НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

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

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

31 травня 2023 року

Київ – 2023

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 25 травня 2023 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 31 травня 2023 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2023. 125 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 31, 2023. Kyiv: PIMEE NAS of Ukraine, 2023. 125 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, старший науковий співробітник
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

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

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

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

Клименко Тетяна Михайлівна
Завідувачка науково-організаційного відділу

Цуркан Оксана Володимирівна
молодший науковий співробітник

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

Цуркан Василь Васильович,
КПІ ім. Ігоря Сікорського;
ІПМЕ ім. Г.Є. Пухова НАН України,
доцент; старший науковий співробітник, к.т.н., доц.,
v.v.tsurkan@gmail.com

СПОСІБ УРАХУВАННЯ ДИНАМІКИ ФОРМУВАННЯ СЦЕНАРІЇВ ТЕСТУВАННЯ УРАЗЛИВОСТЕЙ МОБІЛЬНИХ ПРОГРАМНИХ ЗАСТОСУНКІВ

Анотація. Розглянуто формування сценаріїв тестування уразливостей мобільних програмних застосунків. Продемонстровано упорядкування послідовності кейсів вершинами графа залежностей. Виокремлено обмеженість його застосування за необхідності додавання або видалення нових етапів тестування. Дане обмеження подолано розширенням графу залежностей складником діяльності та інтерпретованого його як динамічний. Використання такого способу дозволило врахувати динаміку формування та відображати сформовані сценарії снепшотами.

Abstract. The formation of vulnerability testing scenarios for mobile applications has been considered. The ordering of the sequence of test cases by graph vertices in the dependency graph has been demonstrated. The limitation of its application has been identified in cases where the addition or removal of new testing stages is required. This limitation has been overcome by expanding the dependency graph with an activity component and interpreting it as dynamic. The use of this approach allows for the consideration of the dynamics of formation and the representation of formed scenarios through snapshots.

Відповідно до [1] послідовність кейсів тестування уразливостей мобільних програмних застосунків упорядковується у сценарій вершинами графа залежностей. Завдяки такому відображенню кожен наступний кейс може реалізовуватися тільки за умови виконання попереднього. Це вказує на існування залежностей між ними і дозволяє обґрунтовувати обирання як етапів тестування, так і встановлення їхньої послідовності. Водночас на практиці поширені випадки необхідності реалізування додаткових кейсів і, як наслідок, появи нових вузлів і залежностей відповідного графу. [1, 2] Тож визначення способу врахування динаміки формування сценаріїв тестування уразливостей мобільних програмних застосунків є актуальним завданням.

Задоволення потреби щодо врахуванням необхідності реалізування додаткових кейсів тестування уразливостей мобільних програмних застосунків досягнуто завдяки використанню динамічного графу залежностей [1, 3, 4]. Таке

розширення дозволило виокремити два складники його представлення, зокрема, статичного графу залежності G у момент часу t_0 та діяльності O в моменти часу t_i, $0 < t_i < n$,

$$G_D = \{G, O\}.$$

Діяльність O характеризується типом дії (наприклад, додавання кейсу тестування, AddNode(); додавання залежності між кейсами тестування AddEdge(); видалення кейсу тестування, RemoveNode(); видалення залежності між кейсами тестування, RemoveEdge()); дією (вказується кейс тестування (вузол) або залежність між кейсами тестування (ребро), які додаються або видаляються); міткою часу t_i. Використання такого способу дозволяє зберігати поточні сценарії тестування уразливостей мобільних програмних застосунків, t_{i-1}, снепшотом S, при переході до наступного. Наприклад, при тестуванні зберігання даних під управлінням операційної системи Android необхідно встановити та налаштувати додаткові інструментальні засоби (Drozer, am). Це потрібно для перевіряння відкритих компонентів (Activities або ContentProviders) зазначеної операційної системи.

Отже, визначено спосіб урахування динаміки формування сценаріїв тестування уразливостей мобільних програмних застосунків. Це досягнуто розширенням графу залежностей складником діяльності та, як наслідок, інтерпретуванням його як динамічного. Таке використання дозволило врахувати необхідність додавання/видалення кейсів при формуванні сценаріїв тестування уразливостей мобільних програмних застосунків. Крім того зберігати сформовані їхні варіанти снепшотами за потреби внесення до них змін.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонішин М. В., Цуркан В. В. *XLI науково-технічна конференція молодих вчених та спеціалістів Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* : збірник матеріалів конференції (Київ, 17 травня 2023 р.). Київ, 2023. С. 28.
2. Antonishyn M. The usage of dependency graphs to test the security of mobile software applications. *Computer and Information Systems and Technologies* : proceedings of the 4th international scientific and technical conference (Kharkiv, 22–23 April 2020). Kharkiv, 2020. P. 44. DOI: https://doi.org/10.30837/IVcsitic2020201369.
3. Mehran S., Kazemi, Goe R. Representation Learning for Dynamic Graphs : A Survey. *Journal of Machine Learning Research*. 2020. Vol. 21. P.1–73. URL: https://www.jmlr.org/papers/volume21/19-447/19-447.pdf (accessed on: 10.05.2023).
4. Sleator D., Tarjan R. A Data Structure for Dynamic Trees. Journal of Computer and Systems science. June 1983. Vol. 26, No. 3. P. 362–391. URL: https://www.cs.cmu.edu/~sleator/papers/dynamic-trees.pdf.

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

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

ОСОБЛИВОСТІ ВИМОГ ДО КІБЕРЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ТА АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ: АНАЛІЗ ТА ПОРІВНЯННЯ

Відповідно до постанови Кабінету Міністрів України від 09.10.2020 № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури» потенційними об'єктами критичної інформаційної інфраструктури (далі – ОКІ) можуть бути: автоматизовані, інформаційні, комунікаційні, інформаційно-комунікаційні системи (далі – ІКС) та автоматизовані системи управління технологічними процесами (далі – АСУ ТП) [1].

Виникає питання, чи достатньою буде умова впровадження на ОКІ, на якому експлуатується АСУ ТП, системи управління інформаційною безпекою (далі – СУІБ), яка побудована за вимогами ідентичними до СУІБ, що захищає ІКС. Однозначно ні, адже АСУ ТП на відміну від ІКС є системою реального часу, в якій вимоги до часу реакції в аварійних ситуаціях є вкрай критичним, а затримка та втрата даних є неприйнятним, що формує свій, притаманний тільки АСУ ТП набір ризиків.

Усі експерти в області інформаційної безпеки погоджуються [2–4], що забезпечення безпеки АСУ ТП відрізняється від забезпечення безпеки звичайних (корпоративних) інформаційних, ІКС. Навіть сам термін «інформаційна безпека», настільки звичний ІТ-фахівцям, як правило, не застосовується до АСУ ТП. Впершу чергу, це пов'язано з тим, що при забезпеченні інформаційної безпеки АСУ ТП необхідно приділяти увагу не тільки і не стільки забезпеченню конфіденційності, скільки забезпеченню безперервності і цілісності самого технологічного процесу [5]. Більш того, безпека технологічного процесу в загальному сенсі – це, перш за все, безпека життя і здоров'я людей та навколишнього середовища.

Відповідно, актуальним залишається питання порівняння ІКС та АСУ ТП з точки зору вимог до їх кіберзахисту, в тому числі у визначені відмінностей у аналізі та оцінці ризиків інформаційної безпеки під час розробки та впровадження на них СУІБ.

Отже, для початку виділимо різницю між ІКС та АСУ ТП. ІКС – це система, що забезпечує обмін, збереження та обробку інформації між різними об'єктами (комп'ютерами, серверами, сенсорами) за допомогою засобів телекомунікацій. ІКС може включати в себе різні компоненти, такі як мережі передачі даних, програмне забезпечення, обчислювальні системи та пристрої збору даних.

АСУ ТП – це система, що забезпечує автоматизоване управління технологічними процесами виробництва, контроль та регулювання технологічних параметрів, моніторинг та діагностику виробництва, а також оптимізацію роботи виробництва в цілому. АСУ ТП може включати в себе різні компоненти, такі як датчики, контролери, програмне забезпечення та пристрої керування.

Відповідно, різниця між ІКС та АСУ ТП полягає в їх призначенні та функціях. ІКС забезпечує обмін та обробку інформації, тоді як АСУ ТП забезпечує автоматизоване управління технологічними процесами виробництва. Однак, ці дві системи можуть взаємодіяти між собою, щоб забезпечити більш ефективне та автоматизоване управління виробництвом.

Далі варто здійснити порівняння вимог до кіберзахисту ІКС та АСУ ТП, оскільки це дві різні області захисту. Основні відмінності включають наступне:

Об’єкти захисту: кіберзахист ІКС зосереджений на захисті інформації та інформаційних систем, тоді як кіберзахист АСУ ТП, як було сказано вище, спрямований на захист виробничих процесів, устаткування та контролюючих систем.

Завдання захисту: завдання кіберзахисту ІКС інколи відрізняються від завдань кіберзахисту АСУ ТП. Кіберзахист ІКС націлений на забезпечення конфіденційності, цілісності та доступності даних, тоді як кіберзахист АСУ ТП зосереджений на запобіганні аварій та забезпеченні безперебійної роботи виробничих процесів.

Рівень ризику: ризик кіберзагроз для АСУ ТП вищий, оскільки порушення безпеки може призвести до аварій виробничих процесів та матеріальних збитків. Однак, порушення безпеки ІКС також може мати серйозні наслідки, такі як витік конфіденційної інформації або недоступність важливих систем.

Засоби захисту: засоби захисту ІКС та АСУ ТП можуть бути різними, в залежності від конкретних вимог та умов застосування. Наприклад, захист АСУ ТП може включати системи моніторингу, контролю доступу, антивірусні програми, фізичні бар’єри та інші технічні та організаційні заходи, які допомагають захистити виробничі процеси. Захист ІКС може включати шифрування даних, контроль доступу, моніторинг мережі.

Різноманітності підходів до кіберзахисту ІКС та АСУ ТП можуть бути зумовлені наступними відмінними функціями та характеристиками систем:

- різний тип даних, які обробляються в ІКС та АСУ ТП. Наприклад, в ІКС можуть бути великі обсяги текстової інформації, в той час як в АСУ ТП можуть бути складні технічні процеси зі значною кількістю сигналів;
- різний рівень доступу до систем. Деякі компоненти ІКС можуть бути доступні для широкого кола користувачів, в той час як АСУ ТП може мати обмежений доступ для забезпечення безпеки;
- різна кількість підключених компонентів. АСУ ТП може містити багато різних пристроїв і компонентів, які потрібно захищати, тоді як ІКС може містити меншу кількість компонентів;
- різний рівень автоматизації процесів. АСУ ТП може мати високий рівень автоматизації процесів, тоді як в ІКС процеси можуть бути виконані вручну;

– різна критичність систем. АСУ ТП може бути критично важливим для безпеки та життєво важливих процесів, тоді як ІКС може бути менш критичним;

– різні типи загроз та атак. Загрози та атаки можуть відрізнятися в залежності від типу системи та її характеристик.

ІКС та АСУ ТП є дуже вразливими до кібератак з причини їхньої відкритості до мережі Інтернет та залежності від програмного та апаратного забезпечення. Серед специфічних загроз для ІКС та АСУ ТП можна виокремити шкідливі програми (віруси, трояни), фішинг, DDoS-атаки, атаки на протоколи керування, мережеві атаки з використанням вразливостей в програмному забезпеченні та апаратурі. Всі ці загрози можуть призвести до порушення безпеки системи та втрати конфіденційної інформації, а також можуть мати серйозні наслідки для промислових процесів та контрольних систем.

Ефективним засобом захисту інформаційних систем, в тому числі ІКС та АСУ ТП, є побудова та впровадження на них СУІБ. Вона забезпечує комплексний захист від різноманітних загроз, включаючи виявлення та блокування шкідливих програм, моніторинг та аналіз мережевої активності, управління доступом до ресурсів системи та інші заходи забезпечення безпеки.

Однак, побудова та впровадження СУІБ для цих систем має свої відмінності, у тому числі в аналізі та оцінці ризиків інформаційної безпеки під час розробки та впровадження СУІБ.

Розробка та впровадження СУІБ для ІКС та АСУ ТП вимагає індивідуального підходу до аналізу та оцінки ризиків інформаційної безпеки. Відмінності в цьому підході полягають у специфічних потребах та вимогах до захисту інформації в кожному з цих випадків.

Для ІКС зазвичай важливим є захист від зовнішніх кібератак та захист від неправомірного доступу до систем та даних. Оцінка ризиків повинна бути спрямована на виявлення потенційних вразливостей в мережі, операційних системах та програмному забезпеченні, а також на визначення можливостей відновлення роботи системи у разі випадку збою або кібератаки.

У випадку АСУ ТП оцінка ризиків повинна враховувати специфіку промислових процесів та обладнання, що керує ними. Важливим є захист від несанкціонованого доступу до систем керування та контролю, а також від вторгнення в мережу через підключення до обладнання. Ризик-аналіз повинен охоплювати планування та запобігання можливих вторгнень, а також виявлення та усунення вразливостей у системах керування.

Отже, під час аналізу та оцінки ризиків інформаційної безпеки для ІКС та АСУ ТП важливо враховувати специфіку кожного з цих випадків та підходити індивідуально до оцінки ризиків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Деякі питання об’єктів критичної інформаційної інфраструктури : Постанова Кабінет Міністрів України від 09.10.2020 № 943. URL: Режим доступу: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.

2. Гончар С. Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури: дис. на здобуття наукового ступеня доктора техн. наук: 05.13.21, Київ, 2020. 326 с.

3. Бакалинський О. О. Модель та методи визначення проектних характеристик систем управління інформаційною безпекою : монографія, Київ, Україна : ТОВ «Три К», 2020. 162 с.

4. Мохор В. В., Богданов О. М., Бакалинский О. О. та Цуркан В. В. Дескриптивний аналіз аналогій між системами управління інформаційною безпекою та масового обслуговування. *Захист інформації*. 2017. Том 19, № 2. С. 119–126. DOI: https://doi.org/10.18372/2410-7840.19.11683.

5. NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security. URL: https://csrc.nist.gov/publications/detail/ sp/800-82/rev-2/final.

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,
учений секретар, к.т.н.,
victoria.choch@gmail.com

БІБЛІОГРАФІЧНИЙ ТА ПАТЕНТНИЙ ЛАНДШАФТ РЕЗУЛЬТАТІВ ДОСЛІДЖЕНЬ ПО ТЕМІ «ЗАХИСТ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»

Побудова патентного або бібліографічного ландшафту дає можливість дати оцінку прогресу у певній технологічній галузі чи географічному регіоні. Вона передбачає аналіз поданих, виданих або чинних патентів, або опублікованих результатів науково-технічних досліджень, а також фізичних або юридичних заявників та винахідників (авторів) відповідних документів, з метою отримання оцінки про стан інновацій у певній галузі [1]. Метою аналізу бібліографічного та патентного ландшафту є виявлення потенційних можливостей, ризиків і прогалин у розвитку наукових досліджень та техніко-технологічних розробок, а також надання інформації для прийняття рішень щодо організації інноваційних проєктів та комерціалізації результатів таких проєктів. У сучасних умовах аналіз тенденцій науково-технічного прогресу можливо тільки при спільному аналізі патентної та науково-технічної літератури та публікацій.

Для проведення процедури побудови бібліографічного та патентний ландшафту та демонстраційного аналізу результатів досліджень по темі «Захист об'єктів критичної інфраструктури» були обрані наступні бази даних: науко-метрична база даних SCOPUS та патентна база даних INPADOC (її безплатний варіант ESPACENET). Обрані бази даних широкодоступні в Україні, хоча для багатьох тем можна запропонувати інші науково-технічні (науково-метричні) та патентні бази даних.

База даних SCOPUS (компанія генератор ElsevierB.V.) характеризується одним з найбільших обсягів колекції документів (біля 80 млн. реферативно-бібліографічних записів), великою кількістю інформаційних атрибутів аналітичного характеру (на додаток до класичних бібліометричних характеристик.

Для експрес-аналізу бібліографічного ландшафту був проведений пошук в базі даних SCOPUS за формулою (1). Результати є актуальними на момент 14/02/2023.

Search SCOPUS =>***KEY («critical infrastructure" OR "Critical Infrastructures»)*** (1)

де «KEY» – інформаційне поле визначених автором ключових слів.

Результат = 6437 публікацій.

Можливе уточнення (фільтрація) результатів пошуку (1) з використання інформаційного пошуку за формулою (2):

Search SCOPUS => ***KEY («Critical Infrastructure Protection»)*** (2)

Результат = 830 публікацій.

Проте цього не варто робити, бо інформаційне поле «KEY» має суб'єктивне наповнення і не відображає в достатній мірі зміст та структуру публікації. Але дана термінологічна конструкція використана при бібліографічному – аналізі контенту і займає 3-є місце серед публікацій за популярністю.

Експрес-аналіз патентного ландшафту дає результати, що представлені на рис. 1 – рис. 3.

Рисунок 1 – Динаміка публікацій свідчить про стабільну інтенсивність протягом більш ніж 10 років, з локальним мінімумом у 2014-2015 році

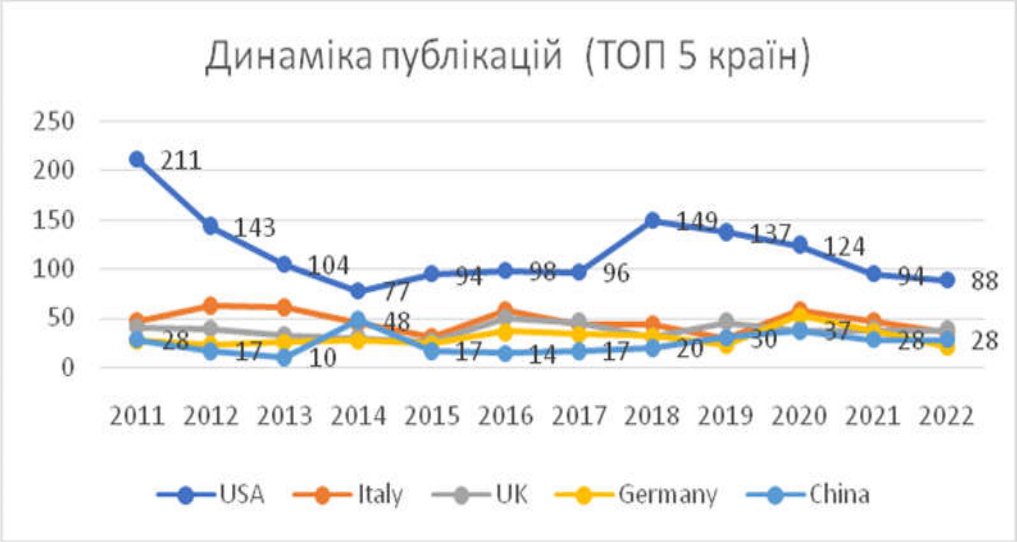

Рисунок 2 – Динаміка публікацій по країнам демонструє безперечне домінування публікацій авторів, які працюють у корпораціях США (у ТОП5 також входять такі країни, як Італія, Велика Британія, Німеччина та Китай

Рисунок 3 – Для побудови патентного ландшафту був проведений пошук в базі даних ESPACENT на технологічній платформі PatentPulse з використанням формули патентного пошуку (3)

$$SearchinPatent\text{-}Pulse => \underline{\textbf{\textit{ta:("critical infrastructure" OR "Critical Infrastructures")}}} \quad (3)$$

де “ta” – Інформаційне поле ключових слів у назві та рефераті патентного документу.

Результат пошуку: 97 патентних сімейств (268 патентів).

Експрес-аналіз патентного ландшафту дає результати, що представлені на Рис.4 - Рис.6.

Рисунок 4 – Динаміка патентування
(кількість патентів/рік пріоритету винаходу)

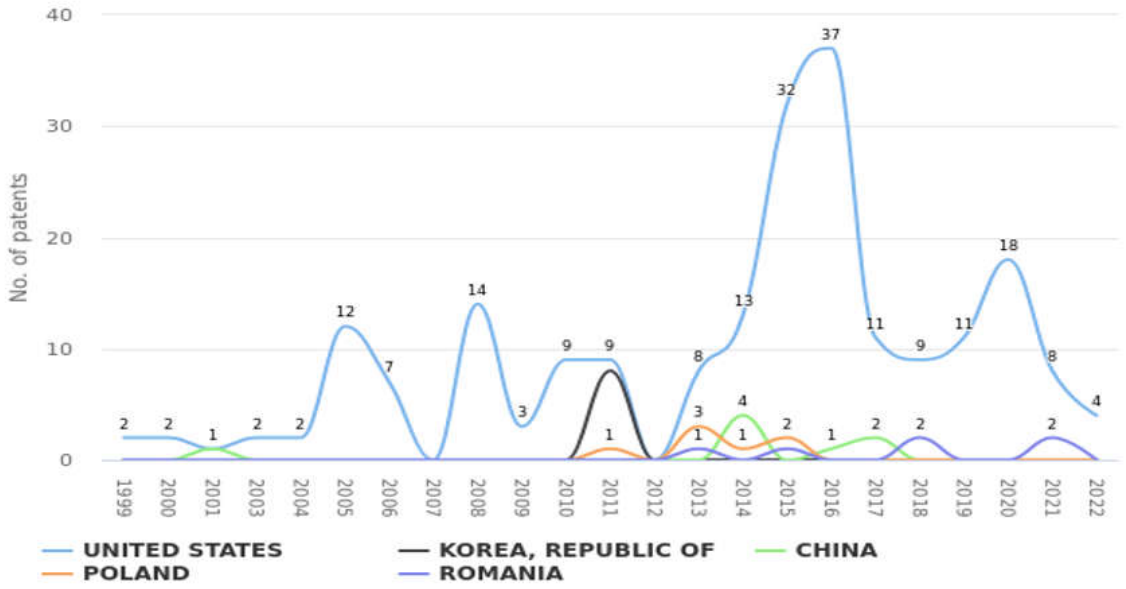

Рисунок 5 – Динаміка патентування ТОП-5 країн

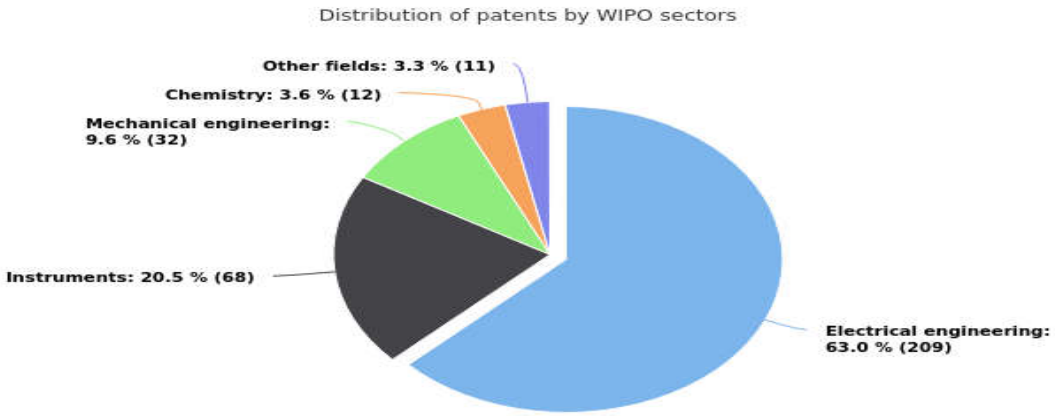

Рисунок 6 – Розподіл тем патентування винаходів

Загальним висновком є констатація факту, що очевидним лідером як наукового публікування, так і патентування є США. Китай присутній в обидвох рейтингах, але значно відстає за рівнем інтенсивності публікування/ патентування від США. Процеси публікування та патентування за останні роки демонструють стабільну інтенсивність з явно вираженим мінімумом у 2013-2014 р.р., та максимумом у 2018-2019 р.р. Тематичний аналіз патентів дає підстави стверджувати, що більше 60 % патентів відносяться до електротехнічних технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Trippe A. Guidelines for Preparing Patent Landscape Reports. Geneva : WIPO Publication No. 946E , 2015. 131 p.

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

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

ВИЗНАЧЕННЯ КООРДИНАТ ВИТОКІВ ПІДЗЕМНИХ ТРУБОПРОВОДІВ В УМОВАХ МАЛОГО ВІДНОШЕННЯ СИГНАЛ-ЗАВАДА

Причини малого відношення сигнал-завада.

Звичайним проявом малого відношення сигналу витоку до завад (сигнал-завада) у реєстрованих датчиками кореляційного течешукача сигналах є обчислена взаємна кореляційна функція (ВКФ) виду рис. 1а. Її характерною рисою є відсутність чіткої кореляції, відсутність явно переважного над іншими осциляціями ВКФ сплеску з обмеженим у часі інтервалом кореляції. Причини цього явища бувають наступними: занадто малий витік, малий тиск у трубопроводі через пошкодження джерела води, через велику кількість чи величину поривів під час гідравлічних випробувань, коли, наприклад, котельній не вистачає води для створення достатнього для потужного шуміння витоку тиску у трубах, внаслідок значного загасання акустичних сигналів від витоків при їх поширенні по трубопроводу зі щільною ізоляцією. У таких випадках пошук витоку є утрудненим, потребує більше часу на ретельні вимірювання і не завжди дає позитивні результати. Далі даються способи визначення місця витоку у таких випадках.

