НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

МАТЕРІАЛИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

27 травня 2022 року

Київ – 2022

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 № 04 від 26 травня 2022 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 27 травня 2022 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2022. 128 с.

В-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, May 27, 2022. Kyiv: PIMEE NAS of Ukraine, 2022. 129 p.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

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

Чемерис Олександр Анатолійович
доктор технічних наук,
заступник директора з наукової роботи

Гончар Сергій Феодосійович
доктор технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук,
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
Завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

Anfimova Galina Viktorovna,
G.E. Pukhov Institute for Modelling Problem in Energy Engineering of NAS of Ukraine,
engineer,
anfimova77@ukr.net

A RISK-ORIENTED APPROACH TO IMPROVING THE QUALITY OF OPERATION AND THE ENVIRONMENT OF URBAN HEAT SUPPLY PIPELINES

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.

Annotation. 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.

It is known that most of the heat supply system of domestic cities has exhausted its resources and is in a state of extreme emergency . Constant bursts of underground pipelines, a large amount of operational diagnostic and repair work to identify and eliminate damage lead to huge financial costs and environmental damage. Emergency mode has become a daily practice organizations operating pipelines. It should be recognized that due to the lack of an adequate large-scale pipeline replacement program, heating networks have become a rather dangerous facility and incidents with human casualties are becoming increasingly likely.

In recent decades, approaches related to the concept of risk have been intensively implemented and applied in various industries [1]. Risk is characterized as "a combination of the probability of an event and its consequences". Examples include the use of elements of risk-oriented approach in industrial safety and labor protection management systems [2], in ensuring environmental requirements at petrochemical facilities [3], in nuclear energy [4] and in gas transmission systems [5].

In G.E. Pukhov Institute for Modelling Problem in Energy Engineering of NAS of Ukraine is conducting research aimed at creating a proactive risk management system

associated with the safe operation of worn-out pipelines of heating networks in urban areas. Based on the experience of many years of work on diagnosing pipelines of Kiev heating networks, a set of measures aimed at improving the quality of their operation has been developed [6]. At the same time, the basis necessary for a reliable assessment of the risks of accidents in the areas of heating networks should be, First of all, accurate data on the current corrosion wear of underground pipelines, obtained with the help of the original specialized modeling system - a set of remote equipment "RASTR" [6]. Many years of experience show that heating networks have a large margin of safety and damage occurs almost exclusively in places of corrosion thinning of pipeline walls. As additional factors, it is necessary to take into account the ratio of normative and actual service life of pipelines, statistics of damage and repairs at different sites in recent years, regime parameters and other circumstances that increase the risk of large-scale accidents, such as high groundwater levels. water supply and much more.

Based on the ranking of the received risks, appropriate organizational and technical measures should be planned, including targeted relocation of small, most corroded sections of pipelines until the moment of the accident, creation of local systems for continuous monitoring of the most responsible sections, etc.

The construction of the proposed system of data collection and risk assessment will reduce the impact of the human factor, as well as move to proactive risk management in the operation of heating pipelines in urban areas.

REFERENCES

1. EJ Henley and H. Kumamoto, “Reliability Engineering and Risk Assessment,” By Englewood Cliffs, Prentice-Hall, New Jersey, 07632. ISBN-0-13-772251-6, 1981.

2. Bulygin Yu . I., Tkacheva VA, Lutkova EM Elements of risk-oriented approach in industrial safety and labor protection management systems of enterprises.

Eastern European Magazine Naukowe (East European Scientific Journal) , # 11 (51), 2019. pp. 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.

Vladimirsky Alexander Albertovich,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine,
Leading Researcher,
av1000000@ukr.net,

Vladimirsky Igor Albertovich,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine,
Senior Researcher,
av1000000@ukr.net,

Kutsan Yuly Grigryevich,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine,
senior scientist,
kutsan.ug@ukr.net,

Krivoruchko Igor Petrovich,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine,
postgraduate student, researcher,
uhmi_igorkr@ukr.net,

Anfimova Galina Viktorovna,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine,
engineer,
anfimova77@ukr.net

PARAMETRIC CORRELATION METHODS FOR OPERATIONAL REMOTE PASSIVE DETERMINATION OF THE COORDINATES OF LEAKS AND ASSOCIATED CORROSION DAMAGE IN UNDERGROUND PIPELINES

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 стоншення стінок трубопроводів, пов’язаних із витоками.

Annotation. 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.

Topicality

Correlation method (CM) has many known advantages [1,2,3] and is one of most common in determining the coordinates of leaks in pipelines . However, the use of CM is often accompanied by significant errors in determining the coordinates of the leaks [1,2,4,5] . Based on numerous published experimental and theoretical data [6,7,8,9,10,11], as well as personal research of the authors [4,5] it is established that the underground pipelines register not only waves of hydraulic shock, but also other waves, propagating at different speeds, with different attenuation.

The idea of determining the leakage coordinates according to the basic L_x formulas for correlation leak detectors [4,14,16]

$$L_x = \frac{L}{2} + \frac{V_{\text{г}} \cdot dT}{2}, \qquad R(dT) = \max_T (R(T)),$$

where $R(T)$ - evaluation of the mutual correlation function of signals from sensors, based on the fact that the signals recorded by sensors that installed on the site underground pipeline of length L, formed by a certain type of powerful acoustic waves that generate a leak, such as hydraulic shock waves with a known propagation speed $V_{\text{г}}$. At the same time, in practice signals of sensors contain other components that are obstacles. To eliminate interference in leak detectors, frequency filters are used, with the help of which they try to identify the frequency band with the most pronounced maximum when searching for leaks $R(dT)$.

However, in some cases, this method of interference suppression is not sufficient due to the multiwave propagation of acoustic signals from the source to the leak detectors and the presence of reflections. Therefore, in the places of registration of signals from the sensors, coherent leakage waves with different delays lead to

interference distortions and noise correlations. There are not only amplitude-frequency, but also time-frequency distortions that cannot be eliminated by applying only amplitude-frequency filtering. The problem of taking into account interference distortions of signals at emergency search of leaks needs to be solved.

The paper presents the results of research and development with projects "Monitor-2" and "Resource-3", which is devoted to the creation of parametric methods for diagnosing underground pipelines, which are the development of a known correlation method for determining the coordinates of leaks damage in conjunction with external interference.

Analysis of publications

In [12] the improvement of correlation signal processing is presented, based on the use of the cross-correlation function (CCF) in the analysis of pressure waves, but to create such waves requires a sharp change in pressure in the pipeline.

In [13] the method of selection sources signals using their frequency-time distributions is presented. The advantage of the method is consistency spatial and frequency selection sources. However this method is developed for non - stationary signals .

In [10] the method of determining the coordinates of the leaks, based on the use of generalized cross-correlation, which allows to take into account the multiwavelength and dispersion of waves. However, this interesting method requires significant hardware costs.

Coherence function is often used in the search for leaks [14], the method of application of the linear phase-frequency spectrum of CCF [15], the method of frequency-time analysis of correlation functions, which includes 3-dimensional representation of narrowband components of CCF [16,17].

There is a method of frequency analysis of correlation functions of vibration signals [18], according to which high-quality digital filters are used to decompose the mutual correlation function into narrowband components. The following parameters are determined for each frequency band: delay at which the maximum correlation is

observed; the quality of the maximum correlation function (expressiveness); power of the narrowband component. It is these parameters: delay, quality and power that reflect the operator's quality of the frequency dependence of the dominant surge in the assessment of CCF, which he analyzes. Therefore, this approach of parametric representation of CCF was adopted as a basis for further development.

It should be noted that the rearrangement of sensors and re-determination of leakage coordinates practiced by some specialists in order to control the repeatability of the obtained leakage coordinates is useful, but in terms of taking into account the influence of multiwave propagation of vibration signals selection of a specific position of sensors on the pipeline for selection of the required type of acoustic waves, adequate in speed of propagation to the value of the speed used to ensure correct results.

Basic part

Development begins with the construction of a diagnostic model of the pipeline section, which simulates the presence of damage as sources of stationary acoustic noise, multiwave propagation of these noises to leak detectors, as well as the presence of external, statistically unrelated interference. The model is designed to formalize existing complications and build adequate algorithms for overcoming them.

The list of diagnostic parameters which in the conditions of interference distortions on size characterize quality of selection of an informative wave of hydraulic shock is formed. The connection of complications with these parameters is analyzed. The connection between the model, parametric analysis and determination of leak coordinates is shown.

Correlation parametric spatial and frequency methods [19, 20] for determining the coordinates of leaks are presented. These methods can be used independently of each other. The spatial method is aimed at overcoming time-frequency distortions of informative correlation, and the frequency method is aimed at overcoming amplitude-frequency noise distortions.

The parametric automated method of the coordinated spatial-frequency selection of coordinates of damages of pipelines is developed. The method is based on the parameters of the next level, namely the parameters of spatial and frequency mismatch of power and quality parameters (signal-to-noise ratio). These parameters allow to reconcile the spatial and frequency selection of the informative correlation formed by powerful waves of hydraulic shock, by estimating the final error of this selection.

The developed method is patented [21] and implemented in the K-10.5M3 correlation parametric leak detector. Software copyrights registered [22].

Received experimental confirmation of the effectiveness of the proposed parametric methods in diagnosing the heating network.

Conclusions

Received results allow to increase the efficiency and accuracy of leak detection in underground pipelines in various and often difficult urban conditions of diagnosis. In addition, it is practically important to determine the significant corrosive thinning of the metal diagnosed in the search for leaks in the pipeline. The possibility of using leakage noise as a causative agent of corrosion thinning places opens the way to optimize the repair of damaged underground pipelines by carrying out in addition to eliminating leakage spot repair in critically corroded areas in the diagnosed, already emptied for repair, leak area and nearby, sections of the underground pipeline. Knowing the extent of corrosion thinning around the leak is important when planning the volume of excavation and is especially in demand when eliminating leaks of pipelines laid in the sleeves under the roads.

REFERENCES

1. Баранов В. М. Акустические измерения в ядерной энергетике. М.: Энергоатомиздат, 1990. 320 с.

2. Дробот Ю. Б., Грешников В. А., Бачегов В. Н. Акустическое контактное течеискание. М.: Машиностроение, 1989. 120 с.

3. Каллакот Р. Диагностика повреждений. М.: Мир, 1989. 512 с.

4. Владимирский А. А., Владимирский И. А. Особенности распространения вибросигналов по трубопроводам тепловых сетей большого диаметра. Моделювання та інформаційні технології . Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України. 1999. Вип. 3. С. 37-41.

5. Владимирский А. А., Владимирский И. А., Семенюк Д. Н. Уточнение диагностической модели трубопровода для повышения достоверности течеискания. Акустичний вісник Інституту гідромеханіки НАН України. 2005. 3 (8). С. 3-16.

6. Иофе В. К., Корольков В. Г., Сапожков В. Г. Справочник по акустике. Москва: Связь, 1979. С.

7. Иродов И. Е. Волновые процессы основные законы. Москва – Санкт-Петербург, 1999. С.

8. Мякишев Г. Я., Синяков А. З. Физика: Колебания и волны. 11 кл.: Учебник для углубленного изучения физики. М.: Дрофа, 2002. 288 с.

9. Павленко Ю. Г. Физика: учебное пособие. Москва, 1998. С.

10. Rewerts, L. E., Roberts, R., and Clark, M. A. Dispersion compensation in acoustic emission pipeline leak location. Review of Progress in QNDE, 16A, D. O. Thompson and D. E. Chimenti, eds., Plenum Press, New York, 427–434.

11. Патент US6138512A, IPC G01M3 / 24; G01S11 / 14; G01V1 / 00; (МПК1-7): G01H17 / 00; КПК G01M3 / 243 (EP); G01S11 / 14 (EP); G01V1 / 001 (EP); Method and apparatus for determining source location of energy carried in the form of propagating waves through a conducting medium / Ronald A. Roberts; Lance E. Rewerts; Mary Amanda Clark. - заяв. 29.07.1998, опубл. 31.10.2000.

12. Niloufar Motazedi and Stephen Beck. Leak detection using cepstrum of cross-correlation of transient pressure wave signals. Mechanical Engineering Science 2018, Vol. 232(15) 2723–2735. DOI: 10.1177/0954406217722805.

13. Adel Belouchrani, Moeness G. Amin, Nadıge Thirion-Moreau, and Yimin D. Zhang. Source Separation and localization using time-friquency distributions. IEEE Signal Process Mag 30 (6): 97–107 IEEE.

14. Leak detection technology and implementation. Stuart Hamilton and Bambos Charalambous. Alliance house. 12 Caxton street. London SW1H 0QS, UK . 2013 IWA publishing.

15. А.Л. Овчинников, Б.М. Лапшин, А.С. Чекалин, А.С. Евсиков. Опыт применения течеискателя ТАК-2005 в городском трубопроводном хозяйстве. Известия Томского политехнического университета [Известия ТПУ]. — 2008. — Т. 312, № 2 : Математика и механика. Физика. Приложение: Неразрушающий контроль и диагностика. — [С. 196-202].

16. V.A. Faerman, A.G. Cheremnov, V.S. Avramchuk, and D.V. Shepetovsky. The leak location package for assessment of the timefrequency correlation method for leak location. International Conference on Information Technologies in Business and Industry 2016 IOP Publishing IOP Conf. Series: Journal of Physics: Conf. Series 803 (2017) 012040 doi:10.1088/1742-6596/803/1/012040.

17. В.С. Аврамчук., В.Т. Чан. Частотно-временной корреляционный анализ цифровых сигналов. Известия Томского политехнического университета. 2009. Т. 315. № 5 С.112-115.

18. 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. - К., 2000. - С. 23-24.

19. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів// Електрон. моделювання, 2021, 43, № **3**, с. 3—17.

20. 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.

21. Патент на корисну модель № 149956; G01M 3/24, G01M 3/18, F17D 5/02. Параметричний кореляційний спосіб визначення координат пошкоджень трубопроводів. Владимирський О.А., Владимирський І.А. Публікація відомостей 15.12.2021, Бюл. №50/2021. Заявник - ІПМЕ ім. Г.Є. Пухова НАН України.

22. О.А. Владимирський, І.А. Владимирський. Науковий твір “Параметричний кореляційний течешукач К-10.5М3. Керівництво з експлуатації К105М3-1.00.04 КЕ”. Свідоцтво про реєстрацію авторського права на службовий твір №110118 від 08.12.2021р. Заявник - ІПМЕ ім. Г.Є. Пухова НАН України.

Владимирський Олександр Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, д.т.н.,
av1000000@ukr.net,

Артемчук Володимир Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, д.т.н.,
ak24avo@gmail.com,

Дюков Володимир Андрійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник,
v.dukov@i.ua

РОЗРОБЛЕННЯ ЗАСОБІВ ВИМІРЮВАННЯ ГЕОМЕТРИЧНИХ РОЗМІРІВ ВИГОРОДКИ АКТИВНОЇ ЗОНИ ЯДЕРНИХ РЕАКТОРІВ

Анотація. Зважаючи на те, що розрахунок напружено-деформованого стану та формозміни вигородки активної зони ядерних реакторів АЕС у процесі експлуатації та аналіз впливу радіаційної повзучості дають суперечливі результати, обґрунтовується необхідність розробки науково-обґрунтованої методики вимірювань геометричних розмірів вигородки.

Annotation. The calculation of the stress-strain state and shape change of the nuclear reactor core baffle during operation and the analysis of the effect of radiation creep give conflicting results. This substantiates the need to develop a science-based method for measuring the actual geometric dimensions of the baffle.

У рамках цільової програми наукових досліджень НАН України «Ядерні та радіаційні технології для енергетичного сектору і суспільних потреб» на 2019-2023 рр. у ІПМЕ ім. Г.Е. Пухова НАН України з 2022р. виконується НДР “Розроблення методичних, програмних та технічних засобів вимірювання геометричних розмірів вигородки активної зони ядерних реакторів”.

Технічне обґрунтування продовження терміну експлуатації енергоблоків має базуватися на експериментальних та теоретичних

дослідженнях, направлених на контроль та діагностування технічного стану елементів конструкції енергоблоків. Особлива увага приділяється корпусу, шахті і вигородці реактора, які є одними з найвідповідальніших за відведення теплоти з активної зони і незамінюваних протягом всього періоду експлуатації елементів конструкції реактора. Вигородка призначена для формування поля енерговиділення, дистанціювання периферійних касет і радіаційного захисту. Особливістю експлуатації вигородки є наявність сильного нейтронного випромінювання і високих температур внаслідок радіаційного розігріву, які призводять до розпухання металу. Потенційну загрозу представляють наступні наслідки радіаційного розпухання вигородки: зменшення в локальних місцях конструктивного зазору між внутрішньою поверхнею вигородки і поверхнею оболонок твелів, зменшення зазору між зовнішньою поверхнею вигородки і внутрішньою поверхнею шахти, зміна фізичних властивостей металу вигородки.

Розрахунок напружено-деформованого стану та формозміни вигородки в процесі експлуатації та аналіз щодо впливу радіаційної повзучості дає суперечливі результати [1, 2].

Мета дослідження [3] полягає у розробленні науково-обґрунтованої методики вимірювань геометричних розмірів вигородки активної зони ядерних реакторів АЄС, а також структури та вимог до спеціальних технічних засобів для їх використання у процесі виконання заходів продовження термінів експлуатації енергоблоків АЕС понадпроектний строк.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Чирков А.Ю., Харченко В.В. Особенности расчетной оценки формоизменения выгородки активной зоны реактора ВВЭР-1000 с учетом радиационного распухания. *Пробл. прочности*. 2020. № 3. С. 5—20.

2. Чирков О.Ю., Харченко В.В. Вплив радіаційної повзучості на визначення формозміни вигородки активної зони реактора ВВЕР-1000 за умов

довгострокової експлуатації. *Допов. Нац. акад. наук Укр*. 2021. № 3. С. 40—47. https://doi.org/10.15407/dopovidi2021.03.040

3. В.О. Артемчук, О.А. Владимирський, В.А. Дюков. Аналіз наукових підходів та технічних засобів вимірювань геометричних розмірів вигородки активної зони ядерних реакторів АЕС. Зб. тез XL Науково-технічної конференції молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ, 11 травня 2022 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2022. – С. 113-114.

Владимирський Олександр Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, д.т.н,
av1000000@ukr.net,

Владимирський Ігор Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.т.н.,
gosho2018@yahoo.com,

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

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

АДАПТАЦІЯ СЕРТИФІКОВАНИХ ЗАСОБІВ ВИМІРЮВАННЯ ПАРАМЕТРІВ РУХУ ДО АКТУАЛЬНИХ ЗАВДАНЬ МАСШТАБНОГО ВІДНОВЛЕННЯ ПОШКОДЖЕНОГО ЛІФТОВОГО ОБЛАДНАННЯ

Анотація. У зв'язку з масштабними руйнуваннями міської інфраструктури в багатьох вітчизняних містах актуальним стає питання проведення термінових та об'ємних аварійно-відновлювальних робіт, у тому числі, ліфтового обладнання. Опрацьовано шляхи адаптації до вирішення нових завдань вимірювачів кінематичних та динамічних параметрів ліфтів.

Annotation. Due to the presence of large-scale destruction in cities, urgent and extensive repair work, including elevator equipment, becomes relevant. The ways of adapting meters of kinematic and dynamic parameters of lifts to solving new problems have been implemented.

У зв'язку з масштабними руйнуваннями міської інфраструктури в багатьох вітчизняних містах актуальним стає питання проведення термінових та об'ємних аварійно-відновлювальних робіт, у тому числі ліфтового

обладнання, ескалаторів, підвісних канатних доріг та ін. Збільшується обсяг не лише сертифікаційних випробувань – на відповідність параметрів руху вимогам нормативних документів [1, 2], але, головним чином, також і діагностичних робіт та виявлення численних несправностей з метою їхнього оперативного усунення. Фактично суттєво підвищуються вимоги до оперативності та функціональності проведення вимірювань.

Групою технічної діагностики ІПМЕ ім. Г.Є. Пухова НАН України опрацьовано шляхи адаптації до вирішення нових завдань раніше розроблених та впроваджених на більшості експертно-технічних центрів та ряді ліфтобудівних підприємств України вимірювачів кінематичних та динамічних параметрів ліфтів ИКПЛ-М3 [3]:

- Підвищення точності вимірювання прискорення лінійного та обертального руху в 2 рази шляхом встановлення нового програмного забезпечення та застосування нової методики калібрування.
- Прискорення та підвищення технологічності процедур підготовчих робіт шляхом доукомплектування вимірювачів новими монтажними комплектами на основі магнітних та електромагнітних утримувачів.
- Організація довічного щорічного технічного обслуговування вимірювачів, проведення їх метрологічного калібрування та продовження гарантійного терміну.
- Суттєве розширення функціональних можливостей вимірювачів шляхом реалізації реєстрації супутніх подій, що автоматично забезпечує повноцінне, комплексне діагностування ліфтового обладнання [4, 5].
- Організація та проведення навчання користувачів та обміну досвідом виконання діагностичних операцій.
- Прийом замовлень на виготовлення модернізованих вимірювачів за заявками вітчизняних підприємств.

Сформульовані пропозиції планується надіслати на адреси галузевих підприємств та організацій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Правила будови і безпечної експлуатації ліфтів = Правила устройства и безопасной эксплуатации лифтов: НПАОП 0.00-1.02-08: Затв. 01.09.2008 № 190 / Державний комітет України з промислової безпеки, охорони праці та гірничого нагляду –Х.: Вид-во "Індустрія". "Основа". 2008. 192 с.

2. ДСТУ EN 81-50:2015 Норми безпеки щодо конструкції та експлуатації ліфтів. Випробування та перевіряння. Частина 50. Норми проектування, розрахування, випробування та перевіряння компонентів ліфта (EN 81-50:2014, IDT) – [Чинний від 2018-01-01]. Київ, 2016. 22 с.

3. Владимирский А.А. Разработка средств контроля параметров движения подъемно-транспортного оборудования. Подъемные сооружения. Специальная техника. 2013. № 2. С.21-24.

4. Владимирський О.А., Владимирський І.А., Криворучко І.П., Анфімова Г.В. Комп'ютерна програма «Вимірювання параметрів руху. Реєстрація подій (Ліфт-3.05-КМ3)» Свідоцтво про реєстрацію авторського права на службовий твір № 112610 від 07.04.2022 р. ІПМЕ ім. Г.Е.Пухова НАН України.

5. Vladimirsky A.A., Vladimirsky I.A., Krivoruchko I.P., Anfimova G.V. Test bench intrinsically safe circuits. Abstracts of the XL Scientific and technical conference of young scientists and specialists of G.E. Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, May 11, 2022 / PIMEE of NAS of Ukraine. 2022. pp. 11-12.

Владимирський Олександр Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, д.т.н.,
av1000000@ukr.net,

Владимирський Ігорь Альбертович,
ІПМЕ ім. Г.Є. Пухова НАН України, к.т.н.,
старший науковий співробітник,
gosho2018@yahoo.com

ПРО ЗАВДАННЯ РОЗВИТКУ ЗАСОБІВ І ТЕХНОЛОГІЙ ОПЕРАТИВНОГО ПОШУКУ ВИТОКІВ ТА ПЕРІОДИЧНОГО КОРОЗІЙНОГО МОНИТОРИНГУ МІСЬКИХ ПІДЗЕМНИХ ТРУБОПРОВОДІВ В УМОВАХ ПОВОЄННОЇ ЕКОНОМІКИ

Анотація. У зв'язку з наявними масштабними руйнуваннями міської трубопроводної інфраструктури багатьох міст і населених пунктів України є необхідність проведення срочних і об'ємних аварійно-восстановних робіт. Розглядаються питання корекції планів НІР і ОКР спрямованих на підвищення ефективності дістанційного діагностування пошкоджень підземних трубопроводів.

Annotation. The Due to the large-scale destruction of the urban pipeline infrastructure of many cities and towns of Ukraine, there is a need for urgent and extensive emergency recovery work. The adjustment of the plans of research and development work aimed at improving the efficiency of remote diagnosing damage to underground pipelines is considered.

У зв'язку з масштабними руйнуваннями міської інфраструктури багатьох вітчизняних міст та селищ актуальним стає питання проведення термінових та об'ємних аварійно-відновлювальних робіт, у тому числі систем холодного та гарячого водопостачання, теплових мереж. Необхідною умовою для цього є наявність точної інформації про місця та ступінь наявних пошкоджень. Найбільш поширена на сьогодні акустична технологія заснована

на реєстрації шумів витоків за допомогою датчиків вібрації. Ці датчики встановлюються на грунт над трубопроводом чи на сам трубопровід у місцях службового доступу – у теплових камерах, колодязях, підвалах будинків. Необхідною умовою визначення місць витоків є створення у трубопроводі надлишкового тиску, який має бути достатньо великим, по перше, для збудження акустичного шуму в місці пошкодження, а по друге, для компенсації загасань при поширенні шуму до датчиків течешукача. У середньому, загасання у трубопроводі інформаційних хвиль гідроудару становить величину близько 0,2 дБ/м. Тобто на відстані 200 м. від витоку до датчика сигнал загасає в 100 разів. Навіть при повністю справному джерелі тепло- чи водо- постачання, за сприятливих умов, потрібний тиск вдається створити не завжди. Наприклад, у період літніх гідравлічних випробувань мереж на щільність при великій кількості поривів або при одному, але великому пошкодженні. У післявоєнний час ця ситуація може загостритися у зв'язку з пошкодженнями джерел та неможливістю їх роботи на номінальній потужності, пошкодженням і труднощами ремонту та відновлення систем технічного забезпечення і т.і., через що тиск у трубопроводах може знизитися.

Вихід слід шукати за двома напрямками:

- Підвищувати чутливість традиційно застосовуваних акустичних методів. Це дає можливість, як і раніше, використовувати розвинене методичне забезпечення поширених методів.
- Використовувати принципово інші методи виявлення та визначення місць пошкоджень стінок трубопроводів, що не потребують наявності в них надлишкового тиску.

У групі технічної діагностики ІПМЕ ім. Г.Є. Пухова НАН України є напрацювання та ведуться роботи з обох цих напрямків. За першим напрямком розроблений та пройшов експлуатаційну перевірку в теплових мережах параметричний кореляційний метод пошуку витоків [1]. Даний метод є розвитком відомого, поширеного кореляційного методу.

