications. Proceedings of the IEEE. April 1989. Vol. 77, No. 4. P. 541-574.

4. Suprunenko, O. Combined approach architecture development to simulation modeling of systems with parallelism. Eastern-European Journal of Enterprise Technologies, 2021, 4(4(112)). P. 74-82. doi: https://doi.org/10.15587/1729-4061.2021.239212.

5. Кузьмук В.В., Супруненко О.А. Средства описания информационных потоков в динамических моделях медицинских программно-аппаратных систем. Theoretical and Applied Science, 2014, 7 (15). С. 11-18. doi: http://dx.doi.org/10.15863/TAS.2014.07.15.2.

6. Супруненко О.О., Онищенко Б.О., Гребенович Ю.Є. Аналітичний підхід при дослідженні властивостей графової моделі програмної системи. Праці міжнародної науково-практичної конференції «Математичне моделювання процесів в економіці та управлінні проектами і програмами» (ММП-2020), Коблево, 14-18 вересня 2020 р. Харків, ХНУРЕ, 2020. С. 110-113.

7. Control-flow patterns. [E-resource] Available at: http://www.workflowpatterns.com/patterns/control/index.php (Accessed 09.12.21).

Станиціна Валентина Володимирівна,
Інститут загальної енергетики НАН України,
старший науковий співробітник,
st_v_v@hotmail.com

ПЕРСПЕКТИВИ ТА ПРОБЛЕМИ ВПРОВАДЖЕННЯ СОНЯЧНИХ СИСТЕМ ТЕПЛОПОСТАЧАННЯ В УКРАЇНІ

Анотація. Впровадження енергоефективних і «зелених» технологій є важливою задачею розвитку систем теплопостачання. Використання сонячних систем теплопостачання призведе до зменшення споживання органічного палива та зниження викидів забруднюючих речовин, сприятиме енергетичній незалежності держави. В роботі наведено огляд світового та українського досвіду впровадження зазначених систем, а також факторів, які впливають на їх економічну ефективність.

Abstract. The introduction of energy efficient and "green" technologies is an important task in the development of heating systems. The use of solar heating systems will reduce the consumption of fossil fuels and emissions of pollutants, will contribute to the energy independence of the state. The paper provides an overview of the world and Ukrainian experience in implementing these systems, as well as factors that affect their economic efficiency.

Сонячне теплопостачання є однією з найбільш розвинених в світі технологій перетворення сонячної енергії для опалення, гарячого водопостачання (ГВП) і охолодження будівель. На сьогодні існують різні типи систем сонячного теплопостачання [0]. Централізовані системи теплопостачання населених пунктів отримали найбільш широке поширення в Данії. Для їх створення використовуються переважно плоскі сонячні колектори (СК). При досить високій вартості сонячного тепла затребуваність геліоустановок в світі пояснюється діючими заходами державного стимулювання [0]. Більшість успішно працюючих масштабних систем сонячного опалення встановлені в Європі. Лише 1% встановлених у світі СК підключено до систем централізованого опалення [0].

На території України енергія сонячної радіації за один середньорічний світловий день складає в середньому 4 кВт·год/м^2 (в літні дні – до 6-6.5 кВт·год/м^2) тобто близько 1500 кВт·год/м^2 за рік. Це приблизно стільки ж, скільки в середній Європі, де використання сонячної енергії носить найрізноманітніший характер [0]. Термін ефективної експлуатації сонячних водонагрівачів у південних областях України − 7 місяців (з квітня по

жовтень), у північних областях – 5 місяців (з травня по вересень). На кінець 2019 р. працювало близько 400 великих сонячних теплових систем (>350 кВт·год; 500м^2), підключених до мереж централізованого теплопостачання та в житлових будинках. Загальна встановлена потужність цих систем − 1615 МВт (2,3 млн м^2). Низкою постанов держава стимулює розвиток сонячної теплоенергетики, однак статистика щодо впровадження систем сонячного теплопостачання відсутня. Так у публічному звіті Держенергоефективності (підсумки 2020 року) інформації щодо впровадження систем сонячного теплопостачання не надається. Відсутня також відповідна інформація у звітній документації щодо програми «Теплий кредит», яка була розрахована на сім років (2014−2020) [0]. Національним планом дій з відновлюваної енергетики на період до 2020 року планувалось, що загальний внесок сонячних систем у 2020 р. буде еквівалентним 200 тис. т н.е.

Використовувати СК доцільно одночасно із газовими чи електричними котловими установками. При створенні комбінованої системи теплопостачання виникають труднощі в узгодженні роботи усіх джерел енергії, а також в досягненні максимальної ефективності від джерела енергії при максимальній економії коштів. Економічно джерело енергії може бути максимально ефективним в проміжок часу, коли навантаження на систему є мінімальним [0]. Інтеграція великих площ СК в елементи будівель є окремою важливою задачею [0].

ККД сонячного колектора обумовлено не тільки його конструктивними параметрами, але і залежить від режимів, в яких він використовується [1]. Розрахунок енергетичного балансу СК і розрахункові методики для оцінки продуктивності сонячних установок представлені в [0].

Для різних регіонів та типів обладнання термін окупності складає від 6 до 15 років. У випадку поєднання сонячної системи з ТН, на останній припадає 28,9% від загальної подачі тепла із середнім коефіцієнтом перетворення 2,55, а сонячна частка становить 71,1% протягом усього опалювального сезону. Порівняно з системою опалення тепловим насосом, сонячна комбінована система може заощадити 53,6% споживання електроенергії [0]. Проте, враховуючи велику вартість обладнання, для такої системи потрібним є пікове джерело на органічному паливі, електрокотел або поєднання з централізованою системою теплопостачання.

Дослідження середньозваженої собівартості теплової енергії за життєвий цикл (LCOH), проведене для 11 систем з 5 країн Європи, показало, що LCOH від системи з СК може бути як нижче, так і вище LCOH від котлів на органічному паливі. Найбільше на вартість теплоенергії впливають

інвестиційні витрати, продуктивність сонячної установки та вартість палива, яке заміщається [0]. Подібне дослідження було проведено для Китаю [0].

Таким чином, вартість теплоенергії від системи з СК можливо визначити досить точно лише для певного проекту, врахувавши кліматичні умови, ступінь утеплення будинку, розташування СК, режими, в яких він експлуатується, та вартість енергоресурсів, які будуть заміщатися, наявність та характеристики пікового джерела. Для умов України впровадження сонячного теплопостачання перспективне в комбінованих системах, з обов'язком ретельним обрахунком проекту і вибору найбільш оптимально розташування СК з утепленням житла; більше перспектив впровадження цих систем в центральних та південних областях країни.

В подальшому планується визначити LCOH для деяких проектів з сонячними системами з метою порівняння їх з іншими перспективним для впровадження в Україні технологіями [0, 0].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Енергетика: історія, сучасність і майбутнє. Книга 5. Електроенергетика та охорона навколишнього середовища. Функціонування енергетики в сучасному світі / К. Б. Денисевич, Ю. О. Ландау, В. О. Нейман [та ін.]; наук. ред. Ю. О. Ландау, І. Я. Сігал. Київ: Б.в., 2013. [Електронний ресурс] URL: http://energetika.in.ua/ua/books/book-5/part-1/section-2/2-1/2-1-1. Дата звернення: 10.12.2021.

2. Бутузов В. А. Солнечное теплоснабжение: статистика мирового рынка и особенности российского опыта. *Теплоэнергетика.* 2018. № 10, с. 78–88. doi: 10.1134/S0040363618100016 URL: https://www.solarthermalworld.org/ sites/default/files/news/file/2019-06-14/russian_report_2018.pdf

3. Ge, T. S., Wang, R. Z., Xu, Z. Y., Pan, Q. W., Du, S., Chen, X. M., … Chen, J. F. (2018). Solar heating and cooling: Present and future development. Renewable Energy, 126, 1126–1140. doi: 10.1016/j.renene.2017.06.081

4. Опарін М. С. Особливості використання комбінованої системи теплопостачання із сонячними колекторами в багатоквартирному житловому будинку : збірник матеріалів Міжнародної науково-технічної конференції "Інноваційні технології в будівництві (2018)", 13-15 листопада 2018 р. Вінниця: ВНТУ, 2018. С. 345-346. [Електронний ресурс] URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/25804/345-346.pdf?sequence =1 Дата звернення: 10.12.2021.

5. Матях С., Суржик Т., Рєзцов В., Іванчук В. Напрями та перспективи розвитку сонячної теплоенергетики. *Відновлювана енергетика*. 2021. 3(66). С. 33-44. https://doi.org/10.36296/1819-8058.2021.3(66).33-44.

6. Разработка схемы и алгоритма управления переключения солнечных коллекторов в системе теплоснабжения С. К. Шерьязов, А. Х. Доскенов, А. С. Чигак С. 230-235. Энергетика – агропромышленному комплексу России : матер. междунар. науч.-практ. конференции (Челябинск, 2017) / под ред. проф., д-ра с.-х. наук М. Ф. Юдина. Челябинск : ФГБОУ ВО Южно-Уральский ГАУ, 2017. [Електронний ресурс] https://юургау.рф/upload/iblock/3cf/Конференция%202017%20Энергетика%20-%20АПК%20России.pdf#page=231. Дата звернення: 10.12.2021.