Робота з кореляційним течешукачем К-10.5М2.

Координата витоку знаходиться за допомогою аналізатора dt ВКФ [1–4], у поєднанні з визначенням 2–4 ВКФ зі зсувом датчиків у місцях доступу до трубопроводу на 0,5–3 м. При цьому відбувається ефективний, сумісний, просторовий та частотний пошук в доступних до реєстрації сигналах корисних звуків витоків за їхньою кореляцією. Розпізнавання цієї кореляції ведеться за наявністю координатних поличок у частотному спектрі координат. Координатні полички є дуже зручним експрес-індикатором чутливості оцінки ВКФ до наявності або відсутності у структурі ВКФ інформативної кореляції. Це також має першорядне значення для реєстрації появи дефекту на ранній стадії, коли він ще не розвинулася у велике пошкодження [4], рис. 1. З рис. 1а видно, що у вихідній ВКФ інтервал вираженої інформативної кореляції відсутній. Це відбувається тому, що основна енергія ВКФ, позначена графіком S_{mf} на рис. 1в, поки що сформована фоновими шумами, про що свідчать сильно осцилюючий вид спектра координат L_{xmf} і низький рівень спектра відносин

сигнал-завада Q_{mf} . Однак, на низьких частотах, в діапазоні, позначеному Δf_K на графіку 1, пошкодження, що з'явилося, вже проявляється у вигляді координатної полички з відносно малими осциляціями по координаті L_{xmf} і у вигляді збільшення спектру Q_{mf} якості – відношення сигнал-завада [4].

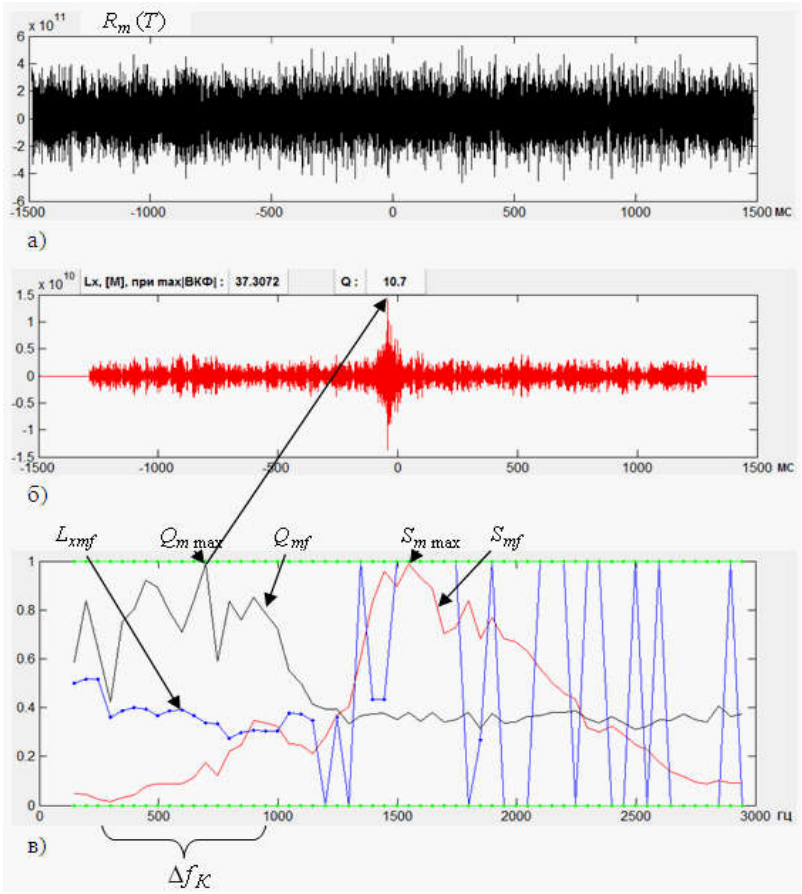

Рисунок 1 – Випадок відсутності у вихідній оцінці ВКФ (а) явного прояву кореляції. Але на параметричному графіку (в) корисна кореляція простежується на частотах Δf_K з підвищеним рівнем спектру якості за чорним графіком та відносно малими коливаннями спектру координат за синім графіком. Червоний графік спектру потужності не є інформативним в наслідок завад. Отримана в діапазоні Δf_K корисна кореляція зображена на графіку (б)

Такий аналіз не однієї, а саме кількох обчислених ВКФ при зсунутих на трубопроводі датчиках потрібен тому, що просторовий розподіл інтенсивності впливу сигналів від витоків на стінку трубопроводу у місцях доступу до трубопроводу є нерівномірним, що особливо важливо враховувати та використовувати при нечіткій кореляції. Критерії вибору остаточної координати – за протяжною по частоті координатною поличкою у синьому графіку L_{xmf} , яка повинна відповідати максимуму Q_{mf} та відносно великому значенню S_{mf} . Максимальному значенню S_{mf} у випадку малого відношення сигнал-завада поличка відповідати не може, бо основна енергія ВКФ, яку відображає червоний графік S_{mf} , при нечіткій кореляції виду рис. 1а, належить стороннім завадам, а не спотвореним шумам витоку.

Робота з термо-акустичним течешукачем А-10Т3.

При пошуку за акустичною ознакою витоку у грунті над трубопроводом доцільно спочатку з'ясувати тиск у трубопроводі. Це дозволяє передбачити характер звуку та його рівні від шуканого витоку. Так, у складному випадку при низькому тиску, наприклад менше 1,5 Атм. та глибині прокладки 1,5–2 м., не слід очікувати яскравого прояву витоку за індикатором рівня шуму. Пляма підвищеної вібрації може бути невеликою, наприклад діаметром 0,5–1 м., тому просторовий крок вимірювань у грунті повинен бути не більше 0,5 м. Іншою ознакою місця витоку у грунті над трубопроводом, яка видає виток навіть при тиску значно менше ніж 1,5 Атм., це характерний звук лиття води, її переливів, звук вихлопів повітряних бульб, які відчуваються у головних телефонах течешукача. Також, при пошуку витоків на теплових мережах, при низькому тиску у трубопроводі, при потужних акустичних завадах під час роботи на теплотрасі, прокладеної біля та вздовж автомагістралі, доцільно використовувати температурний датчик А-10Т3 [5, 6]. Приклади наведено далі.

Пошук витоку за адресою: вул. Шамрило, 7а. Параметри ділянки: діаметр труб 150 мм, довжина 26 м, глибина прокладки від 2 м до 2,5 м, температура теплоносія 65/45°С. Тиск в подавальному трубопроводі 9 атм, у пошкодженому зворотньому трубопроводі – 1,5 Атм. Теплотраса проходить у дворі будинку. Через низький тиск у зворотному трубопроводі корелятор нечітко показав область від 15 м до 24 м. Акустичне обстеження ґрунту над трубопроводом не дало позитивного результату. Обстеження температури ґрунту показало явну межу нагрітої і ненагрітої теплоносієм області теплотраси, яка потрапляє в область, зазначену корелятором – від 16 м до 17 м. Ці дані дозволили точно вказати місце пошкодження. Просторовий розподіл температури наведено на рис. 2.

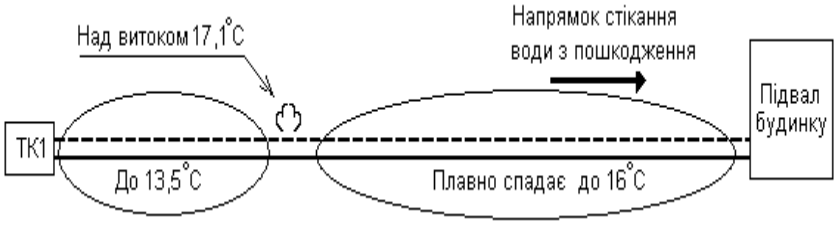

Рисунок 2 – Пошук витоку за адресою: вул. Шамрило, 7а

Пошук витоку за адресою: вул. Уманська, 9. Параметри ділянки: діаметр труб 150 мм, довжина 87 м, глибина прокладки 2,5 метри, температура теплоносія 65/42 ° С. Тиск у подавальному трубопроводі 9 Атм. Теплотраса здебільшого проходить під дорогою з неінтенсивним рухом транспорту. Витік малий на подавальному трубопроводі. Корелятор фіксує не чітке пошкодження в районі від 60 м до 62 м (рис. 3). Акустичне обстеження ґрунту не дало позитивних результатів. В результаті теплометричного обстеження зафіксовано максимальне значення температури на межі нагрітої і не нагрітої теплоносієм області теплотраси з координатою близько 61 м, що підтверджує показання корелятора.

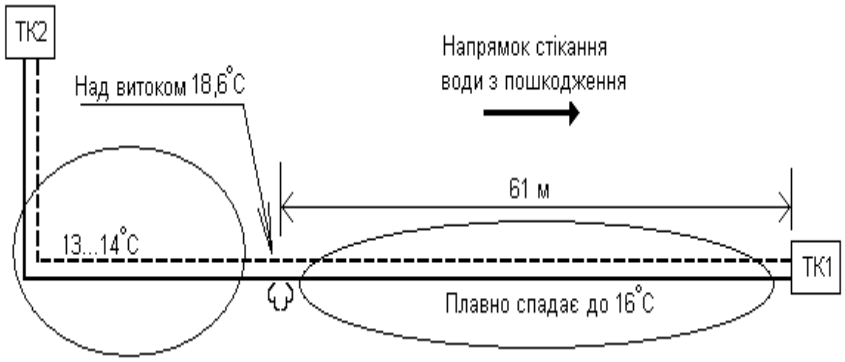

Рисунок 3 – Пошук витоку за адресою: вул. Уманська, 9

Діагностичні роботи виконувались за сприянням та за участю ПАТ «Київенерго».

Застосування теплового датчика А-10.Т3 дозволяє зробити пошук витоку по грунту над теплотрасою незалежним від будь-яких акустичних перешкод, що буває дуже доречним. Датчик обладнано екрануючим сенсором від зовнішніх сонячних променів гумовим екраном, рис. 4. Але датчик чутливий до теплових завад, які впливають на обстежуваний грунт над теплотрасою. Це потрібно враховувати. Так, основною завадою літом є різниця температури між частинами теплотраси у тіні та на сонці. При використанні теплового датчика це враховувалося у такий спосіб. Перед початком обстеження грунту від однієї теплової камери до іншої візуально теплотраса ділилася на дві частини – на сонячну і тіньову, та спочатку обстежувалася більша з них. Як правило, обстеження тільки цієї, більшої частини буває достатнім. Виток, при канальній прокладці, проявляє себе не тільки у місті витікання, а й у поширеній у просторі зоні стікання гарячої води з пошкодження в один бік по каналу прокладки, що спрощує його пошук в умовах локальних теплових завад.

а) б)

Рисунок 4 – Безконтактний датчик теплового випромінювання ИКДТ-2.
а) загальний вигляд; б) вигляд із боку чутливого елемента

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Владимирський О. А., Владимирський І. А. 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. Україна. ІПМЕ ім. Г.Е.Пухова НАН України. С. 31.

2. Владимирський О. А., Владимирський І. А. Просторовий і частотний Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання*. 2021. Том 43, № 4. С. 22–36.

3. Владимирський О. А., Владимирський І. А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання*. 2021. Том 43, № 3. С. 3–16.

4. Vladimirsky A., Vladimirsky I., Dybach O. Parametric Analysis of Correlation Functions for Acoustic Monitoring and Assessment of Underground Piping at NPPs. *Nuclear and Radiation Safety*. 2022. No. 3 (95). pp. 64–70.

5. Владимирский А. А., Владимирский И. А., Криворучко И. П. Термоакустический течеискатель А-10Т3. *XXXVIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* : збірник тез конференції (Київ, 15 травня 2020 р.), Київ, 2020. С 72.

6. Владимирський О. А., Владимирський І. А., Криворучко І. П. Використання комбінованих вимірювань у течешукачах А-20Т та А-10Т при пошуку витоків трубопроводів теплових мереж. *XXXIX науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* : збірник тез конференції (Київ, 12 травня 2021 р.) С 48–49.

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

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

ПРО ТЕХНОЛОГІЮ ВИЗНАЧЕННЯ МІСЦЬ РОЗГЕРМЕТИЗАЦІЇ ПІДЗЕМНИХ ТРУБОПРОВОДІВ З УРАХУВАННЯМ УСКЛАДНЮЧИХ ФАКТОРІВ

Важливість теми врахування ускладнюючих факторів при визначенні місць розгерметизації підземних трубопроводів обумовлена значним загальним зносом сотень кілометрів мереж підземних трубопроводів та їхніми частими пошкодженнями. У багатьох містах України та зарубіжжя пошук витоків вже давно став невід'ємною щоденною складовою виконання необхідних робіт з забезпечення водо- та теплопостачання населення. Поступове подальше зростання загального зносу трубопроводів та потрібність інтенсифікації робіт з оперативного усунення витоків підвищує вимоги до точності та оперативності інструментального визначення їхніх місць. Цьому перешкоджають різноманітні та часто складні умови проведення робіт, які існуючі інструментальні технології враховують далеко не повністю. До того ж загальний знос основної частини мереж приводить не тільки до зростання кількості витоків, але й ускладнює їхній пошук. Тому метою створення цієї технології є збільшення можливостей інструментального визначення місць розгерметизації підземних трубопроводів шляхом адаптації підходів, методів та засобів пошуку витоків до типових для України та інших країн особливостей, що суттєво ускладнюють визначення місць пошкоджень для їх оперативного усунення.

Технологія визначення місць розгерметизації підземних трубопроводів з урахуванням ускладнень (далі – технологія) пройшла виробничу перевірку при пошуку витоків і орієнтована на діагностику у першу чергу підземних трубопроводів зі сталі або чавуну.

Поширена процедура пошуку витоків складається з наступних технологічних операцій: визначення пошкодженої ділянки розгалуженої мережі, визначення або уточнення розташування пошкодженої ділянки – її трасування, визначення довжини пошкодженої ділянки, визначення точних місць розгерметизації трубопроводу для проведення в зазначених місцях розриттів та ремонтів.

Для трасування рекомендується використовувати індукційний трасошукач, для вимірювання довжин – мірне або дорожнє колесо. Оскільки зазначені операції є добре відпрацьованими та для їх проведення існує багато ефективних приладових засобів, вибір цих засобів не є критичним і далі не обговорюється.

Труднощі здебільшого виникають при визначенні пошкодженої ділянки, наприклад, при з'ясуванні причин підвищеного підживлення мережевої води на її джерелі, а також при з'ясуванні точного розташування витоків для виконання у цих місцях розкопок. Труднощям сприяє ряд факторів, що ускладнюють пошук витоків, а саме:

– розгалуженість підземної трубопровідної мережі у поєднанні зі зносом запірної арматури;

– можлива відсутність надходження води, що втрачається через пошкодження, в теплові камери або колодязі, що ускладнює визначення пошкодженої ділянки;

– занадто низький тиск у трубах, що ускладнює пошук акустичними методами;

– неоднозначність показань течешукачами координат пошкоджень через складну хвильову структуру реєстрованих акустичних шумів витоків;

– відсутність чіткої реєстрації течешукачем витоку через мале відношення сигнал-завада у реєстрованих сигналах;

– помилковість показань координат витоків через відмінність фактичної швидкості акустичних хвиль у трубопроводі від заданої у приладі;

– залежність показань приладу від вибору місць встановлення датчиків на трубопровід;

– наявність, крім витоків, критичних стоншень стінок трубопроводів, що резонують з шумом витоку та ряд інших факторів.

Дослідження механізмів впливу даних факторів на показання течешукачів, проведені в ІПМЕ ім. Г.Є.Пухова НАН України (далі – Інститут) показали наявність значного, не використаного резерву врахування цих факторів при пошуку витоків. Для більш повного використання цього резерву проведено низку коригувань схем та видів діагностичних вимірювань, розроблено нові конструкції та принципові схеми течешукачів, спеціальні режими роботи приладів та методичні прийоми їх використання для збільшення можливостей діагностування та її адаптації до складних умов.

Технологія заснована на досягнутих поточних результатах багаторічної роботи та призначена для практичного використання насамперед підприємствами міських теплових мереж та водоканалів.

Опис технології ведеться у наступній послідовності.

Перші два розділи містить стислий опис розроблених в Інституті базових для застосування технології приладів. Це течешукачі термо-акустичний А-10Т3 та кореляційний К-10.5М2.

Термоакустичний течешукач А-10Т3 [1, 2] призначений для визначення місць витоків підземних трубопроводів гарячого та холодного водопостачання, тепломереж, запірної апаратури, інших інженерних комунікацій (паропроводи, внутрішньо будинкові трубопровідні мережі, системи поливу). Інформаційними показниками витоків є рівень вібрації, характерний акустичний звук і температура.

Стосовно підземних трубопроводів течешукач призначений для:

– пошуку пошкодженої ділянки трубопроводу за допомогою віброакустичних вимірювань на поверхні трубопроводу у місцях доступу;

– визначення місць пошкоджень за допомогою акустичних та температурних вимірювань на поверхні грунту над трубопроводом;

– оперативного з'ясування напрямку надходження у місця доступу до трубопроводу та джерела найбільш потужних акустичних сигналів з метою ефективного та безпомилкового застосування кореляційних течешукачів.

Кореляційний течешукач К-10.5М2 [3] призначений для визначення місць витоків у трубопроводах теплових мереж, водопроводах та інших напірних трубопроводах. Місце витікання води із трубопроводу характеризується підвищеним рівнем віброакустичних шумів. Уздовж трубопроводу вібросигнали поширюються на значні відстані. Координати витоку можна визначити за допомогою кореляційної обробки вібросигналів. Для цього на кінцях секції трубопроводу, що діагностується, за допомогою магнітних тримачів встановлюються датчики вібрації. Сигнали з них передаються до блоку оператора, де за становищем максимуму функції взаємної кореляції вібросигналів обчислюється місце витоку. К-10.5М2 є вдосконаленою моделлю течешукачів сімейства К-10. У течешукачі реалізовані режими спостереження форми вібросигналів та спектрів у реальному часі, запис вибірок вібросигналів, розрахунок кореляційних функцій з підвищеною точністю, розвинутий вторинний, параметричний аналіз кореляційних функцій.

Доцільність додавання до кореляційної обробки сигналів ще й обробки отриманих у приладі оцінок кореляційних функцій (ВКФ) викликана тим, що у багатьох випадках ВКФ може мати розмитий, неоднозначний вигляд з таких причин: шум витоку дійшов до датчиків у дуже ослабленому вигляді при малих свищах, або при роботі на протяжному зворотному трубопроводі з ізоляцією з бітумоперліту в теплових мережах, при критично низькому робочому тиску на водопроводі, при нездатності джерела води створити досить високий тиск у магістралі в період літніх випробувань через великі пошкодження; у випадках кількох витоків; через додаткову реєстрацію датчиками відбитих сигналів і хвиль з відмінною від закладеною у приладі швидкістю. Значно підвищити достовірність визначення координати витоку дозволяє створений в Інституті спосіб, що полягає у цілеспрямованій просторово-частотній селекції ВКФ, сформованої найбільш інформаційними вібросигналами витоку. Виконується обчислення кількох ВКФ при різних позиціях датчиків на трубопроводі та проводиться порівняльний аналіз ВКФ за допомогою спеціального режиму Параметричного аналізатора dt ВКФ, або просто Аналізатора ВКФ [4, 5].

На рис. 1 представлені блоки оператора течешукачів.

Третій розділ присвячений урахуванню важливих особливостей при застосуванні найбільш складного з двох основних методів діагностування – кореляційного методу. Описано принцип дії та приклад застосування запропонованого параметричного аналізатора кореляційних функцій, призначеного для більш ефективного вилучення з взаємних кореляційних функцій корисної інформації та її подальшого використання.

Рисунок 1 – Блоки оператора течешукачів А-10Т3 і К-10.5М2

Четвертий розділ присвячений труднощам щодо визначення пошкодженої ділянки розгалуженої мережі підземних трубопроводів і способам їх подолання. Розділ заснований на особистому практичному досвіді співробітників Інституту у вирішенні відповідних завдань за допомогою розроблених течешукачів, застосування двоканального мобільного витратоміра та тепловізора.

П’ятий та шостий розділи присвячені вирішенню проблем достовірного визначення координат витоків для проведення ремонтів трубопроводів. Специфікою вирішення цих завдань є розмаїття умов проведення діагностичних робіт. Через це технологія врахування ускладнюючих факторів полягає у правильному їх аналізі та ретельному проведенні необхідної кількості цілеспрямованих діагностичних вимірювань. На прикладах пошуку витоків розкриваються адекватні умовам можливості розроблених в Інституті приладів та методик діагностування [3–5].

Завершують викладення технології висновки щодо поточного її рівня та перспектив подальшого розвитку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Владимирский А. А., Владимирский И. А., Криворучко И. П. Термоакустический течеискатель А-10Т3. *XXXVIII науково-технічна конференція молодих вчених та спеціалістів інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України* : збірник тез конференції (Київ, 15 травня 2020 р.). Київ, 2020. С. 72.

2. Владимирський О. А., Криворучко І. П. Пристрій для установки вібродатчика з магнітним тримачем на ґрунт при пошуку витоків. Патент на корисну модель № 142320; публ. 25.05.2020р., Бюл. №10.

3. Владимирський О. А., Владимирський І. А. 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. Україна. ІПМЕ ім. Г.Е.Пухова НАН України. С. 31.

4. Владимирський О. А., Владимирський І. А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання*. 2021. Том 43, № 3. С. 3–16.

5. Владимирський О. А., Владимирський І. А. Просторовий і частотний Кореляційні параметричні методи визначення координат витоків підземних трубопроводів. *Електронне моделювання*. 2021. Том 43, № 4. С. 22–36.

Vladimirsky Alexander Albertovich,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Doctor of Technical Sciences, Leading Researcher,
av1000000@ukr.net

Vladimirsky Igor Albertovich,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Candidate of Technical Sciences, Senior Researcher,
gosho2018@yahoo.com

Krivoruchko Igor Petrovich,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Postgraduate student, Researcher,
uhmi_igorkr@ukr.net

Anfimova Galina Viktorovna,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Candidate of Geological Sciences, Engineer,
anfimova77@ukr.net

ADAPTATION OF LEAK DETECTION TOOLS FOR USE ON UNDERGROUND PIPELINES WITH HIGH GENERAL WEAR AND TEAR

Acoustic and correlation leakage detectors are widely used in urban underground pipeline leak location. Acoustic leakage detectors are used for leak location according to the level of acoustic background in the ground above the pipeline. Correlation leakage detectors are used by placing vibration sensors on the pipeline in heat chambers or wells on both sides of leakage, distance to which from one of the sensors is determined according to mutual correlation function of signals from sensors.

In many Ukrainian and foreign cities more than 50% of underground water and heat supply pipelines have exhausted their resources. Significant wear and tear of pipeline networks leads to frequent leaks. Finding and repairing leaks has become a daily practice. The wear and tear of pipe networks causes problems in finding leaks. Difficulties are caused by: wear and tear of shut-off valves, noise in gate valves, wear and tear of air valves, acoustic heterogeneity of pipelines due to numerous alterations, difference in actual acoustic signal velocity along pipes due to corrosion wall thickening, etc. Wear of pipelines leads to high leakages during hydraulic tests of networks, there are problems with high pressure build-up in the damaged section and with reliable identification of fault locations using leak detectors by weak acoustic leakage signals. Similar pressure problems arise from damage to heat and water supply sources during combat operations.

Thus, the wear and tear of a major part of municipal water and heat supply networks places particular demands on the leak location technology and the instruments used. In order to adapt them to different urban conditions the Institute has

developed A-10T3 thermo-acoustic leakage detector and K-10.5M2 correlation leakage detector.

Leak detector A-10T3 is a multifunctional device in terms of leakage search technology with a combination of the following functions: acoustic and thermal leakage search in the ground above the pipeline [1]; identification of a damaged section of the pipeline through correct acoustic measurements in the access areas of the pipeline; identification of sources of acoustic noise in the pipeline through correct measurement and comparison of signal levels in confined spaces of heat chambers and wells.

Parametric correlation method of leakage search based on coordinated parametric spatial-frequency selection of informative signals is implemented in leakage detector K-10.5M2 that is efficient in complicated cases [2, 3]. Leak coordinate is determined by means of correlation function analyzer [2–4] combined with determination of 2–4 its estimates obtained with sensors shifted by 0.5-3 m in the places of pipeline access. An effective, combined spatial and frequency search for leakage noise is carried out. This correlation is recognised by the presence of coordinate fringes in the frequency spectrum of the coordinates. Coordinate fringes are a very convenient proxy for the sensitivity of correlation function estimates to the presence or absence of an informative correlation in its structure. It is also of paramount importance to register the appearance of a defect at an early stage, when it has not yet developed into a large lesion [4]. A technique has been developed for determining leakage coordinates under conditions of a complex wave structure of acoustic signals [2] and a small signal-to-interference ratio [3].