Підвищення його чутливості досягається за рахунок наступних нововведень:

- Реалізації додаткової, вторинної обробки взаємних кореляційних функцій (ВКФ). Ця обробка збільшує обсяг корисної інформації, яка вилучається з ВКФ, перетворює її у завжди важливі для аналізу параметри, які подаються оператору в наочному графічному вигляді. Цим значно покращується розпізнаваність пошкоджень.

- Врахування нерівномірної просторової чутливості датчиків до сигналів витоків у технологічних місцях доступу до трубопроводу. Таке врахування, у поєднанні з традиційним врахуванням частотної залежності відношення сигнал-перешкода, призвело до ефективної узгодженої просторово-частотної селекції ослаблених низьким тиском та загасанням сигналів витоків.

За другим напрямком є такі напрацювання:

- Для пошуку витоків у трубопроводах теплових мереж та гарячого водопостачання завершено розробку акустико-теплометричного течешукача А-10Т3. Течешукач комплектується тепловим датчиком з розподільчою здатністю 0,03° С. і дозволяє за тепловими аномаліями у ґрунті визначати місця витоків у трубопроводах з низьким тиском.

- Проводиться робота щодо створення системи виробничого корозійного моніторингу підземних трубопроводів. Визначення місць корозійних стоншень металу відбувається за відлуннями зондувальних акустичних сигналів, якими збуджується трубопровід. Експериментальна частина відпрацьована на київських теплових мережах за допомогою розробленого в ІПМЕ ім. Г.Є. Пухова НАН України реєстратора акустичних сигналів трубопроводів “РАСТР-1” [2]. Результати показали, що система може застосовуватись як на заповнених трубопроводах під тиском, так і на спорожнених ділянках. Враховуючи той факт, що більш ніж 90% витоків є наслідком корозійного потонання металу, виробничий варіант системи передбачає її використання як за прямим призначенням, так і у якості “активного течешукача” на спорожнених ділянках.

Під час повоєнної економіки особливо гострим очікується дефіцит коштів. У тому числі на планове перекладання ділянок підземних трубопроводів. Через назрілу необхідність регламентної заміни багатьох сотень кілометрів мереж, цих коштів не вистачало навіть у більш сприятливий для країни час. У післявоєнний період важливість переходу від заміни ділянок довжиною 50-200 м. між тепловими камерами до їх точкових ремонтів у критично стоншених корозією місцях, в яких ще не виникли небезпечні витоки, набуває друге дихання. У зв'язку з цим розробка виробничого варіанта системи "РАСТР" групою технічної діагностики інтенсифіковано.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. О.А. Владимирський, І.А. Владимирський. Просторовий та частотний кореляційні параметричні методи визначення координат витоків підземних трубопроводів. Електронне моделювання. 2021. Т. 43. № 4, -с. 22-36. DOI: https ://doi.org/10.15407/emodel.43.04.022

2. О.А. Владимирський, І.А. Владимирський, І.П. Криворучко, М.П. Савчук. Розробка модернізованої системи низькочастотного діагностування стану трубопроводів РАСТР-1М. Моделювання та інформаційні технології. Збірник наукових праць. Інститут проблем моделювання в енергетиці ім.Г.Є.Пухова НАН України. Вип. 78, Київ, 2017 р.-с. 40-45.

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник , д.т.н.,
hilgurt@ukr.net

ПОВОДЖЕННЯ З ПАРАМЕТРАМИ БАЗ ДАНИХ СИГНАТУР РЕКОНФІГУРОВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ЕНЕРГЕТИЦІ

Анотація. Реконфігуровні сигнатурні технічні засоби використовуються для вирішення задач захисту інформації, зокрема в енергетиці, у випадках, коли програмні рішення не забезпечують потрібну продуктивність. Для пошуку найбільш ефективного апаратного рішення необхідно вміти коректно поводитися з параметрами баз даних сигнатур, насамперед – з патернами (фіксованими послідовностями символів), що є складовими частинами сигнатур. В роботі запропоновано техніку впорядкування патернів, яка дозволяє спростити алгоритми обчислення таких параметрів множини патернів, як загальна кількість символів, кількість ненульових пакетів патернів однакової довжини та функції самоподоби.

Annotation. Reconfigurable signature tools are used to solve information security problems, in particular in energy, in cases where software solutions do not provide the required performance. To choose the most effective hardware solution, you need to be able to properly handle the parameters of signature databases, especially – patterns (fixed sequences of characters), which are part of signatures. The paper proposes a pattern ordering technique that simplifies algorithms for calculating such parameters of a set of patterns as the total number of characters, the number of nonzero pattern packets of the same length, and the self-similarity functions.

Сигнатурний підхід завдяки точному виконанню процедури розпізнавання злонавмисної активності все ще залишається актуальною технологією, яка використовується в таких засобах захисту, як мережеві

системи виявлення вторгнень, антивірусні та протиспамові системи захисту та інші технічні засобі безпеки інформації, що використовуються зокрема в енергетичній галузі. Через збільшення розміру баз даних сигнатур і високу пропускну здатність сучасних мереж традиційні програмні рішення більше не можуть відповідати вимогам, що висуваються до продуктивності таких систем. Для прискорення виконання ресурсномісткої обчислювальної процедури множинного розпізнавання рядків (одночасного розпізнавання множини рядків), що здійснюється в сигнатурних засобах захисту інформації, все частіше використовуються апаратні підходи. В якості платформи для реалізації таких рішень зазвичай використовуються реконфігуровні пристрої на базі ПЛІС [1], тому відповідні засоби називають реконфігуровними системами захисту інформації.

Існує багато підходів до побудови апаратних схем та їх модифікацій, що вони використовуються для множинного розпізнавання патернів – фіксованих послідовностей символів, які є складовою частиною сигнатур [2]. Для вибору найбільш придатних рішень для конкретних умов та ефективного їх застосування необхідно вміти поводитеся з параметрами баз даних сигнатур, зокрема, з патернами.

В даній роботі пропонується техніка поводження з патернами баз даних сигнатур, яка дозволяє спростити процедури оцінки та порівняння різних технічних рішень при побудові сигнатурних реконфігуровних систем захисту інформації.

Подамо множину патернів, що мають розпізнаватися сигнатурною системою захисту інформації, у вигляді множини, що характеризується певними параметрами:

$$P = \left\{ p_1,\ p_2,\ p_3, \ldots p_k, \ldots p_\sigma \,/\, \sigma, \Omega, m_{\min}, m_{\max}, \delta, \mu, \mu_z, \nu \right\},$$

де $p_1, p_2, p_3, \ldots p_k, \ldots p_\sigma$, – власне набір патернів, σ – кількість патернів в наборі, Ω – загальна кількість символів в наборі патернів, $m_{\min}$ – довжина найкоротшого патерну в наборі, $m_{\max}$ – довжина найдовшого патерну в наборі,

δ – функція розподілу довжин, μ – перша функція самоподоби, μ_z – перша часткова функція самоподоби, ν – друга функція самоподоби.

Патерни p_k є фіксованими послідовностями символів, код кожного з котрих належить до певного алфавіту Σ. У випадку байтового кодування $\Sigma = \{00_{16}, 01_{16}, 02_{16}, ..., FF_{16}\}$.

Функції самоподоби μ, μ_z та ν – це кількісні параметри набору патернів, які характеризують ступінь подібності патернів між собою, тобто визначають надлишковість, що присутня в множині патернів, яку можна використати для скорочення числа операцій порівняння під час вирішення задачі множинного розпізнавання патернів.

Сутність техніки, що пропонується в якості основи для кількісних оцінок в процедурах оптимізації під час розробки апаратних засобів захисту інформації полягає, в наступному. Відсортуємо всі патерни в множині P за зростанням довжини, як наведено на рис. 1. Складені з квадратів стовпчики тут зображають рядки символів.

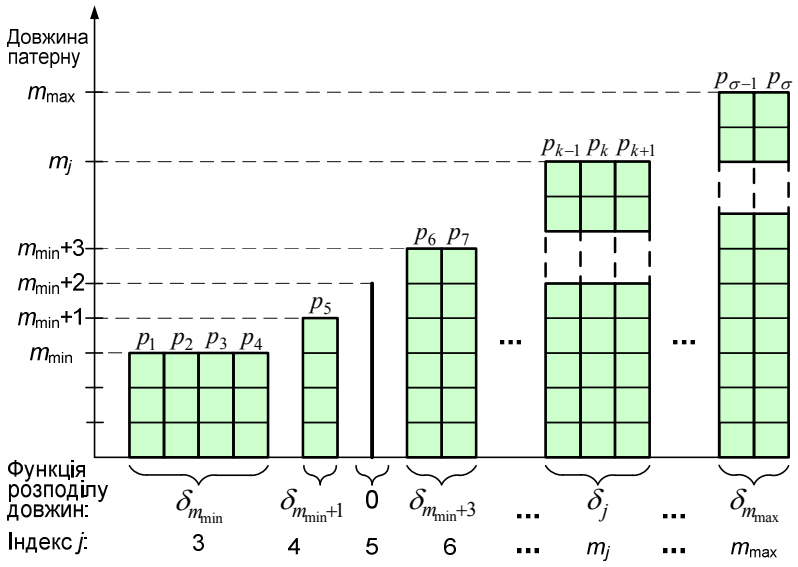

Рисунок 1 – Принцип впорядкування пакетів патернів

Назвемо пакетом сукупність патернів однакової довжини, не звертаючи уваги, як само впорядковані патерни всередині сукупності. Введемо індекс j

таким, що співпадає з довжиною патернів в пакеті $J = m_{\min}, m_{\min+1}, m_{\min+2}, \ldots m_j, \ldots m_{\max}$, де $m_{\min}$ – довжина найкоротшого патерну, $m_{\max}$ – довжина найдовшого патерну, причому кожне наступне значення цього індексу обов'язково на одиницю більше за попереднє, тобто в нумерації немає пропусків. Тоді довжина кожного патерну в наборі співпадатиме з індексом його пакету: $m_j = j$.

Зворотне твердження хибне, тому що для деяких індексів j патерни відповідної довжини можуть бути відсутні. Тому загальна кількість пакетів ξ в наборі патернів P в загальному випадку менша за величину різниці між довжинами крайніх розмірів $(m_{\max} - m_{\min})$.

Функцію розподілу довжин δ як залежність від індексу j визначимо рівною кількості патернів у відповідному пакеті: $\delta(j) = \delta_j$. В прикладі на рис. 1 j = 3, 4, 5, … $m_{\max}$, $\delta(3) = 4$, $\delta(4) = 1$, $\delta(5) = 0$, $\delta(6) = 2$, $\delta(m_{\max}) = 2$.

За допомогою функції розподілу довжин зручно обчислювати кількість ненульових пакетів ξ та загальну кількість символів Ω в наборі.

Загальна кількість символів дорівнює сумі символів у кожному пакеті, яка в свою чергу дорівнює добутку довжини рядків на їх кількість в пакеті:

$$\Omega = \sum_{j=m_{\min}}^{m_{\max}} \delta_j \, m_j = \sum_{j=m_{\min}}^{m_{\max}} \delta_j \, j \; .$$

Для підрахунку кількості пакетів ξ в множині P потрібно визначити функцію нерівності нулю:

$$\mathrm{NotZ}(x) = \begin{cases} 0, & x = 0 \\ 1, & x > 0 \end{cases} .$$

Тоді кількість пакетів в множині *P:*

$$\xi = \sum_{j=m_{\min}}^{m_{\max}} \mathrm{NotZ}\left(\delta_j\right).$$

Для розрахунків кількісних параметрів технічних рішень сигнатурних систем захисту інформації потрібно також визначити функції самоподоби множини патернів *P*.

Перша функція самоподоби $\mu(s, l)$ множини патернів *P* дорівнює сумарної кількості символів з кодом *s* ($s \in \Sigma$), розташованих на *l*-ої позиції всіх патернів цієї множини, причому нумерація позиції *j* символу в патерні здійснюється з кінця патерну до початку. Наприклад, для *P* = {"SHIP", "HIS", "HER", "IN"} μ("S", 4) = 1; μ("H", 3) = 3; μ("I", 2) = 3; μ("P", 1) = 1; μ("S", 1) = 1; μ("N", 4) = 0; μ("N", 3) = 0; μ("N", 2) = 0, де зображення символу в лапках позначає його код у відповідному кодуванні.

Записати в аналітичному вигляді вираз для находження першої функції самоподоби μ складно, проте, використовуючи запропоновану техніку, не викликає труднощів підрахувати всі її значення алгоритмічним чином для подальшого використання при програмній реалізації методів оптимізації реконфігуровних систем захисту інформації.

Перша часткова функція самоподоби $\mu_z(s, j)$ множини патернів *P* дорівнює сумарної кількості символів з кодом *s* ($s \in \Sigma$), розташованих періодично на позиціях $(j-1)\,k\,z$, $j = 2, 3, 4, \ldots (z-1)$, $k = 1, 2, 3, \ldots \lceil m_j/z \rceil$ всіх патернів цієї множини, причому нумерація позиції *j* символу в патерні також здійснюється з кінця патерну до початку. Наприклад, для z=4 і *P* = {"43214321", "HGFA4EDA4CBA", "555515555", "277727} μ_z("4", 4) = 4; μ_z("3", 3) = 2; μ_z("2", 2) = 4; μ_z("1", 1) = 3; μ_z("A", 1) = 3; μ_z("A", 3) = 0, де зображення символу в лапках також позначає його код у відповідному кодуванні.

Перші та друга функції самоподоби дозволяють визначати надлишковість при розрахунках кількісних характеристик схеми розпізнавання

на базі декодованої асоціативної пам'яті та частково декодованої асоціативної пам'яті відповідно [3].

Друга функція самоподоби ν множини патернів P у кількісний спосіб визначає ступень збігу між собою фрагментів різних патернів бази даних сигнатур. Для функції ν також складно сформулювати аналітичний запис, але в неявному вигляді вона присутня в базах даних сигнатур й відіграє важливу роль при розрахунках кількісних характеристик схем на базі алгоритму Ахо–Корасік [4].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гильгурт С.Я. Реконфигурируемые вычислители. Аналитический обзор / С.Я. Гильгурт // Электронное моделирование. – 2013. – Т. 35, № 4. – С. 49-72.
2. Гільгурт С. Методи побудови оптимальних схем розпізнавання для реконфігуровних засобів інформаційної безпеки / С. Гільгурт // Безпека інформації. – 2019. – Т. 25, № 2. – С. 74-81. DOI: 10.18372/2225-5036.25.13824
3. Гільгурт С.Я. Побудова асоціативної пам'яті на цифрових компараторах реконфігуровними засобами для вирішення задач інформаційної безпеки / С.Я. Гільгурт // Електронне моделювання. – 2019. – Т. 41, № 3. – С. 59-80. DOI: 10.15407/emodel.41.03.059
4. Гільгурт С. Побудова скінченних автоматів реконфігуровними засобами для вирішення задач інформаційної безпеки / С. Гільгурт // Захист інформації. – 2019. – Т. 21, № 2. – С.111-120. DOI: 10.18372/2410-7840.21.13768.

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

ЗАДАЧА МОДЕЛЮВАННЯ МОДАЛЬНИХ ХАРАКТЕРИСТИК СКЛАДНОГО ЗБІРНОГО СОНОТРОДУ ДЛЯ УЛЬТРАЗВУКОВОГО ЗВАРЮВАННЯ ПОЛІМЕРІВ

Анотація. Розвинуто підхід до класифікації, чисельного моделювання, проектування та практичної реалізації складних збірних сонотродів для ультразвукового зварювання полімерів.

Annotation. An approach to the classification, numerical modeling, design and practical implementation of complex composite sonotrodes for ultrasonic welding of polymers has been developed.

Сонотрод є важливою частиною акустичної системи обладнання, яке використовує технологію потужного ультразвуку. Що стосується ультразвукового зварювання полімерів, то проектування сонотроду з відповідними модальними характеристиками має важливе значення. Сонотрод є елементом коливальної системи технологічного обладнання, і його функція - передача механічної енергії до об’єкту зварювання.

До сонотродів пред'являють такі особливі вимоги[1]:

він повинен мати резонанс на заданій частоті;

він має відтворювати на своїй робочій поверхні, яка задається формою деталі, однорідний розподіл нормальної складової переміщення;

він повинен мати заданий коефіцієнт посилення нормальної складової переміщення;

він повинен мати достатню втомну міцність та низький рівень вібророзігріву.

При зварюванні деталей із складною конфігурацією поверхні та розмірами в плані, які перевищують половину довжини повздовжної хвилі

коливання (λ/2), виникає потреба в складних збірних сонотродах (СЗ сонотрод). Простим сонотродом, будемо називати такий сонотрод, розмір якого в напрямку робочих переміщень дорівнює λ/2, а в перпендикулярних напрямках не перевищує λ/3. Складним сонотродом, будемо називати сонотрод, який не відповідає вище вказаному. Складним збірним сонотродом будемо називати сонотрод, який складається з декількох сонотродів, при цьому один з них має бути складним. Зазвичай складний збірний сонотрод будується таким чином: до базового сонотроду, який має бути складним додають робочі сонотроди, які можуть бути як простими, так і складними, приклад СЗ сонотрода показано на рис.1.

Рисунок 1 – Приклад складного збірного сонотроду

Задача базового сонотроду - відтворити однорідне поле нормальних переміщень на заданій площині проекції деталі. Задача робочих сонотродів сформувати контур зварного шва та підсилити нормальні переміщення до робочих амплітуд. Приклад складного збірного сонотроду, який наведено на рис.1, у якого базовим є складний сонотрод у формі прямокутного паралелепіпеду з розмірами 220х220 мм, що є перевищенням розміру λ/2 для даного матеріалу, а інші шість сонотродів це прості робочі сонотроди.

Конфігурація базового сонотроду не дозволяє здійснити підсилення нормальних переміщень на робочій поверхні, тому цю функцію повинні перебрати на себе робочі сонотроди.

Була поставлена наступна задача: розробити сонотрод для зварювання прямокутної обичайки з розмірами в плані 210х75 мм, яка має криволінійну складну форму поверхні та складається з двох половин. Коефіцієнт посилення сонотрода має бути не менше 2.

Якщо вирішувати цю задачу звичайним шляхом, як вказано вище, ми стикаємось із значними складнощами практичної реалізації. Тому було використано наступний підхід – проектуються три сонотроди: складний базовий сонотрод та два складних робочих сонотрода. Всі сонотроди збираються в одну модель СЗ сонотроду та піддаються корегуванню до заданих параметрів.

Моделювання виконувалось за допомогою програми Comsol Multiphysics.

Розв'язувалась пружна задача на власні значення однорідного рівняння руху за умов вільної границі. Для обчислювання використовувались властивості матеріалу сонотроду, такі як: модуль пружності, густина та коефіцієнт Пуассона. Обчислювання проводилось методом скінченних елементів. Алгоритм розрахунку полягає у визначенні форми сонотрода, яка забезпечує резонанс на робочій частоті, коефіцієнт підсилення, а також заданий рівень однорідності нормальних переміщень на робочій поверхні.

Спочатку моделювався кожний сонотрод окремо, а потім їх збірка, як СЗ сонотрод.

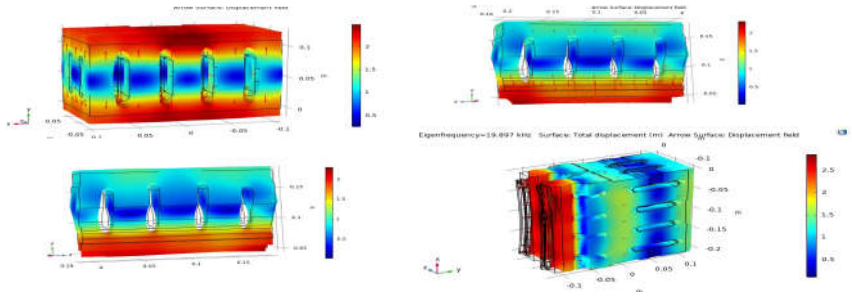

Рисунок 2 – Етапи розрахунку складного збірного сонотроду. Моделювання окремих частин і корегування збірки

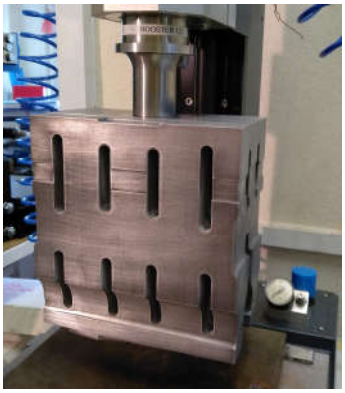

Рисунок 3 – Фото виготовленого складного сонотроду

По результатах моделювання був виготовлений сонотрод з алюмінієвого сплаву Д16Т. Розрахункова частота роботи сонотроду – 19,897 кГц, експериментально визначена частота – 19,934 кГц. Розбіжність складає менше 0,2%, що можна вважати прийнятним узгодженням з результатом розрахунку. Розрахункова однорідність нормальних переміщень на робочій поверхні скрадає 0,96. На практиці виміри однорідності не виконувались, але практична оцінка зварного шва задовольняє вимогам міцності та однорідності.

В роботі розвинуто підхід до класифікації, чисельного моделювання, проектування та практичної реалізації складних збірних сонотродів для ультразвукового зварювання полімерів. В подальшому, треба провести моделювання з урахуванням втомної міцності та довговічності таких сонотродів у постановці зв'язаної задачі термов'язкопружності при гармонічних коливаннях [2].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. И.К. Сенченков Модальная классификация и проектирование сонотродов для ультразвуковой обработки материалов.//Акустичний вісник. 1998.Т.1 №4 С.55-64

2. Сенченков И.К., Карнаухов В.Г., Михайленко В.В., Дяченко С.М. Численное моделирование виброразогрева и тепловых напряжений в стержневом пьезопреобразователе типа Ланжевена. // Прикладная механика, 1996, 32, № 3 с. 80-85.

Джигун ОленаМиколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.т.н.,
elromanenko@gmail.com

ДОВГОСТРОКОВЕ ПРОГНОЗНОЗУВАННЯ ВИРОБНИЦТВА ЕЛЕКТРОЕНЕРГІЇ ВЕС І СЕС*

Анотація. Наведено механізм довгострокового прогнозування виробництва електроенергії ВДЕ. Розглянуто кілька сценаріїв довгострокового прогнозування виробництва електроенергії вітро- і сонячними електростанціями.

Annotation. The mechanism of long-term forecasting of RES electricity production is presented. Several scenarios for long-term forecasting of electricity production by wind and solar power plants are considered.

У світі спостерігається стійка тенденція до розвитку відновлюваних джерел енергії (ВДЕ) та поступового заміщення ними традиційної генерації. Для України розвиток ВДЕ є одним із першочергових завдань для підвищення енергетичної та екологічної безпеки держави. Україна володіє достатнім потенціалом для розвитку ВДЕ та заміщення традиційних паливно-енергетичних ресурсів, тому наша держава поставила перед собою чіткі стратегічні цілі щодо розвитку сфери ВДЕ.

У 2021 році в Україні встановлено 731 МВт потужностей ВДЕ, які отримали «зелений» тариф. За даними Нацкомісії, що здійснює держрегулювання у сферах енергетики та комунальних послуг, сукупна встановлена потужність ВДЕ-об’єктів в Україні станом на кінець 2021 року сягнула 8451 МВт.

*Роботу виконано за цільовою програмою «Підтримка пріоритетних для держави наукових досліджень і науково-технічних (експериментальних) розробок Відділення фізико-технічних проблем енергетики НАН України на 2022 - 2023 рр.» з кодом програмної класифікації видатків 6541230 (прикладні дослідження).

При цьому минулого року найбільше потужностей додалося у вітроенергетиці: було введено в експлуатацію 359 МВт вітроелектростанцій (ВЕС) – у 2,5 разу вище за показник 2020 року (144 МВт) і в 1,2 разу вище за показник введених в експлуатацію сонячних електростанцій (СЕС), які традиційно лідирують у галузі (286 МВт). Отже, на кінець 2021 року загальна потужність ВЕС становить 1673 МВт, промислових СЕС – 6226,9 МВт. Згідно Енергетичної стратегії України на період до 2035 р. [1] обсяг використання енергії ВДЕ в загальній структурі енергопостачання країни повинен складати 25%.

Згідно з дослідженнями, наведеними у [2], у кінцевому споживанні енергії частка ВДЕ збільшиться до 3% у 2035 р. та 15,1% у 2035 р. за рахунок біомаси та сонячної енергетики. Частка ВДЕ у виробництві електроенергії у майбутньому зростатиме до 24% і 28% у 2035 і 2050 рр. відповідно. Враховуючи економічне зростання та збільшення частки споживання електроенергії, прогнозується зростання попиту на електроенергію в Україні на 30 % протягом наступного десятиліття, що перевищить 150 ТВт·год до 2030 р. Щоб задовольнити даний попит, валове виробництво електроенергії має бути збільшено до 190 ТВт·год, що включає також втрати при транспортуванні та власне споживання електроенергії в енергетичному секторі [3].

Відповідно до результатів моделювання, у 2030 році в структурі виробництва електроенергії переважатиме ядерна енергетика (90 ТВт·год при середньому коефіцієнті використання встановленої потужності 75%), ВДЕ (в т.ч. великі ГЕС та ГАЕС) забезпечать близько 60 ТВт·год, існуючі вугільні електростанції – 25 ТВт год, решта – існуюча та нова газова генерація і промислові автовиробники. Лише заміна викопних джерел відновлюваними може призвести до скорочення загальних викидів ПГ у 2030 році до рівня 41% від 1990 року. Для досягнення цієї мети виробництво електроенергії з відновлюваних джерел повинно збільшитися у період з 2020 по 2030 рр. Відповідно до енергетичної стратегії України на період до 2035 року, частка ВДЕ у 2030 складатиме 17 %, а у 2035 – 25 %.