7. Ефремова О. А., Хворова Л. А. Математическое моделирование систем солнечного теплоснабжения. *Известия АлтГУ*. 2017. №4 (96). [Електронний ресурс] URL: https://cyberleninka.ru/article/n/matematicheskoe-modelirovanie-sistem-solnechnogo-teplosnabzheniya. Дата звернення: 10.12.2021

8. Louvet, Y., Fischer, S., Furbo, S., Giovannetti, F., Helbig, S., Köhl, M., … Vajen, K. (2019). Economic comparison of reference solar thermal systems for households in five European countries. Solar Energy, 193, 85–94. doi:10.1016/j.solener.2019.09.019

9. Zhang, R., Wang, D., Liu, Y., Chen, Y., Fan, J., Song, C., & Wang, Y. (2021). Economic optimization of auxiliary heat source for centralized solar district heating system in Tibetan Plateau, China. Energy Conversion and Management, 243, 114385. doi:10.1016/j.enconman.2021.114385

10. Станиціна В.В. Визначення середньої вартості теплової енергії за життєвий цикл теплонасосної станції на артезіанських водах. Зб. тез XXXVII науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 15 травня 2019 р. / ІПМЕ ім. Г.Є. Пухова НАН України. 2019. С. 67-68.

11. Bogoslavska O., Stanytsina V., Artemchuk V., Garmata O., Lavrinenko V. (2021) Comparative Efficiency Assessment of Using Biofuels in Heat Supply Systems by Levelized Cost of Heat into Account Environmental Taxes. In: Zaporozhets A., Artemchuk V. (eds) Systems, Decision and Control in Energy II. Studies in Systems, Decision and Control, vol 346. pp. 167-185. Springer, Cham. https://doi.org/10.1007/978-3-030-69189-9_10.

Amir Sanhinov,
G.E. Pukhov Institute for Modelling Problem in Energy Engineering of NAS of Ukraine,
student,
amir.sanhinov@gmail.com

Viktor Gurieiev,
G.E. Pukhov Institute for Modelling Problem in Energy Engineering of NAS of Ukraine,
senior researcher,doctor habilitatus,
viktor.gurieiev@ipme.com.ua

PARALLELIZATION OF MODE CALCULATION OF ELECTRICAL GRIDS FOR WEB-ORIENTED SIMULATORS

Анотація. Через аварії, атаки чи людські/машинні помилки, електроенергетичні мережі можуть увійти у різні критичні та аварійні стани, що потребують дій від диспетчерів підстанцій. Щоб підвищити ймовірність правильного рішення, здійсненого диспетчерами, потрібні аварійні тренажери та сервісні системи. Протиаварійні тренажери дозволяють диспетчерам практикуватись без унебезпечення енергосистеми, в той час, як сервісні системи допомагають прийняти рішення під час реальних аварій. Розрахунок режиму є основною частиною обох систем, та зазвичай найбільш обчислювально складною. На великих електроенергетичних системах, час розрахунку режиму може з легкістю дійти до межі, де результати тренажерних та сервісних систем стають непридатними для використання на практиці. Це створює необхідність використання кращих алгоритмів та технік оптимізації обчислень. У цій статті, розглядаються різні техніки прискорення розрахунку режиму, та зроблено фокус на техніці оптимізації, що використовує паралелізацію за допомогою графічного процесора та її ефектах на розрахунках режимів Об'єднаної Енергосистеми України на практиці.

Abstract. Due to accidents, attacks or human/computer errors, electrical grids can enter various critical and emergency states that require actions from operators of transformer substations. In order to increase the likelihood of correct decisions being made by the operators, both emergency simulators and assistant systems are needed. Emergency simulators allow operators to practice without endangering the grid, while assistant systems help them make decisions during real emergencies. Mode calculation is a core part of both simulators and assistant systems, and is usually the most computationally expensive one. With large-scale electrical grids, mode calculation time can easily reach a point where simulation and assistant systems become unusable in practice. This necessitates the use of better algorithms and optimization techniques. In this article, various techniques that speed up the mode calculation are overviewed, and focus is made on an

optimization technique that uses GPU parallelization and its effects on the mode calculation of the United Electrical Grid of Ukraine in practice.

Introduction

PORT system by Infotec Ltd. translated to C language is used as a base program[1]. A program is modified so that it includes a version of the mode calculation that works, into smaller, regional grids, and calculating the mode for each of the regional grids separately [3]. While this approach can guarantee a sufficiently small with the help Graphics Processing Unit (GPU). GNU C Compiler (GCC), version 8.5.0 [2] is used as a compiler.

Overview of existing approaches

There exists a wide variety of approaches that ensure comfortable mode calculation time.

The most widely used one in Ukraine is a division of a large-scale grid, such as the United Electrical Grid of Ukrainecalculation time given enough divisions, the accuracy of each calculation goes down.

Since this article focuses on web-oriented simulators, the next most common approach is increasing the number of computers that perform the computation. This has two problems: first, it increases the cost of such systems and their maintenance; second, in addition to information about the electrical grid, calculation data needs to be transmitted and synchronized over the network, which is larger in size and therefore the result is much slower compared to when the calculation data is kept entirely within Random Access Memory (RAM). It is worth noting that modern optic fiber cables are able to send data fast enough to compete with RAM, however the routers are unable to parse it nearly as fast and are the bottleneck of this approach.

The third approach is optimizing the algorithms used for mode calculation. Most of the mode calculation consists of representing the electrical network graph in memory as a data structure, and then solving systems of equations based on Ohm's and Kirchhoff's laws. Most graph representation algorithms as well as equation solver algorithms are well-developed at this point, and drastic developments in this area are not expected.

The fourth and final approach that is overviewed in this article is implementation optimizations of the existing algorithms in the context of the electrical grids specifically. In our previous article, *"Some aspects of optimization of electrical network modeling"*, we showed that the same algorithm, depending on the implementation, can give up to 211 times the difference in time on the United Electrical Grid of Ukraine [4]. Such a difference is explained by the fact that the algorithms are usually presented at higher levels of abstraction, where the details about the underlying physical system are lost and are not accounted for. Some aspects of optimization have been reviewed; however, others were left out due to the scope limitations. In this article, the focus is made on the GPU

parallelization approach and how it affects mode calculation of the United Electrical Grid of Ukraine in practice.

GPU parallelization approach

GPUs, as the name suggests, have been originally designed for graphics processing. They have a much larger number of less powerful cores compared to CPUs, which excel at parallelizable tasks. It is possible to utilize this strength for general-purpose computing, in this case for mode calculation. There are two ways to achieve this:

- using a graphical applied programming interface (GAPI),
- using a general purpose GPU interface (GPGPUI).

Since the PORT program is platform-independent and there is no vendor-independent GPGPUI available at the moment, we have picked a GAPI, specifically OpenGL [5].

To perform a mode calculation, we represent the electrical grid graph as a matrix, encode it and other matrices as textures and pass them to the GPU as uniforms. We can then use shaders to perform calculations on the matrices, and we can use the framebuffer for iterative methods without needing to return data back to the CPU between each iteration [6]. Since the data is passed to the GPU only once, we avoid the constant creation and deletion of processes present in CPU parallelization. The data must still be passed between RAM and Video RAM (VRAM) at least once, however.

Since VRAM is significantly smaller than RAM, this poses a potential overflow problem. This might cause frequent exchange between the RAM and VRAM, leading to performance decrease. Alternatively, it can lead to video drivers crashing, in which case the calculation must be restarted. To avoid this issue, we use compressed sparse row/column (CSR/CSC) representation [7]. This allows for the representation of the United Electrical Grid of Ukraine to be packed in under four gigabytes.

Unlike the CPU parallelization approach discussed in our previous article, which decreased performance on the non-linearized version of the program, GPU parallelization increased the performance two to eight times. The exact execution time depends on the GPU, total and available VRAM, type of VRAM, precision, overflow and other factors. Detailed data performed on various systems and its analysis will be released in future articles. The aim of this article is to demonstrate the order of magnitude of performance increase that can be expected and not to provide specific data.

Conclusions

In this article, several approaches that ensure faster mode calculation have been reviewed. GPU parallelization approach based on OpenGL has been selected, described, implemented in PORT and tested on the United Electrical Grid of

Ukraine. Unlike the CPU parallelization approach reviewed in the predecessor article, it has provided a performance increase of two to eight times.

REFERENCES

1. Gurieiev V.A., Sanhinova O.V. Distributed environment for mode modeling in fully functional mode simulator (PORT) for Ukrainian Energy Systems / Technical Electrodynamics – 2016, - № 5, - p. 67-69.
2. https://gcc.gnu.org
3. Gurieiev V.A., Sanhinova O.V. Distributed environment for mode modeling in fully functional mode simulator (PORT) for Ukrainian Energy Systems / Technical Electrodynamics – 2016, - № 5, - p. 67-69.
4. Sanhinov A., Gurieiev V. Some aspects of optimization of electrical network modeling / International science application conference “Informational Technologies and Security” - 2021
5. https://www.opengl.org
6. https://www.khronos.org/registry/OpenGL/index_gl.php
7. Buluç, Aydın; Fineman, Jeremy T.; Frigo, Matteo; Gilbert, John R.; Leiserson, Charles E. (2009). *Parallel sparse matrix-vector and matrix-transpose-vector multiplication using compressed sparse blocks*(PDF). ACM Symp. on Parallelism in Algorithms and Architectures. CiteSeerX 10.1.1.211.5256.