REFERENCES

1. Vladimirskyi I. A., Krivoruchko I. P. The use of combined measurements in leak detectors A-20T and A-10 T when searching for leaks in pipelines of heat networks. *XXXIX Scientific and Technical Conference of Young Scientists and Specialists of the Institute of Modeling Problems in Energy named after G.E. Pukhov National Academy of Sciences of Ukraine* : collection of abstracts of the conference. (Kyiv, 12 May 2021). Kyiv, 2021. P. 48–49.

2. Vladimirskyi O. A., Vladimirskyi I. A. Patent No. 144444. Parametric correlation method for determining the coordinates of pipeline leaks. Publication of information 09/25/2020, Bull. No. 18.

3. Vladimirskyi O. A., Vladimirskyi I. A. Patent No. 149956. Parametric correlation method for determining the coordinates of pipeline damage. Publication of information on December 15, 2021, Bull. No. 50.

4. Vladimirsky A., Vladimirsky I., Dybach O. Parametric Analysis of Correlation Functions for Acoustic Monitoring and Assessment of Underground Piping at NPPs. *Nuclear and Radiation Safety*. 2022. No. 3 (95). P. 64–70.

Vladimirsky Alexander Albertovich,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Doctor of Technical Sciences, Leading Researcher,
av1000000@ukr.net

Artemchuk Volodymyr Oleksandrovich,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Doctor of Technical Sciences, Senior Researcher,
ak24avo@gmail.com

Dyukov Volodymyr Andreyovych,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Candidate of Technical Sciences, Senior Researcher,
v.dukov@i.ua

PROBLEMS OF CALCULATION ESTIMATES OF CHANGES IN THE SHAPE AND DIMENSIONS OF THE CORE LINER OF VVER-1000 NUCLEAR REACTORS

VVER-1000 reactors are part of the power units of Ukrainian NPPs and are used together with a turbine generator to generate electricity. The long service life of VVER-1000 nuclear reactors makes it necessary to substantiate the operability of the reactor design elements based on the requirements for safe operation.

Particular attention is paid to the reactor vessel, shaft and containment, which are among the most responsible for heat removal from the core and are irreplaceable throughout the entire service life of the reactor components.

The very harsh conditions inside the containment – high radiation and filling of the containment interior with liquid, which introduces distortions in the sensing signals – significantly limit the use of known methods for measuring geometric dimensions.

Domestic and foreign literature describes and analyses in detail the structural damage to materials when they are hit by high-energy particles. Domestic and foreign experts have deeply studied changes in the structural state of metal materials under neutron and simulated irradiation, radiation swelling processes under neutron action, etc. For austenitic steels used in the manufacture of the partition, the problem of swelling is acute, which leads to a sharp decrease in physical and mechanical properties – to a loss of strength and ductility, changes in shape and size.

A number of studies have shown that the flux of neutrons and γ-quanta leads to significant volumetric changes in the VVER-1000 reactor pressure vessel due to an increase in thermoelastic stresses and the process of low-temperature radiation swelling [1]. According to some estimates [2, 3], during the first stage of the vessel operation (17 years, 7000 effective hours per year), thermoelastic stresses relax (by a factor of 2), and during the second stage, the structure deforms due to an increase in thermoelastic stresses and an increase in radiation swelling of steel.

The increase in the diameter of the cavity increases the total gaps between fuel assemblies in the core, which can lead to an increase in fuel assembly distortion during operation; it can lead to mechanical loading of the reactor vessel, deterioration of heat removal conditions and progressive increase in temperatures in the cavity and vessel, which will lead to an increase in radiation swelling of the cavity material; the absence of plane deformation at the free ends of the cavity components will lead to the appearance of transverse gaps, violation of structural integrity and the risk of emergency failures.

In [5], it is proposed to calculate the residual service life using the temperature-dose dependence of radiation swelling of 08H18N10T steel by the formula:

$$S_0=C_D \cdot D^n \cdot exp(-r \cdot (T_{обл}-T_{max})^2),$$

where D is the damaging dose, sna; $T_{обл}$ is the irradiation temperature, °C; T_{max} is the temperature of maximum swelling, °C; r, n, C_D are material constants.

When calculating the conservative temperature-dose dependence of free radiation swelling, which corresponds to the upper estimate of S_0 for a confidence level of 0.95.

This principle excludes an error in the dangerous direction when assessing the strength and safety of any power unit's, but may lead to excessive conservatism of calculations [6] and underestimation of the allowable service life of specific power units.

Paper [7] presents the calculation algorithms developed at the E.O. Paton Institute of the National Academy of Sciences of Ukraine, where isotropic volumetric deformations were set as radiation swelling. The model nonlinearly takes into account the dependence of radiation swelling of the shielding material on the irradiation temperature, stress state, and plastic deformations. The model also describes the change in the yield strength of the welded shaft wall material as a function of irradiation temperature and accumulated radiation dose. After 25 years of reactor operation, the maximum value of swelling deformations in the material of the shell is 1.3 %, after 40 years - 1.8, after 60 years – 3.7.

In a more conservative model, which does not take into account the history of volumetric deformation accumulation, the containment swells by 26% over 60 years of operation, which corresponds to even greater radial outward movement of the outer surface of the containment. The results of the swelling and radial deformation of the containment, obtained taking into account the stress state, indicate that the containment may come into contact with the welded shaft wall during reactor operation. Such contact can have a significant impact on the stress-strain state of the welded shaft structure.

In [8], a Monte Carlo method is described for calculating the neutron fluence and energy release in the VVER-1000 reactor pressure vessel and shaft to calculate the neutron fluence and energy release in the VVER-1000 reactor pressure vessel and shaft. The reactor vessel and the pressure vessel were modelled, and the water gap between the vessel and the pressure vessel was simulated. The method is promising for this type of calculations and opens up wide opportunities for the development of calculation methods. The model can also be improved in the geometric part by expanding the list of reactor structural elements for which neutron fluence and energy

release calculations are required and the list of design points. Despite the in-depth study of the effect of neutron irradiation on materials, there is currently no general theory of material swelling. A number of papers, for example [9, 10], recognise that the calculation of the stress-strain state and shape of the change in the shielding during operation and the analysis of the effect of radiation creep give contradictory results.

All prognostic models of swelling are based on the results of model experiments and have a short time period of application and are corrected when obtaining verification data during the study of real products.

Conclusions. Peculiarities of VVER-1000 reactor containment operation lead to significant changes in its geometry, to loosening of the containment material, which can lead to catastrophic consequences. Predictive models of the shape changes of the containment during long service life have not reached the required degree of accuracy and reliability and can be used to estimate the upper (worst) limits. Due to the long service life of domestic nuclear facilities with VVER-1000 reactors and accumulation of negative impacts, including those not taken into account during their design, instrumental control of the actual dimensions of the containment is extremely important. This will make it possible to adjust prognostic models of the shapes of the containment in order to assess the service life of specific reactor models.

REFERENCES

1. Garner F. A. Results of studies directed toward the possibility that void swelling will strongly affect the operation and safety of western PWRs and Russian VVTRs. *Problems of Nuclear Science and Technology. Series: Physics of Radiation Damage and Radiation Materials Science*. 1998. № 1 (67), P. 62–63.

2. Troyanov V. M., Likhachev Yu. I., Shamardin V. K. et al. Assessment and Analysis of Thermomechanical Behavior of VVER Reactor Pressure Vessel Elements in View of Irradiation Effects. *Collection of Papers of the 5th Interbranch Conference on Reactor Materials Science*. Vol. 2, Part 1, Dimitrovgrad, 1998, P. 3–18.

3. Shamardin V. K., Neustroev V. S., Prokhorov V. I. et al. Evaluation and Analysis of the Thermo-mechanical Behavior of VVER Reactor Pressure Vessel Elements with Account for Irradiation Effects. *Collection of Papers of the 5th Interbranch Conference on Reactor Materials Science*. Vol. 2, Part 1, Dimitrovgrad, 1998. P. 19–39.

4. Neklyudov I. M. State and Problems of Nuclear Reactor Materials in Ukraine. *Voprosy atomnoi nauki i tekhnika*. 2002, No. 3 (81). P. 3–10.

5. Procedure of Performance Assessment of Nuclear Power Plants' Quality Assurance Programs. RD EO 1.1.2.99.0944-2013. URL: https://cutt.ly/Z8J7p9O.

6. Akimov P.A. Experience in Service Life Extension of WWER NPP Equipment and Pipelines. OKB «Gidropress». URL: https://cutt.ly/w8J7xBg.

7. Makhnenko O. V., Mirzov I. V. Research of Stressed and Deformed State of Welded Structures Made of Austenitic Steel under Radiation Irradiation Conditions. *Automatic welding*. 2013, No. 1. P. 7–12.

8. Abdullaiev, A., Soldatov, S., Hann, V., Chernitskyi, S. Calculation of Neutron Fluence and Energy Release in WWER-1000 Structural Components Using Monte Carlo Method. *Nuclear and Radiation Safety*. 2018. No. 1 (77). P. 11–17. DOI: https://doi.org/10.32918/nrs.2018.1(77).02.

9. Chirkov A. Y., Kharchenko, V. V. Special Features of Computational Assessment of the Change in Shape of WWER-1000 Reactor Core Baffle in View of Irradiation-Induced Swelling. *Strength Mater*. 2020. Vol. 52, Iss. 3. P. 339–352. DOI: https://doi.org/10.1007/s11223-020-00184-9.

10. Chirkov O., Kharchenko V. The Impact of Radiation Injury on the Determination of the Form of the Active Zone Partition of the VVER-1000 Reactor under Long-Term Operation Conditions. Supplement. National Academy of Sciences of Ukraine. 2021. № 3. P. 40–47. DOI: https://doi.org/10.15407/dopovidi2021.03.040.

Haidur Halyna,
State University of Telecommunications,
Kyiv, d.t.s., prof.,
gaydurg@gmail.com

Gakhov Sergii,
State University of Telecommunications,
Kyiv, c.m.s., as. prof.
gakhov@ukr.net

DETECTION OF MALICIOUS PROCESSES IN THE ORGANIZATION'S NETWORK TRAFFIC USING SYNTHETIC DATA

Abstract. The article considers the issue of detecting malicious processes in the network traffic of an organization. The architecture of a system for detecting malicious processes in network traffic using synthetic data is proposed.

The problem of malicious processes in network traffic poses several significant challenges and risks to an organization. Malicious processes can lead to security breaches that allow attackers to gain unauthorized access to sensitive data, compromise systems, or disrupt critical operations. Detecting and stopping malicious processes in network traffic is critical to protecting an organization’s assets, ensuring data security, maintaining business continuity, and protecting its reputation.

Detecting malicious processes in an organization's network traffic is the process of identifying and recognizing unauthorized and potentially harmful activities occurring in the network infrastructure. It includes monitoring network traffic data, analyzing patterns, and using various methods to detect signs of malicious behavior or cyber threats.

The development of methods and tools for detecting malicious processes in the network traffic of organizations based on machine learning algorithms and hybrid methods is considered a promising area.

Let us consider the main approaches to detecting malicious processes in the network traffic of an organization. The essence of anomaly detection is to compare the values of the monitored network traffic characteristics with their criteria that define the limits of normal behavior.

The general advantage of anomaly-based methods is the effective detection of unknown threats. However, false inclusion of malicious activities in profiles is a common problem with these methods. Another problem concerns the accuracy of the generated profiles and arises from the complex behavior of network traffic [1, 2].

Statistical anomaly detection methods use statistical properties and tests to determine whether the observed behavior of network traffic differs significantly from the expected behavior. They include a number of methods based on univariate, multivariate time series models and cumulative sums (CUSUM). The advantages of statistical-based methods include the ability to study the expected behavior of a system (without prior knowledge of its normal activity) and the ability to provide

accurate long-term detection of malicious activity. The main disadvantage of statistical methods is the possibility that an attacker will train the system so that malicious traffic is considered normal [2].

Knowledge-based anomaly detection methods try to capture the declared behavior from available system data. They include methods based on finite state machines, description languages, and expert systems. The most common are expert systems that classify the observed data according to a set of rules. This set of rules is derived from various attributes and classes that are identified from the training data. The advantages of knowledge-based methods include their reliability and flexibility. The main disadvantage is the complex and time-consuming task of obtaining high-quality knowledge [2].

Machine learning-based methods establish an explicit or implicit model that allows for the classification of the analyzed patterns. The principles and applicability of machine learning methods are similar to statistical methods. However, machine learning methods allow the detection system to change its response to new information. Well-known methods based on machine learning include Bayesian networks, Markov models, neural networks, fuzzy logic, genetic algorithms, as well as clustering and outlier detection algorithms [2].

The advantages of anomaly detection methods based on machine learning are flexibility, adaptability, and the ability to capture the interdependencies of observed instances. The main disadvantage of machine learning-based anomaly detection methods is their high resource intensity [2].

We see one of the solutions to the above problems of detecting malicious processes based on anomalies in the use of synthetic datasets.

Thus, according to Gartner [3], by 2030, synthetic data will completely eclipse real data in artificial intelligence-based models. Synthetic data is a class of data created artificially. This is a fundamental difference from real data, which is directly observed from real systems. Although real data is almost always the best source of information, it has the following disadvantages: the data is often expensive, unbalanced, inaccessible, or unusable due to privacy rules [3].

In our opinion, the use of synthetic datasets for machine learning to create models for detecting malicious processes in an organization's network traffic has promising prospects.

By using synthetic datasets, machine learning models can be trained on a wider range of data, including rare and previously unseen scenarios, improving their ability to detect new and unknown threats. Synthetic datasets can also help solve the problem of unbalanced datasets, where the number of negative (harmless) samples far exceeds the number of positive (malicious) samples. By generating synthetic malicious samples, the model can be trained on more balanced datasets, improving its ability to detect malicious activity.

Additionally, synthetic datasets can help address privacy concerns associated with using real data. By creating synthetic data that is statistically similar to real data, machine learning models can be trained on data that does not contain any personally identifiable information or sensitive information, protecting the privacy of individuals and organizations.

However, it is important to note that the success of using synthetic data sets for machine learning in detecting malicious processes in an organization's network traffic depends on the quality and accuracy of the data set. A synthetic dataset must be designed to accurately reflect the distribution of real-world data, and it must be diverse enough to cover a wide range of possible attack scenarios. In addition, the machine learning model must be properly trained and validated to ensure that it can effectively detect malicious activity.

An example of the generation of synthetic datasets for research and practical application in cybersecurity is the Canadian Institute for Cybersecurity datasets [4].

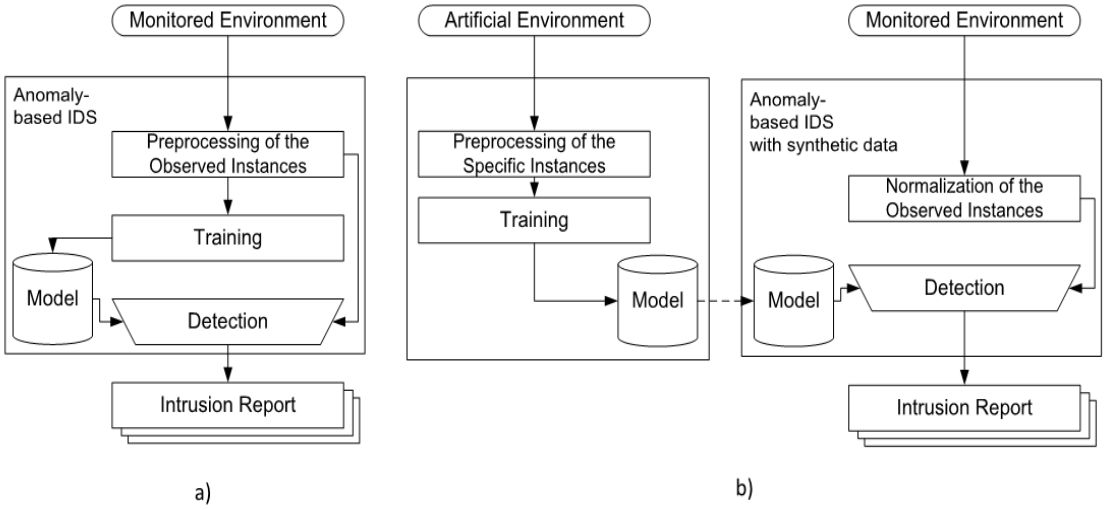

Fig. 1. General functional scheme of an anomaly-based intrusion detection system: a) classical scheme [2]; b) scheme using synthetic data

A general classical functional diagram of an anomaly-based detection system is shown in Figure 1(a). At the preprocessing stage, the observed instances are represented in a predefined form. The detection system creates static or dynamic models (profiles) that represent the normal behavior of users, hosts, network connections, and applications. During the training period, an initial profile is created, which can be done in different ways depending on the type of detection system.

We propose a general functional diagram of an anomaly-based detection system using synthetic data, as shown in Figure 1(b). The fundamental difference of this approach is the creation of an artificial environment - a model of the target information system of the organization. The artificial environment models various malicious processes and events that are reflected in synthetic data sets. It should be noted that the model-target system relationship must be homomorphic.

The machine learning model is trained on the synthetic data sets, stored, and transferred to the target detection system. If necessary, fine-tuning is performed to adapt the model to the target subject area.

In general, the prospects for using synthetic data sets for machine learning to detect malicious processes in an organization's network traffic are promising, but they require careful study and testing to ensure their effectiveness in practice.

REFERENCES

1. Scarfoneand K., Mell P. NIST SpecialPublication 800-94 Revision 1 (Draft). Guide to intrusion detection and prevention systems (IDPS). URL: https://csrc.nist.gov/csrc/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf.

2. Rakas S. V. B., Stojanovićand M. D. Marković-Petrović J. D. A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access*. 2020. Vol. 8. P. 93083-93108. DOI: https://doi.org/10.1109/ACCESS.2020.2994961.

3. Linden A. Is Synthetic Data the Future of AI? Gartner. URL: https://www.gartner.com/en/newsroom/press-releases/2022-06-22-is-synthetic-data-the-future-of-ai.

4. Datasets. Canadian Institute for Cybersecurity. URL: https://www.unb.ca/cic/datasets/index.html.

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, д.т.н., с.н.с.,
hilgurt@ipme.kiev.ua

Кіслов Олексій Геннадійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
alekskislov@i.ua

Попова Валентина Миколаївна,
ІПМЕ ім. Г.Є. Пухова НАН України,
інженер 1 категорії,
popovavn@ukr.net

БАГАТОРІВНЕВІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ЦИФРОВИХ ПІДСТАНЦІЇ

Вступ.

Проблеми інформаційної безпеки, що їх привносить в роботу промислових систем цифровізація систем автоматики та АСУ ТП, можуть бути більш важкими в порівнянні з традиційними галузями застосування інформаційних технологій. Насамперед це стосується об'єктів критичної інфраструктури, зокрема, в енергетичній галузі [1, 2]. Побудова засобів технічного захисту кіберфізичних систем, таких, як цифрові електричні підстанції (ЦПС), що будуються відповідно до стандарту МЕК 61850, успадковує більшість рис класичних засобів захисту традиційних для IT об'єктів, але має певну специфіку.

У даній роботі досліджено відмінності систем виявлення вторгнень (СВВ), які створюються цілеспрямовано для захисту систем диспетчерського контролю та збору даних (SCADA) для ЦПС.

1. Стандарт МЕК 61850.

Електричні підстанції є одними з найчисленніших об'єктів енергетики та відіграють вирішальну роль у всій енергосистемі, виконуючі важливі функції з розподілу та перетворення енергії [3]. Складнощі, що виникають при переводі їх обладнання на цифрову елементну базу, пов'язані в першу чергу зі стандартизацією. Якщо життєвий цикл силового обладнання, такого як трансформатори, комутаційні апаратні роз'єднувачі тощо складає близько 40 років, то керуючі системи оновлюються в середньому кожні 15 років. В результаті змушені спільно взаємодіяти пристрої декількох поколінь, не сумісні між собою.

Для вирішення даної проблеми було створено стандарт МЕК 61850 «Мережі та системи зв'язку на підстанціях» [4]. Головна ідея документа – розробити єдині специфікації, які дозволили б, з одного боку, захистити фінансові вкладення в енергетичне обладнання, з іншого – використовувати

передові обчислювальні та мережеві технології. Перша редакція документу (який насправді містить низку стандартів) з'явилася ще в 2003 році.

Відповідно до стандарту МЕК 61850 система автоматизації інформаційного обміну на енергооб'єкті за схемою ЦПС складається з трьох рівнів [3]: станційний (Station Level) – найвищій рівень, рівень приєднання (Bay Level) та рівень процесу (Process Level) або «польовий» (Field Level) – найнижчий рівень. Кожен рівень виконує притаманні йому функції, за які відповідають певні типи пристроїв. Комунікації можливі як всередині рівнів (горизонтальні), так і між рівнями (вертикальні).

На додаток до традиційних протоколів, таких як FTP або HTTP, стандарт МЕК 61850 вводить нові протоколи, а саме: MMS (Manufacturing Message Specification) – для зв'язку інтелектуальних пристроїв (IED) зі станційним рівнем, GOOSE (Generic Object Oriented Substation Events) – для зв'язку IED між собою, SV (Sampled Values) – для зв'язку між IED та MU. Строго кажучи, MMS є не протоколом, а специфікацією, що описує інформаційну модель пристроїв та даних рівня приєднання. Але, оскільки сервіс MMS, застосовує рівень додатків стандартного стеку протоколів OSI, його також можна умовно вважати протоколом обміну. Принаймні, в технічній літературі з питань використання стандарту МЕК 61850 та вирішення проблем захисту інформації в ЦПС на його основі, скорочення MMS в переважної більшості публікацій згадується саме як протокол.

Достатньо змістовний опис згаданих протоколів, включаючи часові діаграми, можна знайти в літературі, наприклад, в [3]. Зауважимо, що в кіберфізичних системах, побудованих на базі стандарту МЕК 61850, також можуть використовуватися інші мережеві протоколи, наприклад, поширена польова шина MODBUS, або її проприєтарна модифікація MODBUS Plus, протокол часової синхронізації PTP (Precision Time Protocol), протокол виявлення мережевих пристроїв LLDP (Link Layer Discovery Protocol) та ін.

2. Кіберзагрози та вразливості цифрових підстанцій.

Особливості систем СВВ, що створюються для захисту ЦПС на базі стандарту МЕК 61850, обумовлюються специфікою функціонування цифровізованих підстанцій та їх відмінностями від традиційних об'єктів IT-галузі [4].

Розуміння потенційних уразливостей мереж і пристроїв цифрових підстанцій, які можуть погіршити конфіденційність, доступність і цілісність даних, має вирішальне значення для розробки відповідних контрзаходів безпеки та механізмів виявлення вторгнень. Несанкціонований віддалений доступ до мереж підстанції дозволяє зловмиснику обходити фізичний захист і завдавати ЦПС катастрофічної шкоди [5].

Вразливості ЦПС пов'язані, насамперед, із застосуванням спеціалізованих протоколів. Аналіз свідчить про існування дев'яти основних шляхів використання вразливостей так званих багатоадресних протоколів, до яких належать GOOSE та SV, з метою порушення роботи компонентів енергосистеми [6]:

1) компрометація інтерфейсу користувача;

2) переривання процесу синхронізації часу;

3) компрометація шини зв’язку на станційному рівні;

4) отримання доступу до пристроїв рівня приєднання;

5) зміна налаштувань захисного пристрою;

6) захоплення та модифікація повідомлень протоколу GOOSE;

7) компрометація комунікаційної шини на рівні процесу;

8) розміщення підроблених значень у повідомленнях протоколу SV;

9) компрометація міжмережевого екрану для отримання доступу до мережі підстанції.

Незалежно від перелічених способів використання вразливостей, існують певні варіації здійснення конкретної атаки. Нижче перелічені типи різновидів атак з описами, а також потрібні заходи протидії [4].

1. Дублювання (Replay) – старі повідомлення передаються повторно – перевірка узгодженості атрибутів.

2. Безпосереднє вкидання (Naive injection) – передаються сфабриковані повідомлення (команди для GOOSE або виміри для SV) – стандартна перевірка цілісності за стандартом МЕК 61850.

3. Вкидання МЕК 61850 (IEC 61850 injection) – передаються сумісні з МЕК 61850 шкідливі команди (GOOSE) або повідомлення з фальшивими вимірами (SV) – перевірка узгодженості атрибутів контексту (GOOSE) або кореляція вимірювань кількох джерел (SV).

4. Маскування (Masquerade) – передаються повідомлення, що імітують реальну поведінку – перевірка узгодженості та кореляції.

5. Псування (Poisoning) – поле *StNum* надмірно збільшене – перевірка узгодженості атрибутів.

6. Модифікація (Modification) – фальшиві атрибути – перевірка узгодженості атрибутів.

7. Flood-атака (Flooding) – багато повідомлень передаються з високою частотою – перевірка статистики повідомлень.

Оскільки протокол MMS використовує на рівні додатків стандартний стек мережевих протоколів, на нього можуть здійснюватися всі типи атак, притаманні протоколам ІТ-галузі.

3. Багаторівневі системи виявлення вторгнень для ЦПС на базі стандарту МЕК 61850.