Україна володіє значним природним потенціалом для здійснення «зеленого» переходу в усіх секторах економіки. Враховуючи можливості та доступність сучасних технологій відновлюваної енергетики, а також стрімкий їх розвиток, Україні цілком під силу та економічно доцільно до 2050 року досягнути 70% частки ВДЕ у виробництві електроенергії. Причому значну частину (до 15%) має складати виробництво електроенергії за рахунок дахових сонячних електростанцій в домогосподарствах та бізнесі. Передбачається значне збільшення ролі децентралізованого електропостачання, що вимагатиме використання сучасних технологій, пов'язаних з управлінням попитом, розподіленим накопиченням та розподіленою генерацією [4].

Регіональна енергосистема (ЕС) України представляється у вигляді територіального охоплення регіону у розрізі областей (див. малюнок). Таких енергосистем в Україні вісім: Західна —1, Центральна — 2, Північна — 3, Донбаська — 4, Південно-Західна — 5, Дніпровська — 6, Південна — 7 та АР Крим — 8 (тимчасово окупована територія).

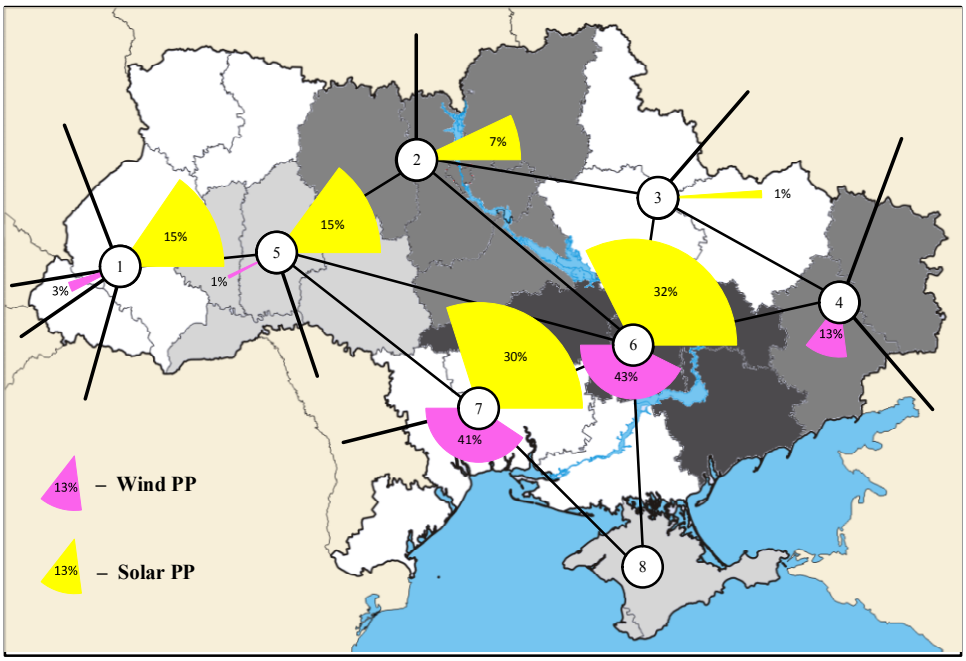

Рисунок 1 – Регіональна енергосистема (ЕС) України

Отже, в Західну ЕС входять Волинська, Закарпатська, Івано-Франківська, Львівська, Рівненська області; Центральну ЕС — Житомирська, КиЇвська, Черкаська, Чернігівська; Північну ЕС — Сумська, Харьківська, Полтавська; Донбаську ЕС — Донецька, Луганська; Південно-Західну ЕС—

Вінницька, Хмельницька, Тернопільська, Чернівецька; Дніпровську ЕС — Дніпропетровська, Запорізька, Кіровоградська; Південну ЕС — Миколаєвська, Одеська, Херсонська.

У розробленій моделі на прогнозному періоді використано часові ряди даних щодо обсягів виробітку електроенергії ВЕС та СЕС минулих періодів з поданням їх у такій математичній формі, яка у довгостроковій перспективі дозволяє враховувати вплив кліматичних змін і динаміку введення нових потужностей ВЕС та СЕС. Всі показники отримано в результаті обробки даних, наведених на сайтах Національної комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг [5], та Національної енергетичної компанії «Укренерго» [6]. В табл. 2 і 3 наведено виробництво електроенергії СЕС і ВЕС у 2021, а також об’ єм виробництва електроенергії у 2030, 2040, 2050 рр., отриманий за прогнозом.

Таблиця 1

Регіональна ЕС	Виробництво електроенергії СЕС, млн кВт·год			
	Базове	Прогнозоване		
	2021	2030	2040	2050
Західна Центральна	951,2	2905	6764	11857
Північна	530,8	3064	8066	14669
Донбаська	75,7	2044	5930	11060
	1,1	1254	3729	6996
Південно-Західна				
Дніпровська				
Південна	897,8	2397	5358	9266
Всього	1880,6	3584	6947	11378
	2005	3753	7207	11765
	6342,2	**19000**	**44000**	**77000**

Таблиця 2

Регіональна ЕС	Виробництво електроенергії ВЕС, млн кВт·год			
	Базове	Прогнозоване		
	2021	2030	2040	2050
Західна	78,0	1753	4566	6484
Центральна	0,0	2875	7705	10997
Північна	0,0	3333	8932	12749
Донбаська	37,7	4143	11040	15742
Південно-Західна				
Дніпровська	5,898	2105	5632	8036
Південна	1686,0	7550	17399	24115
Всього	1996,5	8240	18727	25878
	3804,9	**30000**	**74000**	**104000**

Безхмарна сонячна та безвітряна погода позитивно позначаються на показнику зростання генерації електроенергії. А ось в похмурі дні та негоду спостерігається висока щільність хмарних мас, що викликає зменшення кількості вироблення електроенергії СЕС і ВЕС. Оскільки людина ще не навчилася управляти погодою, то найбільш актуальним розв’язанням даної проблеми є необхідність прогнозування обсягів виробництва електроенергії, у тому числі й довгострокових. Якісне прогнозування дає можливість виробникам та операторам мережевих компаній грамотно управляти показниками продуктивності СЕС і ВЕС, ефективно впроваджуючи «зелену» енергетику в Об'єднану Енергетичну Систему України (ОЕСУ).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Енергетична стратегія України на період до 2035 року «Безпека, енергоефективність, конкурентоспроможність». Розпорядженням Кабінету

Міністрів України від 18 серпня 2017 р. №605-р. Режим доступу: https://mepr.gov.ua/files/images/news_2020/21012020

2. Довгострокове енергетичне моделювання та прогнозування в Україні: сценарії для плану дій реалізації Енергетичної стратегії України на період до 2035 року. Заключний звіт. Київ-Копенгаген, 2019. Режим доступу: https://ens.dk/sites/ens.dk/files/Globalcooperation/long-term_energy_modelling_and_forecasting_in_ukraine_ukrainian.p

3. Аналітичний огляд оновленого національно визначеного внеску України до Паризької угоди. Міністерство захисту довкілля та природних ресурсів України, 2021. Режим доступу: https://mepr.gov.ua/files/docs/klimatychna_polityka

4. Концепція «зеленого» енергетичного переходу України до 2050 року. Міністерство захисту довкілля та прироних ресурсів України, 2020. Режим доступу: https://mepr.gov.ua/news/34424.html

5. http://www.nerc.gov.ua/?id=16021

6. https://ua.energy/peredacha-i-dyspetcheryzatsiya/dyspetcherska-informatsiya/dobovyj-grafik-vyrobnytstva-spozhyvannya-e-e/

Васильєв Олексій Всеволодович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.т.н.,
oleksii.vasyliev@gmail.com,

Чьочь Вікторія Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.т.н.
victoria.choch@gmail.com

МЕТОДИКА ПОШУКУ ЗАКОНОДАВЧИХ ДОКУМЕНТІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Анотація. У матеріалах докладу представлена методика інтегрованого пошуку текстової інформації у базах даних різного рівня структуризації з фінальним формування єдиного масиву інформації для аналізу інформації законодавчого характеру.

Annotation. The report presents a method of integrated search of textual information in databases of different levels of structuring on the financial formation of a single array of information for the analysis of information of a legislative nature.

Основні законодавчі документи провідних країн, як правило, добре відомі фахівцям з питань кібербезпеки. Тому метою інформаційного пошуку та порівняльного аналізу ставиться 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, WebofSciencета ін.) та загальних (Scholar.Google.comта 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 таких публікацій, що задовольняють заданим критеріям пошуку (формулам пошуку), а також можливість виходу (може ускладнюватися необхідністю оплати доступу) на повні тексти знайдених публікацій. Аналіз повних текстів (інколи рефератів) публікацій може дати певні фактичні дані про законодавчі документи, або повну назву та інші атрибути законодавчого акту, інколи включаючи Інтернет-адресу першоджерела.

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

Позначення елементів на Рис. 1. приведені нижче:

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

- **БД1 – Інформаційно-пошукова система SCOPUS** (ElsevierB.V.)[1]. 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 система Web of Science**(Clarivate Analytics) [2]. 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) [3]**. 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) [3].** 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.) [4].** 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 [5].** (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 [6].** (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 проводиться на основі застосування інформаційно-пошукових формул$Ф_i$. На схемі Рис.1 процес виконання відповідних пошукових формул, представлено інформаційними фільтрами.

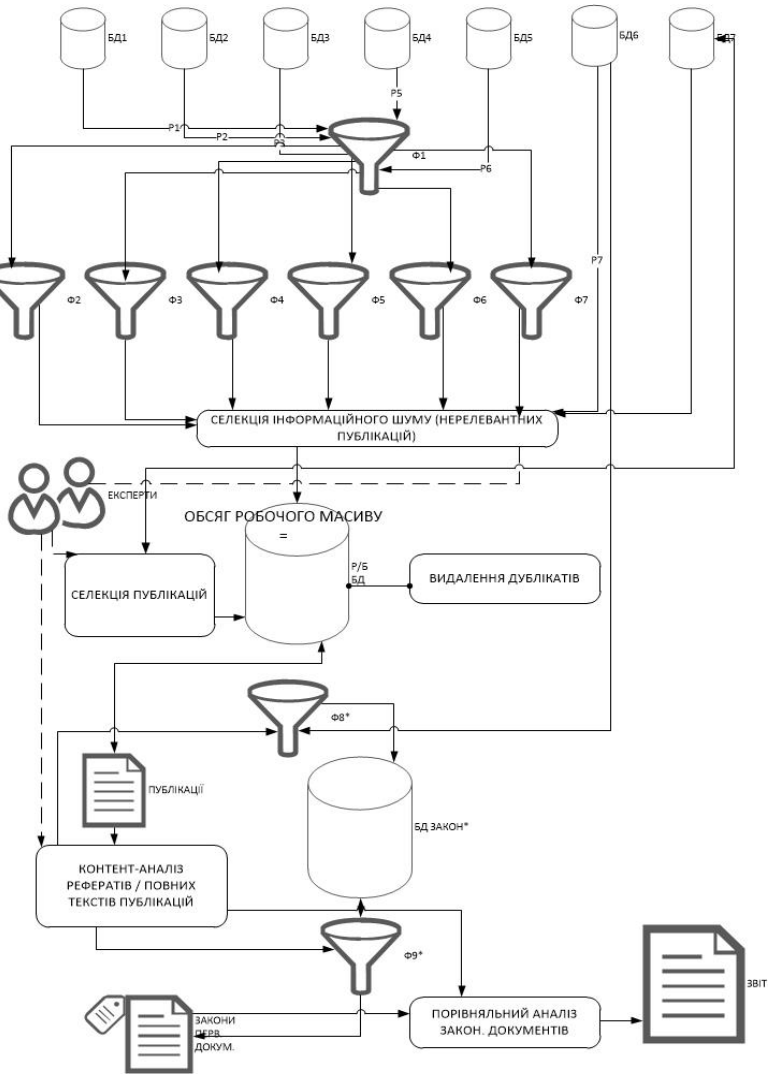

Рисунок 1 – Загальна схема організації та обробки відомостей (та змісту) публікацій та першоджерел

В процесі інформаційного пошуку та обробки знайдених документів створюється 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. Рекомендується 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 імпортуються 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) - Характерною особливістю пошукових формул подібного 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 виконавця 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 виконується 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, в результаті яких отримуються повні тексти першоджерельних законодавчих документів;

- ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАКОН. ДОКУМЕНТІВ – Знайдені законодавчі документи (першоджерело) підлягають порівняльному аналізу по обраній порівняльній схемі і доповненню інформацією, яка була отримана на етапі контент-аналізу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційно-пошукова система SCOPUS. [Електронний ресурс] URL: https: //www.scopus.com. Дата звернення: 09.05.2022
2. Інформаційно-пошукова система Web of Science[Електронний ресурс] URL: https: //www.primayer.com/ products/mikron3. Дата звернення: 09.05.2022
3. Інформаційно-пошукова система EBSCO. [Електронний ресурс] URL: https: //www.ebsco.com. Дата звернення: 09.05.2022
4. Пошукова. Система ScholarGoogle. [Електронний ресурс] URL: https: //www.scholar.google.com . Дата звернення: 09.05.2022
5. Інформаційно-довідкова система LEX-EU. [Електронний ресурс] URL: https://eur-lex.europa.eu. Дата звернення: 09.05.2022
6. Інформаційно-довідкова системаUSCode. [Електронний ресурс] URL: https://uscode.house.gov. Дата звернення: 09.05.2022

Зубок Віталій Юрійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, д.т.н.,
vit@visti.net,

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

МОДЕРНІЗАЦІЯ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В ПЕРІОД ПІСЛЯВОЄННОЇ ВІДБУДОВИ

Після завершення активної фази бойових дій проти російських загарбників гостро постане питання відновлення об'єктів критичної інфраструктури та промислових виробництв України. Нагальним буде і питання вдосконалення їхньої безпеки, зокрема кібербезпеки.

Враховуючи, досвід кібератак на об'єкти критичної інформаційної інфраструктури України, головною метою кіберзахисту повинно стати забезпечення бесперебійного функціонування систем критичного призначення.

Для виконання цієї мети доцільно процесс кіберзахисту розглянути як сукупність технологій, фахівців та операційних процедур.

Технології виступають лише засобом автоматизації процедур та певною мірою доповнюють компетенції фахівців. Персонал повинен забезпечити ефективне використання технологій в рамках існуючих процедур. Процедури повинні враховувати законодавствоУкраїни, міжнародні стандарти та кращі практики з інформаційної безпеки та кіберзахисту. Самі процедури безпеки пропонується розділити за основними функціями кібербезпеки, зокрема такими як ідентифікація ризиків кібербезпеки, кіберзахист, виявлення кіберінцидентів, реагування на кіберінциденти, відновлення стану кібербезпеки [1].

Кожна з вищезазначенихфункцій включає в себе множину заходів кіберзахисту [2]. Таким чином постає питання критеріїв застосування цих заходів для конкретної системи. Такі критерії повинні бути застосовані на

принципах адекватності та ефективності. Зміст поняття адекватності полягає у оцінюванні критичності такої системи, а поняття ефективності – в можливості наявних організаційних та технічних засобів захисту протидіяти існуючим загрозам.

З метою реалізації такого підходу в рамках НДР «Случ» розроблено проєкт НД ТЗІ «Стандартні цільові профілі кіберзахисту автоматизованих систем управління технологічними процесами та вимоги до їх реалізації», де цільові профілі складаються з заходів кіберзахисту, що відповідають рівню негативного впливу [3] в разі порушення функціонування об’єкта критичної інфраструктури.

При застосуванні цих цільових профілів кіберзахисту необхідно враховувати рівень зрілостіпроцесівзабезпечення функціонування [4] систем критичного призначення, де вони впроваджуються.

Враховуючи наявний рівень зрілості, доцільним при оцінюванні ризиків є врахування часу на відновлення функціонування системи у разі виходу з ладу її компонентів, що не мають резервування.

Саме використання цільових профілів кіберзахисту дає можливість систематизувати наявні заходи з забезпечення безпеки, безперебійності функціонування систем критичного призначення.

Таким чином комплекс заходів з кіберзахисту може бути представлений як сума підмножин заходів (множин заходів кожного цільового профілю), а оцінка поточного стану кіберзахисту – як різниця множин цільового профілю і наявних заходів (наявного профілю).

Такий підхід дасть змогу гнучкого управління заходами безпеки з урахуванням змін рівня зрілості системи та оцінки ризиків на поточний момент часу. Зокрема зміни в функціонуванні системи впливатимуть на оцінювання ризиків, оцінка ризиків - на цільовий профіль, цільовий профіль – на поточну оцінку стану захищеності.

Вищевказані залежності можуть бути автоматизовані, використовуючи теорію множин. За такої автоматизації стане можливою більш точна

пріоритезаціяможливих векторів атак, що позитивно вплине на ефективність впроваджуваних заходів захисту.

До ряду питань, які потребують рішення, може належати питання про застосування цільового профілю до всієї системи, чи її критичних компонент. Застосування профілю до компонент систем може знизити витрати на впровадження заходів з кіберзахисту, але такий підхід може не враховувати ряд залежностей, чим спричинить значну кількість помилок при оцінюванні ризиків. Тому рекомендується для кожної системи оцінити допустимий час простою за рік і впроваджувані заходи з кіберзахисту спрямувати на недопущення перевищення цієї величини простою.

Резюмуючи вищезазначене наявність цільових профілів кіберзахисту систем критичного призначення є основою систематизації в управлінні безпекою цих систем. Наявна систематизація спрощує процедури оцінювання ризиків та визначення ефективності впроваджуваних засобів кіберзахисту. Наявні адекватні оцінки зрілості процесів забезпечення функціонування систем критичного призначення дають змогу гнучкого управління безпекою в умовах відновлення функціонування та модернізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Наказ Адміністрації Держспецзв’язку від 6 жовтня 2021 р. № 601 (у редакції наказу Адміністрації Держспецзв’язку від 12 жовтня 2021 року № 616).

2. Framework for Improving Critical Infrastructure Cybersecurity. Effectivefrom 2018-04-02. Officialedition. NIST, 2018. 55 p.

3. Постанова Кабінету Міністрів України «Деякі питання об’єктів критичної інфраструктури» від 09.10.2020 № 1109

4. COBIT 5 A business Framework for the Governance and Management of Enterprise IT.

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

КІБЕРЗАХИСТ ТА КІБЕРОБОРОНА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В умовах гібридної війни кіберпростір стає інформаційним полем боротьби для фахівців з IT, інформаційної та кібербезпеки. Перебої функціонування об'єктів критичної інфраструктури можуть спричинити значні втрати живої сили та технічного забезпечення наших військ. З початком спецоперації Росії також зросла активність кіберспільноти, що характеризується великою кількістю каналів Telegram, тематичних форумів, які налічують тисячі учасників. Така діяльність забезпечується кураторством держави агресора. Це продукує додаткові ризики для кіберпростору. Тому актуальним стає питання переходу від кіберзахисту до кібероборони або їх поєднання.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» під терміном «кібероборона» розуміється сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [1]. Водночас таке визначення не дає чіткого розуміння щодо механізмів реалізації вказаних заходів (процесів). Тобто на об'єкті критичної інфраструктури [2] (далі - ОКІ) на основі такого визначення не можуть бути розроблені операційні процедури з кібероборони. Проте наявними є операції з безпеки критичної інфраструктури, які спрямовані виключно на пасивний захист з пріоритетом недопущення несанкціонованого доступу до системи.

З метою уникнення невизначеності у даному питанні порівняємо компоненти кібероборони та кіберзахисту відповідно до визначень цих термінів у законодавстві (див. рис. 1).

Таке порівняння сприяє введенню додаткового терміну «система активного кіберзахисту (кібероборони)» з таким визначенням «сукупність апаратних та програмних засобів, заходів, методів та компетенцій обслуговуючого персоналу, що можуть бути задіяні як ресурс в активному кіберзахисті (кібероборонi)».

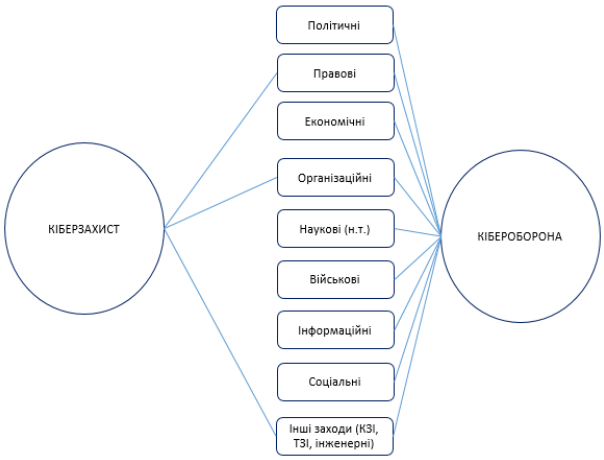

Рисунок 1 – Порівняння «кібероборони» та «кіберзахисту»

Особливістю кібероборони на відміну від кіберзахисту є наявність активної фази, де знайдені вразливості у власній системі повинні стати проекцією цілей у подібних системах противника. Таким чином в системах критичного призначення під час війни є важливою наявність процедур моніторингу стану системи, сканування мереж на вразливості, розгортання інфраструктури хибних цілей, постійного обміну інформацією з активними силами кібероборони.

Таким чином основним завданням кібероборони є забезпечення безперервності функцінування систем критичного призначення об’єктів критичної інфраструктури з використанням активних заходів протидії противнику.

Управління ризиками, як складова кіберзахисту, у такому контексті повинно враховувати окрім наявних ризиків порушення функціонування систем критичного призначення можливість дзеркальних активних дій противника в кіберпросторі щодо ОКІ України.

Враховуючи вищевказане, ефективність кібероборони першочергово

залежить від знань про вертикаль управління та центри прийняття рішень про кібератаки противника, зокрема ресурси противника (основні групи) в розвідці цілей, аналітиці пріоритетів та команди хакерів (червоної команди), однин з варіантів організації хакерського угрупування представлено на рисунку 2.

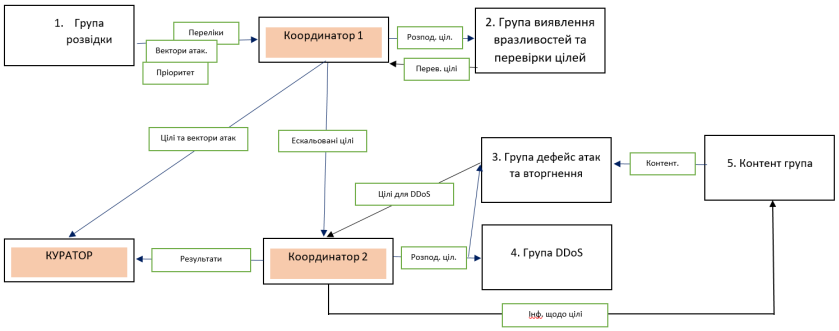

Рисунок 2 – варіант організації хакерського угрупування

Отже, розвиток кібероборони в напрямках розробки технічних рішень, операційних процедур, OSINT&HUMIN, механізмів обміну даними (вразливості активів, випадки атак на ланцюги поставок, управління патчами, моніторинг активності «Darkweb») та тактик активних дій, зокрема розробки векторів активних дій та тактик їх впровадження, враховуючи час, послідовність, дії щодо локалізації інциденту з боку противника тощо, що є необхідною складовою кіберзахисту систем критичного призначення в умовах війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про основні засади забезпечення кібербезпеки України". *Офіційний вебпортал парламенту України*. URL:https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.04.2022).

2. Закон України "Про критичну інфраструктуру". *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 17.04.2022).

Душабаєв Рустам Толкинбайович,
НТУУ «КПІ ім. Ігоря Сікорського»,
студент,
rustam.dushabaev@ gmail.com,

Чемерис Олександр Анатолійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора, д.т.н.,
a.a.chemeris@gmail.com

ВИКОРИСТАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ ОПТИМІЗАЦІЇ РОЗМІРУ ТАЙЛУ

Анотація. Розглядається метод розбиття вкладених циклів натайли та проблема пошуку оптимального розміру тайлу за допомогою генетичного алгоритму. Пропонується використання програмного пакету PLUTO, як інструменту для трансформації вкладених циклів. Даний пакет не запроваджує механізми для пошуку оптимальних розмірів тайлів. Приведено результати роботи системи, дев якості результатів роботи системи були представлені заміри часу виконання тестових програм до оптимізації та після. Програми були взяті на базіперевірочної колекції широко використовуваних алгоритмів різних класів PolyBench.

Annotation. The method of dividing nested loops into tiles and the problem of finding the optimal tile size using a genetic algorithm are considered. It is proposed to use the PLUTO software package as a tool for transforming nested loops. This package does not introduce mechanisms for finding the optimal tile size. The results of the system operation are given, where the results of the system operation time measurements of test programs before and after optimization were presented as the results of the system operation. The programs were taken on the basis of a test collection of widely used algorithms of different classes of PolyBench.

Компілятори, які використовують для підготовки програмного забезпечення, розвиваються та постійно покращують техніки оптимізації програмного коду. Однак, існуючі методи оптимізації не дають ідеального результату, а також, існує множина програм, що потребує додаткової оптимізації. До таких програм відносяться програми, в яких доцільне використання багатовимірних циклів. Такі програмні конструкції утворюють багатовимірний ітераційний простір, який представлено графом залежностей [1].Одним із методівоптимізації таких частин алгоритму є метод розбиття вкладених циклів на окремі, максимально незалежні частини-тайли.

Так як пошук оптимального розміру тайлу є NP повною задачею [2], то буде логічним використати певний нечіткий алгоритм. Авторами пропонується використати генетичний алгоритм.

Хромосомою буде виступати розмір тайлу. Кодування хромосоми було виконано вектором

$$size = (a_1, a_2, ..., a_n),$$

де n − це кількість вкладених циклів, тобто розмірність оператора циклу.

Процедуру схрещування представлено у вигляді комбінування відповідних компонент хромосоми за наступною формулою [3]:

$$a_i = l_i \cdot \lambda + r_i \cdot (1 - \lambda),$$

де a_i − i компонента вектору розміру тайлу, l_i, r_i − відповідна компонента векторів хромосом, що схрещуються, λ − коефіцієнт, що обирається виподковим чином, при чому $\lambda \in [0;1)$. Мутація міняє місцями дві випадкові компоненти.