Цуркан Василь Васильович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старш. наук.співроб.,
v.v.tsurkan@gmail.com

Антонішин Михайло Васильович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
antonishin.mihail@gmail.com

ПРЕДСТАВЛЕННЯ МНОЖИНИ СЦЕНАРІЇВ ТЕСТУВАННЯ УРАЗЛИВОСТЕЙ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ ДІАГРАМАМИ ЕЙЛЕРА-ВЕННА

Анотація. Досліджено процес формування множини сценаріїв тестування уразливостей мобільних програмних застосунків. Серед них виокремлено узагальнені сценарії. Крім того, для операційних системи Android та iOS. Їх відображено як елементи множини сценаріїв тестування уразливостей мобільних програмних застосунків. Відношення між ними представлено використанням діаграм Ейлера-Вена.

Abstract. The process of forming a set of scenarios for testing vulnerabilities of mobile software applications has been studied. Among them, generalized scenarios are singled out. Also, for Android and iOS. They are displayed as elements of a set of vulnerability testing scenarios for mobile software applications. The relationship between them is represented using Euler-Venn diagrams.

Сценарії тестування уразливостей мобільних програмних застосунків визначаються настановами OWASP Mobile securitytestingguide (MSTG). Їх використання дозволяє встановити рівень збереженості насамперед конфіденційності, цілісності та доступності інформації. Однак, реалізування даного підходу на практиці ускладнюється довільністю обирання сценаріїв тестування уразливостей мобільних програмних застосунків. Подолання даного обмеження досягається формалізуванням їх сукупності відповідною множиною [1, 2].

Множинасценаріїв тестування уразливостей мобільних програмних застосунківформується шляхом задання критерія належності елементів. Його вибір залежить від завдання тестування; архітектури, операційної системи, технології розроблення мобільного програмного застосунку, рівня, наявності інструментарію тестування. З огляду на це, належність сценарію тестування уразливостей мобільних програмних застосунків визначається за різновидом операційної системи. Тоді з урахуванням настанов методології OWASP MSTG виокремлюються такі множини (рис. 1) [1]:

U – універсальна множина сценаріїв тестування уразливостей мобільних програмних застосунків, $TG \subset U$, $TG \cap U = TG$

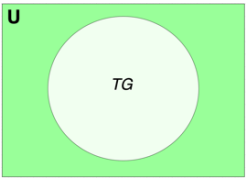
$$TG = TG^{General} \cup TG^{Android} \cup TG^{iOS};$$

$TG^{General}$ –множина узагальнених сценаріїв тестування уразливостей мобільних програмних застосунків незалежно від різновиду операційної системи;

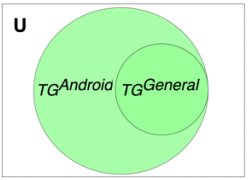
$TG^{Android}$ – множина сценаріїв тестування уразливостей мобільних програмних застосунків під керуванням операційної системи Android;

TG^{iOS} – множина сценаріїв тестування уразливостей мобільних програмних застосунків під керуванням операційної системи iOS.

TG

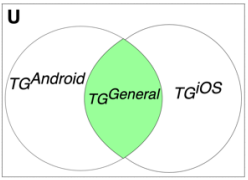


$\overline{TG}$

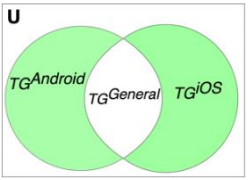


$TG^{Android} = TG^{General} \cup TG^{Android}$

$TG^{iOS} = TG^{General} \cup TG^{iOS}$



$TG^{General} = TG^{Android} \cap TG^{iOS}$



$TG^{Android} \Delta TG^{iOS}$

Рисунок 1 –Діаграми Ейлера-Венна множини сценаріївтестування уразливостей мобільних програмнихзастосунків

Отже, представлення множини сценаріїв тестування уразливостей мобільних програмних застосунків діаграмами Ейлера-Венна дозволяєнаочно відобразити вірогідні відношення між її елементами. Таке формалізування

орієнтоване на запобігання довільності використання настанов OWASP MSTG і, як наслідок, забезпечення відтворюваності отриманих при цьому результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Antonishyn M., Misnik O.Analysis of testingapproachesto Android mobile application vulnerabilities. Information Technologies and Security : selected papers of the XIX international scientific and practical conference (Kyiv, 28 November 2019). Vol. 2577. Aachen, Germany : CEUR Workshop Proceedings, 2019. P. 270-280. URL: http://ceur-ws.org/Vol-2577/paper22.pdf. E-ISSN 1613-0073.(accessedon:14.12.2021).

2. OWASP Mobile security testingguide (MSTG). URL:https://github.com/ OWASP/owasp-mstg/. (accessedon: 14.12.2021).

Яковенко Володимир Миколайович,
ДУ «ІТПМ НАН України»,
м.н.с.,
volodimir@outlook.com

Сокол Олександр Васильович,
ДУ «ІТПМ НАН України»,
пров. інж.,
office.ntcmto@nas.gov.ua

Івлєва Любов Федорівна,
ДУ «ІТПМ НАН України»,
інж. ІІ кат.,
office.ntcmto@nas.gov.ua

Петров Сергій Васильович,
ДУ «ІТПМ НАН України»,
заст. д-ра.,
petrov.s.v@nas.gov.ua

ДОСЛІДЖЕННЯ КРИВОЇ НАМАГНІЧУВАННЯ КІЛЬЦЕПОДІБНИХ ФЕРОМАГНІТНИХ ОСЕРДЬ

Анотація. Обґрунтовано необхідність аналітичного опису залежності магнітної проникності μ_r від напруженості H зовнішнього магнітного поля для матеріалу кільцеподібних феромагнітних осердь, які можуть бути використані в засобах екранування магнітного поля кабельних ліній високої напруги. Проведено експериментальне дослідження магнітних властивостей такого феромагнітного осердя. Для обробки результатів вимірювань використано підхід, що враховує неоднорідність магнітного поля в досліджуваному осерді. Отримано низку співвідношень для аналітичного представлення залежності $\mu_r(H)$, придатних для подальших досліджень з визначення ефективності засобів екранування магнітного поля.

Abstract.This paper deals with the magnetic properties of ferromagnetic cores, which can be used in the facilities of shielding of the high voltage cable line magnetic field. We discuss the necessity of the analytical description of the dependence of the magnetic permeability μ_r on the external magnetic field strength H for annular ferromagnetic cores. To determine this dependence, we carry out the experimental research of magnetic properties of the ferromagnetic core. An approach used to process the measurement results takes into account the heterogeneity of the magnetic field in the core under study. As the result, we develop the relations for the analytical representation of the dependence $\mu_r(H)$, that are suitable for further research of the efficiency of the facilities of the magnetic field shielding.

В [1] і [2] розглянуто два способи зменшення магнітного поля трифазної кабельної лінії електропередавання високої напруги. Перший передбачає використання власних екранів кабелів, з'єднаних на кінцях лінії. Другий спосіб полягає у використанні додаткового контурного екрану. Спільною рисою обох підходів є використання допоміжних кільцеподібних (трубчастих) феромагнітних осердь, які охоплюють кабелі. Це дає змогу збільшити взаємоіндуктивність жил кабелів та екранів (власних чи додаткового) та, відповідно, підвищити ефективність екранування магнітного поля. В [1] і [2] представлено вирази, за допомогою яких можна виявити залежність ефективності екранування від параметрів кабельної лінії та довжини осердь. Водночас, у них не враховується нелінійність магнітних характеристик феромагнітних осердь. Тому подальша розробка виразів для ефективності екранування потребує аналітичного опису залежності магнітної проникності матеріалу осердь від напруженості зовнішнього магнітного поля. Вирішенню останньої задачі присвячено цю статтю.

При розв'язанні задачі було вирішено знехтувати явищем гістерезису матеріалу осердя та вважати, що магнітна індукція функціонально залежить від напруженості магнітного поля відповідно до основної кривої намагнічування. Тому метою є аналітичний опис магнітної проникності, який узгоджується з основною кривою намагнічування матеріалу феромагнітного кільцеподібного осердя.

Для проведення експериментального дослідження основної кривої намагнічування матеріалу осердя було побудовано вимірювальний стенд, схема якого наведена на рис. 1. На схемі прийняті такі позначення: W1 – намотана на осердя котушка, яка створює поле намагнічування; W2 – намотана на осердя вимірювальна котушка; E – джерело живлення; SA1, SA2 – перемикачі; R1, R2 – реостати; Wb – мілівеберметр; A – амперметр. Вимірювання були проведені на основі стандартів [3]-[4] з урахуванням довідкової літератури [5]. Зазначимо, що окремі вимоги щодо проведення експерименту не були виконані через недостатнє дотримання правильності геометричної форми зразка (феромагнітного осердя).