Висновки розслідувань відомих атак на енергооб’єкти (в тому числі – на підприємство «Прикарпаттяобленерго» у 2015 р.) спонукають дослідників зосереджуватися на аналізі поведінки зловмисника, який вже втрутився у роботу ЦПС через заражений людино-машинний інтерфейс та закріпився в мережі SCADA-системи [7]. Якщо припустити, що запобіжні заходи кібербезпеки периметру (міжмережеві екрани) не дали результатів і дозволили це вторгнення, стає життєво важливим існування додаткового рівня захисту, а саме – виявлення вторгнень, здатного реагувати на вищезазначені зловмисні дії. Таким чином, СВВ для SCADA-системи ЦПС стають ефективним інструментом виявлення як зовнішніх зловмисних атак, так і внутрішніх (втому числі – ненавмисних) зловживань. При цьому важливо враховувати максимум

чинників, починаючи з відомостей про логіку поведінки системи на фізичному рівні (включаючи засоби живлення) й до сучасних підходів створення засобів IT-безпеки.

Дотримуючись такого підходу можна виділити чотири рівні (або виміри) виявлення вторгнень [7]:

1) на рівні контролю доступу – Access-Control Detection (ACD);

2) з використанням білого списку протоколів – Protocol Whitelisting Detection (PWD);

3) на основі моделі – Model-based Detection (MBD);

4) багатопараметричне виявлення вторгнень – Multi-Parameter based Detection (MPD).

Складова ACD є свого роду стратегією білого списку стосовно контролю доступу, яка охоплює MAC-адреси на рівні Ethernet, IP-адреси на мережевому рівні та TCP-порти на транспортному рівні (для мережевого трафіку згідно МЕК 61850 використовується TCP порт номер 102). Якщо будь-яка з адрес або портів не входить до відповідного білого списку, детектор виконує попередньо налаштовану дію – в режимі СВВ сповіщає, в режимі роботи як система запобігання вторгнень блокує виявлену атаку, а також реєструє виявлене вторгнення.

Напрям PWD працює на всіх рівнях моделі OSI крім фізичного (з другого по сьомий) і має справу як з типовими для IT-галузі протоколами, так і з мережевими протоколами ЦПС: MMS, COTP, TPKT, SNTP, GOOSE, SMV та IEEE 1588. На рівні процесу детектор СВВ можна налаштувати таким чином, щоб дозволити здіснення трафіку протоколів MMS/COTP/TPKT/SNTP. На рівні приєднання детектор пропускатиме лише трафік GOOSE, SV або IEEE 1588. Тобто детектор СВВ налаштовується на підтримку лише припустимих на відповідному рівні протоколів.

Підхід MBD аналізує файли опису конфігурації ЦПС (так звані SCD-файли) та зміст поточного трафіку за протоколами МЕК 61850, визначає моделі штатної поведінки за допомогою поглибленого аналізу протоколу та порівнює профілі дозволеної поведінки зі спостережуваним трафіком з метою виявлення відхилень. У порівнянні з традиційними IT-мережами, мережі SCADA-систем на цифрових підстанціях мають такі відмінні характеристики, як регулярні потоки трафіку та передбачувану поведінку, що спрощує специфікацію моделей їх поведінки. Напрям виявлення вторгнень типу MBD має потенціал для ідентифікації зловмисних атак і ненавмисних аномалій як на станційному рівні, так і на рівні процесу. В роботі [7] запропоновано використовувати наступні моделі для підходу MBD:

– модель адреси призначення (Destination Address Model);

– польова модель коду протоколу міток (Tag Protocol ID Field Model);

– модель поля EtherType (EtherType Field Model);

– модель пріоритетного поля (Priority Field Model);

– польова модель коду програми (Application ID Field Model);

– модель довжини (Length Model);

– модель поля TimeAllowedToLive (TimeAllowedToLive Field Model);

– модель поля коду (Tag Field Model);
– моделі поля SmpCnt (SmpCnt field Models);
– кореляційні моделі (Correlation Models);
– модель на основі трафіку (Traffic based Model).

Основна ідея багатопараметричного напряму MPD полягає у виявленні можливих загроз для SCADA-системи, що є результатом або внутрішнього ненавмисного використання, або зовнішніх зловмисних атак шляхом моніторингу найбільш чутливих параметрів ЦПС. Ці багатовимірні параметри пов'язані з безпечною та стабільною роботою інтелектуальної підстанції, наприклад дані дистанційного вимірювання та дистанційної сигналізації від станційної шини та шини процесу згідно МЕК 61850. Стратегії багатопараметричного виявлення, такі як критична кореляція сигналу перемикання та порівняння ключового аналогового сигналу, використовують фізичні знання та досвіду експлуатації цифрових підстанцій.

Висновки.

Розглянуті в дослідженні багаторівневі системи виявлення вторгнень для ЦПС на базі стандарту МЕК 61850 забезпечують перевагу перед іншими відомими рішеннями за рахунок більш глибокого застосування специфічних властивостей об'єктів кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sanger D. E., Krauss C., Perlroth N. Cyberattack Forces a Shutdown of a Top U.S. Pipeline. The New York Times (May 8, 2021) URL: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.
2. Radichel T. Colonial Pipeline Hack. 2nd Sight Lab (May 15, 2021). URL: https://medium.com/cloud-security/colonial-pipeline-hack-4486d16f2957.
3. Communication Networks and Systems in Substations. IEC Std. 61850.
4. Quincozes S.E., Albuquerque C., Passos D., Mossé D. A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*. 2021. Vol. 184. Article 107683.
5. Radoglou-Grammatikis P. I., Sarigiannidis P. G. Securing the smart grid : A comprehensive compilation of intrusion detection and prevention systems. IEEE Access. 2019. Vol. 7. P. 46595–46620.
6. Гільгурт С. Я. Підходи до побудови систем виявлення атак на протоколи цифрових електричних підстанцій. *Кібербезпека енергетики* : матеріали наук.-практ. конф. (Київ, 2021 р.). Київ, 2021. С. 34–42.
7. Yang Y., Xu H.-Q., Gao L., Yuan Y.-B., Sezer S. Multidimensional intrusion detection system for IEC 61850-based SCADA networks. *IEEE Trans. Power Deliv*. 2017. Vol. 32, № 2. P. 1068–1078.

Гулак Генадій Миколайович,
ІПММС НАН України,
провідний науковий співробітник, д.т.н., доц.,
h.hulak@ukr.net

Скітер Ігор Семенович
ІПБАЕ НАН України,
старший науковий співробітник, к.ф.-м.н., доц.,
i.skiter@ispnpp.kiev.ua

Гулак Євген Геннадійович,
ІПММС НАН України,
аспірант,
geg180579@gmail.com

МЕТОДИЧНІ АСПЕКТИ ДІЯЛЬНОСТІ ЦЕНТРУ КІБЕРБЕЗПЕКИ ОБ`ЄКТІВ ЯДЕРНОЇ ЕНЕРГЕТИКИ

В умовах збройної агресії ядерна енергетика України по суті є одночасно становим хребтом економіки та найнебезпечнішим елементом критичної інфраструктури. Технологічна складність цієї галузі, високі ризики виникнення нештатних ситуацій на її об'єктах внаслідок реалізації реальних загроз техногенного, природного та антропогенного характеру, включаючи терористичні кібератаки на інформаційні інфраструктури, актуалізують завдання створення галузевого центру кібербезпеки (ГЦКБ).

Підвищена складніть технологічних автоматизованих систем та інформаційно-комунікаційних систем (далі – АС) об'єктів ядерної енергетики (ОЯЕ), велика кількість різновидів та обсягів важливої інформації, що циркулює в цих системах, а також постійне зростання потужності та різноманіття кібератак висувають особливі вимоги до побудови ГЦКБ. Зазначений центр за архітектурою, апаратною і програмною платформами, засобами та технологіями кіберзахисту, рівнем рівнем знань, умінь і навичок персоналу, практичними методиками реагування на кіберінциденти повинен відповідати викликам сучасності.

Збої або відмови апаратної і програмної платформ та спрямовані впливи на автоматизовані системи управління технологічними процесами здатні руйнувати або блокувати інформаційні ресурси. Внаслідок цього ефективність функціонування обладнання ОЯЕ може бути суттєво знижена або створені передумови ситуацій, які матимуть катастрофічні наслідки.

Саме ГЦКБ повинен підтримувати стале надійне функціонування інформаційних і технологічних систем ОЯЕ шляхом розвитку системи кібербезпеки та реалізації превентивних, блокуючих та нейтралізуючих організаційно-технічних заходів. Створення такого центру повинне базуватись на принципах системного підходу з застосуванням відповідних методів прийняття рішень з урахуванням ключових факторів, що впливають на стан кібербезпеки.

Пріоритетними завданнями наукових досліджень у сфері забезпечення кібербезпеки ОКІ є, створення моделі функціонування центру кібербезпеки та забезпечення гарантоздатності автоматизованих систем ОЯЕ як технологічної основи їх функціонування.

Актуальність і практична значущість визначеного завдання відмічена НАН України [1], а також де звернута увага на необхідність забезпечення гарантоздатності автоматизованих систем ОЯЕ, в тому числі в частині забезпечення кібербезпеки об'єктів.

Запропоновані в [2] модель центру кібербезпеки та модель загроз АС ОЯЕ описують взаємодію системи захисту інформації із зовнішніми та внутрішніми факторами та надають можливість формулювати часткові завдання побудови та функціонування ГЦКБ ОЯЕ, включаючи:

– визначення стратегічних і тактичних задач та функцій центру, їх регулярне уточнення;

– ідентифікація ресурсів, що підлягають захисту, та відстежування потенційних загроз безпеки, розробка, супроводження та модернізація моделей загроз;

– формування вимог та параметрів безпеки АС ОЯЕ;

– оцінка параметрів безпеки та їх динаміки;

– реалізація організаційно-технічних заходів для оцінки рівня ризиків та їх мінімізації;

– надання дієвої допомоги персоналу ОЯЕ в випадках виникнення кіберінцидентів для блокування і локалізації загроз, ліквідації їх наслідків та відновлення початкового стану;

– участь у проведенні розслідувань кіберінцидентів, які мали суттєві наслідки;

– організація та проведення тренінгів і навчань персоналу ОЯЕ, формування культури кібербезпеки та оцінка її стану.

На підставі проведеного аналізу були визначені наступні базові принципи побудови ГЦК: інтеграція, централізація, уніфікація, масштабованість, модульність, живучість.

Принципи інтеграції та консолідації доцільно реалізовувати відносно розрізнених масивів даних про ОЯЕ. Принцип централізації реалізується шляхом використання для всіх підсистем автоматизованої системи управління єдиних метаданих та нормативно-довідкової інформації. Принцип уніфікації реалізується в частині єдиної інформаційно-комунікаційної системи для всіх структур та форматів даних. Принцип масштабованості реалізується через можливість поетапної розробки та впровадження без принципової заміни технічної платформи. Принцип модульності реалізується через побудову ЦКБ як сукупності модулів реалізації окремих функцій і завдань, що забезпечує гнучкість підсистем і системи в цілому під необхідну структуру управління безпекою.

Принцип живучості реалізується через забезпечення безперебійної роботи, отримання достовірних результатів, захист від несанкціонованих дій.

Розглядаючи аспекти безпеки, автори [3] звертають увагу на підвищення рівня культури інформаційної безпеки організації, на запобігання впливу методів соціальної інженерії.

Завданнями адміністраторів системи управління ГЦКБ ОЯЕ кібербезпекою є оцінка станів безпеки інформаційної системи ОЯЕ, її динаміки та динаміки її складових, оцінка ефективності управлінських рішень та їх корекції шляхом впровадження організаційно-технічних заходів. При цьому відомості про результати оцінки та зміни стану кібербезпеки системи можуть мати не тільки кількісний, але і якісний характер [4].

Розглянемо інформаційну систему в деякий момент часу $t \in [0,T]$ для N некорельованих рівнозначних за вкладом у кібербезпеку кластерів характеристик станів системи кібербезпеки $Q_1(t), Q_2(t), \dots, Q_N(t)$, $N > 2$. Також будемо вважати, що i-тий кластер містить m_i елементів, які можуть спостерігатися відповідно до поліноміальної схеми розподілу ймовірностей $(p_{i1}(\tau), p_{i2}(\tau), \dots, p_{iM_i}(\tau))$, $\tau \in [0,T]$; $p_{i1}(\tau) + p_{i2}(\tau) + \dots + p_{iM_i}(\tau) = 1$. Зміна розподілу ймовірностей може відбуватися внаслідок проведення менеджментом підприємства організаційних (включаючи навчальні) заходів з персоналом інформаційної системи, яка захищається.

Тоді кожен кластер характеристик безпеки описується як:

$$Q_i(t) = \{\langle k_{ij}, p_{ij}(t)\rangle,\ j \in [1, M_i]\}, i \in [1, N], \quad (1)$$

де M_i – кількість елементів у множині; $p_{ij}(t)$ – ймовірність прояву фактора #j k_{ij} – деякий коефіцієнт, пропроційний тяжкості наслідків для кібербезпеки системи в разі прояву фактора *#j*. При цьому якщо фактор *#j* має більш тяжкі наслідки для безпеки, ніж фактор *#l*, то вважаємо, що має місце строга нерівність $k_{ij} > k_{il}$.

Для всіх кластерів має місце вираз:

$$k_{i1} + k_{i2} + \dots + k_{iM_i} = S, \forall\, i \in [1, N], \quad (2)$$

де S – ціле число, діапазон шкали оцінювання.

Тоді комплексний показник кібербезпеки ОЯЕ W з урахуванням усередненої ваги окремого кластера у загальному показнику рівня загроз інформаційній системі можна визначити як лінійну адитивну функцію виду:

$$W(t) = W(Q_i(t)) = \sum_{j=1}^{M_i} k_{ij} p_{ij}(t) \cdot M_i. \quad (3)$$

На наступному етапі проводиться розвязок задачі кількісної оцінки зміни (динаміки) комплексного показника кібербезпеки в антропогенному факторі системи безпеки після проведених заходів на основі спостережуваних в різні моменти часу кластерів.

При негативній динаміці має формуватись набір управлінських рішень та проводиться оцінка їх ефективності. Для цього пропонується у якості метрики величина $E_i(t_1, t_2)$ яка означає рівень ефективності витрачання коштів на відрізку часу $[t_1, t_2]$. Введемо величину

$$Z_i = sign\left(k_i(t_1) - k_i(t_2)\right) \times \sum_{j=1}^{M_i} \frac{\left(k_{ij}^{(1)} - k_{ij}^{(1)}\right)^2}{k_{ij}}, \quad (4)$$

де $k_{ij}^{(1)}$ – коефіцієнт тяжкості наслідків прояву відповідного фактору в кластері Q_1 в момент часу *t;* $k_{ij}^{(2)}$ – відповідно в кластері Q_2 в момент часу *t.*

Тоді рівень ефективності заходів $F_i(t_1, t_2)$ визначається виразом:

$$E_i(t_1, t_2) = \frac{Z_i}{\Delta t_{12} C(t_1, t_2)}, \quad (5)$$

де $\Delta t_{12} = t_1 - t_2$ – проміжок часу реалізації заходу; $C(t_1, t_2)$ – вартість (у ціновому виразі) реалізованих заходів.

Таким чином маємо наступні варіанти для результатів спостереження стану кібербезпеки на відрізках часу $[t_1, t_2]$ та $[t_2, t_3]$:

а) $E[t_1, t_2] \leq 0$ та $E[t_2, t_3] \leq 0$, що свідчить про практичну неефективність реалізованих заходів;

б) $E[t_1, t_2] \leq 0$ та $E[t_2, t_3] > 0$ означає покращення підходу до заходів з підвищення ККБ;

в) у випадку $E[t_1, t_2] > 0$ та $E[t_2, t_3] > 0$ можливі наступні варіанти:

$E[t_1, t_2] < E[t_2, t_3]$ – більш ефективний підхід;

$E[t_1, t_2] > E[t_2, t_3]$ – гірший варіант;

$E[t_1, t_2] = E[t_2, t_3]$ – такий самий рівень ефективності витрачання коштів.

У підсумку впровадження та оцінки організаційно-технічних заходів центру кібербезпеки ОЯЕ стан безпеки підприємств галузі має бути піднятий на якісно новий рівень, а також забезпечено раціональне використання ресурсів на розвиток системи кібербезпеки інформаційної інфраструктури ОЯЕ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Носовський А. В. Науково-технічний супровід робіт з подолання наслідків чорнобильської катастрофи. *Вісник Національної академії наук України*. 2021. № 7, С. 32–36.

2. Hulak H., Skiter I., Hulak Y. Методологічні засади створення та функціонування центру кібербезпеки інформаційної інфраструктури об’єктів ядерної енергетики. *Кібербезпека : освіта, наука, техніка»*. 2021. Том 4, № 12, С. 172–186.

3. Sas M., Hardyns W., van Nunen K., Reniers G., Ponnet K. Measuring the security culture in organizations: a systematic overview of existing tools. *Security Journal*. 2021. Vol. 34, No. 2, P. 340–357.

4. Skiter I. Модель оцінки рівня культури кібербезпеки в інформаційній системі. *Кібербезпека : освіта, наука*, *техніка»*. Том 1, № 13. С. 158–169.

Гончар Сергій Феодосійович
ІПМЕ ім. Г.Є. Пухова НАН України,
заступник директора з науково-технічної роботи, д.т.н., ст. дослід.,
sfgonchar@gmail.com

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

УДОСКОНАЛЕНА МОДЕЛЬ ІМОВІРНИХ ДЕСТРУКТИВНИХ ДІЙ КОРИСТУВАЧІВ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

На сьогоднішній день все більше зростає роль людського чинника на стан забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) при недостатній кількості методів і засобів його оцінки та захисту [1, 2]. Згідно із [3] ОКІІ – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта. Засоби і методи, які наразі розробляються дають змогу зменшити рівень помилкової інформації, але не досліджують проблему у цілому, в тому числі не проводять оцінку і захист, як від випадкових, так і від умисних деструктивних дій користувачів ОКІІ.

Враховуючи викладене, можна зазначити, що важливою задачею являється прийняття адекватних рішень користувачами ОКІІ в різних інформаційних середовищах і відносинах. Для цього, актуальною задачею є розроблення нових та удосконалення існуючих моделей імовірних деструктивних дій користувачів ОКІІ в умовах наявності дестабілізуючих впливів в аспекті кібербезпеки.

Згідно з нормативним документом в галузі технічного захисту інформації [4] користувачі ОКІІ за рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються в процесі функціонування ОКІІ, можуть поділятися на наступні категорії:

– користувачі, яким надано повноваження розробляти й супроводжувати комплексні системи захисту інформації. Це може бути адміністратор безпеки, співробітники служби захисту інформації;

– користувачі, яким надано повноваження забезпечувати управління ОКІІ. Це можуть бути адміністратори операційних систем, систем керування базами даних, мережевого обладнання, сервісів тощо);

– користувачі, яким надано право доступу до конфіденційної інформації одного або декількох класифікаційних рівнів;

– користувачі, яким надано право доступу тільки до відкритої інформації;

– технічний обслуговуючий персонал, що забезпечує належні умови функціонування ОКІІ;

– розробники та проектувальники апаратних засобів ОКІІ, що забезпечують її модернізацію та розвиток;

– розробники програмного забезпечення, які здійснюють розробку та впровадження нових функціональних процесів, а також супроводження вже діючих;

– постачальники обладнання і технічних засобів ОКІІ та фахівці, що здійснюють його монтаж, поточне гарантійне й післягарантійне обслуговування;

– технічний персонал, що здійснює повсякденне підтримання життєдіяльності фізичного середовища ОКІІ. Це можуть бути електрики, технічний персонал з обслуговування будівель, ліній зв'язку тощо.

Модель імовірних деструктивних дій користувачів ОКІІ запропонована в [5]. В приведеній моделі під зовнішнім дестабілізуючим впливом розуміють множину загроз реалізації інформаційно-психологічного впливу на користувачів ОКІІ. Такі впливи можуть мати на меті дезорієнтацію, дезінформацію, дезорганізацію, придушення, руйнування тощо. Множина факторів внутрішнього дестабілізуючого впливу у приведеній моделі являє собою множину людських потреб, через захищеність яких може розкриватися забезпечення кібербезпеки людино-машинних систем управління. Таким чином, у [5] зазначається, що стан безпеки користувачів ОКІІ, в аспекті кібербезпеки, визначається двома основними чинниками: інформаційно-психологічною задоволеністю людських потреб користувачів і дестабілізуючими (навмисними або випадковими) інформаційно-психологічними та інформаційно-технічними впливами.

У роботах [6, 7] автори зазначають, що цілісна оцінка ризиків кібербезпеки являє собою складну багатокомпонентну та багаторівневу проблему, що включає апаратне забезпечення, програмне забезпечення, середовище та людський фактор. Щоб зрозуміти, яким чином дії користувачів і зловмисників впливають на ризики кібербезпеки ОКІІ, необхідно враховувати характеристики людських чинників, що включають людську поведінку. Зазначається, що джерелом загроз можуть стати погано розроблені політики безпеки, слабо контрольовані системи, які дозволяють уповноваженим співробітникам обходити встановлені політики, а також співробітники, які не знають про існуючі ризики.

Удосконалена модель імовірних деструктивних дій користувачів ОКІІ в умовах наявності дестабілізуючих впливів в аспекті забезпеченнякібербезпеки з урахуванням людських чинників користувачів ОКІІ, що включають характеристики знань/навичок користувачів та його поведінкових характеристик приведена на рис. 1.

У залежності від того, які чинники спонукають користувачів на деструктивні дії, останніх поділяють на типи. Ці типи розділяються у залежності від мети, мотивації і послідовності дій користувачів. Користувачі можуть отримувати доступ до активів ОКІІ законно, використовуючи свої повноваження, або незаконно, використовуючи сприятливі умови та/або несанкціоновано розширюючи свої повноваження. У випадку отримання

користувачем доступу до активів ОКІІ у межах своєї компетенції необхідності у сприятливих умовах немає. На відміну від зовнішнього порушника користувач має легітимний доступ до комунікаційної та/або технологічної системи об'єкта критичної інфраструктури, в межах своєї компетенції.

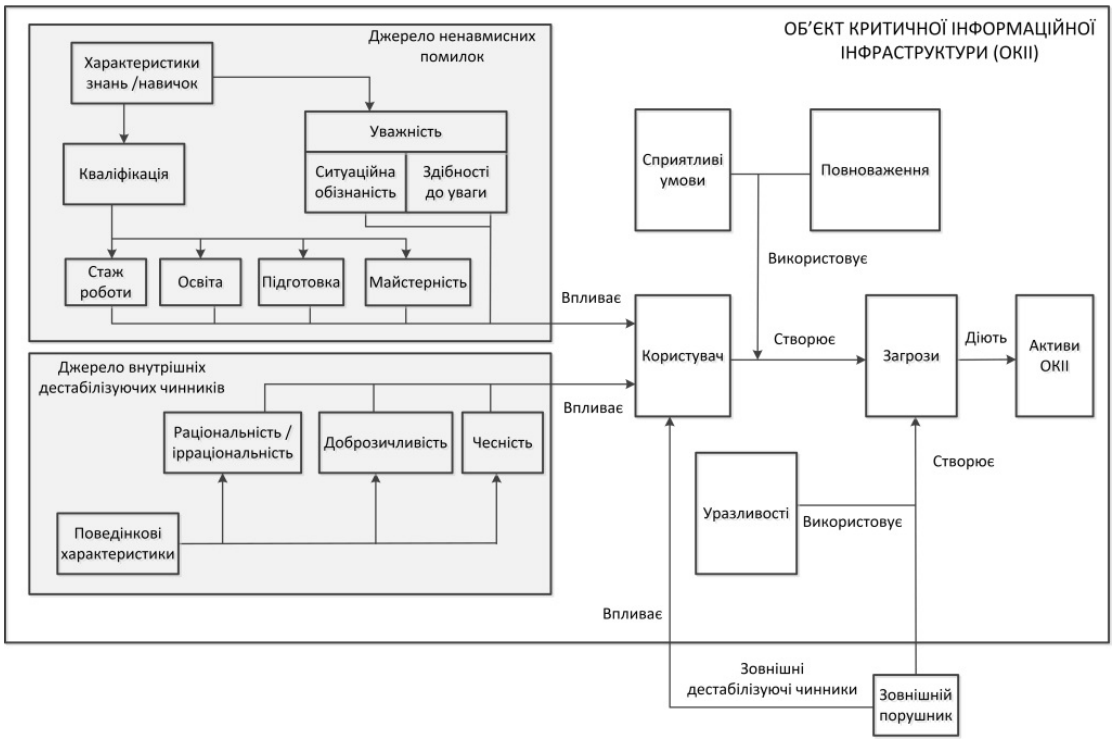

Рисунок 1 – Удосконалена модель імовірних деструктивних дій користувачів ОКІІ

Проведений аналіз показує, що для зменшення імовірності здійснення користувачем ОКІІ деструктивних дій в аспекті кібербезпеки необхідно:

– вчасно виявляти та вживати певних заходів для зменшення впливу внутрішніх дестабілізуючих чинників;

– покращувати відбір співробітників на етапі прийняття на роботу;

– вживати відповідних заходів щодо підвищення їх фахового рівня співробітників для недопущення або мінімізації ненавмисних помилок.