Результати експериментів наведено на рис. 1. Проведені експерименти, при яких визначався час виконання програми і проводився аналіз швидкодії програм до та після тайлінгу з порівнянням запропонованого методу оптимізованого тайлінгу, показують значний приріст швидкодії виконання програм користувача. Так, з послідовною програмою прискорення складає 5.5 разів, а в порівнянні зі звичайним тайлінгом –1.5 рази.

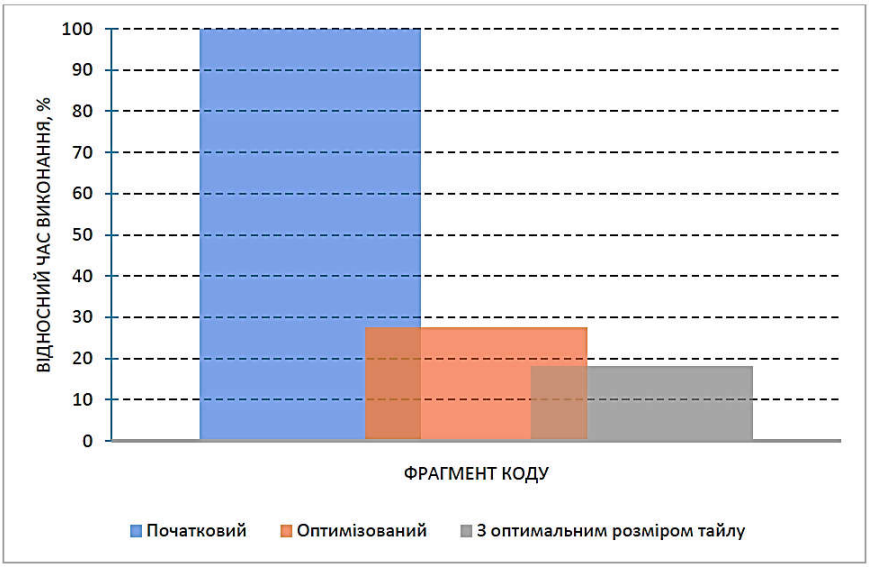

Рисунок 1 – Порівняння часу виконання фрагментів коду

Результати отримані в ході дослідження можуть використовуватися надалі у якості бази для подальших модифікацій та покращень методу розбиття на тайли.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. Петербург: БХВ-Петербург, 2002, 603 с. ISBN: 5-94157-160-7

2. Pierre Boulet, Jack Dongarra, Yves Robert, Frédéric Vivien. Tiling for Heterogeneous Computing Platforms. [Research Report] LIP RR-1998-08, Laboratoire de l'informatique du parallélisme. 1998,2+18p. ffhal-02102006

3. D. E. Goldberg. Genetic Algorithms in Search, Optimization, andMachine Learning. Addison Wesley, 1989 – 432 p.DOI:10.5860/choice.27-0936.

Коваленко Олексій Єпифанович,
Національний університет біоресурсів та природокористування України, професор, д.т.н.,
O.Kovalenko@nubip.edu.ua

ФОРМУВАННЯ СПРОМОЖНОСТЕЙ СИСТЕМ СИТУАЦІЙНОГО УПРАВЛІННЯ БЕЗПЕКОЮ

Анотація. Запропоновано узагальнену модель формування спроможностей кіберконвергентної системи безпеки організації на основі ситуаційного підходу.

Annotation. A generalized model of capability building of the organization 'scyberconvergent security system based on a situational approach is proposed.

Різноманітність та швидка зміна контексту безпеки середовища функціонування кіберконвергентних систем різного призначення обумовлює необхідність застосування в процесі їх функціонування ситуаційного управління. Кіберконвергентна система – це система (система систем), що поєднує в собі на час виконання цією системою (системою систем) свого функціонального призначення необхідні цифрові кібер-сутності з множиною сутностей в традиційних сферах (світах) на основі кібернатичних теорій і технологій, що охоплюють кіберпростір, кібербезпеку, кіберфізіку, кібер-інтелект, кібер-життя тощо.

Спроможності визначають здатність системи виконувати своє функціональне призначення та представляються уформальній моделі архітектури системи окремими сутностями або артефактами [1]. Поняття контексту безпеки широко застосовується у мовах програмування для формального представлення відношень між суб’єктами та об’єктами програми.

У контексті безпеки суб’єкт представляє джерело запиту до ресурсів. Суб'єкт — це сутність, яка отримує доступ до інформації про ресурси або може модифікувати ресурси. Суб’єктом може бути користувач, програма, процес, файл, комп’ютер, база даних тощо.

Узагальнення поняття контексту безпеки стосовно кіберконвергентних систем визначає відношення між кіберсутностями, що представляють суб'єкти системи та кіберсутностями, що представляють ресурси (об'єкти) системи. Суб'єкти системи можна поділити на суб'єкти-просьюмери та суб'єкти-супроводжувачі (суб'єкти-мейнтейнери). Управління контекстом безпеки здійснюється шляхом формуванні потрібних спроможностей у суб'єктів-супроводжувачів безпеки.

Архітектура складових систем кіберконвергентної системи визначається кортежем архітектурних артефактів:

$$A = \langle P, C, R, O, T, G, L, S \rangle,$$

де P – принципи побудови системи, C – модель спроможностей діяльності, R – плани розвитку (дорожня карта), O – оцінки управлінських рішень, T – еталонні технологічні моделі, G – настанови, інструкції, керівництва, L – архітектурні діаграми (ландшафт системи), S – проєктні рішення.

Відношення між артефактами утворюють архітектурну модель системи, яка поєднує в собі регламенти діяльності, структуру діяльності, напрями діяльності, технологічні стандарти, структури та рішення.

Моделі спроможностей діяльності (МСД) (карти спроможностей) надають компактні (на одній сторінці) структуровані представлення ("карти") усіх спроможностей організації, іноді разом з іншою допоміжною інформацією, як-от стратегія та цілі діяльності, коло зацікавлених суб'єктів (стейкхолдери) тощо. МСД, як правило, розробляються спільно архітекторами та керівниками організації, а потім «накладаються» на модель діяльності для визначення перспективних напрямів розвитку, визначення пріоритетів майбутніх витрат на технологічний розвиток та забезпечення узгодженості між новими технологіями та бажаними результатами цільової діяльності. МСД, як правило, є «точками входу» в технологічний процес ситуаційного управління для суб'єктів, що приймають рішення (керівних суб'єктів-супроводжувачів).

Процеси конвергенції у кіберконвергентних системах базуються на корисних спроможностях та принципах, досягнутих складовими кіберсутностями та технологіями системи. Процес ситуаційного управління можна розглядати як ланцюг створення вартості додаткової вартості інформації, а прийняті рішення представляються як інформаційний продукт у формі нових знань. Використання засобів і інструментів кіберсутностей для підтримки архітектурних артефактів забезпечує створення додаткової інформаційної цінності на різних етапах і фазах ситуаційного управління. Загалом процес ситуаційного управління описується як процес перетворення та збільшення цінності інформації на основі використання та конвергенції відповідних кіберсутностей.

Результат процесу ситуаційного управління системою безпеки можна розглядати як інформаційний продукт проектної діяльності. Модель знань цільової сфери застосування системи спрямовує діяльність створення інформаційного продукту процесу управління безпекою [2]. У моделі знань цільової сфери виділяються функції перетворення інформації, пов'язані з процесом ситуаційного управління та наданням чи забороною доступу до ресурсів.

Кожне перетворення інформації під час процесу ситуаційного управління надає певну додаткову цінність результуючій інформації, що акумулюється у вихідній інформації ситуаційного управління. Ці додані інформаційні цінності стосуються сутності відповідного етапу ситуаційного управління. На етапі обізнаності та оцінки ситуації додаткова цінність може бути пов'язана зі структуруванням, фільтрацією, уточненням даних про ситуацію в цільовій області. Крім того, це можуть бути метадані інформації про організацію та зберігання даних у системі ситуаційного управління. На етапі узагальнення та оцінки результатів ситуаційного управління це може бути інформація про ефективність та продуктивність процедур ситуаційного управління для конкретних випадків використання, зокрема щодо системи безпеки.

Висновки

Формування спроможностей системи і цілому та системи (підсистеми) безпеки базується на архітектурі системи. Система безпеки може бути як інтегрованою частиною цільової системи, так поєднана з цільовою системою на принципах конвергенції. Потреби щодо переліку спроможностей та вимоги до рівня їх забезпечення визначаються контекстом безпеки системи, що має ситуаційний характер та представляється як модель впливу ситуації на стан безпеки системи. Конвергентний підхід забезпечує гнучкість, масштабованість та можливості оптимізації системи безпеки відповідно до ситуаційного контексту безпеки. Для застосування конвергентного підходу застосовується модель знань цільової системи щодо виконання функціонального призначення з урахуванням ситуаційних впливів середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. KotusevS.EightEssentialEnterpriseArchitectureArtifacts. [Електронний ресурс] URL: http://www.bcs.org/content/conWebDoc/57318. Дата звернення: 05.05.2022.

2. Kovalenko O.E. Knowledge Based Design of Convergent Systems of Situational Management, Математичні машини і системи. 2019. № 3. – С. 67-74. DOI: 10.34121/1028-9763-2019-3-67-74.

Ковальчук Людмила Василівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, професор, д.т.н.,
lusi.kovalchuk@gmail.com

ПЕРЕВАГИ ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ В ЕНЕРГЕТИЦІ ТА ПРОБЛЕМИ, ЯКІ ПОТРІБНО ВИРІШИТИ ДЛЯ ЇХ ВИКОРИСТАННЯ

В сучасній літературі існує велика кількість різних визначень смартконтракту, при цьому кожне визначення підкреслює якісь певні його особливості, що є актуальними у відповідному контексті. Наведемо деякі з них.

Смарт-контракт (англ. *smart contract* — «розумний контракт»):

- різновид угоди в формі закодованих математичних алгоритмів, укладення, зміна, виконання і розірвання яких можливі лише з використанням комп'ютерних програм (блокчейн платформ) в рамках мережі Інтернет;

- набір обіцянок у цифровому форматі, включно з протоколами, за якими сторони виконують ці обіцянки;

- комп'ютеризований протокол транзакцій, який виконує умови контракту [1], [2];

- регулювання відносин сторін шляхом закріплення їх вираженої волі у формі певного коду, який придатний для зчитування комп'ютером.

Смартконтракт не є ні контрактом, ні «розумним» – це просто певний програмний код, що активується з особистого акаунта та має доступ до виконання функцій, які в ньому прописані. Він працює як детермінована програма, тобто виконує певні дії, якщо виконані певні умови (якщо … – то …)

Вважається, що вперше ідею старт-контрактів висловиви Нік Сабо у 1996 р. [3, 4], хоча незалежно від нього схожі ідеї також висловлювали також – Девід Чаум, Марк Міллєр. У своїх роботах він визначає старт-контракт як «цифрове подання набору зобов’язань між сторонами, яке містить протокол виконання цих зобов’язань» та зазначає, що «нові інституції і нові способи формалізації відносин цих інституцій стали можливі» завдяки використанню смартконтрактів.

Не зважаючи на те, що старт-контракти є дійсно зручним інструментом, вони на даний час не набули значного поширення на рівні державних органів – в першу чергу через те, що їх законодавчий статус не визначений. Так, єдиною країною, де старт-контракти визнані законодавчо, є Білорусь (2016) [5].

Смартконтракти можуть існувати тільки всередині певного середовища, що має безперешкодний доступ виконуваного коду до об'єктів розумного контракту. Найбільш розповсюдженим середовищем існування старт-контрактів є блокчейн. Смартконтракти на блокчейні – застосунок, середовищем існування якого є блокчейн. Вперше смарт-контракти були розроблені в блокчейні Ethereum (2013), співзасновником якого є засновник журналу Bitcoin Magazine Віталік Бутерін. Він висунув ідею універсальної децентралізованої блокчейн-платформи, в якій будь-хто бажаючий може програмно реалізувати різні системи зберігання та обробки інформації. Головна умова — дії повинні бути описані як математичні правила. [6]

Слід зазначити, що некоректно написаний старт-контракт може завдати суттєвих збитків. Так, у червні 2016 року на мережу Ethereum була виконана атака, внаслідок якої з різних гаманців було виведено близько 50 млн USD.

Для програмування старт-контрактів на даний час використовуються такі мови:

- Solidity (схожий на C або JavaScript);
- Vyper iSerpent (схожі на Python);
- LLL (низькорівнева версія Lisp);
- Mutan (заснований на Go).[7][8].

Ці мови дуже спрощені, але мають властивість повноти за Тьюрінгом. Це означає, що вони можуть реалізувати будь-яку логіку, яку можливо запрограмувати. В них є змінні, функції, умови, цикли, класи, наслідування.

Умови існування смартконтракту:

▪ можливість використання ЦП та асиметричного шифрування;

▪ існування відкритих, децентралізованих, доступних сторонам контракту баз даних, яким вони довіряють, для виконуваних транзакцій, робота яких повністю виключає людський фактор;

▪ децентралізація середовища виконання розумного контракту;

▪ правдивість джерела цифрових даних. [9]

Зі смарт-контрактом пов’язані наступні об’єкти:

- підписанти — сторони смартконтракту, які погоджуються з умовами або відмовляються від умов контракту з використанням електронних підписів;

- предмет договору – об'єкт, що знаходиться всередині середовища існування розумного контракту, або ж повинен забезпечуватися безперешкодний, прямий доступ розумного контракту до предмету договору без участі людини;

- умови повинні мати повний математичний опис, який можливо запрограмувати в середовищі існування розумного контракту;

- децентралізована платформа;

- об'єкти розумного контракту.

Зі смарт-контрактом пов’язані як мінімум два відкритих ключі підпису: ключ того, хто створив контракт, та ключ самого контракту. Активувати старт-контракт можна лише з особистого акаунта, але активований старт-контракт в процесі виконання може звертатись до іншого старт-контракту. Взагалі кажучи, змінити старт-контракт, який вже розміщено у блокчейні, неможливо. Проте, за певних умов, його можна знищити і створити новий – лише в тому випадку, якщо в ньому є функція SELFDESTRUCT.

Основні властивості СК:

Розподіленість. СК відтворені а розподілені по всім нодам. (= децентралізація).

Детермінованість. Виконують дії, які в них записані, у відповідності до домовленостей, які в низ записані. Результат завжди прогнозований.

Автономність. Можуть автоматизувати всі види задач, працюючи як самовоконувана програма. Якщо СК не активізований, то він нічого не виконує. Не можна змінювати умови СК після його розробки.

Незмінність. Неможна змінити процес роботи СК після його розробки та активації. Лише якщо він містить певну функцію, через яку можна робити певні зміни.

Відсутність довіри. Сторони можуть взаємодіяти за допомогою СК навіть не знаючи один одного.

Прозорість. Код СК доступний розміщено у БЧ і він доступний всім.

Економність. Не потрібні витрати на «бюрократизацію».

Однією з **основних переваг** смартконтракту є можливість взаємодіяти в умовах повної недовіри і без посередників (невиконання умов анулює контракт).

Недоліки смартконтракту:

- можливі помилки – людський фактор (як було у ETH)

- невизначений юридичний статус (ускладнюється анонімністю, відсутністю посередників)

- не є універсальними; у певних випадках «класичні» договори зручніші.

- оплата за транзакцію, що містить/активує смартконтракт (газ)

Смарт-контракти на платформі блокчейн для розрахунків в електроенергетиці, у порівнянні з "класичними" контрактами, мають такі переваги:

- швидкі розрахунки за фактом споживання;

- зручний вибір трафіку;

- відсутність боржників;

- відмова від послуг посередників (зниження ціни за електроенергію на 5-10%).

Такі старт-контракти створюється за ініціативою однієї із сторін (споживач, мережа, генерація) і укладаються після погодження деталей.

Мета/очікування:

• зниження витрат при розрахунках за рахунок відмови від посередників;

• підвищення гнучкості пропозицій пи виборі тарифу та схеми оплати;

• підвищення ролі рядових споживачів у плануванні обсягів споживання;

• можливість закупок безпосередньо у виробників;

• захист учасників від навмисних маніпуляцій показниками засобів обліку;

• захист мережевих та генеруючи компаній від банкрутства компаній-продавців;

• захист споживачів від недостовірних даних стосовно відключень.

DTEK стосовно застосування старт-контрактів:

В рамках комплексного підходу «3D» (Decarbonization, Decentralization, Digitalization), для укладання *P2P*-контрактів у галузі зеленої енергетики.

Peer-to-peer, p2p **(англ. – рівний до рівного)** - варіант архітектури системи, в основі якої лежить мережа рівноправних вузлів.

Очікування від введення смартконтрактів – дозволять використовувати p2p схему, що призведе до:

- спрощення многорівневої системи, що складається з виробників електроенергії, операторів розподільних мереж, операторів оптових розрахунків, трейдерів та споживачів.

- всі транзакції – через Інтернет;

- електроенергія стане дешевшою;

- за рахунок p2p, будуть мінімізовані втрати при передачі на великі відстані (зараз - 11%, як в бідних країнах; найнижчі – 2-3%, Тринідід і Тобаго, за рахунок відсутньої передачі на великі відстані).

Перша спроба використання p2p контрактів: Бруклін, 2016, продажа «зеленої» енергії сусіду.

За один рік різні компанії (LO3 Energy, Siemens, …) вклали у цю сферу більше за $ 300 млн.

Світові тренди P2P-технологій:

- форум BlockchainEnergyAsia в Сінгапурі;

- велика кількість азіатських блокчейн-проектів в енергетиці;

- P2P ринки електроенергії;

- в Японії запустили найбільший кластер розподілених систем накопичення енергії, що керується штучним інтелектом (більше 3500 домогосподарств), мета – розвантаження державної енергосистеми.

Проблеми на шляху розвитку P2P та СК у енергетиці:

• відсутність тенологічної бази у вигляді сонячних панелей, вітроустановок, накопичувачів енергії;

• невизначений статус всієї криптоіндустрії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Tapscott, Don; Tapscott, Alex (May 2016). *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World* (https://archive.org/details/blockch ainrevolu0000taps). с. 72 (https://archive.org/details/blockchainrevolu0000taps/page/72), 83, 101, 127. ISBN 978-0670069972.

2. https://medium.com/blockchain-hub/to-fork-of-not-to-fork-a9b077718fe3#.xk7ojtacq (https://web.archive.org/web/20170117004456/https://medium.com/blockchain-hub/to-fork-of-not-to-fork-a9b077718fe3#.xk7ojtacq). Архів оригіналу (https://medium.com/blockchain-hub/to-fork-of-not-to-fork-a9b077718fe3#.xk7ojtacq) за 17 січня 2017.

3. Nick Szabo - Smart Contracts: Building Blocks for Digital Markets (https://web.archive.org/web/20180427165653/http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html). www.fon.hum.uva.nl.

Архів оригіналу (http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/L

OTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html) за 27 квітня 2018. Процитовано 29 липня 2017.

4. Nick Szabo. Formalizing and Securing Relationships on Public Networks (https://web.archive.org/web/20170204014018/http://firstmonday.org/ojs/index.php/fm/article/view/548/469). First Monday. Архів оригіналу (http://firstmonday.org/ojs/index.php/fm/article/view/548/469) за 4 лютого 2017. Процитовано 10 грудня 2016.

5. Беларусь первой в мире законодательно закрепила smart-контракт (https://www.belta.by/economics/view/belarus-pervoj-v-mire-zakonodatelno-zakrepila-smart-kontrakt-281784-2017/)

6. Создатель Ethereum Виталик Бутерин: «Блокчейн поможет искоренить коррупцию» (https://web.archive.org/web/20180220033328/https://incrussia.ru/blockchain/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/). Архів оригіналу (https://incrussia.ru/blockchain/sozdatel-ethereum-vitalik-buterin-blokcheyn-pomozhet-iskorenit-korruptsiyu/) за 20 лютого 2018.

7. Руководства, ресурсы и инструменты для разработчиков на Ethereum (https://web.archive.org/web/20211023131023/https://ethereum.org/ru/developers/#smart-contract-languages). Архів оригіналу (https://ethereum.org/ru/developers/#smart-contract-languages) за 23 жовтня 2021. Процитовано 23 жовтня 2021.

8. *Chris Dannen* ntroducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners.

9. Смарт-контракты: как использовать и насколько надежны для сделок (https://cryptonet.biz/ru/smart-kontrakty-kak-ispolzovat-i-naskolko-nadezhny-dlya-sdelok/).

Митько Лідія Олексіївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.ф.-м.н.,
lmitko@ukr.net

ЛЮДСЬКИЙ ФАКТОР У ПРОБЛЕМІ КІБЕРБЕЗПЕКИ ЕНЕРГЕТИЧНИХ ОБ'ЄКТІВ

Анотація. При забезпеченні кібернетичної безпеки енергетичних об'єктів важливу роль відіграє персонал, який задіяний на цих об'єктах. Тому відповідне матеріальне і психологічне забезпечення працівників, підвищення їх кваліфікації є запорукою стабільної роботи обладнання та програмних засобів, що супроводжують функціонування об'єктів енергетики.

Annotation. The personnel involved in the cyber security of energy facilities play an important role. Therefore, the appropriate material and psychological support of employees, their training is the key to stable operation of equipment and software that accompany the operation of energy facilities.

В енергетичній галузі, яка з кожним роком стає більш складною, взаємозалежною та динамічною, постійно з'являються все нові проблеми інформаційної безпеки енергетичних об'єктів в різних сегментах енергетики. Кібербезпека відіграє важливу роль у підвищенні ефективності технологічних процесів, оскільки відмова обладнання робочих систем знижує надійність, безперебійність виробітку та розподілу енергетичних ресурсів. Основним завданням кібербезпеки на конкретному енергетичному об'єкті стає проведення аналізу по вразливості всередині його та проведення контролю доступу, обліку та інформаційної безпеки на об'єкті. Якщо говорити про технологічні об'єкти, слід враховувати специфіку АСУ ТП (автоматизованих систем управління технологічним процесом), SCADA (Диспетчерське управління та збір даних), а також РСУ (розподіленої системи управління). При побудові системи забезпечення інформаційної безпеки необхідно ретельно вивчити об'єкт захисту та самі технологічні процеси та враховувати безліч можливих факторів.

Кіберзлочини, як правило, діляться на 4 етапи: 1) підготовка до кібератаки; 2) проникнення у систему; 3) поширення в системі; 4) нанесення шкоди. Для захисту від кібератакстворюються нові, постійновдосконалюються існуючі технічні та програмні засоби, що виконують комунікаційні функції на цифрових підстанціях, а також застосовуються спеціальні технічні та програмні засоби, щознижують ймовірність атаки ззовні та наслідки від можливих невиявлених помилок у програмному забезпеченні. Але ключовою проблемою кібербезпеки є те, що один і той самий пристрій, програмне забезпечення може бути налаштовано так, щоб забезпечувати кібербезпеку і не допускати кібератаки, а може сприяти кібератакам. Зовнішній вигляд пристроїв при цьому не змінюється, проте їхня функціональність у частині кібербезпеки принципово різна. Відмінність виключно в налаштуваннях, причому може відрізнятися лише незначною кількістю параметрів, а в тисячах параметрів не відрізнятись. Дилетант у питаннях кібербезпеки взагалі зможе виявити проблему шляхом якихось періодичних оглядів устаткування. Тому потрібно залучення спеціально навчених фахівців, які здатні вирішувати подібні завдання. Ймовірність цілеспрямованих кібератак залежить головним чином від двох складових: вартості послуг злому і масштабів наслідків. Чим вище негативний масштаб наслідків, тим більшу ціну буде готовий заплатити потенційний замовник кібератаки. При величезних цінах на "послуги злому" вирішальну роль відіграє лише лояльність фахівців. Відповідно, масштаб наслідків, по суті, і визначає ймовірність серйозної кібератаки. Тому найважливішою вимогою до фахівця з кібербезпеки є вимога правильного та сумлінного виконання своїх обов'язків. Проте, враховуючи масштаб наслідків, а також те, що зацікавленими сторонами в кібератаці можуть бути іноземні держави, на перший план виходять питання політичної та бізнесової лояльності, патріотизму, ефективності спецслужб тощо.

Основним завданням для кіберзахисту енергетичних об’єктів повинна стати постійна робота з персоналом, в рамках якої повинні виконуватись наступні заходи: 1) перешкоджання персоналу завантажувати невідомі файли із

сторонніх ресурсів; 2) створення планів з проведення інформаційно-роз'яснювальної роботи з кібербезпеки енергетичних об’єктів; 3) щоденна перевірка журналів обліку з нестабільної роботи комп'ютерів та SCADA систем. І одним із важливих заходів є матеріальне забезпечення працівників, яке б стимулювало їх до сумлінної роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.https://www.bdew.de/media/documents/Pub_20190226_Cybersicherheit-Faktor-Mensch.pdf

2. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1553779410177&uri=CELEX:52013JC0001

Остапченко Костянтин Борисович,
НТУУ «КПІ ім. Ігоря Сікорського»,
доцент, к.т.н.,
okb2003@ukr.net,

Євдокімов Володимир Анатолійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, к.н. з держ. упр.,
ievdokimov40@gmail.com**,**

Борукаєв Зелімхан Харитонович,
ІПМЕ ім. Г.Є. Пухова НАН України,
завідуючий лабораторією., д.т.н.,
zelimh1948@gmail.com

ІНТЕРФЕЙС ВЗАЄМОДІЇ З БАЗОЮ ДАНИХ «МОДЕЛІ ПРОЦЕСІВ ФУНКЦІОНУВАННЯ РИНКУ ЕЛЕКТРИЧНОЇ ЕНЕРГІЇ»

Анотація. У роботі дано опис особливостей інтерфейсу взаємодії користувача з базою даних «Моделі процесів функціонування ринку електричної енергії».

Annotation. The description of the features of the interface for interfacing with the data base «Models of processes for the functioning of the electricity market» is given.

Вступ. База даних «Моделі процесів функціонування ринку електричної енергії» призначена для автоматизації наступних процесів:

- збирання, накопичення та візуалізації інформації про процеси функціонування ринку електроенергії у зручній єдиній формі для різних його суб'єктів - виробників, постачальників, споживачів, підприємств системи передачі електроенергії та диспетчерського управління задля здійснення зрівняльного аналітичного аналізу цін та тарифів;
- зберігання оперативних даних кінцевих споживачів ринку електроенергії з урахуванням регіону постачання та класу напруги мереж до яких підключений споживач задля забезпечення підвищення точності та

актуальності даних про процеси функціонування ринку електроенергії при проведенні моделюючих розрахунків для всіх користувачів системи.