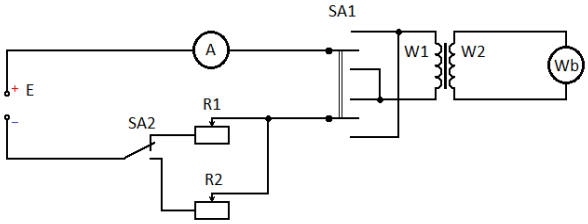


Рисунок 1 – Схема вимірювального стенду

Крива намагнічування отримувалась послідовно, точка за точкою. Котушкою W1 створювалось в осерді магнітне поле, напруженість якого обчислювалась за формулою $H_A = \frac{I \cdot w_1}{\pi\left(r_{зовн} + r_{вн}\right)}$, де I – струм, виміряний амперметром A, w_1 – кількість витків котушки W1, $r_{зовн}$, $r_{вн}$ – зовнішній і внутрішній радіуси феромагнітного осердя. Перемикачем SA1 напрям струму в котушці W1 і поля H в осерді змінювався на протилежний. Відповідна зміна магнітного потокозчеплення Ψ, пов'язана з котушкою W2, вимірювалась мілівеберметром Wb. Виміряне значення використовувалось для розрахунку магнітної індукції $B_{Wb} = \frac{\Psi}{2 \cdot S \cdot w_2}$, де w_2 – кількість витків котушки W2, S – площа поперечного перерізу осердя. Отримавши пару значень H_A і B_{Wb}, переходили до наступної точки на кривій намагнічування, для чого збільшували струм I за допомогою реостата R1 або R2. Зазначимо, що наведені вирази для H_A і B_{Wb} є наближеними, оскільки отримані за припущення про однорідність магнітного поля в осерді.

Щоб при отриманні аналітичного виразу для магнітної проникності взяти до уваги неоднорідність магнітного поля всередині досліджуваного осердя, в представленій роботі для аналізу результатів вимірювань використовується підхід, запропонований в [6]. Вводимо апроксимацію основної кривої намагнічування як певну функцію $B = f\left(\frac{Iw_1}{2\pi r}\right)$. Ця функція містить деякі числові коефіцієнти, значення яких треба визначити при апроксимації експериментальних даних. Інтегруючи функцію f по площі поперечного перетину кільцеподібного осердя й ділячи отриманий результат на величину цієї площі, маємо

$$B_{Wb} = \frac{\int_{r_{вн}}^{r_{зовн}} f\left(\frac{Iw_1}{2\pi r}\right) dr}{r_{зовн} - r_{вн}} = \frac{F\left(Iw_1, r_{зовн}\right) - F\left(Iw_1, r_{вн}\right)}{r_{зовн} - r_{вн}},$$

де на функцію F накладено вимогу $\frac{\partial F\left(Iw_1, r\right)}{\partial r} = f\left(\frac{Iw_1}{2\pi r}\right)$.

Отримане співвідношення встановлює зв'язок між значеннями B_{Wb} та ампер-витками Iw_1 котушки W1. Апроксимуючи ним експериментальні дані, отримуємо значення коефіцієнтів функцій F і f.

Доцільно визначити вигляд функції F, після чого шляхом диференціювання отримати f. Це дозволить уникнути інтегрування порівняно із традиційним підходом, коли на початку визначається вигляд функції f.

Розглянемо такий вигляд функції F:

$$F\left(Iw_1, r\right) = \mu_0 \cdot F_0\left(\frac{Iw_1}{2\pi r}\right) \cdot \left(-r\right),$$

при якому похідна $\partial F\left(Iw_1, r\right)/\partial r$ є функцією змінної $Iw_1/2\pi r$, що задовольняє вимозі, зазначеній вище. Проводячи відповідні перетворення, отримуємо вирази для магнітної проникності μ_r та величини B_{Wb}:

$$\mu_r = \frac{B}{\mu_0 H} = \frac{\partial F_0\left(\frac{Iw_1}{2\pi r}\right)}{\partial\left(\frac{Iw_1}{2\pi r}\right)} - \frac{F_0\left(\frac{Iw_1}{2\pi r}\right)}{\frac{Iw_1}{2\pi r}},$$

$$B_{Wb} = \mu_0 \frac{F_0\left(\frac{Iw_1}{2\pi r_{вн}}\right) \cdot r_{вн} - F_0\left(\frac{Iw_1}{2\pi r_{зовн}}\right) \cdot r_{зовн}}{r_{зовн} - r_{вн}}.$$

Отже, визначення функції F зводиться до пошуку функції F_0, яка є функцією змінної H.

Зауважимо, що питання аналітичного подання кривої намагнічування феромагнетику неодноразово порушувалось у наукових публікаціях. Зокрема, відомо про використання раціональної функції [7], функції експоненти [8], оберненої тригонометричної [9] і гіперболічної [10] функцій.

Розглянемо декілька варіантів функції $F_0(H)$, подібних до тих, що використовуються в літературі при описі кривої намагнічування. Тобто розглянемо випадки, коли функція $F_0(H)$ є раціональною, містить показникові доданки або обернені тригонометричні/гіперболічні функції.

Якщо $F_0 = -\frac{a_1 H}{1 + b_1 H}$, де $H = \frac{Iw_1}{2\pi r}$ – напруженість магнітного поля всередині осердя, a_1, b_1 – числові коефіцієнти, то

$$\mu_r = \frac{a_1 b_1 H}{1 + 2b_1 H + \left(b_1 H\right)^2},$$

$$B_{Wb} = \frac{\mu_0 a_1 Iw_1}{r_{зовн} - r_{вн}} \cdot \left(\frac{r_{зовн}}{2\pi r_{зовн} + b_1 Iw_1} - \frac{r_{вн}}{2\pi r_{вн} + b_1 Iw_1}\right).$$

Якщо $F_0 = -\dfrac{a_1 H + a_2 H^2}{1 + b_1 H + b_2 H^2}$, де a_1, a_2, b_1, b_2 – числові коефіцієнти, то

$$\mu_r = \frac{(a_1 b_1 - a_2) H + 2 a_1 b_2 H^2 + a_2 b_2 H^3}{1 + 2 b_1 H + (b_1^2 + 2 b_2) H^2 + 2 b_1 b_2 H^3 + b_2^2 H^4},$$

$$B_{Wb} = \frac{\mu_0 I w_1}{r_{зовн} - r_{вн}} \times$$

$$\times \left(\frac{2\pi a_1 r_{зовн}^2 + a_2 I w_1 r_{зовн}}{4\pi^2 r_{зовн}^2 + 2\pi b_1 I w_1 r_{зовн} + b_2 (I w_1)^2} - \frac{2\pi a_1 r_{вн}^2 + a_2 I w_1 r_{вн}}{4\pi^2 r_{вн}^2 + 2\pi b_1 I w_1 r_{вн} + b_2 (I w_1)^2} \right).$$

Якщо $F_0 = -\left[\eta_1 \cdot \left(1 - e^{-\xi_1 H}\right) + \eta_2 \cdot \left(1 - e^{-\xi_2 H}\right) + \eta_3 \cdot \left(1 - e^{-\xi_3 H}\right) \right]$, де η_1, η_2, η_3, ξ_1, ξ_2, ξ_3 – числові коефіцієнти, то

$$\mu_r = \eta_1 \left(\frac{1 - e^{-\xi_1 H}}{H} - \xi_1 \cdot e^{-\xi_1 H} \right) +$$

$$+ \eta_2 \left(\frac{1 - e^{-\xi_2 H}}{H} - \xi_2 \cdot e^{-\xi_2 H} \right) + \eta_3 \left(\frac{1 - e^{-\xi_3 H}}{H} - \xi_3 \cdot e^{-\xi_3 H} \right),$$

$$B_{Wb} = \mu_0 [\eta_1 \left(1 - \frac{r_{зовн} \cdot e^{-\xi_1 \frac{I w_1}{2\pi r_{зовн}}} - r_{вн} \cdot e^{-\xi_1 \frac{I w_1}{2\pi r_{вн}}}}{r_{зовн} - r_{вн}} \right) +$$

$$+ \eta_2 \left(1 - \frac{r_{зовн} \cdot e^{-\xi_2 \frac{I w_1}{2\pi r_{зовн}}} - r_{вн} \cdot e^{-\xi_2 \frac{I w_1}{2\pi r_{вн}}}}{r_{зовн} - r_{вн}} \right) + \quad .$$

$$+ \eta_3 \left(1 - \frac{r_{зовн} \cdot e^{-\xi_3 \frac{I w_1}{2\pi r_{зовн}}} - r_{вн} \cdot e^{-\xi_3 \frac{I w_2}{2\pi r_{вн}}}}{r_{зовн} - r_{вн}} \right)]$$

Якщо $F_0 = -\eta \cdot \arctan(\xi H)$, де η, ξ – числові коефіцієнти, то

$$\mu_r = \frac{\eta \cdot \arctan(\xi H)}{H} - \frac{\eta \xi}{1 + (\xi H)^2},$$

$$B_{Wb} = \mu_0 \eta \frac{\arctan\left(\xi \frac{Iw_1}{2\pi r_{зовн}}\right) \cdot r_{зовн} - \arctan\left(\xi \frac{Iw_1}{2\pi r_{вн}}\right) \cdot r_{вн}}{r_{зовн} - r_{вн}}.$$

Якщо $F_0 = -\eta \cdot \operatorname{arsinh}(\xi H)$, де η, ξ – числові коефіцієнти, то

$$\mu_r = \frac{\eta \cdot \operatorname{arsinh}(\xi H)}{H} - \frac{\eta \xi}{\sqrt{1 + (\xi H)^2}},$$

$$B_{Wb} = \mu_0 \eta \frac{\operatorname{arsinh}\left(\xi \frac{Iw_1}{2\pi r_{зовн}}\right) \cdot r_{зовн} - \operatorname{arsinh}\left(\xi \frac{Iw_1}{2\pi r_{вн}}\right) \cdot r_{вн}}{r_{зовн} - r_{вн}}.$$

Для знаходження коефіцієнтів апроксимуючих виразів застосовувався інструментарій системи комп'ютерної алгебри *Wolfram Mathematica*. Найбільш точну апроксимацію експериментальних точок забезпечує остання з наведених форм для F_0. Для цього випадку отримані такі значення числових коефіцієнтів: η = 332011 А/м, ξ = 0,0312411 м/А. На рис. 2 показані результати вимірювань індукції B_{wb} і графік апроксимуючої функції $B_{wb}(Iw_1)$.