Таким чином, із урахуванням викладеного можна зазначити, що на імовірність здійснення користувачами деструктивних дій в аспекті порушення кібербезпеки ОКІІ впливають такі фактори:

– наявність необхідної та достатньої нормативно-правової бази з питань забезпечення кібербезпеки ОКІІ;

– наявність уразливостей у системах кіберзахисту, які можуть використовуватися при здійсненні кібератак;

– наявність чи відсутність сприятливих умов для реалізації кіберзагроз;

– можливість безконтрольного використання користувачами ОКІІ своїх повноважень;

– рівень кваліфікаціїкористувачів ОКІІ;

– морально-психологічний клімат в колективі, який впливає на поведінкові характеристики користувача ОКІІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мохор В. В., Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. *Електронне моделювання*. 2019. Том 41, № 6, С. 65–76.
2. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури : монографія. Київ : «Альфа реклама», 2019. 176 с.
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII: Закон України від №. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
4. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Затверджено наказом ДСТСЗІ СБ України від 13.12.2002 за № 84.
5. Гончар С. Ф., Леоненко Г. П. Аналіз факторів впливу на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури. *Information Technology and Security*. 2016. Vol. 4, Iss.2 (7), P. 262–268.
6. Henshel D., Cains M. G., Hofmann B., Kelley T. Trust as a human factor in holistic cyber security risk assessment. *Procedia Manufacturing*. 2015. No. 3. 2015. P. 1117–1124.
7. Takayuki H., Tetsou S. Extended FRAM model based on cellular automaton to clarify complexity of socio-technical systems and improve their safety. *Safety Science*. 2020. No. 123. P. 2–16.

Горожанова Анастасія Олександрівна,
10guards,
консультант з кібербезпеки,
ah@10guards.com

СУЧАСНА ПРАКТИКА ПОБУДОВИ ТА СЕРТИФІКАЦІЇ СУІБ. ЕФУКТИВНА СУІБ

Система управління інформаційною безпекою СУІБ (information security managementsystem, ISMS) – частина загальної системи управління, яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки (ІБ) [3].

Для процесів СУІБ застосована модель PDCA (плануй-виконуй-перевіряй-дій; Plan-Do-Check-Act):

– Plan – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;

– Do – фаза реалізації та впровадження відповідних заходів;

– Check – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;

– Act – виконання превентивних і коригуючих дій.

Побудова СУІБ дозволяє чітко визначити як взаємопов’язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування і т.д.

Основні функції системи управління інформаційною безпекою:

– виявлення та аналіз ризиків ІБ;

– планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

– контроль цих процесів;

– внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління інформаційною безпекою базується на наступних принципах:

– комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризик утворюючі фактори, що діють в інформаційній системі організації та за її межами;

– узгодженість з бізнес-задачами і стратегією організації;

– високий рівень керованості;

– адекватність інформації, яка використовується і генерується;

– ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

– безперервність управління;

– процесний підхід – зв’язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв’язку між етапами.

На даний момент державним стандартом, який визначає вимоги до побудови СУІБ є ДСТУ ISO/IEC 27001:2015, який базується на міжнародному стандарті ISO/IEC 27001:2013 [1].

Даний стандарт встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації. Він також включає в себе вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації. Вимоги, викладені в ISO/IEC 27001 є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру.

Ключовою для СУІБ є система управління ризиками. Адже нові загрози виникають майже щомиті, старі видозмінюються і стають дедалі небезпечнішими. Тому відповідно до нових реалій та загроз, міжнародна організація зі стандартизації (ISO) оголосила про випуск оновленої версії стандарту ISO 27001 25 жовтня 2022 року.

Перелік засобів контролю інформаційної безпеки в нормативному Додатку А нового стандарту ISO/IEC 27001:2022 повністю походить з переглянутого керівництва ISO/IEC 27002:2022. Каталог засобів контролю безпеки опублікували ще у лютому 2022 року, отже, зміни до переліку в новому стандарті були вже якийсь час передбачувані.

Основні зміни у ISO/IEC 27001:2022.

Раніше Додаток А включав загалом 114 засобів контролю (які використовують для ідентифікації та усунення ризиків безпеки) в рамках 35 цілей контролю, поєднаних у 14 пунктів [2].

У новому стандарті ISO/IEC 27001:2022 цілі контролю скасували, а засоби контролю переглянули, осучаснили та доповнили. Тобто, перелік засобів контролю у Додатку А став простішим та сучаснішим. Колишні 14 пунктів Додатку тепер зосереджені на чотирьох основних темах:

– A.5. Організаційні заходи захисту (Process and Policies) (включає 37 заходів);
– A.6. Заходи захисту персоналу (People) (включає 8 заходів);
– A.7. Фізичні заходи захисту (Physical) (включає 14 заходів);
– A.8. Технологічні заходи захисту (Technological) (включає 34 заходи).

Загалом у Додатку А нової версії тепер є 93 заходи контролю, до яких додали 11 нових, зокрема:

– A.5.7. Розвідка загроз (Threatintelligence (cyber/cloud/DP));
– A.5.23. Інформаційна безпека при використанні хмарних сервісів (Information security for cloudservices (cloud));
– A.5.30. Готовність інформаційно-комунікаційних технологій до забезпечення безперервної діяльності (ICT readiness for businesscontinuity);
– A.7.4. Моніторинг фізичної безпеки (Physical security monitoring (physical));
– A.8.9. Управління конфігурацією (Configurationmanagement);
– A.8.10. Видалення інформації (Informationdeletion (Dataprotection));
– A.8.11. Маскування даних (Datamasking (DP));
– A.8.12. Запобігання витоку даних (Dataleakageprevention (DP/Cyber));

– A.8.16. Моніторинг активності (Monitoringactivities);
– A.8.23. Веб-фільтрація (Webfiltering (cyber));
– A.8.28. Безпечне кодування (Securecoding (Cyber&Application security)).

Хоча зміни в стандарті значні, вони не вимагають абсолютно нового підходу до інформаційної безпеки чи кардинальних змін у існуючій системі управління інформаційною безпекою. Вони представляють собою адаптації, які були вкрай необхідні для сприяння розумінню та важливості інформаційної безпеки.

Організації, які зараз сертифіковані за стандартом ISO 27001:2013, матимуть три роки для переходу на стандарт ISO/IEC 27001:2022. Перехідний період розпочався 31 жовтня 2022 року та закінчується 31 жовтня 2025 року. Сертифікати на основі ISO 27001:2013 закінчаться або будуть відкликані в кінці перехідного періоду.

В енергетиці інформаційна безпека є надзвичайно важливою через критичну природу енергетичної інфраструктури та потенційний вплив порушень безпеки. Впровадження СУІБ може допомогти енергетичним організаціям захистити конфіденційну інформацію, забезпечити безперервність операцій і запобігти несанкціонованому доступу до критично важливих систем. Дотримання відповідних стандартів, таких як ISO/IEC 27001, є особливо цінним для демонстрації прихильності до інформаційної безпеки в енергетичному секторі. Однак стандартизація – лише перший етап, для побудови ефективної СУІБ необхідний комплексний підхід.

В свою чергу, комплексний підхід охоплює ретельну оцінку зрілості, впровадження захисних механізмів на організаційному та технічному рівнях, а також координацію процесів компанії та безпечний обмін інформацією.

Комплексна оцінка зрілості створює основу для процесу впровадження СУІБ. Вона допомагає організаціям визначити свій поточний стан безпеки та визначити пріоритетні сфери, які потребують вдосконалення. Ця оцінка дозволяє розробити індивідуальні стратегії та заходи для ефективного усунення конкретних вразливостей.

Захисні механізми відіграють життєво важливу роль у захисті інформаційних активів:

– організаційні механізми встановлюють необхідні політики, процедури та інструкції для формування культури безпеки в організації. Чітко визначивши ролі та обов’язки, а також сприяючи підвищенню обізнаності та навчанню співробітників, організації можуть підвищити загальний рівень безпеки;

– на технічному рівні важливим є впровадження відповідних заходів. Це включає розгортання таких технологій, як брандмауери, шифрування та контроль доступу для захисту ІТ-інфраструктури, систем та мереж.

Координація процесів компанії та безпечний обмін інформацією гарантує, що інформаційна безпека буде безперешкодно інтегрована в усі аспекти діяльності організації. Усуваючи ризики безпеки на кожному етапі процесу та враховуючи міркування безпеки у взаємодії з постачальниками та партнерами, організації можуть мінімізувати вразливості та зміцнити свою загальну позицію безпеки.

Інвестиції в систему управління інформаційною безпекою (СУІБ) можуть принести організації кілька переваг. Однак, перш ніж приймати рішення, важливо врахувати як переваги, так і потенційні недоліки.

Переваги інвестування в СУІБ:

– посилення безпеки. СУІБ забезпечує системний підхід до виявлення, управління та зменшення ризиків інформаційної безпеки, тим самим зміцнюючи загальний стан безпеки організації. Вона допомагає захистити конфіденційні дані, інтелектуальну власність та критичні системи від несанкціонованого доступу, крадіжки або пошкодження;

– відповідність нормативним вимогам. Впровадження СУІБ може допомогти організаціям відповідати законодавчим, нормативним і галузевим вимогам, пов’язаним із захистом даних та інформаційною безпекою. Відповідність таким стандартам, як ISO/IEC 27001, може продемонструвати прихильність організації до захисту інформації;

– управління ризиками. Системи СУІБ пропонують структуровану методологію для оцінки ризиків, створення засобів контролю та моніторингу інцидентів безпеки. Такий проактивний підхід дозволяє організаціям виявляти вразливі місця, мінімізувати потенційні загрози та ефективно реагувати на порушення або інциденти безпеки;

– безперервність бізнесу. СУІБ включає в себе стратегії забезпечення доступності та безперервності критично важливих бізнес-операцій навіть під час руйнівних подій. Впроваджуючи відповідні засоби контролю та заходи резервного копіювання, організації можуть пом’якшити вплив інцидентів і зберегти свої послуги та репутацію;

– конкурентна перевага. Демонстрація сильної прихильності до інформаційної безпеки може відрізнити організацію від конкурентів. Клієнти, партнери та зацікавлені сторони часто надають перевагу роботі з компаніями, які можуть продемонструвати надійні заходи безпеки, забезпечуючи конкурентну перевагу на ринку [4, 5];

– покращене реагування на інциденти. СУІБ встановлює процедури для ефективного виявлення, реагування та відновлення після інцидентів безпеки. Це дозволяє організаціям мінімізувати вплив порушень, скоротити час простою і зберегти свою репутацію;

– постійне вдосконалення. Системи СУІБ наголошують на культурі безперервного вдосконалення. Регулярний моніторинг, аудит та огляди засобів контролю безпеки допомагають визначити сфери, які потребують вдосконалення, гарантуючи, що заходи безпеки організації залишаються актуальними та ефективними [6].

Недоліки інвестування в СУІБ:

– фінансові інвестиції. Впровадження СУІБ може вимагати значних фінансових інвестицій, особливо для невеликих організацій з обмеженими ресурсами. Витрати можуть включати початкове налаштування, навчання, інфраструктуру безпеки та поточне обслуговування. Вкрай важливо порівняти витрати з потенційними вигодами;

– зобов’язання організації. Успішне впровадження СУІБ вимагає залучення вищого керівництва та співробітників всієї організації. Опір або відсутність підтримки з боку зацікавлених сторін може перешкоджати ефективності СУІБ та обмежувати її переваги;

– час та ресурси. Створення та підтримка СУІБ може бути трудомістким процесом. Він вимагає проведення оцінки ризиків, розробки політик і процедур, навчання співробітників, а також регулярного перегляду та оновлення засобів контролю безпеки. Організаціям необхідно виділяти спеціальні ресурси для ефективного управління цією діяльністю;

– складне впровадження. Впровадження СУІБ може бути складним завданням, особливо для організацій з різноманітними системами, процесами та зацікавленими сторонами. Це вимагає всебічного розуміння діяльності організації та потенційних ризиків для безпеки. Належне планування, експертиза та співпраця мають важливе значення для подолання цих складнощів [7];

– складність сертифікації. Отримання сертифікації за такими стандартами, як ISO/IEC 27001, вимагає суворого процесу аудиту, документування та дотримання вимог. Це може бути складним і тривалим процесом, особливо для організацій з обмеженими ресурсами або менш зрілими програмами безпеки;

– організаційні збої. Впровадження СУІБ може вимагати змін в існуючих процесах, системах та робочих процесах. Це може призвести до тимчасових збоїв і опору з боку співробітників, які звикли до встановлених процедур. Належне управління змінами та комунікаційні стратегії є життєво важливими для пом’якшення цих викликів.

– обмежена сфера застосування. СУІБ впершу чергу зосереджена на управлінні інформаційною безпекою і може не охоплювати інші аспекти управління ризиками або бізнес-операцій. Організації повинні забезпечити відповідність СУІБ загальній стратегії управління ризиками та доповнювати інші системи, які вони можуть мати [8].

Не зважаючи на те, що існує правова база та міжнародні стандарти для забезпечення кібербезпеки, енергетичний сектор має власні особливості, які потребують значної уваги та зусиль у протидії кіберзагрозам. Особливо коли енергетична кібербезпека України є невід’ємною складовою енергетичної кібербезпеки Європи [9].

І виклики з якими стикається енергетична галузь України, включають наступні [10]:

1. Розгалужена інфраструктура – це про різні географічні зони та розподілені мережі. Це ускладнює підтримку видимості інформаційних технологій, систем, та виправлення вразливостей у пристроях.

2. Організаційна складність – це про велику кількість різних бізнес-підрозділів. Така різноманітність призводить до появи великої кількості окремих політик для різних підрозділів. Наприклад, деяким підрозділам можуть дозволяти використання неперевірених технологій чи імпровізованих технічних рішень. І якщо описати в такій політиці велику кількість обов’язків та вимог

для всіх співробітників, підрядників, постачальників які беруть участь у даному процесі, то політика вийде дуже об'ємною, складною та швидше за все не робочою. Навіть підприємства з чітким розподілом обов'язків між членами команди безпеки потребують визначеного і структурованого процесу для забезпечення обміну інформацією з питань безпеки. Чіткі внутрішні процеси між командами є важливими в електроенергетиці, де різні методи виробництва та частини ланцюга генерації, передачі та розподілу енергії можуть використовувати різні технології. І обмін критичною інформацією, досвідом та координація реагування на окремі інциденти стають ключовими у забезпеченні кібербезпеки.

3. Застарілі технології – це про відсутність або обмежене обслуговування постачальниками. У разі настання інциденту, час реагування розтягується, через залежність від роботи постачальника.

4. Дорога модернізація та обслуговування – це про оновлення застарілих мереж для віддаленого моніторингу, що однозначно покращать видимість та управління системами. Але це не надає негайної вигоди енергетичному бізнесу, тому такі зміни є важко впроваджуваними.

5. Мультивендорне технологічне середовище – це про поєднання спеціалізованого нового та декількох поколінь старого обладнання, що призводить до порушення взаємодії, пошкодження чи руйнування систем.

6. Порушення ланцюгів постачання – це про купівлю інформації, обладнання, програмного забезпечення та всіх видів послуг у сторонніх постачальників по всьому світу, де зловмисники можуть впровадити скомпрометовані компоненти в систему або мережу в будь-який момент життєвого циклу системи. І саботаж ланцюгів постачання іноді здійснюється ненавмисно у вигляді елементів, які не відповідають чинним стандартам безпеки, або навмисно, як частина прихованих зусиль, спрямованих на полегшення майбутньої атаки.

7. Відсутність фізичної безпеки – це про збереження цілісності важливих об'єктів енергетичної інфраструктури: ЦОД, об'єкти передачі та розподілу енергії. Прикладом є незахищені панелі керування, фізичний доступ до яких дозволить отримати локальний контроль над пристроєм чи технологією. І такі фізичні вразливості і відсутність мережевої безпеки дозволять зловмисникам отримати привілеї та руйнувати мережі завдаючи серйозних збитків. Тому енергетичні підприємства повинні інтегрувати фізичну безпеку на всіх рівнях організації. Починаючи з генерального директора, працівники повинні чути послідовні, узгоджені повідомлення, які підкреслюють, що безпека – це відповідальність кожного, і наголошення на конкретних діях, які будуть потрібні в разі виникнення окремих загроз.

Тож кіберзагрозами для енергетичного сектору є як типові загрози: крадіжки даних та програми-вимагачі, так і застаріла інфраструктура, екологічні проблеми та посилений контроль зі сторони регуляторів, оскільки енергетичний сектор є частиною критичної інфраструктури. Також, у таких підприємствах існують прогалини в [10]:

– здатності усвідомлювати ризики, які пов’язані з кібербезпекою бізнес-процесів;

– достатності спеціалістів;

– наявності засобів захисту та контролю операційних та інформаційних систем.

Тому для формування ефективної СУІБ слід почати з комплексної оцінки зрілості кібербезпеки, щоб оцінити поточний рівень зрілості підприємства, та визначити можливості для нарощування додаткових зусиль. Крім того, потрібно визначити пріоритети для захисту найбільш важливих інформаційних активів і систем, які визначають цінність бізнесу. Створити додаткові зони безпеки в мережі для забезпечення захисту ІТ-систем, які можуть мати значний вплив на операції. Навчити персонал, призначити відповідальних та впровадити відповідні політики. І все це необхідно щоб створити надійну, ефективну та працюючу СУІБ, а відповідно і захистити енергетичний сектор від нових загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). [Чинний від 2015-12-18]. Київ, 2016, 22с.
2. Нова версія стандарту ISO/IEC 27001:2022: чим ІТ-компаніям корисний цей стандарт та як його впровадити. AIN.UA. URL: https://ain.ua/2022/12/06/nova-versiya-standartu-iso-iec-270012022-chym-it-kompaniyam-korysnyj-czej-standart-ta-yak-jogo-vprovadyty/.
3. Побудова систем управління інформаційною безпекою (СУІБ). УнІТ. URL: http://unit.com.ua/ua/postroenie-sistemy-upravleniya-infor/.
4. IT Governance. Benefitsof ISO 27001 implementation. URL: https://www.itgovernance.eu/en-ie/iso-27001-ie#:~:text=ISO%2027001%20benefits%20Protect%20your%20data%2C%20wherever%20it,or%20in%20the%20Cloud.%20Increase%20your%20attack%20resilience.
5. ISO/IEC 27001 Information Security Management. The Advantagesofan ISMS. URL: https://msecb.com/the-value-and-benefits-of-iso-iec-27001-certification/#:~:text=Implementation%20of%20Information%20Security%20Management%20System%20%28ISMS%29%20using,competitive%20advantage%3B%20and%20Increases%20customer%20confidence%20and%20trust.
6. BenefitsofanInformation Security ManagementSystem (ISMS). URL: https://www.rajstartup.com/blog/benefits-of-information-security-management-system.
7. DigitalGuardian. Pros and ConsofImplementing ISO 27001. URL: https://www.digitalguardian.com.
8. ISO 27001 Academy. ISO 27001 Implementation Challenges and Howto Tackle Them. URL: https://iso27001academy.com.
9. Що таке енергетична безпека і чому це надважливо для України? URL: https://hmarochos.kiev.ua/partner/energobezpeka/.
10. Cybersecurity in the energyindustry URL: https://cybersecurityguide.org/industries/energy/.

Давиденко Анатолій Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, д.т.н., с.н.с.,
davidenkoan@gmail.com

Гільгурт Сергій Якович,
ІПМЕ ім. Г.Є. Пухова НАН України,
старший науковий співробітник, д.т.н., с.н.с.,
hilgurt@ipme.kiev.ua

Потенко Олександр Сергійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
науковий співробітник,
alexpo84@gmail.com

Кіслов Олексій Геннадійович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник,
alekskislov@i.ua

ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА СПРОЩЕНОГО АЛГОРИТМУ ПОШУКУ ЛІНІЙНИХ БЛОКОВИХ КОДІВ

Вступ.

З метою протидії завадами у каналах передачі інформації, в тому числі – в системах автоматизації об'єктів енергетики, використовуються коригуючи коди, які дозволяють не тільки виявляти, але й виправляти помилки [1]. Лінійний блоковий (коли інформація кодується словами) код довжини n і розмірністю k позначається як (n, k)-код і однозначно визначається так званою породжувальною матрицею G. Множення вхідного слова даних, поданого у вигляді бітового вектора $\overline{v}$, на цю матрицю дає в якості результату слово закодованої інформації у вигляді бітового вектора $\overline{c}$:

$$\overline{c} = \overline{v}\,G = (v_1, v_2, v_3, ..., v_k) \begin{bmatrix} 1 & 0 & ... & 0 \\ 0 & 1 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & 1 \end{bmatrix} \begin{bmatrix} a_{1,k+1} & a_{1,k+2} & ... & a_{1,n-k} \\ a_{2,k+1} & a_{2,k+2} & ... & a_{2,n-k} \\ ... & ... & ... & ... \\ a_{k,k+1} & a_{k,k+2} & ... & a_{k,n-k} \end{bmatrix}.$$

У наведеному вигляді коригуючий код поданий у формі так званого систематичного коду [2], тобто складається з квадратної одиничної матриці та прямокутної матриці кінцівок коду, яка визначає надлишковість перетворення інформації таким кодом. Отже, ширина n породжувальної матриці за визначенням більша за її висоту k.

Найважливішою характеристикою коригуючого коду є кількість помилок, яку він здатний виправити. Ця величина напряму пов'язана з мінімальною кодовою відстанню даного коду. Оскільки цінність коригуючого коду тим вища, чим більшу кількість помилок він здатний виправити, задачу пошуку найкращого коду можна сформулювати, як пошук такої породжувальної матриці, для якої мінімальна відстань коду приймає максимально можливе значення. При цьому на практиці для створення коригуючи кодів можуть бути використані тільки матриці з ***непарними значеннями*** кодової відстані.

1. Складнощі пошуку порождувальних матриць коригуючих кодів.

Відображення результатів пошуку кодів з максимальними значеннями мінімальної кодової відстані у традиційному поданні – у вигляді таблиці, де по вертикалі та горизонталі відкладено відповідно основні параметри коду n та k, не є наочним. В роботі [3] запропоновано більш зручну форму подання породжувальних матриць лінійних блокових кодів, коли параметр k відкладається по вертикалі, а по горизонталі – кількість надлишкових бітів, тобто різниця $n - k$ (табл. 1).

Таблиця 1 – Результати розрахунків мінімальної кодової відстані

n - k / ***k***	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
4	4	4	4	5	6	6	7	8	8	8
5	3	4	4	4	5	6	7	8	8	8
6	3	4	4	4	5	6	6	7	8	8
7	3	4	4	4	5	6	6	7	8	8
8	3	4	4	4	5	6	6	7	8	8
9	3	4	4	4	5	6	6	7	8	8
10	3	4	4	4	4	5	6	7	8	8
11	3	4	4	4	4	5	6	7	8	8
12	2	3	4	4	4	5	6	7	8	8
13	2	3	4	4	4	5	6	7	8	8
14	2	3	4	4	4	5	6	7	8	8

При такому поданні нескладно помітити деякі закономірності, що здатні суттєво вплинути на підходи до обчислення породжувальних матриць. Аналізуючи зміст наведеної таблиці, приходимо до наступних висновків.

1. Матриць з непарними значеннями мінімальної кодової відстані, які мають практичний інтерес, значно менше, ніж з парними.

2. Закономірний характер їх розташування в просторі параметрів (у вигляді «стовпчиків», що інколи «надломлюються» із зсувом праворуч) дозволяє вилучити з розрахунків значну кількість розмірностей коду, для яких отримання непарної відстані гарантовано неможливе.

3. Існують локації, в яких навпаки – поява непарної відстані очікується, фактично, з вірогідністю 0,5. На цих ділянках є сенс шукати найкращі коди.

Справа в тому, що кількість логічних операцій, потрібних для пошуку мінімальної кодової відстані шляхом повного перебору всіх можливих комбінацій, зростає за гіперекспоненційним законом і дуже швидко призводить до надвеликих витрат машинного часу, що вимушує використовувати для вирішення даної задачі високопродуктивні обчислювальні середовища, зокрема, суперкомп'ютерну мережу грід [4, 5].

Врахування закономірностей, згаданих вище, дозволяє помітно скоротити загальний час пошуку шляхом виключення розрахунків матриць з такими співвідношеннями параметрів, для яких гарантовано буде отримано парне (тобто некорисне) значення мінімальної кодової відстані.

На жаль, даний підхід дозволяє прискорити ресурсноємний процес пошуку породжувальних матриць лише в невеликих межах. Застосування численних евристик, технік та прийомів щодо оптимізації програмного коду з метою скорочення часу розрахунків теж призводить до деякого результату, але він також швидко нівелюється по мірі зросту розміру коду.

В табл. 2 наведено залежність часу розрахунків (у секундах) лінійного (*n, k*)-коду від його довжини *n* для деяких значень параметрів [1].