Відмітною особливістю бази даних «Моделі процесів функціонування ринку електричної енергії» є застосування об’єктного підходу до моделювання сутностей предметної області об’єкта автоматизації, що надає можливості уніфікувати подання різних суб’єктів ринку електроенергії, адаптування до можливих змін у процесах його функціонування та створення єдиних засобів взаємодії різних користувачів інформаційно-моделюючої системи аналізу процесів лібералізованого ринку електроенергії. В насідок такої особливості до створення бази даних розроблювана на її основі інформаційна система набуває рис не проблемно-орієнтованої, а функціонально-орієнтованої системи, що надає можливості її застосування у прийнятті організаційних управлінських рішень в широких галузях використання.

1. Інтерфейс взаємодії з базою даних

Примірник Бази даних «Моделі процесів функціонування ринку електричної енергії» розроблений і створений в системі управління базою даних (СУБД) Oracle. Для доступу і використання Бази даних використано інтегрований інструментальний засіб проектування і адміністрування базою даних Oracle SQL Developer [1].

Oracle SQL Developer -це графічний інструмент для розробки баз даних. За допомогою SQL Developer можна переглядати об'єкти бази даних, запускати SQL-команди, редагувати і налагоджувати PL/SQL-програми. SQL Developer підвищує продуктивність і спрощує підтримку користувацької бази даних при виконанні завдань з її розвитку. SQL Developer може підключатися до будь-якої СУБД Oracle від версії 9.2.0.1 і може працювати в середовищі Windows, Linux, Mac OSX.

Кожному користувачеві БД обов'язково необхідно отримати від адміністратора БД логін і пароль та знати налаштування параметрів з’єднання з сервером СУБД Oracle.

Для початку роботи з базою даних необхідно створити нове з'єднання. Для цього виберіть в головному меню програми пункт File / New. У діалоговому вікні виберіть пункт DatabaseConnection і натисніть Ok.

Відкриється діалогове вікно New / SelectDatabaseConnection (рис. 1).

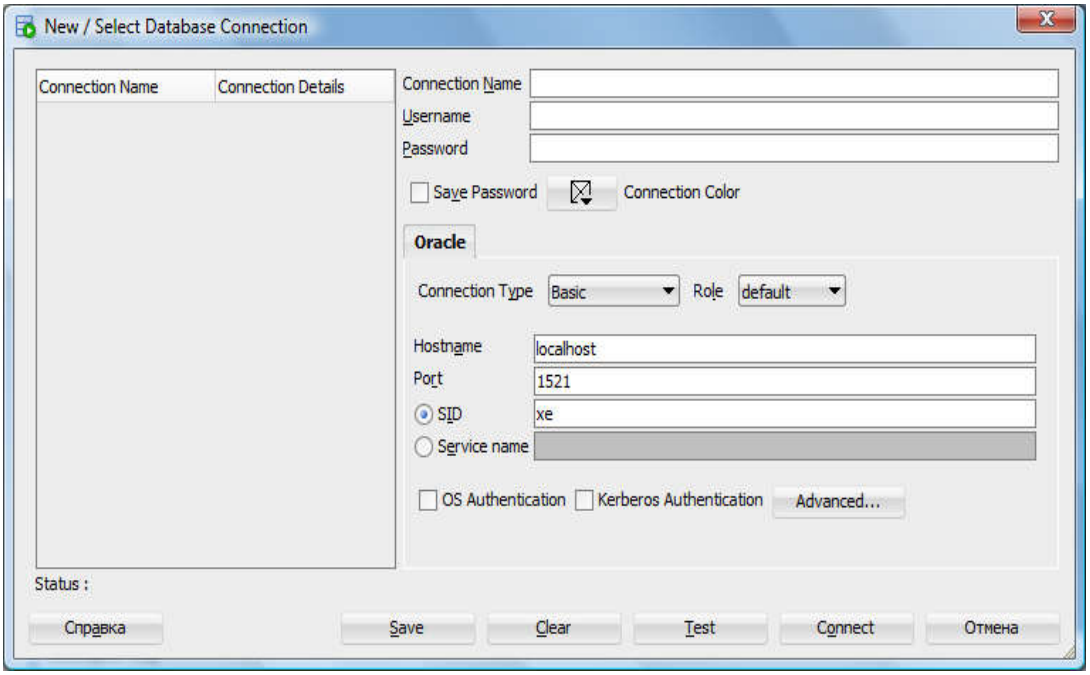

Рисунок 1 - Вікно створення нового з‘єднання з базою даних

Спочатку налаштовується підключення до бази даних. Для цього вводиться в поля ConnectionName назву з'єднання, ім'я користувача і пароль (пароль можна не вводити в разі, якщо з цим підключенням буде працювати кілька користувачів). Потім встановлюєтьсяConnectionType - Basic, Hostname - адреса або ім'я машини, де працює база даних, Servicename - ім'я бази даних і натисніть Save.

Підключення до бази даних відбувається шляхом вибору в лівій навігаційній панелі головний екран додатка необхідного з‘єднання та введення імені користувача і його паролю. В разі успішного підключення створюється робоче вікно поточного з‘єднання під обраною назвою (рис. 2).

Вікно Oracle SQL Developer зазвичай використовує ліву навігаційну частину для пошуку і вибору об'єктів, праву частину для відображення інформації про вибрані об'єкти та головне меню з панеллю інструментів.

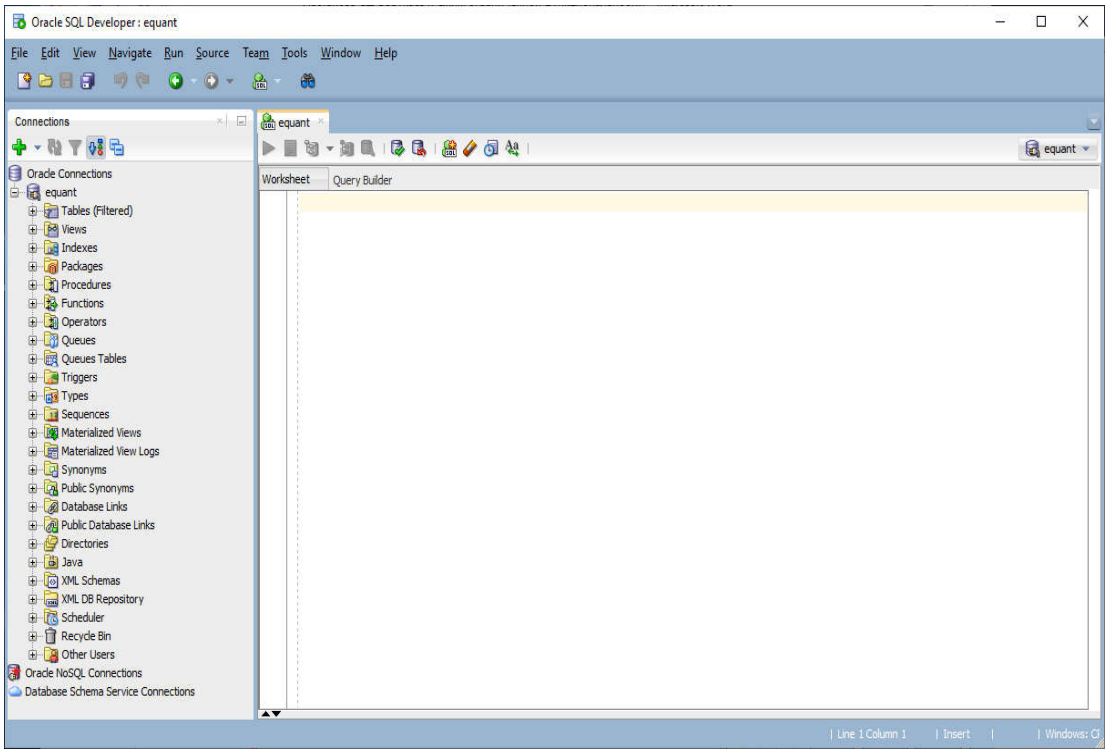

Рисунок 2 - Робоче вікно підключення до бази даних

Основна панель інструментів (розташована під головним меню) містить піктограми для виконання різних дій, які за замовчуванням включають наступне:

1) New - створює об’єкт бази даних;

2) Open - відкриває файл;

3) Save - зберігає будь-які зміни в обраному на даний момент об'єкті;

4) SaveAll - зберігає будь-які зміни на всіх відкритих об'єктах;

5) Back - переходить до області, яку відвідану останньою;

6) Forward - переміщується до області після поточної у списку відвіданих панелей.

7) Open SQL Worksheet - відкриває робочий лист редактора команд SQL. Якщо не використовувати стрілку спадаючого меню, щоб вказати підключення до бази даних, яке потрібно використовувати, буде запропоновано вибрати з'єднання.

Ліва частина вікна Oracle SQL Developer містить навігаційні панелі, зокрема панель підключень Connections, піктограми для виконання дій та

ієрархічне відображення дерева для поточної навігаційної панелі (рис. 3). Будь-які інші навігатори можуть бути обрані з пункту головного меню View, наприклад, панель звітів Reports.

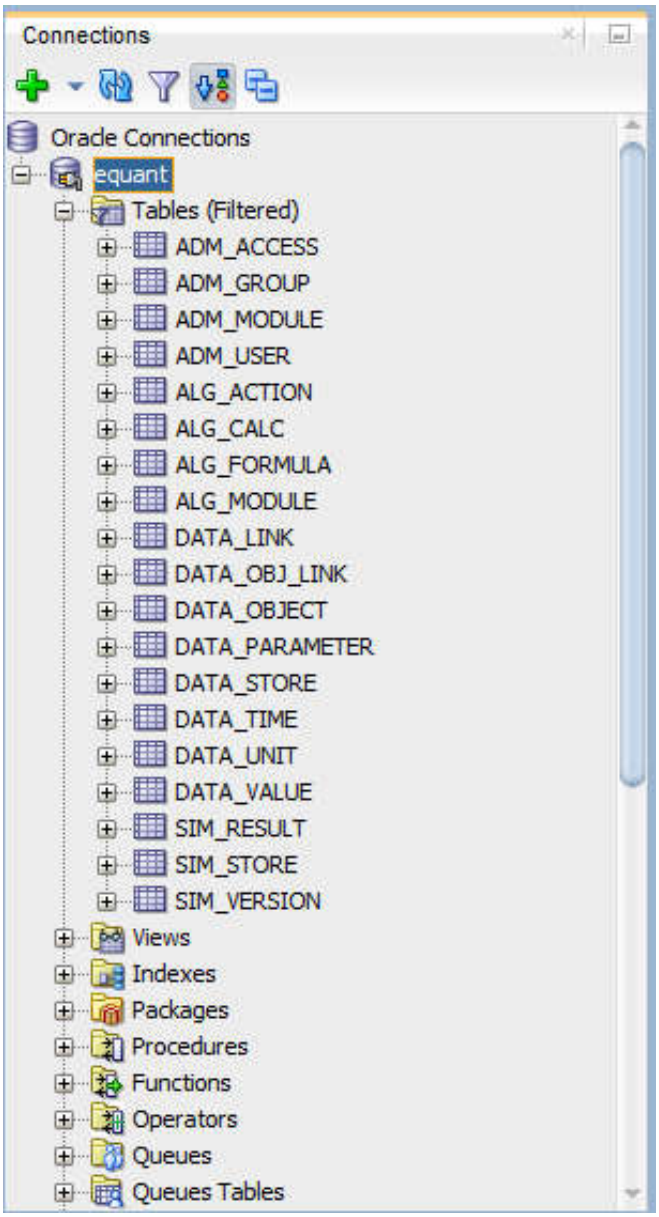

Рисунок 3 - Навігаційна панель Connections

У правій частині вікна Oracle SQL Developer є вкладки та панелі для вибраних або відкритих об'єктів, як показано на рис. 4, де відображається інформація про таблицю з назвою DATA_PARAMETER. Якщо тримати вказівник миші на назві вкладки, то відображається підказка про власника об'єкта та з'єднання з базою даних.

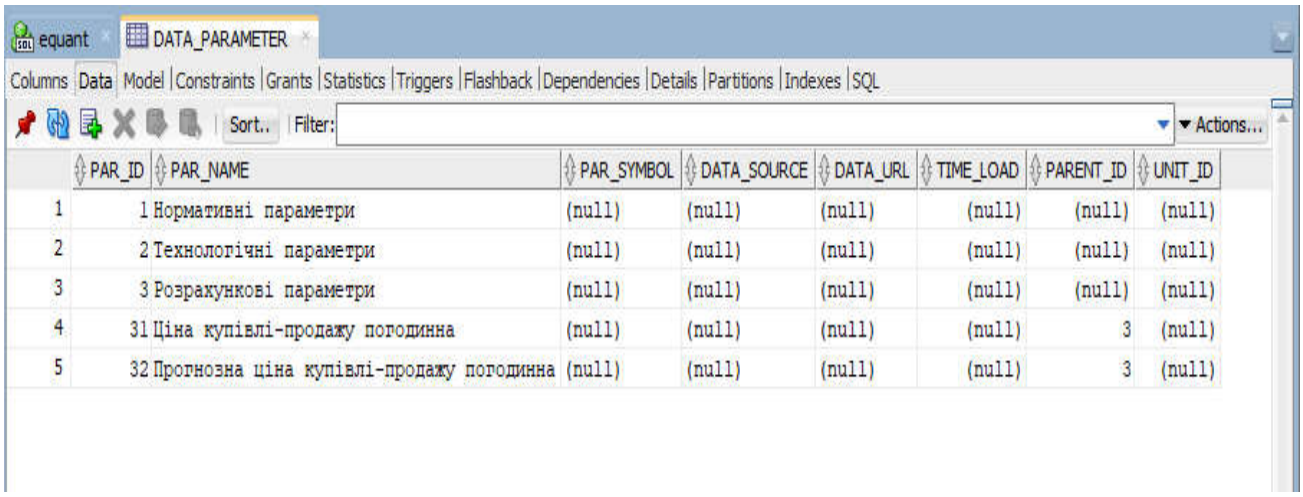

Рисунок 4 - Інформаційне вікно панелей обраного об‘єкта бази даних

Для таблиць і представлень ця інформація згрупована під вкладками, які позначені вгорі. Наприклад, для таблиць вкладки - стовпці, дані (для перегляду та зміни самих даних), індекси, обмеження тощо; і можна натиснути заголовок стовпця під вкладкою, щоб сортувати рядки сітки за значеннями в цьому стовпці. Для більшості об'єктів вкладки включають SQL, який відображає оператор SQL для створення об'єкта.

Мовою взаємодії з базою даних є мова SQL та основні її команди маніпулювання insert, update, delete та формування запитів select, які забезпечують режими функціонування бази даних.

2. Режими функціонування БД

У даній версії передбачено наступні основні режими функціонування Бази даних, які пов’язані з виконанням основних операцій над потоками даних: введення даних, зміна/видалення даних, пошук та фільтрація даних, запитування агрегованих даних для формування аналітичної інформації для звітів.

2.1. Введення даних до об’єктів бази виконується командою insert або за допомогою інтерфейсу роботи з даними обраного об’єкта (рис. 5).

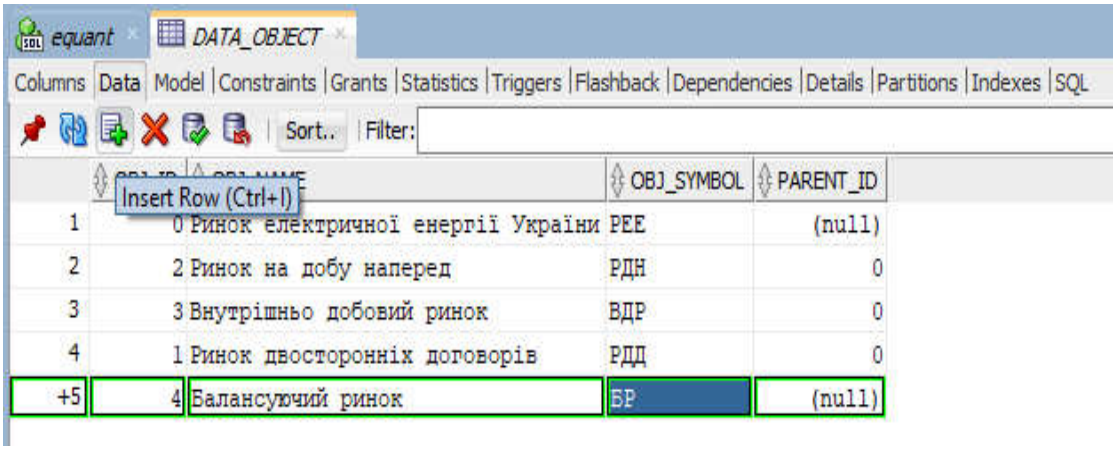

Рисунок 5 – Додавання даних до об’єкта бази даних

Приклад команди введення даних до об’єкту:

Insertinto DATA_OBJECT (OBJ_ID,OBJ_NAME,OBJ_SYMBOL,PARENT_ID) values (4,'Балансуючий ринок','БР',null);

Зміна/видалення даних до об’єктів бази виконується командою uodate/delete або за допомогою інтерфейсу роботи з даними обраного об’єкта (рис. 6 та 7).

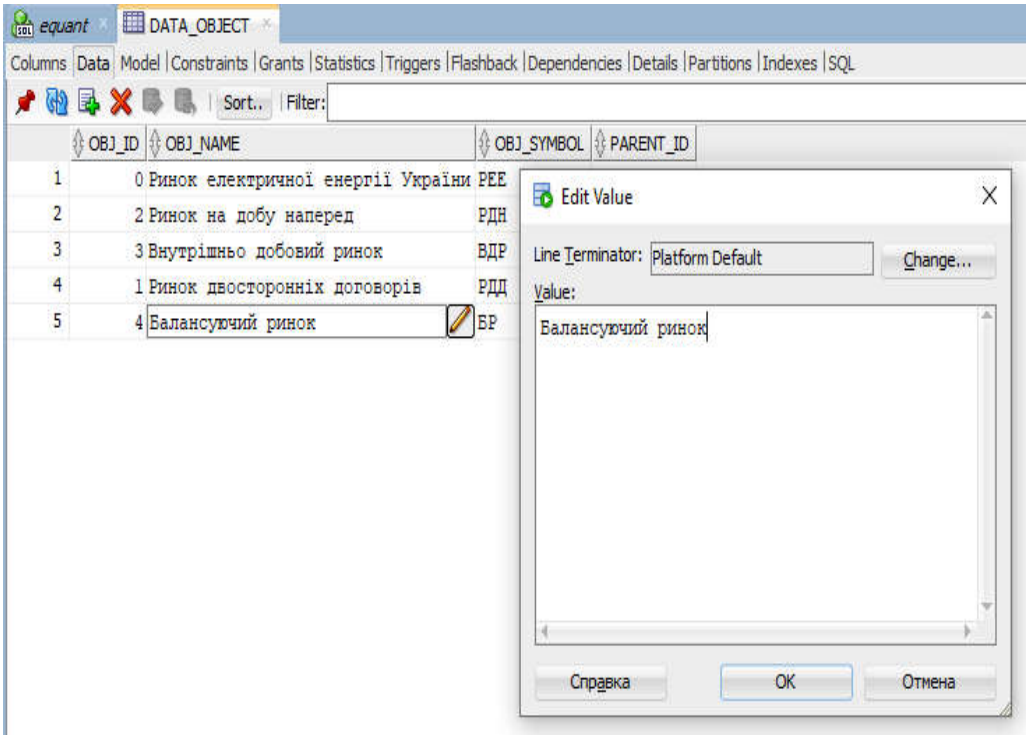

Рисунок 6 – Редагування даних до об’єкта бази даних

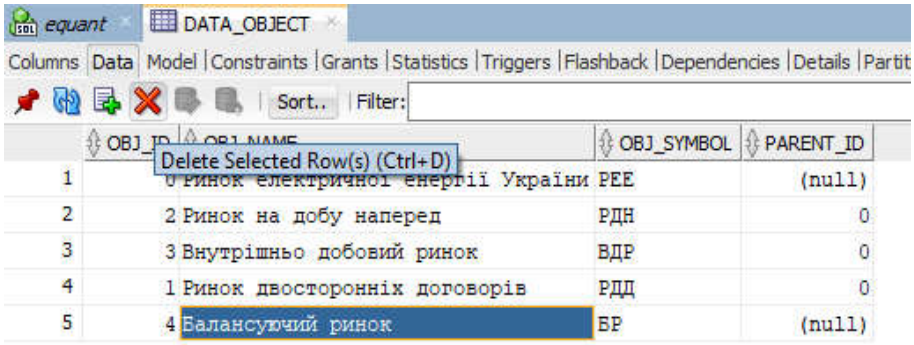

Рисунок 7 – Видалення даних з об’єкта бази даних

Приклад команди зміни (редагування) даних об’єкта:

Upate DATA_OBJECT set OBJ_NAME='Балансуючий ринок' where OBJ_ID =4;

Приклад команди видалення даних з об’єкту:

Deletefrom DATA_OBJECT where OBJ_ID=4;

2.3. Пошук та фільтрація даних виконується командою select або за допомогою інтерфейсу роботи з даними обраного об’єкта (рис. 8).

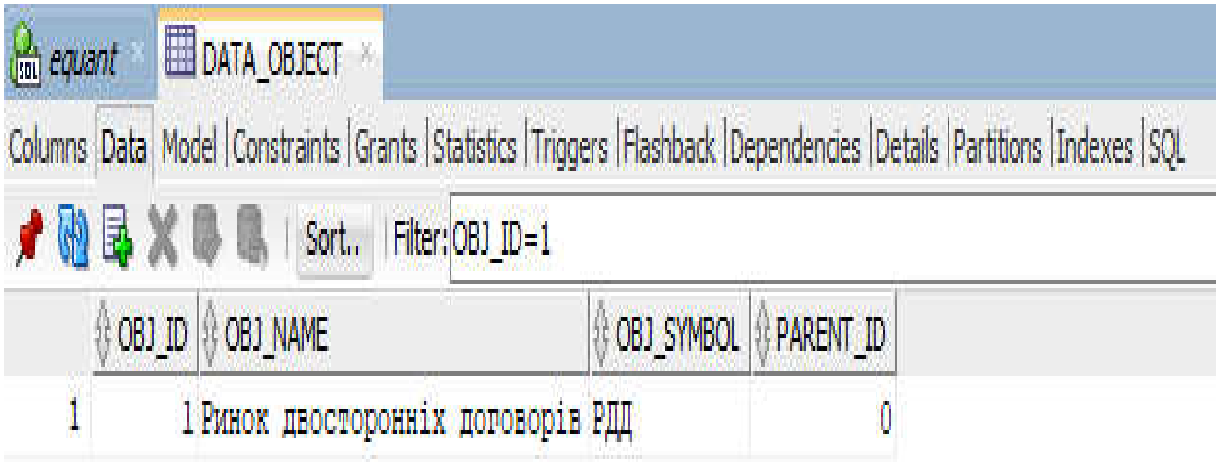

Рисунок 8 – Пошук даних об’єкта бази даних

Приклад виконання пошуку даних командою select у вікні-листі SQL Worksheet з результатами у табличній формі наведено на рис. 9.

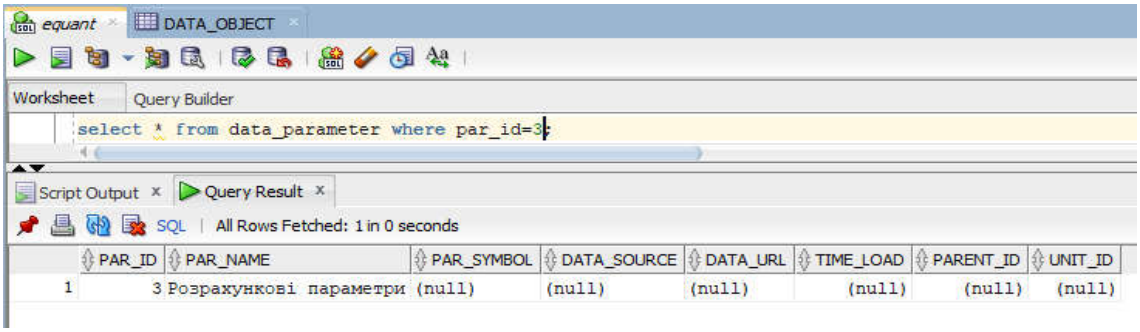

Рисунок 9 – Пошук даних командою select

Приклад виконання фільтрації даних (за умови співпадіння) командою select у вікні-листі SQL Worksheet з результатами у табличній формі наведено на рис. 10.