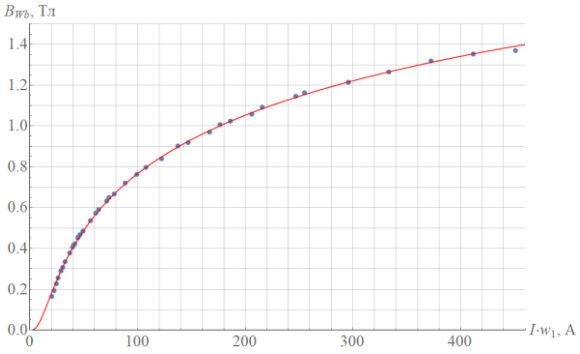


Рисунок 2 – Результати вимірювань магнітної індукції B_{wb} (точки) та їхня апроксимація (суцільна лінія)

Відзначимо, що функція $B_{wb}(Iw_1)$ на інтервалі $(0, +\infty)$ змінює знак кривини, що відповідає експериментальним даним, на відміну від функції $F_0(Iw)$, маючи при цьому ту ж кількість коефіцієнтів.

На рис. 3 показані результати обчислення відносної магнітної проникності на основі експериментальних значень B_{wb} і H_A і графік функції $\mu_r(H)$.

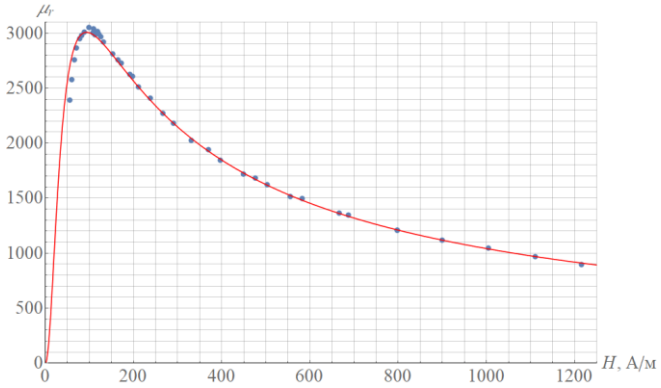


Рисунок 3 – Відносна магнітна проникність, що відповідає значенням B_{wb} і H_A (точки), графік функції $\mu_r(H)$ (суцільна лінія)

Відзначимо недолік, характерний для всіх розглянутих форм функції F_0 : функція $\mu_r(H) \to 0$ при $H \to 0$, що суперечить експериментальним даним, оскільки феромагнітний матеріал має початкову ненульову магнітну проникність при $H = 0$. Водночас на рис. 2 можна побачити, що на переважному інтервалі значень H апроксимаційна функція B_{wb} добре узгоджується із результатами експериментальних досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Розов В.Ю., Гринченко В.С., Ткаченко А.О. Расчет магнитного поля трехфазных кабельных линий при двустороннем замыкании собственных экранов кабелей, охваченных ферромагнитными сердечниками // Електротехніка і електромеханіка. – 2017. – № 5. – С. 44-47.

2. Розов В.Ю., Гринченко В.С., Ерисов А.В., Добродеев П.Н. Эффективное контурное экранирование магнитного поля трехфазных кабельных линий при ограниченном тепловом воздействии на силовые кабели // Електротехніка і електромеханіка. – 2019. – № 6. – С. 50-54.

3. ГОСТ 8.377-80 Материалы магнитомягкие. Методика выполнения измерений при определении статических магнитных характеристик. Москва, 1980. 21 с.

4. IEC 60404-4 Magnetic materials. Part 4: Methods of measurement of d.c. magnetic properties of magnetically soft materials (IEC 60404-4:1995+A1:2000+A2:2008). Geneva, 2008. 60 p.

5. Катаев В.А. Методы измерений электрических и магнитных свойств функциональных материалов. Екатеринбург, Уральский государственный университет им. А М. Горького, 2010. 264 с.

6. Nakata T., Takahashi N., Fujiwara K., Nakano M., Ogura Y., Matsubara K. An improved method for determining the DC magnetization curve using a ring specimen // IEEE Transactions on Magnetics. – 1992. – vol. 28, iss. 5. – pp. 2456-2458.

7. Rivas J., Zamarro J., Martin E., Pereira C. Simple approximation for magnetization curves and hysteresis loops // IEEE Transactions on Magnetics. – 1981. – vol. 17, iss. 4. – pp. 1498-1502.

8. El-Sherbiny M. Representation of the magnetization characteristic by a sum of exponentials // IEEE Transactions on Magnetics. – 1973. – vol. 9, iss. 1. – pp. 60-61.

9. Trutt F.C., Erdelyi E.A., Hopkins R.E. Representation of the magnetization characteristic of DC machines for computer use // IEEE Transactions on Power Apparatus and Systems. – 1968. – vol. PAS-87, iss. 3. – pp. 665-669.

10. Бессонов Л.А. Теоретические основы электротехники. Москва, Высшая школа, 1996. 640 с.

Чьочь Вікторія Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
учений секретар Інституту,
Victoria.choch@gmail.com

Васильєв Олексій Всеволодович,
ІПМЕ ім. Г.Є. Пухова НАН України,
с.н.с.,
oleksii.vasyliev@gmail.com

ПЕРСПЕКТИВИ РОЗВИТКУ ТА ВИКОРИСТАННЯ НЕЙРОННОЇ КРИПТОГРАФІЇ У ТЕХНІЧНИХ СИСТЕМАХ. РЕЗУЛЬТАТИ НАУКО-МЕТРИЧНОГО АНАЛІЗУ

Анотація. У матеріалах докладу представлено результати бібліометричного аналізу та оцінки перспектив розвитку та практичного використання нейронної криптографії у технічних системах. Оцінки основані на методах кластерного аналізу бібліографічного опису документів та патентної статистики.

Abstract. The report presents the results of bibliometric analysis and evaluation of the prospects for the development and practical use of neural cryptography in technical systems. Estimates are based on methods of cluster analysis of bibliographic description of documents and patent statistics.

Поняття «нейронна криптографія» вперше було застосовано у 1995 році і за узагальненим визначенням є розділом криптографії, який присвячений застосуванням стохастичних алгоритмів, в тому числі нейронних методів для шифрування і крипто-аналізу [1].Практичне використання методів нейронної криптографії дещо обмежується через великий обсяг обчислень і високі вимоги до потужності комп'ютерних систем. Не дивно, що до останніх часів цей розділ криптографії вважався чисто теоретичним.

На початковому етапі досліджень цієї теми була поставлена задача створення бібліографічної бази даних доступних публікацій та колекції їх повних текстів. У результаті виникла можливість отримати оцінку розвитку та використання нейронної криптографії у реалізації реальних технічних систем.

Методика рішення такої задачі полягає у розробці пошукових формул для наукометричних баз даних, які доступні на даний момент. Були обрані система Scopus (https://www.scopus.com) та система Lens (https://www.lens.org). Особливістю другої системи є можливість проводити достатньо вичерпний патентний пошук. Обидві системи пропонують потужні можливості бібліометричного та патентного аналізу для отримання оцінок перспективності та практичного застосування нейронної криптографії. Необхідно взяти до уваги факт, що одним з критеріїв патентоздатності є

промислова придатність. Після отримання результатів інформаційно-патентного пошуку за відповідними формулами, які наведені нижче, означені результати були проаналізовані на основі кластерних методів, які дали можливість оцінити перспективність методів нейронної криптографії на основі аналізу діаграми динаміки публікування,а придатність до практичного застосування на основі аналізу динаміки патентування та розподілу патентів по рубриках патентної класифікації. Обмеження методики полягало у використанні ключових слів, які носять суб'єктивних характер використання таких слів авторами, в умовах відсутності онтологічної схеми поняття «нейрона криптографія». Додатково фіксувались рейтинги публікацій і статей по країнах, для оцінки географії наукових досліджень у цій галузізнань.

Відповідні пошукові формули для БД Scopus (1) та для БД Lens (2) є ідентичними по суті, проте враховують відмінності синтаксису пошукових мовозначених систем. Пошук проводився 10.12.2021 року. Результати пошуку зафіксовані у локальній інформаційній системі менеджменту бібліографічних записів Zotero для подальшого використання.