Таблиця 2 – Витрати часу на обчислення мінімальної кодової відстані

k / ***n***	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
40	9	5	8					
41	13	8	10	29				
42	14	9	13	30	129			
43	15	12	15	33	134	248		
44	20	13	16	35	139	278	237	
45	114	19	19	37	141	749	275	256
46	157	100	25	40	145	795	1411	562
47	164	560	66	45	146	796	1926	1191
48	236	601	925	87	152	805	5186	1833
49	2039	719	1323	579	195	814	5554	10222
50	2545	2066	9520	1017	669	843	5367	12740
51	3294	3885	12400	17762	1054	1325	5661	40933
52	6616	3017	11528	32744	8710	1721	5949	44197
53	37997	9360	13057	152864	17660	10218	6695	44529
54	151153	38789	17617	170317	291377	28878	14488	46169
55	163655	77426	51653	298072	484709	167779	29946	56533
56	261207	84538	88434	208767	1518554	359496	170976	66190

2. Спрощений алгоритм пошуку порождувальних матриць.

З метою більш суттєвого прискорення розрахунків в роботі [4] було запропоновано низку прийомів, які дозволили знизити ресурсноємність обчислень. В результаті початкову кількість операцій, яка дорівнювала $k \cdot (n-k) \cdot n \cdot 2^k \cdot 2^{k \cdot (n-k)}$, вдалося знизити таким чином, що обчислювальна складність зменшилася до $O(2^{k \cdot (n-k)}/k!)$ без втрати точності розрахунків. Також був запропонований ***спрощений алгоритм***, який за рахунок вилучення з розглядання деяких комбінацій дозволив позбутися квадратичного ступеня двійки та має обчислювальну складність $O(2^n)$. Оскільки спрощений алгоритм не здійснює повний перебір, виникає природне питання – наскільки здобуті за його допомогою результати можуть відрізнятися від результатів роботи повного алгоритму.

В табл. 3 наведено дані, які дозволяють порівняти використання обох алгоритмів – прискореного повного та спрощеного.

Таблиця 3 – Порівняння результатів повного перебору та спрощеного алгоритму

n-k / ***k***	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**
6	5	6	6	7	8	8	8	8	9	10	10	11	12	12	12	13	14	15	16	16
7	5	6	6	7	8	8	8	8	9	~~9~~	10	11	~~11~~	12	12	12	13	~~13~~	14	14
8	5	6	6	7	8	8	8	8	8	9	10	10	11	12	12	12	13	~~12~~	~~13~~	14
9	5	6	6	7	8	8	8	8	8	9	10	10	11	~~11~~	12	12	**?**	12	13	14
10	4	5	6	7	8	8	8	8	8	9	~~9~~	10	10	11	12	12	12	12	13	14
11	4	5	6	7	8	8	8	8	8	8	9	10	10	11	12	12	12	12	**?**	13
12	4	5	6	7	8	8	8	8	8	8	9	10	10	11	~~11~~	12	12	12	12	**?**
13	4	5	~~5~~	6	6	6	7	8	8	8	8	9	10	10	11	12	12	12	12	12
14	4	5	~~5~~	6	6	6	7	~~7~~	8	8	8	9	10	10	11	~~11~~	12	12	12	12
15	4	4	5	6	6	6	7	~~7~~	8	8	8	9	~~9~~	10	10	11	12	12	12	12
16	4	4	5	6	6	6	7	~~7~~	8	8	8	8	9	10	10	**?**	11	12	12	12
17	4	4	5	6	6	6	6	7	~~7~~	8	8	8	9	10	10	10	11	12	12	12
18	4	4	5	6	6	6	6	7	~~7~~	8	8	8	9	~~9~~	10	10	11	12	12	12
19	4	4	5	6	6	6	6	7	~~7~~	8	8	8	**?**	9	10	10	11	12	12	12
20	4	4	5	~~5~~	6	6	6	7	~~7~~	8	8	8	8	9	10	10	11	12	12	12
21	4	4	4	5	6	6	6	6	7	8	8	8	8	9	10	10	10	11	12	12
22	4	4	4	5	6	6	6	6	7	8	8	8	8	**?**	9	10	10	10	11	12
23	4	4	4	5	6	6	6	6	7	8	8	8	8	8	9	10	10	10	11	12
24	4	4	4	5	6	6	6	6	7	~~7~~	8	8	8	8	9	10	10	10	10	11
25	4	4	4	5	6	6	6	6	7	~~7~~	8	8	8	8	9	10	10	10	10	11
26	4	4	4	5	6	6	6	6	7	~~7~~	8	8	8	8	8	9	10	10	10	10
27	4	4	4	5	6	6	6	6	7	~~7~~	8	8	8	8	8	9	10	10	10	10
28	4	4	4	5	~~5~~	6	6	6	6	7	8	8	8	8	8	9	10	10	10	10
29	4	4	4	5	~~5~~	6	6	6	6	7	8	8	8	8	8	9	10	10	10	10
30	4	4	4	4	5	6	6	6	6	7	8	8	8	8	8	8	9	10	10	10

Тут бежевим кольором позначено результати, яки збігаються для обох способів обчислення породжувальних матриць; зеленим (із закресленими літерами) – матриці, для яких спрощений алгоритм знайшов код з непарним значенням, що насправді не є максимально можливою величиною кодової відстані; пурпурним – місця, для яких повний алгоритм показав кращій результат – знайшов менше значення параметра (n - k), що має сенс кількості надлишкових бітів, тобто код з меншою надмірністю. Символом «?» (у жовтих комірках) позначені клітини, для яких не вдалося прогледіти всі можливі комбінації алгоритмом повного перебору внаслідок його надзвичайно високої ресурсноємності. Особливості пошуку породжувальних матриць є такими, що результати обчислень для всіх комірок, розташованих нижче тих, які помічені символом «?», також є невідомими.

Як можна бачити, майже в половині випадків, для яких вдалося виконати порівняння, спрощений алгоритм показує вірний результат. В решті ситуацій його результат гірше теоретично можливого лише на одиницю (лише код (32,8) виявився виключенням). Отже, можна зробити припущення, що і в переважній кількості інших випадків цей алгоритм надаватиме рішення, не більш, ніж на один біт надмірності, гірші за теоретично можливі.

Висновки.

У роботі експериментальним шляхом доведено працездатність запропонованого спрощеного алгоритму пошуку породжувальних матриць для лінійного блокового коригуючого коду. Показано, що з великою вірогідністю результат, отриманий за допомогою даного алгоритму, не буде гірше теоретично можливого більше, ніж на один біт.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Давиденко А. М., Гільгурт С. Я., Потенко О. С., Кіслов О. Г. Підхід до забезпечення цілісності інформації в кіберфізичних системах. *XL Щорічна науково-технічна конференція молодих вчених і спеціалістів* : тези доп. (Київ, 11 травня 2022 р.). Київ, 2022. С. 57–58.
2. Винничук С. Д., Давиденко А. М., Гільгурт С. Я., Потенко О. С. Нижняя оценка максимального кодового расстояния для линейных блоковых кодов (n, k) над полем GF(2). *Моделювання-2012* : тези доп. міжнар. наук.-техн. конф. (Київ, 16–18 травня 2012 р.). Київ, 2012. С. 150–153.
3. Давиденко А. М., Гільгурт С. Я., Потенко О. С., Кіслов О. Г. Поводження з породжувальними матрицями завадостійкого кодування інформації в кіберфізичних системах. *XLI Щорічна науково-технічна конференція молодих вчених і спеціалістів* : тези доп. (Київ, 17 травня 2023 р.). Київ, 2023. С. 57–58.
4. Винничук С. Д., Давиденко А. Н., Гільгурт С. Я., Потенко А. С. Применение грид-системы при исследовании линейных блоковых кодов. *Системи обробки інформації*. 2013. Вип. 7 (114). С. 61–64.
5. Evdokimov V., Davydenko A., Hilgurt S. Using GRID for Centralized Synthesis of FPGA-based Information Security Systems. *Pattern Recognition and Information Processing (PRIP'2021)* : Proceedings of the 15th International Conference (Minsk, 21–24 Sept. 2021). Minsk, 2021. P. 115–118.

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

ВПЛИВ СЕЗОННИХ ЗМІН КЛІМАТУ НА ВИРОБНИЦТВО ЕЛЕКТРОЕНЕРГІЇ ГІДРОЕЛЕКТРОСТАНЦІЯМИ УКРАЇНИ

На початку XXI століття в енергетичному комплексі України гідроелектростанції (ГЕС) посідають третє місце після атомних (АЕС) та теплових (ТЕС). Для успішної роботи АЕС потрібна вода для охолодження системи, тому їхнє функціонування залежить від кількості водних ресурсів. Зменшення водних ресурсів може призвести до зменшення доступності води для охолодження.

Гідроенергетичні ресурси поряд із вітро- та сонячними ресурсами належать до відновлюваних джерел енергії, їх використання в Україні становить близько 11 млрд. кВт·год. Найбільше значення для гідроенергетики має кліматообумовлена зміна стоку рік. Зниження припливу води у водосховище ГЕС призводить до скорочення виробництва гідроелектроенергії, а зростання притоку збільшує виробництво енергії. При цьому при зміні кліматичних умов гідроенергетичний потенціал експлуатації ГЕС може змінитися та призвести до зміни об'єму стоку. Зміни інтенсивності та частоти екстремальних погодних явищ (повінь та посух) можуть призвести до зменшення виробництва електроенергії [1].

Водночас у теплу пору року збільшується підвищення температури повітря, що у поєднанні з можливим дефіцитом опадів може призвести до зменшення водних ресурсів, доступних для охолодження ТЕЦ та АЕС. Збільшення кількості днів із температурою повітря +25°С негативно позначиться на передачі електроенергії, оскільки з підвищенням температури повітря потужність ліній електропередачі знижується, а втрати потужності збільшуються [2].

Проведено аналіз модельних даних для визначення загальних тенденцій зміни клімату за усередненими кліматичними характеристиками на всій території України [3]. Для цього отримано середні значення прогнозованих рядів даних, які мали усереднення, внаслідок чого були отримані набори даних, і за місячними даними розраховувалися температура повітря та кількість опадів, середні за сезони, рік та десятиліття XXI ст. Протягом періоду, що досліджується (2025–2050 рр.), спрогнозовано стійке підвищення температури повітря.

Для розрахунку використано статистичні дані середньорічних температур повітря, середньорічної кількості опадів та обсяги виробництва електроенергії гідроелектростанціями України за п' ятирічними періодами (1996–2000, 2001–2005, 2006–2010, 2011–2015, 2016–2020 рр.) [4].

У третє та четверте десятиліття XXI століття прогнозується підвищення середньорічної температури повітря за 1,8ºС. До середини XXI ст.

прогнозується підвищення температури до періоду дослідження 2001–2010 рр. від 0,2 до 2,1ºС. Отже, до кінця XXI ст. прогнозують підвищення температури усереднене на всій території України щодо 2001–2010 років від 0,7 до 3,0 ºС.

За сценарієм помірної концентрації парникових газів RCP4.5, наведеним в [5], очікується, що порівняно з показниками станом на кінець XX сторіччя середньорічні температури повітря можуть зрости на 1,2°С–3°С до середини і на 1,6°С–3,5°С до кінця XXI століття.

За сценарієм високої концентрації парникових газів RCP8.5 [5], якщо порівнювати з показниками станом на кінець XX століття, можливе зростання середньорічних температур на 1,7°С–4,1°С до середини та на 3,4°С–6,2°С до кінця XXI століття. В табл. 1 надані середньорічні температури і обсяги виробництва електроенергії гідроелектростанціями України у 2000–2050 рр. При цьому річна кількість опадів варіюється по всій Україні: дуже вологі й дуже посушливі роки. Очікується, що ця мінливість збережеться і в майбутньому.

Таблиця 1 – Середньорічні температури і обсяги виробництва електроенергії гідроелектростанціями України у 2000- 2050 рр.

Рік	RCP4.5				RCP8.5			
	Δt=3ºС		Δt=2,1ºС		Δt=4,1ºС		Δt=2,9ºС	
	$t_{\text{пр}}$	g_{HPP}	$t_{\text{пр}}$		$t_{\text{пр}}$		$t_{\text{пр}}$	
2000	8,2	12148	8,2	12148	8,2	12148	8,2	12148
2005	8,5	11547	8,5	11547	8,5	11547	8,5	11547
2010	8,4	11748	8,4	11748	8,4	11748	8,4	11748
2015	9,3	9946	9,3	9946	9,3	9946	9,3	9946
2020	9,9	8744	9,9	8744	9,9	8744	9,9	8744
2025	10,1	8277	9,3	9907	11,0	6522	9,9	8673
2030	10,7	6996	9,9	8729	11,3	6006	10,2	8207
2035	10,5	7636	9,6	9318	10,9	6694	9,9	8828
2040	10,7	7209	9,8	8925	11,9	4800	10,7	7119
2045	11,0	6568	10,1	8336	12,0	4456	10,9	6808
2050	11,2	6141	10,3	7943	12,3	3939	11,1	6342

Проведений аналіз дозволяє оцінити вплив кліматичних змінних (таких як атмосферні опади та температура) на виробництво електроенергії ГЕС. У разі потепління клімату підвищується вразливість ГЕС. Причиною цього є підвищення середньорічних температур та скорочення основних джерел живлення гірських річок внаслідок зниження кількості атмосферних опадів у вигляді снігу та інтенсивного танення сезонного снігового покриву. Дослідження показало, що в умовах зміни клімату слід розглядати всі можливі альтернативи задоволення попиту, що одночасно зростає, на електричну енергію і збільшення обсягів водоспоживання. Одним з напрямків може з’явитися розробка та впровадження в практику інноваційних конструкцій малих ГЕС, здатних адаптуватися до змін клімату і, як наслідок, витрати води в річках.

На підставі проведеної оцінки впливу змін клімату для енергетичної галузі, визнаючи важливість гідроенергетики для подальшого розвитку електроенергетики України, слід приділити велику увагу вивченню впливу сезонних змін клімату на виробництво електроенергії гідроелектростанціями. Для адаптації гідроенергетики до змін клімату доцільно уточнити гідроенергетичний потенціал малих та середніх річок, враховуючи, що гідроенергетика є перспективною та економічно ефективною складовою відновлюваних джерел енергії. Крім того, доцільно розробити нові правила експлуатації водогосподарських та гідроенергетичних систем, беручи до уваги, що спостерігаються очікувані зміни клімату. В результаті можливості збільшити вироблення гідроенергії використовуються не повністю, виникають надзвичайні ситуації. Для раціонального управління роботою водосховищ потрібні нові підходи та правила експлуатації гідровузлів та їх каскадів з урахуванням змін гідрометеорологічного режиму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ландау Ю. О., Сташук І. В. Значення гідроенергетики в розвитку ОЕС України відповідно до НЕС-2035 і екологічні виклики. *Гідроенергетика України*. 2018. № 1–2. С. 3–6.
2. Ландау Ю. О. Пріоритетні напрямки розвитку гідроенергетики України в умовах євроінтеграції. Національний інститут стратегічних досліджень. Серія «Національна безпека». Київ, 2014. Вип. 8.
3. Виробництво електроенергії в Україні у 2021 році. URL: https://vse.energy/news/pek-news/electro/1935-power-generation-202112.
4. Вплив зміни клімату в Україні, 2021. URL: https://www.metoffice.gov.uk
5. Розроблення сценаріїв зміни кліматичних умов в Україні на середньо- та довгострокову перспективу з використанням даних глобальних та регіональних моделей. Звіт про науково-дослідну роботу. Київ, 2013.

Здоренко Юрій Миколайович,
Національний університет «Полтавська політехніка імені Юрія Кондратюка», доцент кафедри компютерних інформаційних технологій та систем, к.т.н.,
zdorenkoviti@gmail.com

Здоренко Марина Сергіївна,
marishkina84@gmail.com

МЕТОД ВИЯВЛЕННЯ 0-DAYАТАК В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТУКТУРИ

Кібернетичний захист інформаційно-комунікаційних мереж (ІКМ) об'єктів критичної інфраструктури, а саме енергетичної галузі є важливою складовою забезпечення безпеки держави. Системи виявлення атак для таких мереж потребують постійного удосконалення. Аналіз потоків даних, що передаються в цих мережах дозволяє здійснювати виявлення можливої атаки та здійснити заходи щодо її попередження на основі наявних відомостей про такі атаки в минулому. Тому поява невідомих або модифікованих атак робить неефективним використання систем виявлення на основі сигнатурних методів. Трафік за номальними характеристиками не завжди свідчить про наявність нової (0-day) атаки. Тому для ІКМ об'єктів критичної інфраструктури, пропонується реалізувати новий метод виявлення атак, який ґрунтується, на використанні даних про рівень аномальності трафіку.

Використання сигнатурних методів аналізу, як було зазначено вважається малоефективним. Тому задачу виявлення нової або модифікованої атаки пропонується вирішувати з використанням підходів на основі штучного інтелекту. В умовах недостатньої (неточної) інформації про можливу атаку обґрунтованим є використання нечітких систем логічного виводу [1].

Для налаштування та адаптації параметрівтаких систем застосовуються підходи, які можуть бути основані на використанні математичного апарату штучних нейронних мереж. Це дозволить обрати початкові параметри для налаштування нечітких систем логічного виводу, а також, у разі потреби, змінювати їх в процесі функціонування ІКМ.

У якості вхідних величин нейро-нечіткої системи для класифікації атак пропонується використати величину, що характеризує рівень аномальності трафіку та дані про кількість вхідних та вихідних пакетів з відповідною ознакою, а саме: IP-адреса відправника та одержувача, порт відправника та одержувача, загальна кількість вхідних (вихідних) пакетів.

Вихідна величина визначається в процесі навчання нейронної мереж із використанням алгоритму оберненого поширення помилки, як функціонально залежна від вхідних величин.

Передбачається, що використання пропонованого методу на основі даних про рівень аномальності значно удосконалить процес виявлення невідомих або модифікованих атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Здоренко Ю. М., Фесьоха В.В. Нейро-нечітка система виявлення вторгнень в інформаційно-телекомунікаційних мережах. *Збірник наукових праць ВІТІ*. 2018. Вип. № 3. С. 83–89.

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

МОДЕЛЮВАННЯ ЗБІРНОГО СОНОТРОДУ ДЛЯ УЛЬТРАЗВУКОВОГО ЗВАРЮВАННЯ НЕТКАНИХ ПОЛІМЕРНИХ МАТЕРІАЛІВ

При зварюванні нетканих матеріалів виникають задачі використання розвинутих, по геометрії, сонотродів протяжністю більше ніж довжина стрижневої хвилі коливань матеріалу сонотроду. Особливу увагу викликаюсь задачі в яких треба отримати криволінійний дискретний зварювальний шов. Для цієї операції краще використати збірний двоступінчастий сонотрод [1].

Була поставлена наступна задача: розробити сонотрод для зварювання декілька шарів тонкого нетканого матеріалу сорока чотирма точками, кожна діаметром 3 мм, які повинні розташовуватися по колу діаметром 3 мм, які повинні розташовуватися по колу діаметром 215 мм. Коефіцієнт посилення сонотрода має бути не менше 5.

Моделювання збірного двоступінчастого сонотроду відбувається в три етапи: моделювання робочого стрижневого сонотроду, як елемент другої ступені, моделювання базового плаского чи криволінійного сонотроду, як елемент першої ступені, а потім перевірка сонотродів в зібраному вигляді [2].

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

Розв’язувалась пружна задача під дією гармонійною збуджувальною силою з врахуванням дисипативних втрат матеріалу сонотродів на робочій частоті за умов вільних границь сонотродів. 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.

На рис. 1 показано епюру середньоквадратичних переміщень поверхні збірного сонотроду під дією збуджувальної сили. Червоними стрілками показано розподілення гармонійної збуджувальної сили на поверхні плаского сонотроду. На рис. 2 показано амплітудно-частотну характеристику модуля переміщення вихідної точки на поверхні робочого сонотроду (синя крива) та однієї з точок прикладання збуджувальної сили (зелена крива).

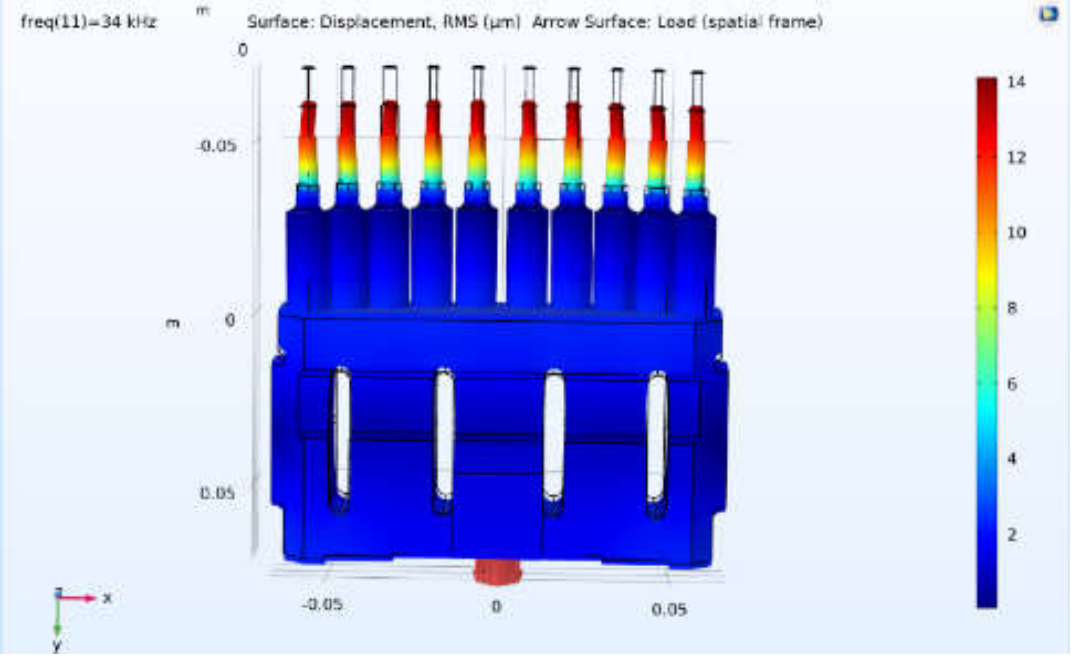

Рисунок 1 – Епюра коливань збірного сонотроду

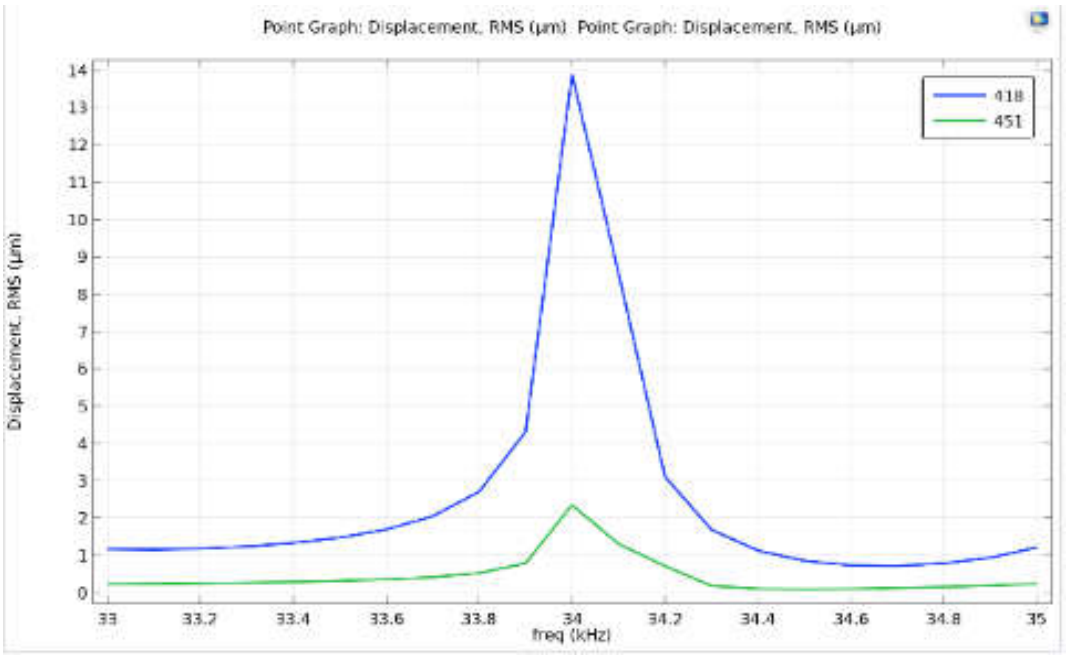

Рисунок 2 – Амплітудно-частотна характеристика вихідної та вхідної точки на поверхні збірного сонотроду

По результатам моделювання була виготовлена робоча модель зварювальної системи збірних сонотродів (рис. 3), яка складалася з чотирьох збірних сонотродів та виконувала зварювання 44 точок, які розташовані на колі діаметром 215 мм при довжині половинної стрижневої хвилі 75 мм, для даного матеріалу.