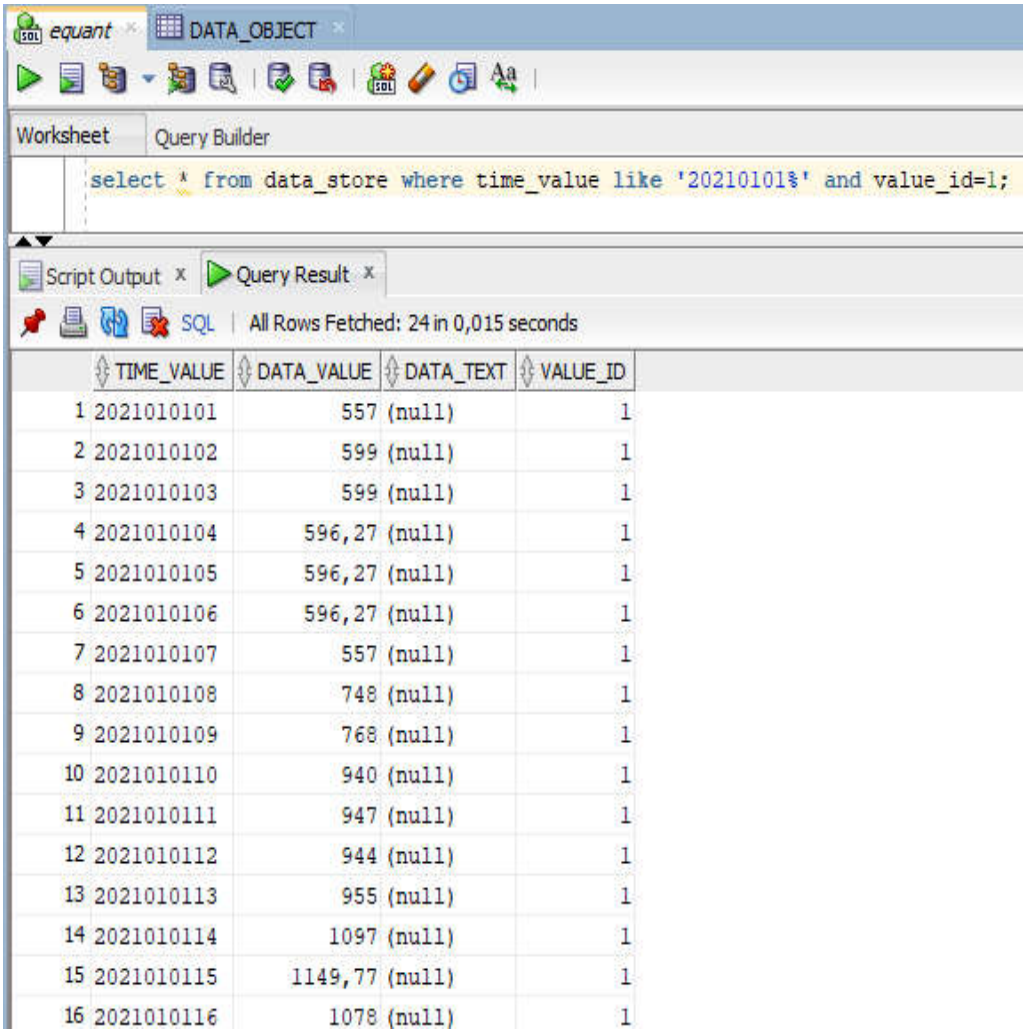

Рисунок 10 – Фільтрація даних командою select

2.4. Запитування агрегованих даних для формування аналітичної інформації для звітів виконується командою select з опцією групування даних groupby у вікні-листі SQL Worksheet з результатами у табличній формі (рис. 11).

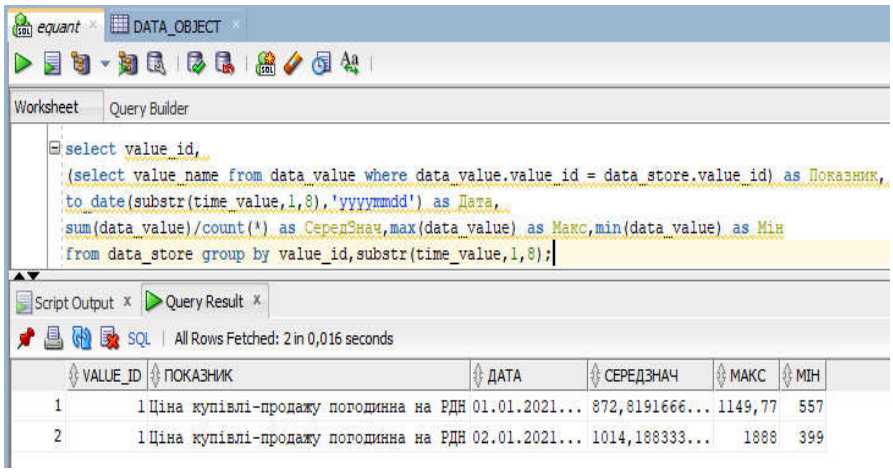

Рисунок 11 – Запит агрегованих даних

2.5. Експорт інформації. Експорт інформації може бути обраний через меню Actions (рис. 4) панелі інструментів інтерфейсу роботи з даними обраного об’єкта. Експорт можливий для наступних форматів: json, text, xml або у форматі команди insert.

База даних в подальшому підлягає вдосконаленню за рахунок розширення функцій з візуалізації аналітичних даних та завантаження даних із зовнішніх інформаційних систем.

Роботу виконано за держбюджетною темою «Розроблення системи моделювання ОЕС України з великими частками обсягів виробництва електроенергії енергоблоками АЕС та енергетичними установками, щовикористовують ВДЕ» (шифр: Модель ОЕСУ). КПКВК 6541230.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. https://www.oracle.com/cis/database/technologies/appdev/sqldeveloper-landing.html

Огір Олена Олександрівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
науковий співробітник, к.т.н.,
lenaogir@gmail.com,

Цуркан Оксана Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
otsurkan24@gmail.com

КІБЕРБЕЗПЕКА ТА СТІЙКІСТЬ ОБ'ЄКТІВ ЕНЕРГЕТИЧНОГО СЕКТОРУ В СУСПІЛЬСТВІ ТА ДЕРЖАВІ В ЗВИЧАЙНИХ, КРИТИЧНИХ І НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Сучасне суспільство практично повністю залежить від стану захищеності інформації та кіберінфраструктури у всіх сферах життєдіяльності людини. Можливість використовувати як інформаційні, так і кібертехнології, і навіть інформаційно-комунікаційні мережі задля досягнення своєї мети, мають як державні структури країни, так і кримінальні та терористичні організації. У зв'язку з цим забезпечення кібер- та інформаційної безпеки критично важливої інфраструктури держави стало вирішальною умовою забезпечення обороноздатності держави, зокрема в умовах війни з Росією.

ІПМЕ ім. Г.Є. Пухова НАН України в рамках проекту «ЕЛЕКТРОН» здійснює проведення первинної державної експертизи комплексної системи захисту інформації в автоматизованих системах та на об'єктах критичної інфраструктури, також оцінку інформаційної безпеки в автоматизованих системах та перевірку ефективності, підтримку комплексів та систем захисту інформації від несанкціонованого доступу на об'єктах енергетики. Кібербезпека та стійкість об'єктів енергетичного сектора характеризує ступінь виконання енергетичними комплексами їх функцій у суспільстві та державі у звичайних, критичних та надзвичайних обставинах. Підприємства та установи енергетичного сектора України відіграють провідну роль у розвитку та функціонуванні держави. Промисловість залишається основним споживачем

електроенергії, хоча її частка у загальному споживанні електроенергії у світі знижується. У промисловості електроенергія використовується для приведення в дію різних механізмів та технологічних процесів. На сьогоднішній день коефіцієнт електрифікації силового приводу у промисловості становить 80%. Об'єкти енергетичного сектора є стратегічно важливими та повинні безперервно функціонувати та забезпечувати надання якісних послуг [1, 2].

Як показав аналіз, проведений у ході першого етапу роботи над проектом «ЕЛЕКТРОН», основні кібератаки об’єктів інфраструктури розрізняються за своїми наслідками та способами впливу. Атаки на енергокомпанії в 2015 році не були повністю самоорганізованими. Проте у 2016 році шкідливі програми вже передбачали самоорганізацію дій у процесі атак та стали більш працездатними.Також, проведені дослідження дали можливість констатувати, що програмне забезпечення CrashOverride здатне фізично руйнувати енергосистеми. CrashOverride має можливість відправляти команди в електромережу на увімкнення або вимкнення живлення. За їх даними, CrashOverride може використовувати відому вразливість обладнання Siemens, зокрема цифрового реле Siprotec. Такі реле встановлюються для захисту та управління розподільними та передаючими електромережами. Фахівець з американської компанії з кібербезпеки SANS Institute встановив, що відключення цифрового реле може призвести до теплового навантаження електромережі. Таким чином, CrashOverride може забезпечити спланову атаку на кілька критичних вузлів енергетичного комплексу, що може призвестидо відключення електроенергії у всій державі, оскільки навантаження переміщується з одного регіону в інший [3].

У грудні 2015 року було зафіксовано підвищену постійну загрозу (APT) в автоматизованій системі управління енергосистемою. Атаку зазнали внутрішні мережі української енергокомпанії Прикарпаттяобленерго [4]. Було зупинено 30 підстанцій. Близько 230 тисяч громадян втратили енергопостачання на термін від однієї до шести годин. В ході атаки використовувалося шкідливе програмне забезпечення BlackEnergy. Група

BlackEnergy розпочала атаку на українську електромережу за допомогою сімейства ПЗ BlackEnergy та KillDisk. Після атаки з'ясувалося, що група BlackEnergy складається як мінімум із двох підгруп – TleBots та GrayEnergy.Зокрема, у грудні 2016 року команда GreyEnergy розробила черв'яка, схожого на NotPetya, а пізніше ще більш просунута версія цієї шкідливої програми використовувалася групою TleBots під час атаки у червні 2017 року. GreyEnergy має ширші цілі, ніж група TleBots. GreyEnergy насамперед цікавиться промисловими мережами різних організацій, які відповідають за критичну інфраструктуру, і, на відміну від TleBots, група GreyEnergy не обмежується лише Україною [4].

Виходячи з вищесказаного, очевидно, що однією з першочергових проблем забезпечення кібербезпеки критично важливих об'єктів енергетики та енергетичних систем загалом є розробка як нових методик та інструментів, так і опрацювання можливих сценаріїв кібератак. Визначення порядку аналізу загроз та оцінки ризику, у тому числі критичність інформаційних технологій цільових функцій енергетичного сектора та вартість захисту ресурсів і IT-систем. Визначення порядку тестування та складу тестів для визначення слабких місць аналізованих систем, аж до організації штучних кібератак з метою визначення надійності та виявлення слабких місць діючих систем захисту та складу рекомендованих заходів щодо підвищення надійності функціонування систем, перелік можливих кібератак та дій, необхідних для їх відображення, регламент заходів щодо ліквідації наслідків кібер вторгнень. Щодо цифрової безпеки в Україні, мета зосереджується на підвищенні безпеки поточних додатків, послуг та інфраструктур шляхом інтеграції найсучасніших рішень та інструментів безпеки, на підтримці та створенні провідних ринків і ринкових стимулів у Європі орієнтованих на користувачів, у тому числі, наприклад, таких як, правоохоронні органи, служби швидкого реагування, оператори критичної інфраструктури, постачальники послуг IT, виробники IT, оператори ринку та громадяни. Проект ELECTRON дозволить забезпечити впровадження систем нового покоління, здатних протистояти енергетичним системам проти

кібератак, підвищуючи конфіденційність даних за допомогою трьох основних ініціатив: оцінка ризиків, виявлення та запобігання аномаліям, пом'якшення збоїв та прискорення відновлення систем, усунення внутрішніх загроз шляхом навчання та сертифікації персоналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Концепція розвитку сектору безпеки та оборони України, запроваджена Указом Президента України від 14 березня 2016 р. № 92 – 2016.
2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 березня 2016 р.№ 96 [Officer Vision of Ukraine – 2016], № 23.
3. Bruce Middleton, A History of Cyber Security Attacks: 1980 to Present – New York: Auerbach Publications, 2017.
4. "GreyEnergy: A Successor to BlackEnergy," White Paper (GreyEnergy, October2018),URL: https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf(link%20is%20external

Пахольченко Дмитро Віталійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
dimapakholchenko@gmail.com

Бакалинський Олександр Олегович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.т.н.,
baov@meta.ua

ПЕРЕЛІК ЕТАПІВ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА РІВНІ ЇХ КРИТИЧНОСТІ

Анотація. Перелік етапів реагування на кіберінциденти та рівні їх критичності допоможуть швидко та ефективно реагувати на кіберінциденти, зменшувати ризики їх повторного виникнення, зосереджуючись на виявленні, аналізу, визначенню пріоритетів та вирішенню інцидентів, здійснювати постійний контроль та моніторинг ІТ-систем, а також документувати кожен крок для подальшого аналізу та винесення уроків, які допоможуть підвищити стійкість систем до інцидентів.

Annotation. A list of cyber incident response and criticality levels will help respond quickly and effectively to cyber incidents, reduce the risk of recurrence by focusing on detecting, analyzing, prioritizing and resolving incidents, continuously monitoring and monitoring IT systems, and documenting every step of the way further analysis and lessons learned that will help increase the resilience of systems to incidents.

Масштаб, частота та вплив інцидентів кібербезпеки зростають і становлять основну загрозу для функціонування мережевих, інформаційних, комунікаційних або технологічних систем, особливо з початком ведення ворогом повномасштабної збройної агресії проти України. Такі інциденти можуть перешкоджати здійсненню господарської діяльності, спричинити значні фінансові втрати, підірвати довіру користувачів та завдати значної шкоди

економіці України.

Одним із чинників здатності держави забезпечувати захищеність власних ресурсів та активів в умовах політичної кризи та триваючої війни є спроможність забезпечувати кіберзахист власних інформаційних ресурсів, в тому числі тих, що належать до об'єктів критичної інформаційної інфраструктури (далі – ОКІІ).

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» суб'єкти забезпечення кібербезпеки у межах своєї компетенції, у тому числі підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури (далі – ОКІ), здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків [1].

Проте в чинному нормативному полі відсутній єдиний спільний механізм щодо впровадження та виконання заходів при виявленні, реагуванні та нейтралізації кіберінцидентів для швидкої мінімізації втрат і руйнувань, виправлення вразливостей, якими скористалися зловмисники, а також відновлення надання основних послуг.

Відповідно авторами пропонується запровадити перелік етапів реагування на кіберінциденти, які засновуються на публікації Національного інститут стандартів і технології (NIST) [2] та допоможуть швидко та ефективно реагувати на кіберінциденти.

Етапи реагування на кіберінциденти: підготовка, виявлення та аналіз, стримування, усунення, відновлення, заходи після інциденту.

Етап підготовки спрямований на забезпечення готовності реагування на кіберінциденти, а також запобігання їм, і передбачає виконання таких заходів:

розробка та оновлення політик безпеки;

затвердження детального плану реагування на кіберінциденти, перевірка використання його та, за необхідністю внесення коригувань до нього;

оцінка ризиків;

визначення критичних інформаційних активів;

визначення критичних інцидентів безпеки;

створення, перевірка, проведення навчань;

створення або визначення команди реагування на інциденти CSIRT/CIRT/CERT, порядку комунікації з правоохоронними органами, CERT-UA.

Етап виявлення та аналізу передбачає виявлення подій, які можуть спричинити виникненню інциденту, узагальнення інформації щодо них та наявності вразливостей, і передбачає такі заходи:

забезпечується постійний контроль та моніторинг ІТ-систем;

здійснюється виявлення аномалій, виявлення та аналіз, а також підтвердження інцидентів безпеки;

при виявленні інциденту, виконується початковий аналіз його з метою визначення масштабності, причини виникнення і яким чином відбувається інцидент (інструменти або методи, які використовувалися для атаки, якими вразливими місцями скористалися);

відбувається збір додаткових даних з різних джерел, їх дослідження, встановлення типу інциденту;

при аналізі виникнення інциденту команда суб’єкта взаємодії отримує достатньо інформації для визначення наступних заходів, як стримування, усунення та відновлення;

всі зібрані дані документуються, а команда суб’єкта взаємодії інформує про кіберінцидент відповідно до класифікації (таксономії) кіберінцидентів та протоколу обміну інформацією про кіберінциденти.

Етап стримування спрямований на забезпечення розроблення суб’єктами взаємодії цілеспрямованої стратегії відновлення, а також визначення та реалізацію першочергових заходів стримування для запобігання поширенню загрози. При здійсненні довгострокового стримування відбувається внесення тимчасових виправлень до систем задля можливості їх застосування до завершення налаштування систем (їх елементів), які відтворені з їх неуражених копій.

Етап усунення наслідку кіберінциденту спрямований на реалізацію заходів з видалення шкідливого програмного забезпечення з усіх уражених систем, усунення наслідків впливу інциденту, визначення першопричин інциденту та вжиття заходів для запобігання атакам подібного типу у майбутньому.

Етап відновлення передбачає реалізацію суб'єктом взаємодії заходів з відновлення системи до штатного режиму функціонування та переконання в її стабільному функціонуванні, що передбачає:

підключення раніше ізольованих уражених сегментів після відновлення до основної системи;

вжиття заходів із запобігання додатковим атакам;

тестування, перевірка та контроль відновлених після ураження систем для їх повернення до штатного функціонування з урахуванням встановленого часу для відновлення.

Етап заходів після інциденту передбачає:

аналіз отриманого досвіду інциденту після його закінчення, проведення навчань та зустрічей з метою обміну досвідом;

перегляд та внесення змін до політик та документації за результатами дослідження інциденту;

оцінку дій щодо реагування на інцидент з метою покращення процесів реагування на кіберінциденти у майбутньому.

Водночас, для встановлення типу інциденту пропонується запровадити єдиний механізм щодо визначення рівня критичності кіберінцидентів [3] (таблиця 1).

Рівень 0 вказує на необґрунтовану або несуттєву подію. Нульовий рівень загроз від настання кіберінциденту, наявність несуттєвих подій та стале функціонування критичної інфраструктури.

Рівень 1 вказує на те, кіберінцидент навряд чи вплине на економіку та промисловість, соціально-політичний стан, здоров'я та безпеку населення. Не існує жодної незвичайної активності, окрім звичайного занепокоєння про відомі хакерські дії, віруси та іншу зловмисну діяльність.

Таблиця 1

Рівень критичності кіберінциденту
Рівень 5 Критичний (Чорний, BLACK)
Рівень 4 Серйозний (Червоний, RED)
Рівень 3 Високий (Помаранчевий. ORANGE)
Рівень 2 Середній (Жовтий, YELLOW)
Рівень 1 Низький (Зелений, GREEN)
Рівень 0, (Білий, WHITE)

Рівень 2 вказує на те, кіберінцидент може вплинути на економіку та промисловість, соціально-політичний стан, здоров'я та безпеку населення. Існує потенціал для кіберзловмисної діяльності, при якому спостерігається збільшення хакерських дій, вірусів або іншої зловмисної діяльності.

Рівень 3 вказує на те, кіберінцидент може мати явний вплив на економіку та промисловість, соціально-політичний стан, здоров'я та безпеку населення. Зростання хакерських дій, вірусів або іншої зловмисної діяльність, які уражують системи критичної інфраструктури або можуть вплинути на надання основних (життєво необхідних) послуг.

Рівень 4 вказує на те, кіберінцидент може мати значний вплив на економіку та промисловість, соціально-політичний стан, здоров'я та безпеку населення. Зростання хакерських дій, вірусів або іншої зловмисної діяльності, які націлені на перебій надання основних (життєво необхідних) послуг.

Рівень 5 вказує на те, кіберінцидент створює безпосередню загрозу для надання широкомасштабних послуг критичної інфраструктури, стабільності влади або життю громадян. Критичне зростання хакерських дій, вірусів або іншої зловмисної діяльності, в наслідок яких здійснюється постійний перебій надання послуг критичної інфраструктури та/або руйнується один чи більше секторів критичної інфраструктури.

У висновку можна зазначити, що перелік етапів реагування на кіберінциденти та рівні критичності кіберінцидентів допоможуть швидко та ефективно реагувати на кіберінциденти, зменшувати ризики їх повторного виникнення, зосереджуючись на виявленні, аналізу, визначенню пріоритетів та вирішенню інцидентів, здійснювати постійний контроль та моніторинг ІТ-систем, а також документувати кожен крок для подальшого аналізу та винесення уроків, які допоможуть підвищити стійкість систем до інцидентів.

Такий підхід допоможе у подальшому використовувати отриману інформацію для подальшого аналізу та винесення уроків, які допоможуть підвищити стійкість систем до інцидентів, а також в якості доказів для пошуку та притягнення до відповідальності осіб, які незаконним шляхом намагалися здійснити несанкціонований доступ до інформаційних систем, що спричинило виникнення кіберінцидентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Верховна Рада України. 7 сесія. (2017, жовт. 5). Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України. [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-viii.

2. NIST Special Publication (SP) 800-61 Rev. 2: Computer Security Incident Handling Guide.

3. National cyber incident responst plan. December 2016. U.S. Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA).

Бакалинський Олександр Олегович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, к.т.н.,
baov@meta.ua

Пахольченко Дмитро Віталійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
аспірант,
dimapakholchenko@gmail.com

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НОРМ МІЖНАРОДНОГО ГУМАНІТАРНОГО ПРАВА В ПИТАННЯХ ВЕДЕННЯ КІБЕРОБОРОНИ

Анотація. Відповідно до норм міжнародного гуманітарного та національного права досліджується роль та місце держави, збройних сил, сил оборони та цивільного/мирного населення в кібероборонні України.

Annotation. In accordance with the norms of international humanitarian and national law, the role and place of the state, armed forces, defense forces and civilian population in cyber defense of Ukraine is studied.

24 лютого 2022 року Президент України Володимир Зеленський ввів у дію рішення Ради національної безпеки і оборони України «Про введення в дію плану оборони України та Зведеного плану територіальної оборони України». Однією із складових частин плану оборони України є план кібероборони.

Законодавство визначає кібероборону, як сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [1].

Керівну роль у кібероборонні держави відіграє Міністерство оборони України та Генеральний штаб Збройних Сил України, які, відповідно до компетенції, здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони), здійснюють військову співпрацю з

НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз та впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [2].

Безпосередніми учасниками кібероборони є основні суб'єкти національної системи кібербезпеки та сили оборони – Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави [3].

В будь-якій збройній боротьбі основну роль відіграють люди, які прямо чи опосередковано, а іноді вимушено, дотичні до неї, у відповідності до норм міжнародного гуманітарного права людина в збройній боротьбі може відігравати наступні ролі [4]:

1. Комбатанти:

– особи, які входять до складу збройних сил країн, які перебувають у стані військового конфлікту, і мають право безпосередньо брати участь у військових діях;

– особовий склад сухопутних, військово-морських і військово-повітряних військ;

– партизани (із знаками розрізнення та зброєю, яка носиться не скриваючись);

– екіпажі торгових морських суден, та екіпажі літаків цивільної авіації сторін, задіяних у військовому конфлікті, при умові що судна та літаки переобладнані у військові;

– вояки, які беруть участь у національно-визвольних війнах.

Застосування насильницьких військових заходів до комбатантів (аж до знищення) вважається законним, проте комбатант, який потрапив до ворогуючої сторони, користується статусом військовополоненого.

2. Некомбатанти:

– особи, які входять до складу збройних сил та надають їм допомогу, але безпосередньої участі у воєнних діях не беруть;

– медичний, духовний персонал, інтенданти, військові кореспонденти, юристи тощо.

До вказаних осіб не має застосовуватися зброя, якщо вони зайняті виконанням своїх безпосередніх обов'язків. Їх функції зводяться лише до обслуговування та забезпечення бойової діяльності збройних сил і вони мають право застосовувати зброю тільки в цілях самооборони.

Некомбатанти мають спеціальний правовий статус у разі затримання їх ворогом, вони не повинні вважатися військовополоненими.

3. Цивільне або мирне населення.

Визначається міжнародним гуманітарним правом як особи, які не є членами збройних формувань і не беруть прямої участі у бойових діях під час збройного конфлікту.

Починаючи з 2014 року населення України поділилось саме за таким принципом, але з 24 лютого 2022 року додались наступні фактори:

– 40 000 людей із 52 країн прийняли пропозицію президента Володимира Зеленського «приєднатися до захисту України, Європи та світу» та були зараховані до Міжнародного легіону територіальної оборони України;

– приблизно 300 000 відповіли на твіт міністра цифрової трансформації України Михайла Федорова, який закликав IT-фахівців з усього світу приєднатися до IT-армії України;

– сформовані національні сили, які діють згідно законодавства та приймають участь у кібероборони України.

І ось саме щодо ролі кожної людини, яка приймає участь в кібероборони України виникають думки різних фахівців, наприклад Роберт М. Лі, генеральний директор компанії з промислової кібербезпеки Dragos, який керував розслідуванням кібератак на українські електромережі в 2015 році, прямо сказав, що «хто не працює від імені уряду та веде серйозні розмови про «злом» або запуск кібератак проти Росії, будь ласка, зрозумійте – з повагою –

ви ідіот і тільки погіршите ситуацію» [5].

З іншого боку багато людей відкликнулись саме за зовом сердця на призив керівництва України та виступило на захист як Батьківщини, так і країни, на яку було здійснено віроломний напад. Виходячи з існуючого міжнародного та національного права, учасники кібероборони України, на наш погляд, можуть бути поділені на такі основні групи: хактивісти, кібертерористи, кіберзлочинці та кібероборонці [6; 7], статус останніх в національному законодавстві не визначено.

Хактивісти, які своєю професійною чи волонтерською діяльністю не пов'язані з національними оборонними структурами, цілком очевидно, мають більше свободи висловити свою підтримку державі (в тому числі і іноземній), яка знаходиться у збройному протистоянні. Оскільки їхню активну підтримку можна розглядати як форму участі держави, можливості, доступні для військовослужбовців, членів добровільних організацій національної оборони та державних службовців, для них, зрозуміло, більш обмежені.

Про формування Міжнародного легіону територіальної оборони України оголосив міністр закордонних справ України, що ґрунтується на указі президента України від 2016 року, який дозволяє неукраїнцям вступати до Збройних сил України.

Проте, за твердженням Міністерства оборони росії, іноземні бійці, які приєднуються до Легіону, не розглядаються як комбатанти згідно з міжнародним правом (саме у викривленій інтерпретації росії), тобто вони не мають права на статус військовополонених.

Що стосується ІТ-армії, її структури, організації та державної приналежності – ІТ-армія не буде розглядатися як організована збройна група для визначення статусу комбатанта, тому питання, що стосуються бойових дій та різних форм участі цивільного населення, мають велике значення. Наприклад, за думками Ann Väljataga [5], дослідника прав людини у цифровій сфері, хоча привілей вважатися військовополоненим може не має великого значення для кібербійця, інші аспекти, такі як стати легітимною військовою

ціллю та мати обмежений юридичний імунітет від кримінального переслідування, можуть стати дуже важливими.

Хоча ІТ-армія за своїм складом є міжнародною, вона була створена і певною мірою координується українським урядом, безпосередньо Міністерством цифрової трансформації, яке ставить її під ефективний контроль України. Однак, незважаючи на чіткі стосунки з воюючою державою, члени ІТ-армії навряд чи відповідатимуть критеріям, встановленим для статусу комбатантів, оскільки переважна більшість не належить до Збройних сил України чи нерегулярних сил, хоча ІТ-армія позиціонується, як частина оборонного апарату України. Тому ІТ-армію найкраще можна охарактеризувати як щось середнє між спонсорованим державою хакерством і децентралізованим хактивізмом.