Аналіз результатів по БД Scopus:

SCOPUS TITLE-ABS-KEY («neuro- cryptograph"» (1)
OR(neuralPRE/1cryptograph)ORneurocryptograph**
*ORneuralcryptograph**

Результат - 88 публікацій. За типом публікацій більшість отриманих записів представляя собою тези науково-технічних конференцій

Динаміка публікування наукових публікацій представлена на Рис.1, розподіл по країнам громадянства авторів публікацій представлений на Рис.2

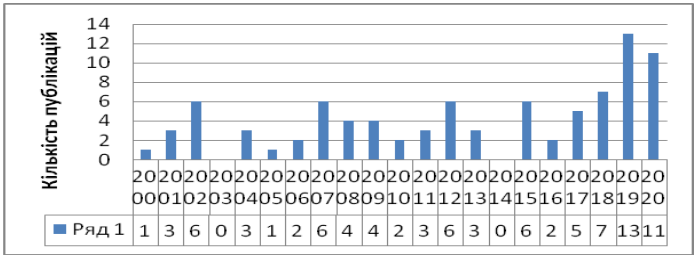


Рисунок 1 – Кількість публікацій

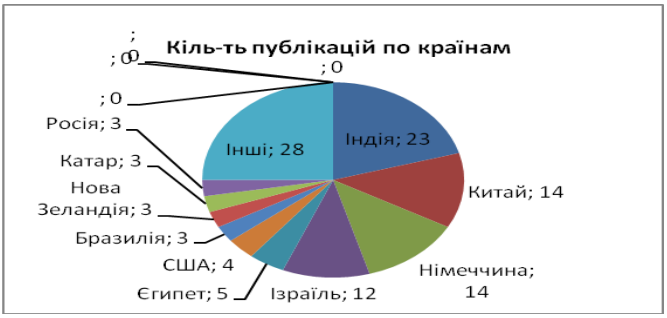


Рисунок 2 – Кількість публікацій по країнах

Аналіз результатів пошуку наукових публікацій по БД `Lens

Lens<< *(Title: (neuro-cryptography) OR (Abstract: (neuro-cryptography) OR Full Text: (neuro-cryptography))) OR ((Title: ("neural cryptography") OR (Abstract: ("neural cryptography") OR Full Text: ("neural cryptography"))) OR ((Title: (neuralcryptography) OR (Abstract: (neuralcryptography) OR Full Text: (neuralcryptography))) OR (Title: (neurocryptography) OR (Abstract: (neurocryptography) OR Full Text: (neurocryptography)))))* (2)

Результат –123 публікації. Різниця кількості знайдених документів, у по-рівнянні із результатом (1), полягає у різних джерельних базисах Scopusta Lens.

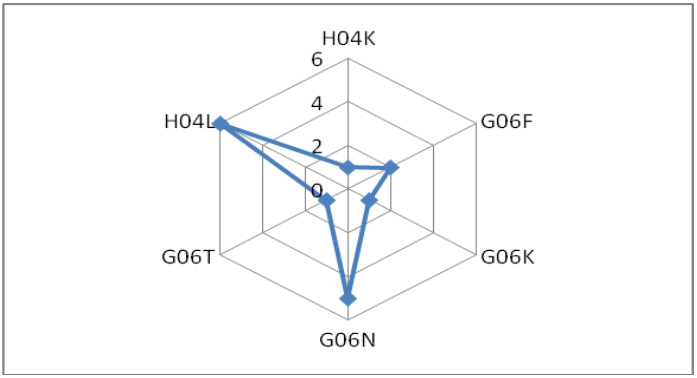


Рисунок 3 – Розподіл патентних документів по галузям практичної діяльності.

H04K	Секретний зв’язок	1
G06F	Обробляння цифрових даних за допомогою електричних пристроїв	2
G06K	Розпізнаванняданих; представленняданих	1
G06N	Комп'ютернісистеми, щогрунтуються на біологічних моделях	5
G06T	Обробляннядanихзображення для загальних потреб	1
H04L	Пристрої для секретного абозахищеногозв’язку	6

Аналіз результатів патентного пошуку по БД Lens:

Пошук здійснювався за пошуковою формулою (2). Результат – знайдено 9 патентів. Такий нечисленний результат може свідчити, що практичне використання методів нейронної криптографії не стало масовим.

Динаміка патентування вельми проста: у 2021 році зареєстровано 3 патенти, у 2020 – 5 патентів, ще 2 у 1999-2000 роках.

Розподіл патентування по країнах: Китай -4 патенти, Литва – 2 патенти, Тайвань, Австралія, Японія – по 1 патенту.

Розподіл патентів за класами Міжнародної патентної класифікації (перші 4 символи класифікації, що відповідають галузям практичного використання винаходів) представлено на Рис.3.

На основі отриманих даних, які будуть уточнюватися шляхом розробки онтологічної схеми поняття «нейронна криптографія» та детальним вивченням знайдених повних текстів публікацій та патентів, можна зробити наступні висновки:

1. Публікаційна активність продовжується у період 2000-2021 роки з очевидною тенденцією до зростання. Це свідчить про перспективність цього напрямку досліджень.

2. Географія проведення досліджень демонструє постійний інтерес до цієї теми в наукових установах Німеччини та Ізраїлю (країни де цей напрям був започаткований). Найбільша публікаційна активність відбувається у Китаї та Індії. Останні роки вона розвивалась у країнах Близького сходу, які відрізняються великими інвестиціями у розвиток власної науки та освіти.

3. Основну масу знайдених наукових публікацій представляють матеріали міжнародних конференцій (переважно видавництво IEEE). Треба відзначити помітну частину публікацій наукових товариств, таких як American Physical Society та ін. Доля наукових публікацій відкритого доступу не перевищує 25%

4. Динаміка патентування за темою нейронна криптографія показує лише початок цього процесу. Активне патентування почалось лише у 2020 році.

5. Розподіл патентів по галузевим класам (перші 4 символи) Міжнародної патентної класифікації презентує напрями інженерних розробок або винаходів, які готують для них основу (патенти на способи обробки даних). Серед практичних розробок необхідно виділити системи

передачі даних, системи захищеного зв’язку та системи шифрування зображень.

6. Географія патентування дещо відрізняється від аналогічних процесів наукових публікацій. Першу позицію займає Китай, на другому місці на даний момент опинилася Литва, патентування також відбувається у Тайвані, Австралії та Японії. Таким чином, узагальнений центр процесів патентування прийшовся на країни Східної та Південно-Східної Азії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kinzel, W., &Kanter, I. (2002). Neural cryptography. Paper presented at the ICONIP 2002 - Proceedings of the 9th International Conference on Neural Information Processing: Computational Intelligence for the E-Age, , 3 1351-1354. doi:10.1109/ICONIP.2002.1202841

Шкарупило Вадим Вікторович,
ІПМЕ ім. Г.Є. Пухова НАН України,
с.н.с., доцент, канд. техн. наук,
shkarupylo.vadym@gmail.com

Душеба Валентина Віталіївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
зав. відділом №5, доцент, канд. техн. наук,
vdusheba@ukr.net

ПІДХІД ДО СИНТЕЗУ ФОРМАЛІЗОВАНИХ ПОДАНЬ НЕФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК НА ЕТАПІ ПРОЄКТУВАННЯ

Анотація. Викладено підхід до синтезу формалізованих подань нефункціональних характеристик розроблюваної системи критичного призначення на етапі проєктування названого процесу. Підхід будується на оперуванні концептами атомарної і складеної імітаційних дискретно-подійних моделей.

Abstract. An approach to formalized representations of non-functional properties of safety-critical system under development synthesis to be applied at design stage of engineering process is described. Approach is based on manipulation with the concepts of atomic and coupled discrete event simulation models.

Результати попередніх досліджень показали, що темпоральна логіка дій TLA (Temporal Logic of Actions), відповідні формалізмиTLA+ і PlusCalє дієвими засобами контролю функціональних характеристик (ФХ) розроблюваних систем критичного призначення (СКП) вже на етапі проєктування процесу розроблення [1-4]. Названі засоби є інструментами синтезу формальних специфікацій (ФС) – формалізованих подань досліджуваних ФХ системи, що уможливлюють здійснення їх автоматизованого контролю вже на етапі проєктування процесу розроблення – за рахунок залучення формальних методів перевірки на моделі (ModelChecking, MC) [5, 6]. При цьому процес розроблення розглядається як послідовність наступних етапів: аналіз вимог, проєктування, реалізація, валідація.

Було показано, що часові витрати на залучення вищеназваних MC-методів істотним чином залежать, зокрема, як від специфіки їх реалізації (на основі алгоритму обходу у ширину чи обходу у глибину теорії графів), так і від структури ФС [7, 8]. Разом із цим, контроль показників НФХ СКП, як правило, здійснюється саме на заключному етапі валідації процесу розроблення [9]. Для цього було залучено формалізм DEVS (Discrete Event System Specification) [10].

Доцільність виявлення та своєчасного усунення помилок проєктних рішень на рівні НФХ саме на етапі проєктування, а не на етапі валідації, пояснюється скороченням супутніх цьому матеріально-часових витрат.

Під певною НФХ розуміємо часову затримку, обумовлену реалізацією відповідної ФХ або її складової.

Запропонований підхід подано на рис. 1.