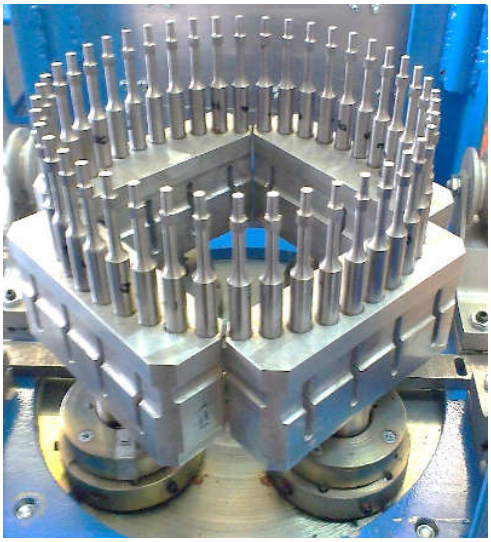

Рисунок 3 – Робоча модель зварювальної ультразвукової системи
зі збірними сонотродами

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сенченков И. К. Модальная классификация и проектирование сонотродов для ультразвуковой обработки материалов. *Акустичний вісник*. 1998. Том 1, № 4. С.55–64.

2. Дяченко С. М. Задача моделювання характеристик складного збірного сонотроду для ультразвукового зварювання полімерів. *Кібербезпека енергетики* : матеріали науково-практичної конференці (Київ, 27 травня 2022 р.). Київ : ІПМЕ ім. Г.Є.ПуховаНАН України, 2022. 129 с.

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

СИСТЕМА ОБМІНУ ЗНАННЯМИ ТА ДОСВІДОМ МІЖ ФАХІВЦЯМИ З КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Не зважаючи на розвиток інформаційних технологій та технологій кібербезпеки, людина залишається найвразливішим місцем будь-якої інформаційно-комунікаційної або технологічної системи об'єктів критичної інфраструктури.

Причинами такої вразливості людини є недостатність знань, досвіду, відсутність відповідних інструкцій, мотивації тощо. Зосередимось на проблемі знань та досвіду. Природньо склалося так, що з підвищенням рівня знань та досвіду фахівця, фахівець отримує більш вигідні пропозиції роботи і змінює своє місце роботи. В умовах війни з рф існує дефіцит фахівців для критичної інфраструктури, який зумовлений підвищеними ризиками для життя таких фахівців та їх загибеллю від ракетних ударів. Саме в цей момент часу система залишається найбільш вразливою. Новий спеціаліст який прийшов працювати потребує часу для ознайомлення з системою, визначення її слабких місць, аналізування наявних ризиків. Кіберінциденти та нештатні ситуації, які можуть виникнути в цей проміжок часу також зазвичай потребуватимуть більше часу для їх усунення, що може мати значні негативні наслідки для об'єкта критичної інфраструктури, в тому числі і на безпеку життя громадян.

Таким чином постає проблема зменшення часу для опанування новим фахівцем своєї сфери відповідальності. Ця проблема може бути вирішена шляхом передачі знань і досвіду від попередника. Однак передати такі знання та досвід з урахуванням частої зміни персоналу та інших факторів не можливим без використання засобів інформатизації.

Таким чином пропонується створення та впровадження системи обміну знаннями та досвідом між фахівцями (далі – платформа) з інформаційних технологій та кібербезпеки.

Основними критеріями такої системи повинно бути довірене середовище, ефективна взаємодія, обмін знаннями та досвідом, можливість пошуку ефективних рішень. Зокрема довірене середовище, забезпечене підтвердженням приналежності фахівця до організації його роботодавцем дасть змогу створення статистичних даних про проблеми кіберзахисту в галузі та підвищить ефективність взаємодії в галузі та фахівцями з інших галузей. Обмін знаннями та досвідом може бути забезпечений профілем користувача, де користувач може додати перелік програмного та програмно-апаратного забезпечення, що його оточує, переглянути історію чатів з інформацією про виявлені проблеми іншими фахівцями, в тому числі виявлені попередником та їх варіанти рішень. Водночас є можливість і задати питання, де учасники системи можуть допомогти, підвищивши власний рейтинг, якщо порада буде оцінена іншими

фахівцями. Така платформа стане предметом зацікавленості вендорів, так як вони безпосередньо зацікавлені у виявлені та вирішенні проблем з їх продуктами, які не були виявлені в процесі тестування перед виходом в продаж.

Цілями такої системи повинні бути накопичення знань та досвіду, забезпечення швидкого пошуку інформації, створення рейтингів вразливостей, рекомендацій користувачів, надійності вендорів, генерація ретроспективного аналізу, прогнозування. Такі цілі можуть бути досягнені шляхом залучення до платформи фахівців з автоматизованих систем управління технологічними процесами, інформаційних технологій та кібербезпеки, вендорів, представників команд реагування на комп'ютерні надзвичайні події (CERT), менеджерського складу (CIO, CTDO, CISO), аудиторів інформаційної безпеки та аудиторів систем управління інформаційною безпекою.

Таким чином основними цінностями системи стануть спільні цілі, довіра, бажання прогресу, мотивація.

Звісно, для того щоб впровадження системи набуло поширення, вона повинна бути простою у користуванні, адаптивною, інтерактивною, сприяти стратегічним комунікаціям та бути ефективною.

Концепція такої системи поєднує професійний форум, маркетплейс та спортивні змагання. Концепція професійного форуму реалізується через обмін повідомленнями (коментарями), маркетплейс представлений можливістю користувача обрати програмне забезпечення та додати його з інформацією про нього до власного профілю, спортивні змагання – рейтингуванням фахівців відповідно до їх участі в наповненні баз даних платформи. Таким чином реалізується принцип «використовуй знання та поширюй їх». Важливо також відмітити, що локалізація фахівців спростить обмеження в знанні англійської мови, та можливі неточності перекладу при використанні автоматизованих засобів перекладу технічного тексту. За своєю суттю кабінет користувача стане його віртуальним портфелем, яким зможе користуватися його наступник, а на новому місці роботи у випадку однакових програмних та апаратних засобів при їх додаванні фахівцем у свій новий електронний кабінет він зможе знов використовувати свій попередній досвід. Наявність рейтингу дасть можливість оцінити фахівцю свій внесок, роботодавцю рейтинг стане додатковим аргументом щодо заохочень фахівця.

Для реалізації такої системи запропоновано наступну архітектуру:

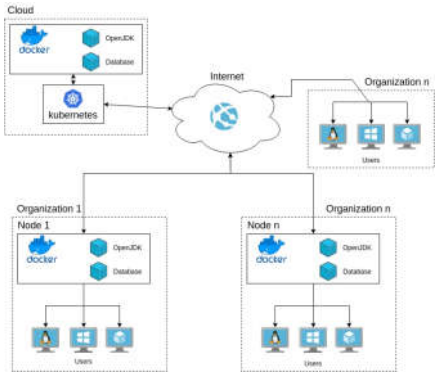

Рисунок 1 – Архітектура системи обміну знаннями та досвідом між фахівцями

Представлене рішення призначене для збору, обробки, аналізування та обміну даними кібербезпеки з метою підвищення ефективності засобів кіберзахисту. Також доцільним є інтеграція в платформу існуючих сервісів зі збору, обробки та візуалізації інформації з відкритих джерел.

На основі результатів дослідження з візуалізації рівня ризику інформаційної та кібербезпеки, візуальної аналітики, що представлені в розділі 3 цієї роботи розроблено макет інтерфейсу платформи (див. рис. 2).

Рисунок 2 – Інтерфейс системи обміну знаннями та досвідом між фахівцями

Інтерфейс складають ряд інформаційних блоків (дашбордів). Зверху вікна надана інформація про кількість зареєстрованих учасників в кожній категорії користувачів. Таке представлення сприяє підсвідомій довірі до користувачів до експертного рівня користувачів платформи. Нижче зображено візуалізацію кількості представників в кожній галузі критичної інфраструктури не залежно від категорії користувачів. Нижче зліва на право представлено показники трендів виявлених вразливостей (проблем) в галузі. Наступний віджет показує активність представників кожної галузі в обговоренні на платформі. Показник активності формується шляхом пропорційного оцінювання загальної кількості коментарів з галузі, до кількості коментарів з високими оцінками інших користувачів. Окремо представлено графік внесків користувачів за їх категоріями. Справа також представлений віджет останніх оновлень з інформацією про програмне та апаратне забезпечення, інформація про вразливості якого тільки з'явилася. Нижче від вищевказаного віджету представлений віджет з псевдонімами (нікнеймами) кращих фахівців за рейтингом коментарів, як рекомендація для заохочення відповідними вендорами за їх внесок у тестування продуктів та знання. В нижньому правому куті вікна надано кнопки для повідомлень про кіберінциденти до Державної служби спеціального зв'язку та захисту інформації України, Команди реагування на комп'ютерні надзвичайні події (CERT-UA) та зв'язку з командою розробників платформи. Зліва представлено меню платформи, де користувач може вибрати розділи «Власні інформаційні активи» (Assets) (див. рис. 3) для редагування даних про них та, де може продивитися нові коментарі та повідомлення щодо власних інформаційних активів, «Проблеми» (Issues), де

можна подивитись класифікацію наявних проблем з активами користувача за матрицею Mitre (див. рис. 4), Дані «Feeds», де користувач може прочитати більше інформації, пов’язаної з його обладнанням, зокрема випадки (кейси), що мали місце, окремо побачити посилання, якими обмінювалися в коментарях до конкретного інформаційного активу, поради тощо (див. рис. 5).

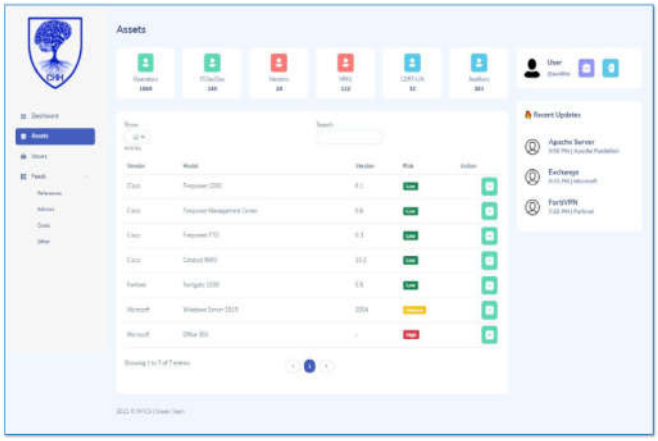

Рисунок 3 – Інтерфейс розділу меню «Власні інформаційні активи»

У даному розділі меню платформи після додавання до переліку власних інформаційних активів програмного та програмно-апаратного забезпечення з зазначенням його версії, користувачу доступна оцінка ризику використання такого активу. Оцінка ризику використання певного інформаційного активу формується за результатами збору та аналізу інформації з відкритих джерел та локальної бази даних платформи. Підхід до такого оцінювання базується на основі досліджень представлених в розділах 2 та 3 цієї роботи, як поєднання принципів роботи технологій автоматизації обміну інформацією про безпеку (SCAP) та розроблених багатофакторних підходів до оцінювання ризиків. Також користувач може додати дані про власний актив, які анонімізовано будуть відразу будуть доступними іншим користувачам платформи, що експлуатують такі ж активи. Вподальшому планується розробка нейронної мережі з використанням технологій штучного інтелекту, яка на основі порівняння

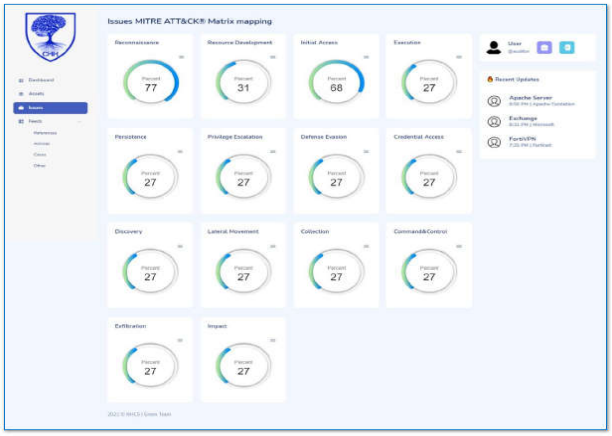

Рисунок 4 – Інтерфейс розділу меню «Проблеми»

переліків обладнання (шаблонів конфігурацій) зможе оцінювати ризик використання того чи іншого активу в рамках зв'язків з іншими і показувати загальний ризик для системи.

У даному пункті користувач може побачити кількісні показники наявних проблем з його активами відповідно матриці MITRE ATT&CK, що сприятиме комплексному розумінню власної системи при оцінюванні наявних ризиків.

Зокрема для створення уніфікованого аналізування даних з системи про загрози розроблено вимоги до класифікації кіберзагроз [1].

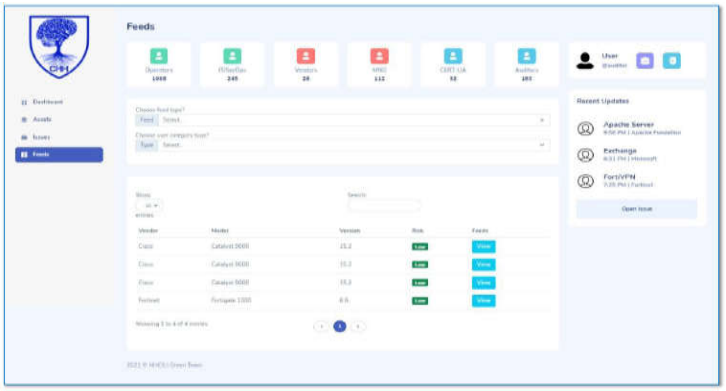

Рисунок 5 – Інтерфейс розділу меню «Дані»

У даному розділі користувач може вибрати тип даних, які він отримав та відсортувати їх за категорією користувачів, які їх надали (аудитори, адміністратори тощо). Така інформація є корисною абсолютно для всіх категорій користувачів так як допомагає сформувати матеріали (презентації) для переконання менеджменту у доцільності впровадження відповідних додаткових заходів з кібербезпеки.

Водночас дослідження в розділі 3 з соціальної інженерії показали, що фахівець з захисту для ефективної протидії зловмиснику також повинен бути постійно мотивованим не менше зловмисника у досягненні цілей, а його керівник не повинен допустити появи незадоволеного такого фахівця, так як тоді такий фахівець може становити загрозу у досягненні організації власних цілей.

Таким чином постало завдання дати можливість керівнику оцінювати стан підлеглого фахівця, а фахівцю отримати візуалізацію його розвитку та порівняти власні досягнення з іншими учасниками платформи (представниками галузі кібербезпека). Для цього була розроблена окрема сторінка профілю користувача «MyLandscape», де він та його керівник може побачити внесок користувача у систему «Myvalue» та графік активності фахівця на платформі «MyProgress» (див. рис. 6). Ці графіки формуються динамічно у часі, таким чином якщо фахівець перестав вносити інформацію в систему, то відсоток його внеску буде зменшуватися, а графік активності спадати. Такі поведінки графіків будуть свідчити про необхідність підвищення кваліфікації фахівця та створення додаткових механізмів мотивації. Вчасне виявлення такої проблеми допоможе керівнику утримати кадри, не створюючи додаткові ризики для організації.

Загальна система мотивації у розробленому рішенні побудована таким чином, що кожен користувач бачить свій внесок, що по суті є об'єктивною оцінкою його досвіду та знань. Керівник, який бачить оцінку фахівця мотивований його утримати, також керівник бачить оцінку внеску власних фахівців як оцінку внеску організації у загальний внесок галузі. Таким чином галузь може формувати аргументовані потреби до забезпечення кадрами та технічними засобами і ефективно їх розподіляти у разі задоволення цих потреб, бачити і аналізувати вплив від задоволення цих потреб, що водночас може позитивно вплинути на корупційні ризики при найманні некваліфікованого персоналу або закупівель послуг, обладнання та програмного забезпечення. Обмін якісними знаннями та практичним досвідом стане спільним інтересом. Спільна зацікавленість у швидкому вирішенні та попередженні проблем з кібербезпекою.

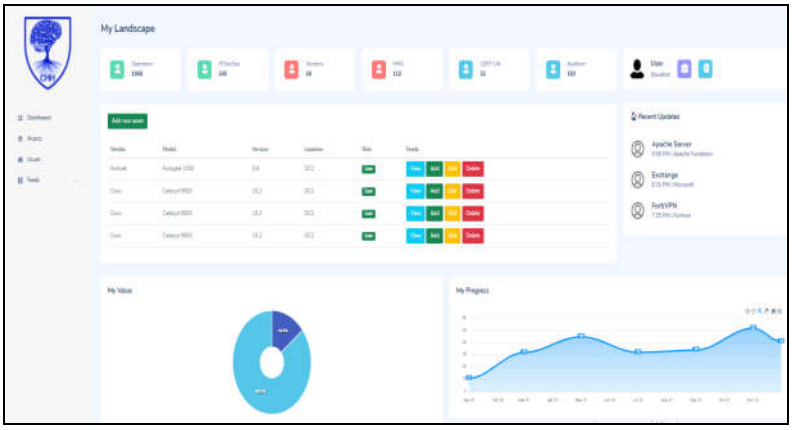

Рисунок 6 – Інтерфейс особистої сторінки користувача

Таким чином впровадження такої платформи вирішить проблеми накопичення, збереження знань та досвіду в рамках організації, сформує довірене експертне середовище зі спільними цілями та цінностями, дасть можливість оцінити знання та досвід кожного фахівця, оцінити зрілість процесів кібербезпеки в рамках галузі, адекватно оцінити потребу у спеціалістах певної категорії та їх професійний рівень, сприятиме процесам управління ризиками та служитиме у підтримці прийняття рішень.

До переваг такої платформи можна віднести універсальність так як вона може бути впроваджена як на глобальному рівні для користувачів з державних органів та об'єктів критичної інфраструктури, так і локально в межах організації, збереження досвіду, поширення перевірених рішень наявних проблем, формування бази знань для розробки загальних та галузевих стандартів, допомога в управлінні ризиками, оптимізація робочого часу фахівця з кібербезпеки, оперативна підтримка рішень, мотивація для створення спільної безпеки.

Окремо варто виділити цінність даних системи при реагуванні на кіберінциденти та їх управління, зокрема наявність можливості ретроспективного аналізу проблем, що виникали допоможуть швидко виявити причину кіберінциденту та вжити ефективних заходів з недопущення його повторення [2].

Така штучно сформована спільнота фахівців з урахуванням наявного розподілу ролей (категорій фахівців) наявними процесами буде мати перспективи до саморозвитку. Також до перспектив розвитку самої системи можна віднести можливість впровадження технологій штучного інтелекту, створення механізмів ретроспективного аналізу для оцінювання правильності прийнятих рішень, впровадження механізмів швидкого пошуку даних, розробка і додавання інших рейтингів для бізнес аналітиків, інтеграція систем оповіщення у випадку появи нових проблем (месенджери, електронна пошта).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Komarov M., Davydiuk A., Onyskova A., Tkachenko V. Honchar, S. Requirements for a Taxonomy of Cyber Threatsof Critical Infrastructure Facilities and an Analysis of Existing Approaches. *Systems, Decision and Controlin Energy II. Studies in Systems, Decision and Control* / In: Zaporozhets, A., Artemchuk, V. (eds). Vol. 346. Cham : Springer, 2021. P. 189–205. DOI: https://doi.org/10.1007/978-3-030-69189-9_11.

2. Давидюк А. В., Сергеєв С. М., Ткаченко В. В. Аналіз підходів до управління кіберінцидентами систем критичного призначення. *Проблеми інформатизації* : матеріали Дев’ятої міжнародної науково-технічної конференції (Черкаси, 18–19 листоп. 2021 р.). Черкаси, 2021. С. 54.

Давиденко Анатолій Миколайович,
ІПМЕ ім. Г.Є. Пухова НАН України,
провідний науковий співробітник, д.т.н., с.н.с.,
davidenkoan@gmail.com

Висоцька Олена Олександрівна,
Національний авіаційний університет,
доцент кафедри комп'ютеризованих систем захисту інформації, к.т.н.,
lek_vys@ukr.net

Потенко Олександр Сергійович,
ІПМЕ ім. Г.Є. Пухова НАН України
науковий співробітник,
potenko@ipme.kiev.ua

ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ АНАЛІЗУ ГРАФІЧНИХ ЗОБРАЖЕНЬ

Анотація. Запропонована розробка програмного застосунку для контролю доступу до програмного забезпечення шляхом онлайн-контролю присутності користувача на робочому місці. Пропонується мультифакторна автентифікація з використанням біометричних параметрів користувачів, а саме, рис обличчя. Проблема класифікації зображень вирішується за допомогою нейронних мереж. Для навчання нейронних мереж запропоновано оригінальний набір даних.

Ключові слова: контроль доступу, класифікація зображень, нейронні мережі, методи глибокого навчання.

Постановка задачі. Біометричні методи автентифікації користувачів все частіше використаються в світі. Це сканування відбитків пальця, сканування радужки ока, фіксація відео зображення з вбудованих фото та відеокамер. Це характерно як для смартфонів так і для планшетів та ноутбуків. Такі методи також використовуються в корпоративних середовищах, підприємствах та інших установах для контролю доступу до десктопів, мейнфреймів, серверним платформам. Однак такі системи вразливі [1]. Наприклад, коли система залежить від розпізнавання обличчя по зображенню, її можна обдурити досить простими методами: роздрукованими фотографіями, зображеннями на екранах телефонів/планшетів, будь-якими іншими носіями з високою розподільною здатністю.

Такі атаки називаються спуфінгом, а відповідні зображення – спуфами. Навіть фірму Samsung, яка спеціалізується на комп'ютерному зорі, ця проблема не обійшла стороною. 26 із 60 телефонів різних моделей можна легко розблокувати, показавши якісний портрет перед селфі-камерою. Актуальність роботи обумовлюється значним поширенням таких атак.

Метою роботи є розробка програмного застосунку для захисту інформаційних систем на основі аналізу графічних зображень, який шляхом он-

лайн ідентифікації користувача блокуватиме критичні додатки під час його відсутності на робочому місці.

Реалізація. Для досягнення поставленої мети вирішувалися наступні завдання: аналіз засобів і методів захисту інформації на основі аналізу графічних зображень для визначення способу захисту; розробка програмного застосунку, для захисту інформаційних систем на основі аналізу графічних зображень моніторингу присутності користувача на робочому місці; тестування створеного програмного застосунку для порівняння із сучасними аналогами.

Автентифікувати людину можна за ознаками, пов'язаними з її фізіологічними особливостями, які однозначно ідентифікують людину. До таких ознак належать: геометрична будова кисті, відбитки пальців, особливості малюнка сітківки, райдужної оболонки ока, портрет (наприклад, інфрачервона карта людини), характеристики та особливості мови, почерк, клавіатурний і комп'ютерний почерк [2], інші фізіологічні особливості людини, що робить її «особливою».

За даними консалтингової компанії «International Biometric Group» з Нью-Йорка, відзначається, що з $127 млн виручки від продажу біометричних пристроїв 44% припадає на сканери відбитків пальців. На другому місці за попитом – системи розпізнавання рис обличчя – 14%, далі – пристрої розпізнавання форми долоні (13%), голосу (10%) та райдужної оболонки ока (8%). Для задач моніторингу перша технологія не зовсім зручна в зв'язку з необхідністю фіксації пальця на сканері. Тому розглянемо системи розпізнавання рис обличчя.

Задача класифікації зображень, зараз переважно вирішується за допомогою нейронних мереж [3]. Загалом для навчання нейронних мереж та їх якісної роботи потрібен великий масив даних (набір даних). Для поставленої задачі можна ввести обмеження в 5000 оцифрованих фотографій. Для вдалої протидії спуфінгу набір даних повинен містити однакову кількість спуфів і реальних зображень для максимально реалістичного імітування атаки на системи розпізнавання обличчя.

Для збору облич була обрана платформа YouTube із сотнями тисяч відео різної тематики, на яких присутні люди. Ідея полягала в тому, щоб аналізувати відео з людьми та витягувати з них окремі кадри. Це дозволяє імітувати реальну ситуацію розпізнавання обличчя, де може бути багато людей і фон непередбачуваний. Для створення підробок було вирішено використовувати частини зображень, підготовлених на попередньому етапі, генеруючі з них спуфи. Розмір кінцевого набору даних: 5321 зображення. З них 49% – підробки, 51% – не підробки (рис.1).

Розробка програмного застосунку: Мова реалізації – Python 3.8.0. Вибір версії 3.8.0 здійснено через сумісність з пакетами Face recognition 1.4, Cmake 3.25.0, Dlib 19.19, які нам потрібні на основі розробленого алгоритму. Пакет Face recognition 1.4 реалізує модель розпізнавання обличчя на основі бібліотеки Dlib, заснованій на методах глибокого навчання.

Для запуску застосунку адміністратор системи повинен запустити програму facerec.py за допомогою командного рядка. Для автоматичного

запуску програми, при старті системи, необхідно розмістити CMD скрипт, який запускає програму в папці C:\Documents and Settings\All Users\Start Menu\Programs\Startup.