Залежно від характеру операцій, які вона проводить, а також від того, як вони керуються та організовані, добровольці в ІТ-армії можуть бути юридично класифіковані як [5; 6]:

– цивільні особи, які опосередковано підтримують бойові дії,

– цивільні особи, які безпосередньо беруть участь у бойових діях,

– цивільні особи, які влаштовують масове повстання (levée en masse).

Водночас, до боротьби приєдналися хакерські спільноти або групи, наприклад, Anonymous або NB65, які діють заплутаним неієрархічним способом, без отримання інструкцій або без звітності перед будь-яким державним органом.

Їх члени можуть кваліфікуватися як:

– цивільні особи, які безпосередньо беруть участь у бойових діях,

– цивільні особи, які опосередковано підтримують бойові дії,

– просто злочинці.

Розрізнення має важливе значення, оскільки перша категорія перетворює залучених цивільних осіб на законні військові об’єкти (цілі) відповідно до міжнародного гуманітарного права, а остання підпорядковує їх правоохоронним процедурам мирного часу.

Необхідно зауважити на те, що під час безпосередньої участі у бойових діях, географічної віддаленість від бойового простору не виключає прямої участі. Незалежно від місця дії, три елементи визначають безпосередню участь у бойових діях [4]:

– має бути досягнутий «поріг шкоди», який поширюється на будь-які наслідки, що негативно впливають на військові операції або військову спроможність сторони в конфлікті;

– прямий причинно-наслідковий зв'язок між діянням і шкодою, що виникла або може бути наслідком цього діяння або скоординованої військової операції, невід'ємною частиною якої є цей акт (прямий причинний зв'язок);

– умисел у вчиненні діяння безпосередньо спричинити необхідний поріг шкоди на підтримку сторони конфлікту та завдати шкоди іншій (воюючий зв’язок).

Якщо особа, яка займається кіберактивністю проти воюючої держави, підпадає під визначення цивільного, що безпосередньо приймає участь у бойових діях, вона стає законною військовою ціллю. Участь вважається систематичною на всіх етапах підготовки, визначення цілі, активної операції та оцінки післядій. Цифрову участь у бойових діях слід сприймати так само серйозно, як і його кінетичні еквіваленти.

Цивільні особи, які підтримують Україну (в тому числі і громадяни України) шляхом проведення кібероперацій, призначених для найсерйознішого впливу – взяття під управління систем промислового контролю, можуть, відповідно до міжнародного гуманітарного права, отримати транскордонну військову відповідь у будь-якій із операційних областей.

Непряма участь у бойових діях включає засоби підтримки війни держави-учасника, яка не відповідає трьом критеріям: матеріально-технічна допомога, фінансова підтримка, харчування, підвищення обізнаності та пропаганда. У кіберсфері це, пасивний захист критичних мереж України та велика частка операцій, спрямованих на підвищення обізнаності чи зупинку кампанії з дезінформації противника. Отримання розвідувальних даних,

розкриття даних і DDoS-атаки слід аналізувати окремо, беручи до уваги будь-який причинний зв'язок із остаточною військовою шкодою.

Багата кількість кібератак, в тому числі поширення інформації (наприклад про втрати московітів в Україні) не підпадають під поняття безпосередньої участі у збройному конфлікті і не мають розумного причинного зв'язку з військовою шкодою, в такому випадку зловмисники не ризикують втратити свій цивільний статус. Вони вчиняють низку кіберзлочинів, які криміналізуються Кримінальним кодексом росії та більшістю інших держав, які мають закони про кіберзлочинність.

Під час міжнародного збройного конфлікту жителі неокупованої території, які беруть участь у кібероперацій у рамках збройних сил, користуються імунітетом і статусом військовополонених. Levee en masse складається з мешканців території, на якій ведеться війна, але яка ще не окупована іноземними військами.

Концепція була спочатку введена для того, щоб люди, які спонтанно протистояли вторгненню, не маючи часу на офіційну організацію в бойові загони, могли отримати обов'язки та привілеї комбатантів (статус військовополонених та обмежений юридичний імунітет). Хактивістські групи, які складаються з членів з усього світу і не мають наміру створити структуру, що нагадує бойові підрозділи, навряд чи відповідають таким критеріям. Українська ІТ-армія має високий рівень організації та певний рівень підпорядкованості українському уряду, що також слабо співпадає з Levee en masse [4; 6].

У висновку можна зазначити, що кожна особа, яка планує брати участь у будь-якій діяльності, натхненній бажанням допомогти державі, яка стала жертвою невиправданого вторгнення, має усвідомлювати свою позицію по відношенню до будь-якого державного органу і конкретної групи активістів, до якої вона планує приєднатися. Найважливішим фактором, який визначає законність та загальну безпеку, залишається характер діяльності. Просто витоки інформації та антипропагандистські злами не перетворюють цивільного на

законного чи незаконного бойовика, завдяки цим діям не знищуються танкові колони ворога, а, іноді атаки, які не мають військової мети можуть ставити під загрозу операції розвідки, або операції, які реалізуються в традиційних доменах. Хактивістські операції з потенційно неконтрольованими або невибірковими наслідками, такими як атаки ланцюга поставок з відкритим кодом або будь-що, що націлено на критично важливу інфраструктуру, ніколи не варті того ризику – військового, гуманітарного чи кримінального – який вони несуть.

З іншого боку, в ситуації війни, в якій виживання української нації стоїть як першочергова задача, а збройні сили російської федерації не приховують свої дії щодо геноциду української нації, необхідно пам’ятати що не є кримінальним правопорушенням діяння (дія або бездіяльність) [9], яке заподіяло шкоду правоохоронюваним інтересам, якщо це діяння було вчинене в умовах виправданого ризику для досягнення значної суспільно корисної мети. Тобто, будь-яка атака, яка буде здійснена з військовою метою, буде виправдана, якщо її наслідки будуть спрямовані на отримання переваги над противником і досягнення перемоги та завдана противнику шкода не більше ніж відгорнута. На наш погляд, розробка та прийняття закону, який би визначав ландшафт взаємовідносин учасників кібероборони у кіберпросторі в умовах військового часу, визначав завдання сил кібероборони України, права та обов’язки фізичних та юридичних осіб, які залучаються до заходів кібероборони, є своєчасним та актуальним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Верховна Рада України. (2017, жовт. 5). Закон № 2163-VIII, Про основні засади забезпечення кібербезпеки України. [Електронний ресурс]. Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-viii.

2. Верховна Рада України. (1991, груд. 6). Закон № 1932-XII, Про оборону України. [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

3. Верховна Рада України. (2018, черв. 21). Закон № № 2469-VIII, Про національну безпеку України. [Електронний ресурс]. Режим доступу: *https://zakon.rada.gov.ua/laws/show/2469-19//*

4. Женевська конвенція 1949 року та додаткові протоколи I, II, III до Женевської конвенції [Електронний ресурс]. Режим доступу: *https://www.icrc.org/en/doc/assets/files/publications/icrc-002-0173.pdf*.

5. Cyber vigilantism in support of Ukraine: a legal analysis Ann Väljataga March 2022, [Електронний ресурс]. Режим доступу: https://ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-pub.pdf.

6. Талліннський посібник 2.0 з міжнародного права, застосовного до кібероперацій (Tallinn Manual 2.0) Cambridge University Press. Режим доступу: *https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4*
FFD83EA790D7C4C3C28FC9CA2FB6C9.

7. Верховна Рада України (1907, жовт. 18) IV КОНВЕНЦІЯ про закони і звичаї війни на суходолі [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/995_222#Text.

8. Верховна Рада України (2001, лист. 23) Конвенція про кіберзлочинність (Convention on Cybercrime) [Електронний ресурс]. Режим доступу: *https://zakon.rada.gov.ua/laws/show/994_575#Text*.

9. Верховна Рада України (2022, квіт. 23) Кримінальний кодекс України [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/
2341-14#Text.

Христинець Наталія Анатоліївна,
Луцький національний технічний університет,
старший викладач кафедри комп'ютерної інженерії та кібербезпеки, hrystynets.at.ua@gmail.com

ЕТАПИ ПРОГРАМУВАННЯНА ASSEMBLERДРАЙВЕРІВ КЛАВІАТУРИ ТА ЕКРАНУ ДЛЯ МІКРОЯДРА ОПЕРАЦІЙНОЇ СИСТЕМИ

Додавання будь-якого драйвера пристрою передбачає виділення для цього пристрою ресурсів процесора: ініціалізація обробника переривань від апаратних засобів та встановлення номеру, за яким буде викликатись обробник з таблиці IDT, каналів запитів переривань тощо. Тому, важливим моментом лишається розподіл цих ресурсів власне ядром ОС.

Драйвери тестового екрану і клавіатури є необхідними компонентами мікроядра операційної системи. Загалом, усі драйвери операційної системи «(окрім віртуальних), а також інші розширення в деякому розумінні є не чим іншим, як набором бібліотек динамічного компонування» [1, с.319]. Для їх написання на asm[2-3] спочатку були підключенінеобхідні хедери з інтерфейсом функціоналу, що було використано у драйверах: stdlib.h – власноруч розроблена стандартна бібліотека; interrupts.h – функції для створення обробників переривань від пристроїв; tty.h – інтерфейс драйверів клавіатури та екрану; scancodes.h – масиви з набором символів, або команд, які можуть бути отримані з клавіатури (рис. 1).

Наступним етапом проектування стало оголошення іменованого типу (TtyChar) для структури даних єдиного символу (ASCII-код та його атрибути: колір символу, фону і т.д.). Оголошувались змінні, які далі будуть містити в собі дані про:

- ширину консолі (скільки символів може поміститись)(tty_width);
- висоту консолі (tty_height);
- позиція апаратного курсору (cursor);
- атрибути тексту (text_attr);

- відео буфер, куди будуть виводитись символи (tty_buffer);

- номер порту вводу/виводу, через який можна отримувати дані дисплею та налаштовувати цей дисплей (tty_io_port).

```
void init_tty()
{
    tty_buffer = (void*)0xB8000;          // start of video buffer
    tty_width = *((uint16*)0x44A);        // number of column we read at 0x44A
    tty_height = 25;                      // number of lines
    tty_io_port = *((uint16*)0x463);      // base I/O port for controlling the display controller
    cursor = (*((uint8*)0x451)) * tty_width + (*((uint8*)0x450));   // calculate cursor position, at 0x450 we have
    text_attr = 7;                        // fill the screen with blue color and display the white inscription
    set_int_handler(irq_base + 1, keyboard_int_handler, 0x8E);      // we will set the keyboard interrupt handler,
}
```

Рисунок 1 – Фрагмент коду написання драйверів мікроядра

Написано макрос для визначення розміру символьного буферу, цей макрос запам'ятовувуєостанні 16 введених з клавіатури скан-кодів клавіш (KEY_BUFFER_SIZE), безпосередньо символьний буфер (key_buffer[]), «вказівники» на початок та кінець буферу (key_buffer_head, key_buffer_tail) та прототип функції обробника перериванньвід клавіатури (keyboard_int_handler()).

Функція init_tty() ініціалізує вищевказані параметри телетайпу (екрану):

- tty_buffer – містить адресу початку відео буферу екрану 0xB8000;

- tty_width – ширина телетайпу зчитується з області даних BIOS зпа адресою 0x44A;

- tty_height – висота – 25 символів – задаємо саамі;

- tty_io_port – порт, через який відбувається зв’язок із контроллером дисплею;

- cursor – обчислюється позиція апаратного курсору;

- text_attr – значення 7, тобто 00000111 – зелений текст на чорному фоні;

- встановлено обробник переривань від клавіатури по перериванню IRQ 1 (тобто +1 від початку бази таблиці обробників переривань).

У результаті проектування, інтерфейс драйверів клавіатури та екрану tty.h дозволяє ініціалізувати обробку переривань цих пристроїв, що свідчить про злагоджену роботу ядра системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кравець В. О. Системне програмування. Асемблер під Win32 API.– Харків: НТУ “ХПІ”, 2008. – 512 с.
2. Мікропроцесорна техніка: Лабораторний практикум [Електронний ресурс]URL: https://ela.kpi.ua/bitstream/123456789/41748/1/Mikroprotsesorna-tekhnika_LabPrakt.pdf. Дата звернення: 05.04.2022.
3. Assembler: Abstract [Електронний ресурс] URL: https://medium.com/@it_root.corp/assembler-abstract-1a9b70e58615 . Дата звернення: 05.04.2022

Худинцев Микола Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
докторант,
Міжнародний університет кібербезпеки (м. Київ),
член правління,
mykola.khudyntsev@icu-ng.org

КОНЦЕПЦІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЕНЕРГЕТИЧНОЇ ГАЛУЗІ УКРАЇНИ

Анотація. Доповідь присвячена обґрунтуванню основних положень концепції забезпечення кібербезпеки у енергетичномусекторі України на 3 рокита визначенню пріоритетних підходів і заходів для підвищення рівня кібербезпеки галузі.

Annotation. The report is devoted to substantiating the main provisions of the concept of cybersecurity in the energy sector of Ukraine for 3 years and identifying priority approaches and measures to improve the level of cybersecurity in the sector.

Впровадження організаційно-технічної моделі (ОТМ) кібербезпеки та кіберзахисту – завдання, покладені Законом України «Про основні засади забезпечення кібербезпеки України»[1] на Державний центр кіберзахисту та Державну службу спеціального зв’язку та захисту інформації України.

У грудні 2021 році затверджене Положення про організаційно-технічну модель кіберзахисту [2], у якому визначено, що ОТМ кіберзахистує комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем.

ОТМ кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки.

Концептуальні засади впровадження ОТМ кібербезпеки та кіберзахисту були розроблені у 2020-2021 роках в роботах О. Потія, А. Семенченко,

Д. Дубова, О. Бакалинського, Д. Мялковського, М. Худинцева, Р. Боярчука, О. Лебідя, О. Трофимчука, [3-4].

В серпні 2021 рокуу другій редакції Стратегії кібербезпеки України [5] визначено, що в Україні має бути сформована ефективну модель відносин у сфері кібербезпеки, заснована на довірі, зокрема шляхом запровадження галузевих (секторальних) центрів забезпечення кібербезпеки та команд реагування на кіберінциденти, всебічного сприяння їх розвитку, взаємодія цих центрів з Національним координаційним центром кібербезпеки.

До переліку секторів (підсекторів), основних послуг критичної інфраструктури держави [6] включено паливно-енергетичний сектор (електроенергетика, нафтова промисловість, газова промисловість, ядерна енергетика), інформаційний сектор, системи життєзабезпечення, харчову промисловість та агропромисловий комплекс, охорону здоров'я, ринки капіталу та організовані товарні ринки, транспорт і пошту, промисловість, цивільний захист населення та територій, фінансовий сектор.

Діяльність з запровадження галузевих (секторальних) центрів забезпечення кібербезпеки (ГЦК) та команд реагування на кіберінциденти (ГКР, галузевих CERT/CSIRT) має спиратися на галузеві нормативні документи. В якості базового галузевого нормативного документа пропонується розглядати галузеві (секторальні) концепції забезпечення кібербезпеки строком на 3-5 років (з передбаченим подовженням терміну).

На розгляд Міністерства енергетики України було представлено проєкт концепції забезпечення кібербезпеки у енергетичному секторі України на 3роки, який було прийнято для подальшого опрацювання [7].

Документ містить наступні розділи: вступні положення, концептуальні положення забезпечення кібербезпеки в енергетичному секторі, стан забезпечення кібербезпеки та проблеми, які потребують розв'язання, мета та цілі реалізації концепції, принципи формування та шляхи реалізації концепції,

очікувані результати, обсяг ресурсів та джерела фінансування. Вперше визначені терміни «енергетичний сектор»[1] та «суб'єкт енергетичного сектору»[2].

До основних концептуальних положень забезпечення кібербезпеки в енергетичному секторі включені:

- гармонізація з іншими нормативно-правовими актами,
- підходи та пріоритети в реалізації концепції,
- стандартизація вимог з кібербезпеки,
- впровадження процесу самооцінки та звітування щодо рівня кібербезпеки,
- створення безпечного середовища,
- дотримання та забезпечення верховенства права та прав людини у кіберпросторі,
- дотримання кращих світових стандартів енергетичної безпеки та кібербезпеки,
- ефективне управління, прозорість і підзвітність,
- гарантії незалежності,
- розвиток кадрового потенціалу та соціальний захист працівників.

Найбільший інтерес та актуальність поставленої задачі складають система запропонованих підходів та заходів забезпечення кібербезпеки, які враховують стан безпеки та рівень зрілості відповідних систем окремих суб'єктів енергетичного сектору, а також екосистеми енергетичного сектору щодо інформаційної безпеки та кібербезпеки в цілому.

Для забезпечення кібербезпеки у енергетичному секторі запропоновано впровадження наступних підходів та заходів, які стосуються, в основному, стандартизації вимог з кібербезпеки, гармонізації вітчизняної нормативно-

[1]Енергетичний сектор – сукупність сил, заходів та засобів електроенергетичного, ядерно-промислового, вугільно-промислового, торфодобувного, нафтогазового та нафтогазопереробного комплексу (паливно-енергетичного комплексу), а також сфери ефективного використання паливно-енергетичних ресурсів, енергозбереження, відновлюваних джерел енергії та альтернативних видів палива, нагляду (контролю) у галузях електроенергетики і теплопостачання, використання ядерної енергії, ядерної та радіаційної безпеки, безпеки постачання електричної енергії та природного газу

[2]Суб'єкт енергетичного сектору – орган, установа, підприємство або інша організація, яка здійснює свою діяльність в енергетичному секторі

правової бази у сфері інформаційної безпеки та кібербезпеки з відповідними базами провідних світових лідерів, впровадження процесу самооцінки (внутрішнього аудиту інформаційної безпеки) та звітування щодо рівня кібербезпеки, створення безпечногосередовища:

- Визначення показників надійності та нормативних вимог до аудиту кібербезпеки;
- Вдосконалення моніторингукіберризиків;
- Стандартизація обов'язкових до виконання мінімальних вимог з кібербезпеки;
- Впровадження процесу регулярного аудиту та звітування щодо рівня кібербезпеки;
- Пріоритетизація вимог безпекидо ланцюжка постачання технологій (технологічних рішень);
- Розробка критеріїв рейтингівризиків втрати (пошкодження) майна та активів;
- Розробка вимог до техніки безпеки стосовно мінімально необхідного рівня кібербезпеки та наслідків від його порушення;
- Впровадження процесу оцінювання технологічних (технічних) рішень, що впливають на ризики операційної діяльності;
- Розробка системи індикаторів моніторингу стану кібербезпеки (для звітування, обміну відомостями та прийняття операційних рішень);
- Розробку планів реагувань на кіберінциденти;
- Визначення рівня кваліфікації, забезпечення проведення обов'язкової періодичної перевірки якості знань та професійних навичок персоналу з питань кібербезпеки;
- Організація та методичне забезпечення проведення періодичних внутрішніх та незалежних аудитів (у т.ч. розробка параметрів та методики оцінки рівня кібербезпеки, розробка та оприлюднення шаблонів оцінки, обробка та узагальнення результатів);

- Впровадження механізмів моніторингу, звітування, оцінки діяльності суб'єктів енергетичного комплексу з питань кібербезпеки;
- Гармонізаціянормативних вимог енергетичної безпеки, безпеки енергопостачання, інформаційної безпеки, кібербезпеки, а також положень організаційних та технічних внутрігалузевих документів з питань кібербезпеки;
- Розробка критеріїв та переліку суб'єктів, правил та обсягів обміну інформацією про кіберінциденти та кіберзагрози в енергетичній сфері;
- Розробка планів дій у випадку настання надзвичайних ситуацій у енергетичній сфері, ліквідації їх наслідків, у т. ч. в особливий період;
- Підвищення рівня обізнаності і розвиток навичок населення, пов'язаних з належним реагуванням на загрози енергетичної безпеки та кібербезпеки;
- Імплементація до системи нормативних документів енергетичного сектору міжнародних стандартів та рекомендацій (ISO27001, NIST CybersecurityFramework, COBIT та ін.);
- організація участі суб'єктів енергетичного сектору у міжнародному обміні відомостями про кіберзагрози, кіберінциденти та кібератаки;
- Організація досліджень із забезпечення кібербезпеки в процесі створення та експлуатаціїтехнологічних систем,систем прийняття рішень (підтримки прийняття рішень), експертних, геоінформаційних, інформаційно-аналітичних систем, систем моніторингу, управління, контролю, «розумних», кіберфізичних,інтелектуальних систем (у т. ч. з використанням технологій штучного інтелекту та великих даних);
- Дотримання принципу наскрізного керування[3], який є обов'язковим для забезпечення належного управління та нагляду за безпекою (кібербезпекою);
- Впровадження персональної відповідальності за порушення вимог безпеки (кібербезпеки) на рівні суб'єкта енергетичного сектору, підрозділу, окремого працівника.

[3]widegovernance (англ.)

Оцінювання результатів реалізації Концепції має здійснюватися на підставі застосування індикаторів високого рівня та індексів (рейтингів) кібербезпеки [8], які свідчать про розвиток сил, заходів та засобів кібербезпеки суб'єктів енергетичного сектору.

Результати дослідження можуть бути використані Міністерством енергетики України, окремими підприємствами паливно-енергетичного комплексу, іншими суб'єктами забезпечення кібербезпеки для розробки галузевих (корпоративних) нормативних документів у відповідній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Відомості Верховної Ради України (ВВР),№45, 2017. – с.403.
2. Постанова Кабінету Міністрів України, №1426. – 29.12.2021https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.
3. О.Потій, А.Семенченко, Д.Дубов, О.Бакалинський, Д. Мялковський, Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України, Захист інформації, т.23, №1, 2021. – с.47-60. Режим доступу: https://jrnl.nau.edu.ua/index.php/ZI/article/view/15434/22419.
4. R.Boyarchuk, M.Khudyntsev, O.Lebid, O.Trofymchuk, Organizational and Technical Model of National Cybersecurity and CyberProtection, Workshop on Cybersecurity Providingin Information and Telecommunication Systems, Kyiv, Ukraine, CPITS'2021, 2021. – V.2923,pp. 37-46, ISSN 1613-0073.Access mode: http://ceur-ws.org/Vol-2923/paper5.pdf.
5. Затверджено Указом Президента України від 26.08.2021, №447/2021https://zakon.rada.gov.ua/laws/show/447/2021#Text.
6. Постанова Кабінету Міністрів України від 09.10.2020 № 1109https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n42
7. Міненерго працює над створенням галузевого операційного центру кібербезпеки. [Електронний ресурс] URL:

http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245542980. Дата звернення: 15.05.2022.

8. Худинцев М.М. (заг. ред.), Жилін А.В., Давидюк А.В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог), Монографія,Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. – К.: 2021. – 240 с. ISBN 978-966-136-887-2.

Kotsiuba I.V.,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine, mchaikin@outlook.com
PhD,
i.kotsiuba@gmail.com

Chaikin M.M.,
G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine,
graduate student,
mchaikin@outlook.com

PROBLEMS OF COMPLIANCE WITH CYBERSECURITY REQUIREMENTS IN THE ENERGY INDUSTRY OF UKRAINE IN WAR CONDITIONS AND THEIR COMPARISON WITH WORLD PRACTICES AND REQUIREMENTS

The relevance of cybersecurity of energy sector facilities has been especially evident since the beginning of the open aggression of the Russian Federation against Ukraine starting from February 24, 2022.

It is worth noting that the requirements for cyber security for critical infrastructure objects are described in the following legal documents:

- Law of UkraineOn the Basic Principles of Cybersecurity in Ukraine;
- Law of Ukraine On information protection in information and communication systems;
- Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects.

According to Article 8 of Law of Ukraine On information protection in information and communication systems, for systems that are subject to protection and do not process information classified as restricted, and such systems include process control systems, it is necessary to build and certify information security management system, according to the state standard of technical conditions of Ukraine ISO 27001:2013. Two other documents describe the requirements for critical infrastructure objects, the list of which should be compiled by the Cabinet of

Ministers of Ukraine, but such a list has not yet been created and, therefore, the requirements are advisory in nature.At the moment, the only energy-company that has built and certified its information security management system in accordance with the requirements of the law is Ukrenergo (according to information from official sites).

It should be noted that energy cybersecurity has its own characteristics:

- **Real-time requirements:** In an electricity grid, supply and demand must be balanced at any moment, meaning industrial control systems must react within fractions of a second, which leaves no time for sophisticated authentication procedures.
- **Mix of advanced and legacy technologies**: Energy system components have a very long lifespan, of several decades. It is consequently very likely that the grid will be controlled by a mix of advanced technologies with cybersecurity certification, and older devices which need to be protected in other ways.
- **Cascading effects of disruption**: Due to the interconnected nature of an electricity system, a serious disruption in one part of the grid can also spread to interconnected grids, potentially leading to a blackout over a wide area. This would also affect other services that depend on electricity, notably transport, telecommunications, water supply and finance.

After a series of attacks on energy infrastructure around the world, the governments of advanced countries began to develop their requirements for the cybersecurity of energy as part of a critical infrastructure. Next, we will look at approaches to this issue in the EU, the US and Australia.

European Union:

The key EU law for the protection of critical infrastructure6 is Council Directive 2008/114/EC [1] on critical European infrastructures. It establishes procedures for identifying and designating European critical infrastructures (ECI) and introduces a common approach for assessing their protection and the need to improve it. The Directive applies only to the energy and transport sectors. It requires owners or operators of designated ECI to prepare advanced business continuity plans

(operator security plans) and to nominate Security Liaison Officers that act as contact points to the national authority responsible for critical infrastructure protection.