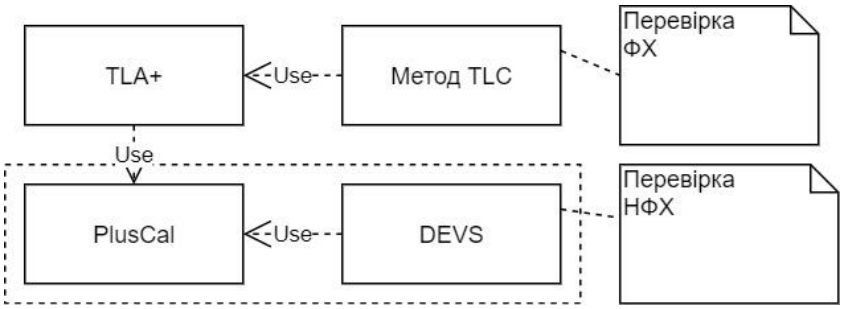


Рисунок 1 – Специфіка запропонованого підходу

На рис. 1 пунктирною областю виокремлено акцент підходу. Показано, що формалізоване подання ФХ, синтезоване засобами алгоритмічної мови PlusCal, використовується у якості основи, згідно якої будується формалізоване подання НФХ розроблюваної СКП. Контроль ФХ при цьому здійснюється формальним МС-методом TLC (TLAChecker).

Відтворення структури і зав'язків, формалізованих засобами алгоритмічної мовиPlusCal, здійснюється шляхом оперування концептами «атомарної» і «складеної» DEVS-моделей. Кожна атомарна модель (АМ) є поданням складової реалізації заданої ФХ, доповненої також і відповідним значеннямпоказника НФХ (значенням супутніх часових витрат).

Ключова ідея в основі запропонованого підходу – отримати результуючу складену модель (СМ) згідно PlusCal-подання – шляхом поєднання АМ складових або конструкцій на їх основі – допоміжних СМ. Це дасть змогу отримати оціночне значення досліджуваного показника НФХ шляхом агрегування – у відповідності до алгоритму взаємодії АМ, заданого у PlusCal-поданні.

Таким чином, запропоновано підхід, у якому викладається механізм синтезу засобів контролю показників НФХ СКП вже на етапі проєктування процесу розроблення. Названий підхід сполучається із засобами контролю ФХ. При цьому останні розглядаються у якості вихідних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. LamportL. Specifyingsystems: TheTLA+ language and tools for hardware and software engineers. Boston : Addison-Wesley, 2002. 382 p.

2. Lamport L. The PlusCal algorithm language. Theoretical Aspects of Computing : 6th Int. Colloquium, part of LNCS, (Kuala Lumpur, Malaysia, Aug. 2009). 2009. Vol. 5684. P. 36-60.

3. Verhulst E., Boute R. T., Faria J. M. S., Sputh B. H. C., Mezhuyev V. Formal Development of a Network-Centric RTOS: Software Engineering for Reliable Embedded Systems. Springer Publishing Company, Inc., 2011. 236 p.

4. Resch S., Paulitsch M. Using TLA+ in the Development of a Safety-Critical Fault-Tolerant Middleware. Software Reliability Engineering Workshops : Proc. 2017 IEEE International Symposium (Toulouse, France, 23-26 October 2017). P. 146-152. DOI: https://doi.org/10.1109/ISSREW.2017.43

5. Clarke E.M., Grumberg O., Kroening D., Peled D., Veith H. Model checking: 2nd ed. Massachusetts: The MIT Press, 2018.

6. Pakonen A., Tahvonen T., Hartikainen M., Pihlanko M. Practical applications of model checking in the Finnish nuclear industry. Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies : Proc. 10th International Topical Meeting (San Francisco, CA, USA, 11-15 June 2017). P. 1342-1352.

8. Shkarupylo V. V., Tomičić I., Kasian K. M. The investigation of TLC model checker properties. Journal of Information and Organizational Sciences. 2016. Vol. 40, No. 1. P. 145-152.

9. Shkarupylo V. V., Tomičić I., Kasian K. M., Alsayaydeh J. A. J. An Approach to increase the Effectiveness of TLC Verification with Respect to the Concurrent Structure of TLA+ Specification. International Journal of Software Engineering and Computer Systems. 2018. Vol. 4, No. 1. P. 48-60. DOI: https://doi.org/10.15282/ijsecs.4.1.2018.4.0037

10. Шкарупило В. В., Кудерметов Р. К., Польська О.В. DEVS-орієнтована методика валідаціїкомпозитних веб-сервісів. Радіоелектроніка, інформатика, управління. 2015. № 4. С. 79–86. DOI: 10.15588/1607-3274-2015-4-12

11. Concepcion A.I., Zeigler B.P. DEVS formalism: a framework for hierarchical model development. IEEE Transactions on Software Engineering. 1988. Vol. 14, No. 2. P. 228-241. DOI: https://doi.org/10.1109/32.4640

Золкін Олексій Юрійович
ІПМЕ ім. Г.Є. Пухова НАН України,
магістр,
alexzolkin19@gmail.com

Чемерис Олександр Анатолійович
ІПМЕ ім. Г.Є. Пухова НАН України,
заст. директора
a.a.chemeris@gmail.com

ХМАРНА ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ДЛЯ IP-ТЕЛЕФОНІЇ

Анотація. В роботі представлено структуру системи IP-телефонії, яка побудована на мікросервісній архітектурі. Показано переваги такого типу архітектури над монолітною архітектурою. Також, такий підхід дозволяє перенести більшість сервісів до хмари. Перенесення в хмару, відмова від пропріетарної апаратної частини та використання мікросервісної архітектури дозволять використовувати гнучкі бізнес стратегії, підвищити швидкість розробки.

Abstract. The paper presents the structure of the IP-telephony system, which is based on microservice architecture. The advantages of this type of architecture over monolithic architecture are shown. Also, this approach allows you to move most services to the cloud. Transfer to the cloud, abandonment of proprietary hardware and the use of microservice architecture will allow the use of flexible business strategies, increase the speed of development.

Системи IP-телефонії є невід'ємною частиною життя і роботи багатьох людей. Вони використовуються в багатьох сферах, від побуту до великих підприємств і розподілених бізнесів їх тисячами робітників. Побудова такої комплексної системи є актуальною проблемою, враховуючи широту ринку і наявний сильний попит на все більш гнучкі та динамічні що матимуть цінову перевагу на ринку і надаватимуть можливості глибокого та тісного налаштування під потреби кожного конкретного замовника (кастомізації). Побудова такої системи є комплексною задачею, до якої слід підходити з точки зору аналізу існуючих систем IP-телефонії, їх сильних і слабких сторін, для того щоб, враховуючі поставлені цілі, покращити їхню архітектуру і бізнес модель з урахуванням майбутнього розвитку і збереження актуальності і конкурентноспроможності в умовах підвищення динамічності ринку. Результатом проектування має бути система що покращить ефективність на одиницю ціни для кожного передбаченого бізнес-застосування, надаватиме можливість глибшої кастомізації фінального продукту, дозволить будувати гнучку бізнес стратегію для максимально ефективної адаптації до мінливих умов ринку а також підвищить ефективність розробки, підтримки та інтеграції системи.

Підкреслюють дві основні (базові) функції телефонії – 1) забезпечення голосового зв'язку між абонентами, які знаходяться на відстані один від одного, та 2). передача і обробка службової інформації або сигналізація [1]. В наступному розділі проведено аналіз систем IP-телефонії, які використовують звичайні підходи до системної організації їх функціонування. Далі розглядаємо підхід з використанням мікросервісного підходу до побудови систем IP-телефонії.

Мікросервісні архітектури інформаційних систем широко використовують в різних галузях завдяки множині властивостей, що роблять такі системи значно ефективнішими для широкого класу задач. Зокрема в банківській сфері ефективність мікросервісних архітектур доведена практичним використанням [2].

На даний момент часу є велика кількість різних провайдерів даних послуг які можуть задовольнити попит на ринку, але основна стратегія, якої вони дотримуються — це пропрієтарні комплекси, що включають в себе одразу всі компоненти готової системи: комп’ютерні потужності, пропрієтарне програмне забезпечення і зобов’язання замовника послуг користуватися лише сервісами провайдера, такими як технічна підтримка, початкове налаштування, інтеграція комплексів в технічну інфраструктуру замовника, тощо. Дані програмно-апаратні комплекси є основним будівничим блоком проектування і побудови високорівневої архітектури та інфраструктури як при запуску нової системи, так і при підтримці, модифікації або розширенню існуючої. Далі проведемо аналіз сильні та слабкі сторони даного підходу.

Говорячи про позитивні сторони даного підходу із високою пропріоритезацією, слід розділити іх на зони розробки та взаємодії із ринком.

Щодо технічної частини, слід виділити максимально тісну інтеграцію апаратної та програмної частини, що дозволяє втілити в життя набагато більшу кількість апаратно специфічних програмних оптимізацій для підвищення ефективності роботи апаратно-програмного комплексу як неподільної одиниці. Чіткий контроль апаратної частини, а також підгонка програмної частини під неї дозволяє спростити і стандартизувати процес інсталяції, налаштування, технічної підтримки, ремонту та інших аспектів роботи комплексу.

Щодо взаємодії з ринком, сюди входить вся бізнес частина: маркетингові стратегії, логістика, вертикальні та горизонтальні інтеграції та інше.