Cybersecurity Act: Regulation (EU) 2019/881 (Cybersecurity Act) [2], which is part of the 2017 cybersecurity package and entered into force in June 2019, aims to strengthen the EU's response to cyber-attacks, improve cyber-resilience and increase trust in the digital single market. The Act empowers ENISA – now referred to as the European Union Agency for Cybersecurity – to improve coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies. It establishes an EU cybersecurity certification framework for the development of tailored certification schemes for specific categories of information and communication technology products, processes and services. Companies will need to certify their products, processes and services only once to obtain certificates that are valid across the EU. The Act provides ENISA with more financial and human resources to carry out its new tasks and also addresses the issue of legacy infrastructure – that is, older technology with a lifespan of 30-60 years, designed before cybersecurity concerns existed.

Commission Recommendation on energy cybersecurity: In April 2019, the Commission issued Recommendation (EU) 2019/553 [3], which contains guidelines that Member States and key stakeholders (particularly energy grid operators) should take into account when making decisions about infrastructure. These measures include cybersecurity risk analysis and preparedness, in particular for legacy systems, updating software and hardware, and establishing an automated monitoring capability for security events in legacy environments.

Electricity Risk Preparedness Regulation: Regulation (EU) 2019/941 [4] is focused specifically on crisis prevention and crisis management in the electricity sector. It envisages the development of common methods to assess risks to the security of electricity supply, including risks of cyber-attacks; common rules for managing crisis situations and a common framework for better evaluation and monitoring of electricity supply security.

The European Commission organises regular information-sharing events, such as the high-level event on cybersecurity in the energy sector, held on 9 July 2019.

Network code on energy cybersecurity: The recast of the Electricity Regulation (Regulation (EU) 2019/943) gives the Commission a mandate to develop a network code for cybersecurity. The Smart Grids Task Force has been doing preparatory work since 2017, and released its second interim report in July 2018 [5]. The report recommends setting up an early warning system for the energy sector in Europe, cross-border and cross-organisation risk management, minimum security requirements forcritical infrastructure components, a minimum protection level for energy system operators, a European energy cybersecurity maturity framework and supply chain risk management.

United States of America:

In the United States, the first significant piece of legislation to address the growing challenge of cybersecurity in the energy sector was the 2005 Energy Policy Act. Signed into law less than two years after the North-east blackout of 2003 left 50 million North Americans without power, the act granted the Federal Energy Regulatory Commission (FERC) the ability to appoint an Electric Reliability Organization (ERO) that would develop and enforce mandatory reliability standards for all bulk power electric utilities in the country. The North American Electric Reliability Corporation (NERC), a private non-profit organisation, was designated as the ERO for the United States and several Canadian provinces in 2006. The NERC is responsible for developing a list of critical infrastructure protection standards (NERC-CIPs), which are delivered to the FERC for review. Of the eleven CIPs currently subject to enforcement, ten are dedicated to cybersecurity standards and one relates to the physical security of energy grids.

On January 8, 2015, the Energy Department released guidance to help the energy sector establish or align existing cybersecurity risk management programs to meet the objectives of the Cybersecurity Framework released by the National Institutes of Standards and Technology (NIST) in February 2014. The voluntary

Cybersecurity Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure and was developed in response to Executive Order 13636 “Improving Critical Infrastructure Cybersecurity” through collaboration between industry and government. In developing this guidance, the Energy Department collaborated with private sector stakeholders through the Electricity Subsector Coordinating Council and the Oil & Natural Gas Subsector Coordinating Council. The Department also coordinated with other Sector Specific Agency representatives and interested government stakeholders.

As a result, in 2015, the Energy Sector Cybersecurity Framework Implementation Guidance [6] was developed and adopted, which is a comprehensive guide to creating a cybersecurity system in the energy industry.

Australia:

After the start of a new phase of the Russian-Ukrainian war on February 24, 2022, the Australian government issued a warning about the need to be ready for cyber attacks from pro-Russian attackers and began to develop appropriate requirements. It is planned that the requirements will meet the requirements of MITER ATT&CK framework. [7]

Analyzing world experience, it is obvious that Ukraine needs to comply, first of all, with the requirements of the EU, but at the moment only the basic Law of Ukraine "About Critical Infrastructure" has been adopted. It will enter into force only on June 15, 2022 and will finally create a special body that will have to develop requirements for the protection of critical infrastructure and create a register of critical infrastructure objects. Also, according to the text of the Law, a list of types of organizations is included, which, according to their type of activity, belong to critical infrastructure. Energy is included in this list. In addition, an important innovation of this law is the introduction of a risk-based approach and the requirement for insurance of security risks.

However, since the Law has not yet entered into force, the register of critical infrastructure facilities has not been created, and the requirements have not been

developed and put into effect, it can be stated that special requirements for the protection of critical infrastructure, including in the field of cyber security, including in energy - does not exist.

It should also be noted that all the considered approaches - European, American and Australian have one common feature, which makes them insufficient in the conditions of the war in Ukraine. They do not assume that part of the country's territory and objects can be captured and controlled by the enemy for a long time, which allows the enemy to gain long-term and complete access to the entire infrastructure from internal network terminals. In addition, there is no well-established and standardized procedure for removing the IT infrastructure from attack after the release of the object.To do this, it is necessary to generalize into single standards the experience and standards of digital forensics, and approaches to responding to and investigating cyber incidents developed by organizations such as NIST and SANS.

In addition, liability for non-compliance with information protection requirements provided by Article 363 of the Criminal Code of Ukraine "Violation of the rules of operation of computers, automated systems, computer networks or telecommunications networks or the procedure or rules of information protection, which is processed in them, if it caused significant damage to the person responsible for their operation, "- shall be punishable by a fine of five hundred to one thousand tax-free minimum incomes or restriction of liberty for up to three years with deprivation of the right to hold certain positions or certain activities for the same period.

This measure of punishment is not significant, which also leads to problems with meeting even the current requirements.

Thus, studies have shown that, in the context of the war in Ukraine, the key problems for cybersecuritycompliance in EPES are:

1. There are no clear and mandatory requirements and standards for ensuring cybersecurity in the energy sector;

2. Insufficient level of penalties for failure to comply even with the existing general requirements for the protection of information in information systems;

3. The absence of a regulator that can check energy infrastructure facilities for compliance with requirements;

4. The lack of developed procedures in the world to ensure the cyber security of the state's power system in the event that a number of key objects of this infrastructure are captured by the enemy for a long time, including special requirements, if possible, cutting off the captured sections of the IT infrastructure from the general infrastructure of the power company;

5. The absence of special requirements, protocols and procedures, and as a result, of specialists capable of ensuring the return of the infrastructure liberated from the enemy to its original protected state and the removal of all possible software tabs left by the enemy.

To solve these problems, it would be optimal to involve world experts, especially from the US and the EU, since the experience gained in Ukraine will be unique and will certainly be of interest to our allies.

REFERENCES

1. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, URL: https://eur-lex.europa.eu/eli/dir/2008/114/ojApplication date: 15.05.2022.

2. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), URL: https://eur-lex.europa.eu/eli/reg/2019/881/ojApplication date: 15.05.2022.

3. Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector (notified under document C(2019) 2400), URL:https://eur-lex.europa.eu/eli/reco/2019/553/ojApplication date: 15.05.2022.

4. Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 (Text with EEA relevance.), URL: https://eur-lex.europa.eu/eli/reg/2017/1938/ojApplication date: 15.05.2022.

5. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (Text with EEA relevance.), URL: https://eur-lex.europa.eu/eli/reg/2019/941/ojApplication date: 15.05.2022.

6. Energy Sector Cybersecurity Framework Implementation Guidance, URL: https://www.energy.gov/sites/default/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdfApplication date: 15.05.2022.

7. 2022-02: Australian organisations should urgently adopt an enhanced cyber security posture, URL:https://www.cyber.gov.au/acsc/view-all-content/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-postureApplication date: 15.05.2022.

Цуркан Оксана Володимирівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
otsurkan24@gmail.com

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

Яшенков Вадим Петрович,
ІЕЗ ім. Є.О. Патона НАН України,
науковий співробітник,
vadym.yashenkov@gmail.com

Клименко Тетяна Михайлівна,
ІПМЕ ім. Г.Є. Пухова НАН України,
завідувачка відділу,
klimenko-t@ukr.net

РІВНІ АНАЛІЗУВАННЯ УРАЗЛИВОСТЕЙ СОЦІОТЕХНІЧНИХ СИСТЕМ ДО ВПЛИВІВ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Анотація. Приділено увагу процесу аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії. Показано необхідність встановлення їх наявності/відсутності. До того ж врахування особливостей впливів соціальної інженерії з огляду на використання маніпулятивних форм. З огляду на це визначено рівні аналізування уразливостей соціотехнічних систем. Це дозволило виокремлювати як екторів впливів соціальної інженерії, так і встановлювати їхні особливості.

Annotation. Attention is paid to the process of analyzing the vulnerabilities of socio-technical systems to the effects of social engineering. The necessity of identifying their presence/absence is shown. In addition, the peculiarities of the social engineering effects in view of the use of manipulative forms is taken into account. Due to this, the levels of analysis of vulnerabilities of socio-technical systems are determined. This made it possible to single out both the actors of the influences of social engineering and to identify their features.

Протидія впливам соціальної інженерії на безпеку соціотехнічних систем досягається аналізуванням уразливостей їх користувачів. У цьому випадку необхідно встановити наявність/відсутність таких впливів, з одного боку. Тоді як з іншого – виявити їхні особливості з огляду на використання відповідних маніпулятивних форм. Тому визначення рівнів аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії є актуальним завданням.

Рівні аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії відображаються підграфом виду [1, 2]

$$\underset{\sim}{G_S} \subseteq \underset{\sim}{G}$$

де $\underset{\sim}{G_S}$ – підграф нечіткого направленого соціального графу $\underset{\sim}{G}$.

Таке відображення дозволяє залежно від кількості вершин виокремлювати рівні ектора, пари екторів (діад), трьох екторів (тріад). Так, на рівні пари екторів задається підграф двома вершинами та дугою між ними. Вони можуть знаходиться у одному з двох станів, наприклад [1, 3]:

– вплив соціального інженера, v_1, на користувача соціотехнічної системи, v_3 , $\underset{\sim}{G_S} = \{((v_1, v_3) \mid \underset{\sim}{\mu_G}(v_1, v_3))\}$;

– відсутність впливу соціального інженера, v_1, на користувача соціотехнічної системи, v_3, $\underset{\sim}{G_S} = \{((v_1, v_3) \mid 0)\}$

На рівні трьох екторів можливе врахування особливостей впливів соціальної інженерії. Це досягається представленням підграфу трьома вершинами та дугами між ними, наприклад [1, 3]:

– опосередкований вплив соціального інженера, v_1, з урахуванням обману як маніпулятивної форми, v_2, на користувача соціотехнічної системи, v_3, $\underset{\sim}{G_S} = \{((v_1, v_2) \mid \underset{\sim}{\mu_G}(v_1, v_2)), ((v_1, v_3) \mid 0), ((v_2, v_3) \mid \underset{\sim}{\mu_G}(v_2, v_3))\}$;

– безпосередній вплив соціального інженера, v_1, на користувача соціотехнічної системи, v_3, $\underset{\sim}{G}_S = \{((v_1, v_2) \mid 0), ((v_1, v_3) \mid \underset{\sim}{\mu}_G(v_1, v_3)), ((v_2, v_3) \mid 0)\}$.

Отже, визначення рівнів аналізування уразливостей соціотехнічних систем дозволило виокремлювати як екторів впливів соціальної інженерії, так і встановлювати їхні особливості. Насамперед використання маніпулятивних форм стосовно користувачів зазначених систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Герасимов Р., Крук О., Цуркан О., Яшенков В. Метод аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії. *Information Technology and Security*. January – June 2020. Vol. 8, Iss. 1. P. 31–39. DOI: https://doi.org/10.20535/2411-1031.2020.8.1.218001.

2. Tsurkan O. V., Herasymov R. P., Kruk O. M., Presentation the interaction of the subject and the object of socio-engineering influence with a social graph", *Computer and Informational Systems and Technologies* : Fourth International Scientific and Technical Conference, Kharkiv, 2020, P. 46. doi: 10.30837/IVcsitic2020201371.

3. Moderson J. N., Nair P. S., Fuzzy Graphs and Fuzzy Hypergraphs. Heidelberg, Germany: Physica-Verlag Heidelberg, 2000. DOI: 10.1007/978-3-7908-1854-3.

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

ПРАКТИЧНІ АСПЕКТИ ТЕСТУВАННЯ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ ЯК ЕЛЕМЕНТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ГАЛУЗІ ЕНЕРГЕТИКИ

Анотація. Виокремлено мобільні програмні застосунки як елемент критичної інформаційної інфраструктури галузі енергетики. Проаналізовано способи тестування їх уразливостей, зокрема, розглянуто статичний, динамічний.Встановлено обмеженість використання даних способів на практиці. Подолання встановленого обмеження досягнуто завдяки запропонованому комбінованому способові тестування уразливостей мобільних програмних застосунків. З огляду на практичні аспекти його використання можливепоєднаннярізноманітних сценаріїв порушення властивостей інформації. До того ж з урахуванням розроблення і виконання експлойтів.

Annotation. Mobile software applications as an element of critical information infrastructure of energy sector are singled out. Methods of testing their vulnerabilities are analyzed and it has been paid attention on static and dynamic vulnerabilities. Practical limited use of these methods has been established. Overcoming this limitation is achieved due to the proposed combined method of testing vulnerabilities in mobile software applications. Given the practical aspects of its use, a combination of different scenarios of violation of the properties of information is possible. In addition, it has been considered the development and implementation of exploits.

Одним із основних елементів критичної інформаційної інфраструктури галузі енергетики є мобільні програмні застосунки. Вони тестуються стосовно наявностівразливостей. Це дозволяє встановлювати збереженість властивостей інформації, яка обробляється мобільними програмними застосунками. З огляду на це, більшість організацій зі стандартизації та сертифікації орієнтовані на

рекомендування і застосування власних підходів до тестування уразливостей. Разом з тим, загальноприйнятим для них є використання стандарту OWASP MASVS та методології OWASP MSTG. Даними нормативними документами визначаються сценарії тестування уразливостей мобільних програмних застосунків [1–3]. Тож виокремлення його практичних аспектів є актуальним завданням.

Встановлено обмеженість використання відомих інструментальних засобів (зокрема,статичного та/або динамічного способів)[4]. Для її подолання запропоновано виконання декількох різних сценаріїв тестування уразливостей мобільних програмних застосунків шляхом комбінування статичного, динамічного способів, а також використання експлойтів (рис. 1, 2).

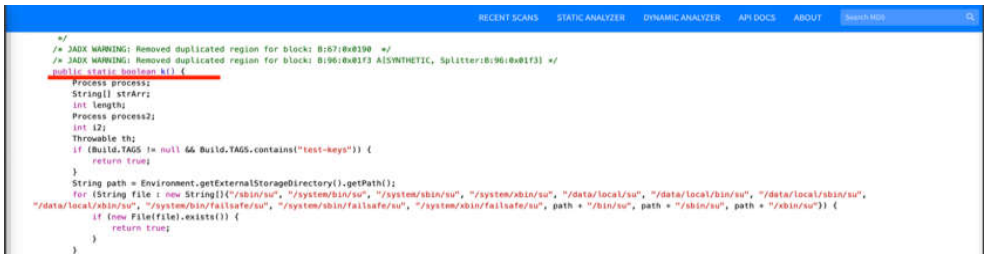

Рисунок 1 – Приктичний аспект аналізування вихідного коду функціоналу перевірки запуску мобільного програмного застосунку у статичному аналізаторі

Рисунок 2 – Практичний аспект обходження механізмів захисту мобільного програмного застосунку

Отже, досліджено мобільні програмні застосунки як елемент критичної інформаційної інфраструктури. Показано обмеженість використання статичного

та динамічного способів тестування їх уразливостей. Для її подолання запропоновано комбінований спосіб розв'язадання даного завдання. Зважаючи на це, приділеного увагу практичним аспектам його використання стосовно збереження властивостей інформації у мобільних програмних застосунках.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Antonishyn M., Misnik O. Analysis of testing approaches to Android mobile application vulnerabilities, *Information Technologies and Security* : Selected Papers of the XIX International Scientific and Practical Conference. Vol. 2577. Aachen, Germany : CEUR WS, 2019. P. 270-280. URL: http://ceur-ws.org/Vol-2577/paper22.pdf. E-ISSN 1613-0073.
2. OWASP Mobile security testing guide (MSTG). URL: https://github.com/OWASP/owasp-mstg/ (дата звернення: 14.02.2022).
3. OWASP Mobile security application verification standard (MASVS). URL: https://github.com/OWASP/owasp-masvs/ (дата звернення: 14.02.2022).
4. National Institute of Standards and Technology, NIST 800-163. Vetting the Security of Mobile application. URL: https://doi.org/10.6028/NIST.SP.800-163r1 (дата звернення: 14.02.2022).

Мохор Володимир Володимирович,
ІПМЕ ім. Г.Є. Пухова НАН України,
директор,член-кореспондент НАН України, д.т.н., професор,
v.mokhor@gmail.com

Цуркан Василь Васильович,
НТУУ «КПІ ім. Ігоря Сікорського»;
ІПМЕ ім. Г.Є. Пухова НАН України,
доцент; старший науковий співробітник
v.v.tsurkan@gmail.com

ІНТЕГРОВАНА СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СФЕРИ ЕНЕРГЕТИКИ

Анотація. Показано необхідність гарантування безпечності надання енергетичних послуг і оброблення інформації насамперед про їх споживачів. Запропоновано розроблення і впровадження на об'єктах критичної інфраструктури сфери енергетики інтегрованої системи управління інформаційною безпекою. Це дозволить забезпечити збереженість цілісності, доступності, конфіденційності та приватності інформації з прийнятним рівнем ризику.

Annotation. The necessity of guaranteeing the security of energy services and processing information about their consumers is shown. The development and implementation of an integrated information security management system at critical energy infrastructure facilities is proposed. This will ensure the integrity, accessibility, confidentiality and privacy of information with an acceptable level of risk.

Відповідно до [1] об'єктами сфери енергетики надаються життєво важливі послуги. Їх порушення може призвести до настання негативних наслідків як для окремих громадян, так і країни загалом. Сукупністю таких об'єктів визначається критична інфраструктура сфери енергетики. Цим обумовлюється забезпечення її інформаційної безпеки та, зокрема, кібербезпеки. Для цього на об'єктах критичної інфраструктури сфери

енергетики розробляються системи управління інформаційною безпекою [2–4]. Упровадженням таких систем досягається збереженість властивостей інформації (конфіденційності, цілісності та доступності) з прийнятним рівнем ризику. Завдяки цьому гарантується належність його оброблення і, як наслідок, безпечність надання енергетичних послуг.

Разом з тим окрема увага приділяється збереженню приватності інформації насамперед споживачів енергетичних послуг [5]. Тож розроблення інтегрованої системи управління інформаційною безпекою об'єктів критичної інфраструктури сфери енергетики є актуальним завданням.

Інтегрованою системою об'єднуються діяльності управління інформаційною безпекою, кібербезпекою та приватною інформацією. Характерною особливістю такого об'єднання є орієнтованість на збереження цілісності, доступності, конфіденційності та приватності інформації об'єктів критичної інфраструктури сфери енергетики. Для цього як базова виокремлюється система управління інформаційною безпекою. Це вказує на задоволеність вимог [3] і можливість формулювання на їх основі побажань і очікувань від реалізування настанов [4] і [5]. Такий підхід дозволяє розробити системи управління кібербезпекою і приватною інформацією з урахуванням задоволених вимог [3]. Як наслідок, функційність їхніх елементів визначається з огляду на заходи, що направлені на змінення, утримання, уникнення та/або розподілення ризиків інформаційної безпеки. Кожен з них характеризується назвою, категорією та набором атрибутів. Серед атрибутів виокремлюються: врахування впливу на ризик; збереження властивостей інформації (конфіденційність, цілісність, доступність, приватність); діяльність зі забезпечення кібербезпеки; можливості забезпечення інформаційної безпеки; можливості забезпечення приватності інформації; домени забезпечення безпеки.

Отже, розроблення інтегрованої системи управління інформаційної безпеки об'єктів критичної інфраструктури дозволить гарантувати належність оброблення ризиків і, як наслідок, безпечність надання життєво важливих

енергетичних послуг і оброблення інформації пронасамперед їх споживачів з прийнятним рівнем ризику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру : Закон України від 16.11.2021 №1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 05.05.2022).

2. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету міністрів України від 19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text(дата звернення: 05.05.2022).

3. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. [Valid from 2013-09-25; revised 2018-12-04]. URL: https://www.iso.org/standard/54534.html (accessed on: 05.05.2022).

4. ISO/IEC 27032:2012. Information technology. Security techniques. Guidelines for cybersecurity. [Valid from 2012-07-16; revised 2018-12-13]. URL: https://www.iso.org/ standard/44375.html (accessed on: 05.05.2022).

5. ISO/IEC 27701:2019. Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines. [Valid from 2019-08-05]. URL: https://www.iso.org/standard/71670.html (accessed on: 05.05.2022).

ЗМІСТ

ANFIMOVA G.V.
A risk-oriented approach to improving the quality of operation and the environment of urban heat supply pipelines 4

VLADIMIRSKY A.A., VLADIMIRSKY I.A., KUTSAN Y.G., KRIVORUCHKO I.P., ANFIMOVA G.V.
Parametric correlation methods for operational remote passive determination of the coordinates of leaks and associated corrosion damage in underground pipelines..……. 7

ВЛАДИМИРСЬКИЙ О.А., АРТЕМЧУК В.О., ДЮКОВ В.А.
Розроблення засобів вимірювання геометричних розмірів вигородки активної зони ядерних реакторів… …… 15

ВЛАДИМИРСЬКИЙ О.А., ВЛАДИМИРСЬКИЙ І.А., КРИВОРУЧКО І.П., АНФІМОВА Г.В.
Адаптація сертифікованих засобів вимірювання параметрів руху до актуальних завдань масштабного відновлення пошкодженого ліфтового обладнання……. 18

ВЛАДИМИРСЬКИЙ О.А., ВЛАДИМИРСЬКИЙ І.А.
Про завдання розвитку засобів і технологій оперативного пошуку витоків та періодичного корозійного мониторингу міських підземних трубопроводів в умовах повоєнної економіки…… 21

Гільгурт С.Я.
Поводження з параметрами баз даних сигнатур реконфігуровних систем захисту інформації в енергетиці…….. 25

ДЯЧЕНКО С.М.
Задача моделювання модальних характеристик складного збірного сонотроду для ультразвукового зварювання полімерів……. 31

ДЖИГУН О.М.
Дострокове прогнознозування виробництва електроенергії ВЕС і СЕС. 35

ВАСИЛЬЄВ О.В., ЧЬОЧЬ В.В.
Методика пошуку законодавчих документів у сфері кібербезпеки …… 41

ЗУБОК В.Ю., ДАВИДЮК А.В.
Модернізація систем безпеки інформації об’єктів критичної інфраструктури в період післявоєнної відбудови…….. 47

ДАВИДЮК А.В.
Кіберзахист та кібероборона критичної інфраструктур…… 50

ДУШАБАЄВ Р.Т., ЧЕМЕРИС О.А.
Використання генетичного алгоритму для оптимізації розміру тайлу…… 53

КОВАЛЕНКО О.Є.
Формування спроможностей систем ситуаційного управління безпекою…… 56
КОВАЛЬЧУК Л.В.
Переваги використання смарт-контрактів в енергетиці та проблеми, які потрібно вирішити для їх використання…… 60
МИТЬКО Л.О.
Людський фактор у проблемі кібербезпеки енергетичних об’єктів……. 67
ОСТАПЧЕНКО К.Б., ЄВДОКІМОВ В.А., БОРУКАЄВ З.Х.
Інтерфейс взаємодії з базою даних «моделі процесів функціонування ринку електричної енергії»…….. 70
ОГІР О.О., ЦУРКАН О.В.
Кібербезпека та стійкість об'єктів енергетичного сектору в суспільстві та державі в звичайних, критичних і надзвичайних ситуаціях…… 80
ПАХОЛЬЧЕНКО Д.В., БАКАЛИНСЬКИЙ О.О.
Перелік етапів реагування на кіберінциденти та рівні їх критичності…. 84
БАКАЛИНСЬКИЙ О.О., ПАХОЛЬЧЕНКО Д.В.
Особливості застосування норм міжнародного гуманітарного права в питаннях ведення кібероборони…….. 90
ХРИСТИНЕЦЬ Н.А.
Етапи програмуванняна assemblerдрайверів клавіатури та екрану для мікроядра операційної системи…… 99
ХУДИНЦЕВ М.М.
Концепція забезпечення кібербезпеки енергетичної галузі україни…… 102
KOTSIUBA I.V., CHAIKIN M.M.
Problems of compliance with cybersecurity requirements in the energy industry of ukraine in war conditions and their comparison with world practices and requirements……..... 109
ЦУРКАН О.В., ГЕРАСИМОВ Р.П., ЯШЕНКОВ В.П., КЛИМЕНКО Т.М.
Рівні аналізування уразливостей соціотехнічних систем до впливів соціальної інженерії……. 117
АНТОНІШИН М.В.
Практичні аспекти тестування мобільних програмних застосунків як елементів критичної інформаційної інфраструктури галузі енергетики…… 120
МОХОР В.В., ЦУРКАН В.В.
Інтегрована система управління інформаційною безпекою об’єктів критичної інфраструктури сфери енергетики…… 123

МАТЕРІАЛИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»
27 травня 2022 року

Відповідальні за випуск:

О.В. Цуркан, Т.М. Клименко

Місце проведення: Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України; м. Київ, вул. Генерала Наумова, 15. Їхати від станції метро «Академмістечко» автобусом № 97, № 97к або марш. таксі № 497, № 200к, № 408, № 437 до зупинки «Інститут моделювання».

З питаннями щодо конференції звертатися:

ІПМЕ ім. Г.Є. Пухова НАН України, вул. Генерала Наумова, 15, кім. 303, Цуркан Оксана володимирівна, тел. 424-91-62, 068-014-57-22, e-mail: otsurkan24@gmail.com

---

Інститут проблем моделювання в енергетиці
ім. Г. Є. Пухова НАН України,
вул. Генерала Наумова, 15, Київ, 03164, Україна,
тел.: +38 044 424 91 62, факс: +38 044 424 10 63
веб сайт: https://ipme.kiev.ua/