Якщо казати про негативні сторони, можемо, по аналогії із пунктом вище, розділити їх на 2 категорії: розробка та взаємодія із ринком. Щодо технічної частини, слід виділити сильну зв’язність та монолітну структуру. Так як програмне забезпечення запускається на конкретній апаратній платформі та є прив’язаним до неї то це накладає обмеження на гнучкість архітектури цього програмного забезпечення. Також це накладає обмеження на комп’ютерні потужності та еластичність системи. До того ж, постає

питання інтеграції з уже існуючими системами різних замовників, що у випадку апаратно-програмних комплексів може створювати проблеми.

Щодо взаємодії з ринком, ми можемо бачити низьку гнучкість та швидкість адаптації до змін. Розвиток Програмного забезпечення та апаратної частини нерозривно зв'язані, то ж замовник часто не має широкого вибору під час налаштування під свої бізнес задачі. Якщо додати до рівняння цінову політику, то такий підхід далеко не найпривабливіший для фінального замовника, так як апаратна частина має за замовченням підтримувати повний пакет функціональності(інакше при розширенні пакетів послуг доведеться купувати нові апаратно програмні комплекси, що є дуже не ефективним підходом), тому всі замовники, хто не користується повним пакетом функціональності що надається програмною частиною, вимушені переплатити за непотрібно потужну апаратну частину. Також, не маючи доступу до програмного забезпечення окремо, для підвищення потужності системи замовник вимушений купувати додаткові апаратно-програмні комплекси, в ціну яких входить уже куплене раніше програмне забезпечення, що підвищує вартість готової системи. Враховуючи це, провайдерам стає доволі складно аргументувати велику різницю в ціні комплексів які надають різну функціональність через те що різниця тільки в програмному забезпеченні, яке в базовій версії і так присутнє, просто в частково вимкнутому стані(підхід feature toogle доволі популярний в системах такого типу), тому ринок змушує провайдерів знижувати ціну і зменшувати свою прибутковість.

Побачивши сильні та слабкі сторони даного підходу, ми можемо виділити ключові зміни, які нам потрібно застосувати для покращення вищезазначених характеристик системи.

У нас є три основні напрямки в яких ми будемо розвивати телекомунікаційні системи для вирішення вищеозначених проблем: розділення апаратної та програмної частини, використання мікросервісної архітектури та надання можливості переходу в хмару.

При розділенні апаратної та програмної частини ми, з одного боку, отримуємо гнучкість у проектуванні та імплементації програмного забезпечення. І, на додачу, замовник в праві обирати будь яку апаратну частину під свої потреби і не вимушений іти на компроміси. Провайдер же знімає з себе тягар розробки і підтримки апаратної частини та може сфокусувати ресурси на розробці більш якісного, безпечного, надійного та функціонального програмного забезпечення що дає конкурентну перевагу на ринку.

При переході на мікросервісну архітектуру, провайдер зможе вести паралельну розробку свого програмного забезпечення в багатьох напрямках що підвищить швидкість розробки. Також це буде аргументом у ціноутворенні, тому що віднині замовник бачитиме що, купуючи додаткову функціональність, він фізично купує додаткове програмне забезпечення яке буде запущено в нових сервісах, а не просто перемикач десь в середині

монолітної програмної частини. Також цей перехід дозволить мати більш оптимізований процес розгортання системи під час навантаження, так як він буде зачіпати лише навантажені сервіси. До того ж, інтеграція із системами замовника може бути виконана набагато простіше, так як все що потрібно зробити команді розробки на стороні замовника — виконати публічні контракти системи провайдера та розгорнути свої сервіси в середині тої ж самої інфраструктури.

І, нарешті, перехід у хмару. Це виступає об'єднанням всіх плюсів вищеописаних підходів та допомагає нівелювати недоліки. Програмне забезпечення від провайдера, що готове до розгортання в хмарі, додане до самої хмари та провайдера хмарних обчислень що відповідає за стан і підтримку апаратної частини дає нам на виході набагато меншу участь замовника в організації роботи його системи, порівняно із апаратно-програмними комплексами. Замовнику тепер не потрібно вирішувати питання для організації роботи цих комплексів, всю апаратну частину забирає на себе провайдер хмарних обчислень. До того ж, хмарні обчислення не прив'язані до програмного забезпечення, що в них використовується, тому підвищити потужності у разі збільшення навантаження набагато швидше, легше та ефективніше з точки зору витрат, так як при падінні навантаження ресурси можна вивільнити і за них не платити.

Як ми бачимо, дані підходи дозволяють прибрати головні недоліки існуючих систем. Проаналізувавши принципи і підходи до їх вирішення, нам слід перейти до імплементації.

Опис системи слід розділити на декілька секцій: загальна структура системи, множина мікросервісів та приклад сервісу(опис та UML діаграма).

Структура системи нагадує стандартні мікросервісні системи, тобто має в собі як бізнес сервіси так і сервіси технічної природи(діскавері, API гейтвей та інші). Говорячи про бізнес сервіси, слід зазначити підходи відділення окремих сервісів один від одного. В загальному порядку слід користуватися доменною моделлю, але такі сервіси можуть стати завеликими. Більш практичним буде додатково розділяти сервіси одної доменної моделі за принципом Single Responsibility, керуючись моделлю акторів цього принципу. В загальному випадку це означатиме мінімум один сервіс на одну частину бізнес функціональності. Як було описано вище, слід враховувати маркетингові стратегії та забезпечувати зручний поділ системи, в ідеалі постачаючи неповний пакет сервісів для неповних пакетів функціональності, надаючи можливість додати до системи нові сервіси для розширення цього пакету.

Описуючи множину мікросервісів, слід зазначити деякі особливості притаманні телеком-домену [3]. По перше, це різні edge-proxy сервіси, що проводять маршрутизацію вхідного та вихідного трафіку. Це стосується, в першу чергу, трафіку обраного протоколу зв'язку, так як вони є першим ступенем під час визначення шляху для трафіку дзвінка користувача. По друге, це та звані call switch сервіси. Це окремі сервіси одної системи що

відрізняються лише налаштуваннями. Для ефективного скейлінгу кожен бізнес сервіс має мати як мінімум один call switch налаштований під конкретні бізнес потреби. Ця система займається обробкою та виконанням команд протоколу зв'язку(наприклад SIP) що генеруються бізнес сервісами. Говорячи про взаємодію бізнес сервіса та call switch, бізнес сервіс на основі вхідних даних та поточного стану системи вирішує, за якими правилами слід провести роутинг дзвінка, почати нові дзвінки, поставити на утримання та інше. Це є імплементацією бізнес логіки системи. Після виконання своєї логіки, бізнес сервіс віддає команди на call switch у формі команд протоколу обраного протоколу зв'язку. Зі свого боку, call switch проводить інтерпретацію цих команд та їх виконання в рамках сесій дзвінків користувачів. Для наочності, приведемо приклад частини одного із сервісів. Це абстракції та імплементації, що використовуються при обробці уже завершеного дзвінка із ціллю визначення розміру оплати та збереження статистики і історії дзвінків.

На Рис.1 і 2 зображені діаграми класів одно із сервісів, що відповідає за обробку сесіій користувачів. На Рис.1 зображена частина сервісу яка відповідає за обробку даних сесій та розбиття сесії за бізнес направленостями. На Рис.2 зображена частина сервісу, що відповідає за видначення бізнес направленності сесій та відповідність їх заздалегіть визначеним бізнес критеріям. В ці критерії входять як технічні аспекти дзвінка(чи стався він всередині мережі, чи використовувався міжнародний телефонний код та інше) так і критерії, що відповідають функціоналу системи(чи ставалася переадресація дзвінка, чи було очікування на лінії та інше).

Як ми змогли побачити, внесення вищезазначених покращень зможе позбавити існуючі телекомунікаційні системи їх основних недоліків. Перенесення в хмару, відмова від пропріетарної апаратної частини та використання мікросервісної архітектури дозволять використовувати гнучкі бізнес стратегії, підвищити швидкість розробки шляхом розподілення роботи між багатьма командами, підвищення привабливості пропозиції на ринку, підвищення ефективності використання комп'ютерних ресурсів та оптимізація відповідних витрат, а також швидкість розгортання, гнучкість та гарні можливості підбору унікальних варіантів системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Черкасов Д. І. Основи технології VoIP та IP-телефонії / Дмитро Черкасов // Телеком. Военная связь, № 2. - 2017- С. 98-104.
2. Григоров А. Из монолитов в микросервисы: новые возможности для ДБО / Андрей Григоров // Расчеты и операционная работа в коммерческом банке, №1 (143) - 2018 – с.10-15.
3. Voice over IP Fundamentals / Jonathan Davidson // VoIP: An In-Depth Analysis - 2006 — с.146-166

ЗМІСТ

МАТЕРІАЛИ
ІІІ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІІ

«БЕЗПЕКА ЕНЕРГЕТИКИ В ЕПОХУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ»

22 грудня 2021 року
м. Київ

Оператор конференції – ТОВ «ІНФОРМАТІО»

Формат 60×90/16. Тираж 100.
Підписано до друку 15.12.2021. Заказ № 12

Інститут проблем моделювання в енергетиці
ім. Г.Є. Пухова Національної академії наук України,
Україна, 03164, Київ, вул. Генерала Наумова, 15,
тел.: +38 044 424 10 63
https://ipme.kiev.ua/, ipme@ipme.kiev.ua