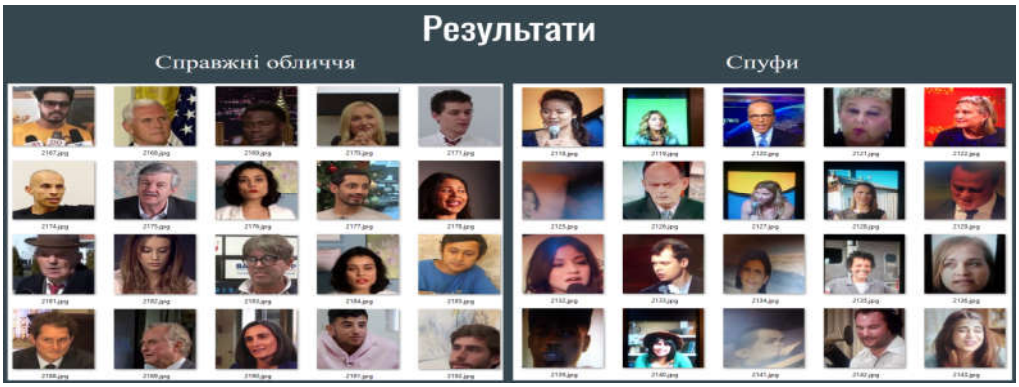

Рисунок 1 – Кінцевий набір даних з 5321 зображення

Після запуску система, за допомогою вебкамери аналізує обличчя користувача (рис. 2). Якщо користувачем виявиться адміністратор, то система запропонує або продовжити роботу у звичному режимі (запустить застосунок, з яким користувач працював під час останнього сеансу), або попросить вибрати новий застосунок зі списку, або запропонує увійти в налаштування системи. В режимі налаштування системи адміністратор може додати або видалити користувачів, та назначити їм додатки, з якими вони матимуть можливість працювати.

Якщо система розпізнає користувача без прав адміністратора, то вона запропонує роботу в звичайному режимі (запустить застосунок, з яким користувач працював під час останнього сеансу), або дасть можливість вибрати інший застосунок зі списку дозволених адміністратором системи.

У разі відсутності користувача в базі даних системи, програма попросить невідомого користувача звернутися до адміністратора системи.

Програмний застосунок постійно стежить за наявністю користувача перед комп’ютером, і у разі його відсутності, буде заблоковано програму, я якою він працював.

Рисунок 2 – Приклад успішного розпізнання

Висновки. Запропонований програмний застосунок можна використовувати для контролю доступу до критично важливих застосунків шляхом онлайн-контролю присутності користувача на робочому місці. Крім того, додаткова практична цінність програмного рішення полягає у використанні бібліотек з відкритим кодом, що дозволить провести подальшу перевірку запропонованого рішення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vysotska O., Davydenko A. Dodatkowe uwierzytelnianie uprawnionych użytkowników według geometrii ich twarzy w systemach informatycznych wykorzystujących technologię singlesign-on. *Inżynier XXI wieku*. Part of the Monograph «Przetwarzanie, transmisja I bezpieczeństwo informacji» (10 grudnia 2021), Bielsko – Biała, Polska, 2021, S. 257-268. DOI: https://doi.org/10.53052/9788366249868.27
2. Vysotska O., Davydenko A. Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor *Authentication. Advances in Intelligent Systems and Computing*. 2020. Vol. 938. P. 356–368.
3. Patent UA 150034 U; G06N 3/04; The basic element for building a neural network that can adapt / Davydenko A; G.E. Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine. –u 2021 04761, 20.08.2021 p. – Publ. 22.12.2021, vol. № 51.

Коробейніков Федір Олександрович,
ІПМЕ ім. Г.Є. Пухова НАН України,
здобувач,
fkorobeynikov@gmail.com

ЦІЛІ КІБЕРБЕЗПЕКИ ТА КІБЕРРЕЗИЛЬЄНТНОСТІ: ПОРІВНЯННЯ СПРЯМУВАНЬ

Анатація. У цій роботі через порівняння цілей кібербезпеки та кіберрезильєнтності демонструється роль взаємозв'язку обох концепцій у побудові дієвої стратегії управління ризиками організації. Незважаючи на їх спільну спрямованість, кібербезпека та кіберрезильєнтність мають різні, але взаємодоповнюючі цілі. Мета цього дослідження – висвітлити ці відмінності та пояснити, як їхня синергія, а також кожна концепція окремо, впливають на підтримання надійного та динамічного стану захищеності інформаційних систем.

Abstract. This study elucidates the interplay between the goals of cybersecurity and cyber resilience, illustrating their collective role in constructing an effective organisational risk management strategy. Despite their shared objectives, cybersecurity and cyber resilience exhibit distinct yet complementary aims. The purpose of this research is to illuminate these differences and expound upon how their synergy, as well as each concept independently, contributes to maintaining a robust and dynamic posture of information systems protection.

Вступ.

В наш час потреба у створенні резильентних систем стає дедалі актуальнішою. У зв'язку з постійно змінним ландшафтом загроз, посиленням політичної, соціальної та кліматичної нестабільності, тотальною глобалізацією цифрових мереж і зростаючою залежністю більшої частини жителів нашої планети від технологій при отриманні основних послуг, стандартні стратегії кібербезпеки вже не можуть забезпечити гарантоздатність систем.

Приймаючи той факт, що сучасний рівень технологій передбачає принципову неможливість існуючих стратегій кібербезпеки гарантувати повну захищеність інформаційних активів, було створено і впроваджено кіберрезильєнтність, як новий підхід до забезпечення гарантованого функціонування інформаційних систем, шляхом створення адаптивних механізмів, що поглинають наслідки руйнівних інцидентів, атак, або внутрішніх збоїв і підтримують роботоспроможність критичних процесів місій або організацій.

Кібербезпека: парадигма фортифікації.

Кібербезпека насамперед спрямована на запобігання несанкціонованому доступу, використанню, розголошенню, порушенню, модифікації або знищенню інформації. Вона охоплює низку процесів і структур, призначених для захисту мереж, пристроїв, програм і даних від атак, пошкодження або несанкціонованого доступу.

Найбільш значущі стандарти з кібербезпеки: NIST SP 800-160 v1 [1] та ISO/IEC 27001 [2], містять настанови щодо концепцій створення механізмів кібербезпеки, спроектованих «з акцентом на захист від втрати інформаційних активів» [3]. Основною ціллю кібербезпеки є створення та підтримка системи, що гарантує непроникність і невразливість цифрового середовища організації. Кібербезпека спрямована на виявлення та усунення вразливостей *до того*, як вони можуть бути використані, тим самим забезпечуючи конфіденційність, цілісність та доступність (CIA triad – confidentiality, integrity and availability) інформаційних активів. Її характерною рисою є планомірність і послідовність дій: «Коли організація визначає необхідність внесення змін до системи управління інформаційною безпекою, зміни повинні проводитися в плановому порядку» [2].

Але, експоненціальне зростання кількості типів і загальної кількості інформаційних активів, а отже, і вразливостей, і пов'язаних з ними ризиків, призвело до того, що концепція кібербезпеки перестала задовольняти потреби в комплексному захисті інформаційних систем, що стало причиною розвитку нової концепції – кіберрезильентності. Присвячений їй стандарт NIST SP 800-160, v.2 акцентує увагу на тому факті, що важливим кроком є: «перехід від кібербезпеки (з акцентом на захист, запобігання та підтримку функціональності) до резильєнтності (з акцентом на передбачення, відновлення й адаптацію)» [3].

Генезис кіберрезильєнтності.

Концепція кіберрезильєнтності зародилася в сфері досліджень у галузі інженерної безпеки і стала окремою дисципліною на початку 2000-х років завдяки значному внеску таких людей, як професор Ерік Холлнагель [4]. Він вважається одним з першопрохідців у цій галузі, але його робота в першу чергу зосереджена на резильєнтності в широкому, системно-орієнтованому контексті.

Застосування концепції резильєнтності до сфери інформаційної безпеки, створення того, що ми зараз називаємо «кіберрезильєнтністю», було поступовим процесом. Багато організацій, включаючи державні органи, такі як Національний інститут стандартів і технологій (NIST) і Команда комп'ютерної готовності до надзвичайних ситуацій США (US-CERT), а також структури, такі як MITRE [5], відіграли певну роль у формуванні та просуванні цієї концепції. Таким чином, розвиток і еволюція концепції кіберрезильєнтності є колективним досягненням багатьох лідерів думок, організацій і обставин.

Дихотомія між кібербезпекою та кіберрезильєнтністю.

Незважаючи на спільну спрямованість щодо протидії загрозам що стосуються інформаційних систем організації, кібербезпека та кіберрезильєнтність мають різні цілі, які відображають різні погляди на природу цифрових загроз.

На момент написання цієї роботи, основним документом, що описує парадигму кіберрезильентності та фреймворк її побудови, є стандарт NIST SP 800-160, v.2, у якому дається точне визначення цього поняття: «Кіберрезильєнтність – це здатність передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, навантажень, атак чи компрометацій систем, які використовують чи забезпечуються кіберресурсами» (Cyber

resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources).

Всі дискусії про кіберрезильєнтність зосереджені на гарантуванні виконання місії або бізнес-функцій та ґрунтуються на припущенні, що супротивник все ж таки подолає захист і встановить довготривалу присутність в системах організації [3].

Тобто, відразу чітко підкреслюється відмінність від стандартних стратегій кібербезпеки, які містять вказівки щодо систем, спроектованих з акцентом на забезпечення конфіденційності, цілісності та доступності інформаційних активів (цілі кібербезпеки). В другому томі стандарту на чільне місце стає гарантування життєздатності критичних систем, що включають кіберресурси – вбудовуючи в них елементи резильентності, пропонується забезпечити здатність передбачати атаки, витримувати їх, відновлюватись і адаптуватися до загроз (цілі кіберрезильєнтності) гарантовано виконуючи покладені на них місії, незважаючи на збої, несприятливі умови, стреси, атаки, компрометації тощо.

Кібербезпека ж за своєю суттю є привентивною – вона спрямована на захист активів організації від загроз. На відміну від неї, кіберрезильєнтність допускає можливість успішних атак і в першу чергу зосереджується на безперервності бізнесу шляхом відновлення мінімально необхідної функціональності для задоволення лише критичних потреб (допускаючи при цьому навіть втрату частини активів).

Кібербезпека часто є статичною, зосереджуючись на встановлених протоколах і засобах контролю для запобігання відомим загрозам. З іншого боку, кіберрезильєнтність є динамічною і передбачає безперервний процес адаптації і навчання, що обумовлено мінливим характером кіберзагроз.

Але, хоча кібербезпека і кіберрезильєнтність мають різні цілі, їх не слід розглядати як взаємовиключні стратегії. Навпаки, вони повинні працювати в тандемі, формуючи комплексний підхід до управління ризиками, пов’язаних з інформаційними системами.

Добре захищена організація (завдяки надійній кібербезпеці), яка може гарантовано виконувати свої основні функції і відновитися навіть після успішних атак (завдяки кіберрезильєнтності), краще орієнтується в складному ландшафті цифрових загроз. Кібербезпека та кіберрезильєнтність – це дві концепції, які доповнюють одна одну.

Крім того, з широким впровадженням і використанням систем штучного інтелекту можна зробити припущення, що захист інформаційних систем, заснований виключно на принципах кібербезпеки (без урахування кіберрезильєнтності), може виявитися неефективним. Дивлячись у майбутнє, може виникнути нагальна потреба у розробці нових концепцій захисту від гібридних атакуючих систем, особливо тих, що використовують штучний інтелект.

Слід також зазначити, що окрім кібербезпеки та кіберрезильентності, NIST у SP 800-160, v.2 представляє ще два поняття, які обумовлюють надійність

(trustworthiness) інформаційних систем: експлуатаційну стабільність і безпечність (reliability and safety), які розглядають різні аспекти надійності, і кожна з них формулює власний проблемний домен [3].

Висновки.

У роботі проведено порівняльний аналіз концепцій кібербезпеки та кіберрезильєнтності, що базується на порівнянні їхніх цілей. Визначено, що кібербезпека спрямована на запобігання атакам, у той час як кіберрезильєнтність визнає неминучість деяких порушень і зосереджується на швидкому відновленні, адаптації та гарантуванні працездатності ключових систем. Доведено, що обидві концепції є дієвими компонентами комплексної стратегії управління кіберризиками лише тоді, коли вони застосовуються разом. Майбутні дослідження мають бути зосереджені на подальших стратегіях інтеграції, щоб органічно, в рамках однієї моделі, поєднати принципи кібербезпеки та кіберрезильєнтності, а також на пошуку нових концепцій захисту інформаційних систем від гібридних загроз, що базуються на використанні систем штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST Cybersecurity Framework. URL: https://www.nist.gov/cyberframework/framework.
2. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. URL: https://www.iso.org/standard/27001.
3. NIST Special Publication 800-160, Volume 2. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. URL: https://nvlpubs.nist.gov/nistpubs/Special Publications/NIST.SP.800-160v2r1.pdf.
4. Hollnagel E., Professor. Google Scholar. URL: https://scholar.google.com/citations?user=X9XNLZMAAAAJ&hl.
5. Deborah J. Bodeau D. J., Graubart R. MITRE. Cyber Resiliency Engineering Framework. September 2011. URL: https://www.mitre.org/news-insights/publication/cyber-resiliency-engineering-framework.

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

ВИКОРИСТАННЯ ФОНОВОГО ЗОБРАЖЕННЯ МНЕМОСХЕМИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗРОБКИ ТРЕНАЖЕРНИХ ЗАВДАНЬ

Під час розробки тренажерних завдань розробник має на графічному редакторі створити схему, яка буде повторювати мнемосхему існуючої розподільчої мережі. Відстань між компонентами та їх з'єднання мають бути ідентичними тому, як вони зображені на мнемосхемі [1]. Під час розробки тренажерних завдань, розробник дивиться на мнемосхему, і тільки після цього повертається до роботи з графічним редактором. Так як, мережі можуть буди великими за кількістю компонентів на ній, розробник може витрати багато часу на перегляд мнемосхеми, а не за роботою у графічному редакторі. Також, частою є помилка, коли відстань між компонентами на графічному редакторі тренажерного заняття не відповідає відстанні між компонентами на мнемосхемі. Відповідно, розробник починає переставляти компоненти мнемосхеми, що значно збільшує час розробки тренажерного заняття [2]. Так як час розробки тренажерного заняття впливає на економічну складову компанії, яка створює тренажерне заняття, варто зменшувати час розробки тренажерного заняття. Для зменшення допустимості помилки неправильного розташування компонентів, у графічний редактор було додане фонове зображення мнемосхеми (рис. 1).

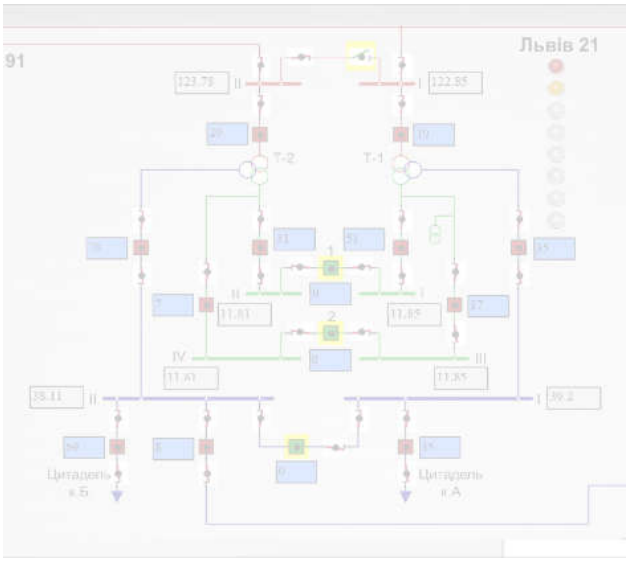

Рисунок 1 – Приклад фонового зображення мнемосхеми

Фонове зображення мнемосхеми допомагає точно розмістити компонент і врахувати відстань між компонентами у існуючій мнемосхемі. В графічному редакторі воно являє собою компонент, який як і інші компоненти присутній у

бібліотеці, але воно ніяк не впливає на модель розрахунку значень напруг і струмів. Зображення має бути освітленим, так як без зміни кольору розробник буде плутати зображення з компонентами, які він вже додав в графічний редактор (більш кольорові компоненти, це компоненти які додав розробник). Завдяки фоновому зображенню розробник має інформацію про позиції на мнемосхемі наступних компонентів: трансформатор, вивід струму і напруги, роз'єднувач, вимикач, шина вузла, гілки. Слід зазначити, що деякі структурні компоненти (вузол, стрілка струму), відсутні на мнемосхемі, і розробник має самостійно знайти місце для розташування цих компонентів. Фонова мнемосхема також може допомогти у перевірці коректності моделі розрахунку значень напруг і струмів. Якщо в тренажерне завдання задати такі самі технологічні параметри які є на фоновому зображенні, і значень у виводів напруг і струмів тренажерного завдання збігається з значеннями виводів на зображенні, відповідно модель розрахунку в тренажерному завданні працює правильно.

Додання фонового зображення мнемосхеми зменшує вірогідність помилки під час розміщення компонентів мнемосхеми, що значно знижує час розробки тренажерного заняття.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лєпатьєв А. О., Самойлов В. Д. Тренажерна підготовка персоналу та галузева комп'ютерна технологія побудови занять. *Безпека енергетики в епоху цифрової трансформації* : матеріали III науково-практичної конференції (Київ, 22 грудня 2021 р.). Київ, 2021. С. 85–89.

2. Лєпатьєв А. О. Ручна підготовка даних для моделі розрахунку режиму розподільчої мережі. *Безпека енергетики в епоху цифрової трансформації* : програма та матеріали II науково-практичної конференції (Київ, 28–29 грудня 2020 р.). Київ, 2020. С. 48–49.

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

КІБЕРБЕЗПЕКА В ЕНЕРГЕТИЦІ НА ФОНІ ШВИДКОГО РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

В останній час швидкими темпами зростає цифровізація усіх складових існування людства з постійною інтеграцією життєво важливих ресурсів у глобальні телекомунікаційні мережі. І якщо раніше вважали, що цифровізація допоможе зробити більш ефективним доступ до управління ресурсами, а особливо, енергетичних, то на сьогодні можна констатувати, що широкомасштабні кібератаки можуть паралізувати не тільки цифрові електромережі, але і матеріальні виробництва. При цьому перебої в системі електропостачання загрожують не тільки функціонуванню систем зв'язку, транспорту та закладам охорони здоров'я, але й можуть загрожувати національній безпеці країни. Досить часто функціонування систем, що забезпечують життєдіяльність соціуму, порушується із-за кібератак.

Серед кібератак найпоширенішими є програмне забезпечення, яке називають найчастіше зловмисним, оскільки воно призначене для вимкнення систем, що дозволяє зловмисникам отримати доступ до конфіденційної інформації або даних. Дані стосовно кібератак в США за 2022 рік мають наступну картину [1].

Через зловмисне програмне забезпечення було здійснено 2,8 мільярдів атак. При цьому експерти з кібербезпеки Sonicware виявили понад 270228 варіантів зловмисного програмного забезпечення, які ніколи раніше не зустрічалися. Біля 30% вторгнення зловмисного програмного забезпечення відбувається шляхом електронних листів з різними варіантами як вкладень, так і посилань. При цьому в США у березні 2022 року було виявлено найбільшу кількість нових зловмисних програм, а саме – 59259, які були зареєстровані на той момент.

Програми-вимагачі на сьогодні є однією з найбільш руйнівних кіберзагроз, яка в останні роки стає все більш поширеною. В США за перші півроку 2022 року на кожного клієнта було приблизно 638 спроб програм-вимагачів. Серед тих, хто потерпав від цих програм, було 92% тих, хто не використовував ефективні заходи запобігання втраті даних. І саме за цими програмами стоїть 30% усіх витоків інформації у 2022 році, що спричинило збитки на суму понад 49 207 908 доларів США. Сюди не включені невидимі бізнес-збитки, такі як даремно витрачений час, втрачена заробітна плата, тощо. І не зважаючи на зниження глобальних атак програм-вимагачів на 23% у 2022 році, у світі все ще було 236,1 мільйона атак.

Фішинг досить часто використовується для доступу до систем або активів організації з метою викрасти дані та отримувати доступ до інших цілей, використовуючи особисту інформацію організації. У середньому для виявлення

та локалізації пов’язаних із фішингом зломів витрачалось 295 днів. За кожні 10 днів 2022 року блокувалося більше мільярда фішингових листів, при цьому 18% фішингових листів, які були відкриті, прийшли із мобільних пристроїв. Оскільки людьми легше маніпулювати, ніж кібербезпекою, то фішингові електронні листи вважаються найризикованішою формою кібератак.

З метою порушення роботи онлайн-сервісів і, можливо, втрат даних клієнтів, використовуються атаки розподіленої відмови в обслуговуванні (DDoS), або пристроїв (Інтернет речей). Цей тип атак в США найбільш поширений в ігровій індустрії і тривалість таких атак рідко сягає півтори години.

Статистика кібербезпеки за галузями в США за 2022 рік говорить про те, що на першому місці потерпала від кібератак охорона здоров’я, потім фінансова сфера, державні органи, освіта і енергетична галузь.

Організації повинні вживати активних заходів для захисту від кібератак. Це включає розробку плану реагування на інциденти, регулярні аудити безпеки та багатоетапне навчання з кібербезпеки. Крім того, організації повинні використовувати багаторівневий підхід до безпеки, який поєднує технології, процеси та людей. Це допоможе забезпечити максимальний захист вашої організації та зменшить ризики, пов’язані з витоком даних.

Згідно з дослідженнями IBM, людська помилка є основною причиною порушень кібербезпеки і сягає 95%. Тобто, якби якимось способом вдалося прибрати людську помилку, тоді 19 із 20 кібератак не було б взагалі [2]. Основними чинниками, які впливають на людські помилки, є можливості, середовище та недостатня обізнаність.

Ефективна стратегія кібербезпеки в енергетичній галузі вимагає скоординованого підходу, в якому мають бути задіяні співробітники, процеси та технології організацій. Ефективна програма кібербезпеки включає навчання співробітників передовим методам забезпечення безпеки та застосування автоматизованих технологій кіберзахисту в існуючих IT-інфраструктурах. Ці елементи працюють разом для створення декількох рівнів захисту від потенційних загроз у всіх точках доступу до даних. Вони виявляють ризики, захищають посвідчення, інфраструктуру та дані, виявляють аномалії та події, реагують на першопричини та аналізують їх, а також допомагають відновитись після подій.

Стрімкий розвиток штучного інтелекту привносить в сучасний світ свої переваги так і ризики, коли мова йде про кібербезпеку об’єктів, особливо енергетичних. Інтелектуалізація та кібербезпека є двома взаємопов’язаними концепціями у сучасному світі. Інтелектуалізація, що включає штучний інтелект, машинне навчання, тощо, призначена для автоматизації та оптимізації багатьох процесів і підвищення їх ефективності. Однак, зі збільшенням кількості та складності технологій, ступінь уразливості систем промислової автоматизації та загрози кібератак збільшуються. Недостатня кібербезпека може призвести до витоків даних, порушення конфіденційності та цілісності інформації, а також до відмов у роботі систем та потенційної загрози життю та здоров’ю людей, які використовують ці системи.

У зв’язку з цим кібербезпека стає одним з основних питань при впровадженні технологій інтелектуалізації. Правильне планування та реалізація заходів щодо забезпечення кібербезпеки стали важливим елементом при розробці та експлуатації інтелектуальних систем [3]. І, коли мова йде про кібербезпеку, то впершу чергу потрібно розробити комплекс заходів щодо захисту від зовнішніх і внутрішніх загроз, таких як хакерські атаки, віруси, шпигунство, та інші види активності, які можуть завдати шкоди автоматичним системам. Кібербезпека в енергетичному секторі є критичним аспектом з огляду на значущість наслідків в разі кібератак. Штучний інтелект (ШІ), будучи однією з новітніх технологій, також може впливати на кібербезпеку в енергетичному секторі, що пов’язано з кібератаками на інформаційну інфраструктуру електростанцій, мереж енергопостачання, системи автоматизованого керування та моніторингу. Це може призвести до серйозних наслідків, включаючи випадання сервісів, втрату даних та можливе порушення безпеки та життєзабезпечення.

ШІ, з одного боку, може допомогти виявляти і пом’якшувати кіберзагрози за допомогою аналізу даних, що відповідають різним категоріям поведінки атак, а також автоматичні цілочисленні рішення щодо відновлення роботи систем, якщо сталося переривання. З іншого боку, ШІ може також стати об’єктом кібератак, що може створити нові проблеми в роботі енергетичних мереж. Отже, в енергетичному секторі необхідно вдосконалювати цілісність та безпеку інформаційних систем та переконуватися, що вони захищені від потенційних кібератак. Крім того, використання новітніх технологій, таких як ШІ, має ґрунтуватися на прозорих протоколах безпеки та належної забезпеченості інфраструктури систем, щоб зберігати переваги цих технологій і уникати можливих загроз.

Створення інтелектуальних систем таких як ChatGPT теж можуть бути потенційною метою кібератак, тому кібербезпека є одним із важливих аспектів розробки та експлуатації таких систем. Компанія OpenAI, розробник ChatGPT, стверджує, що забезпечує кібербезпеку шляхом використання різних технологій, таких як шифрування, протоколи безпеки та інші заходи безпеки, які запобігають несанкціонованому доступу до інтелектуальних моделей та інформації, що обробляється цими моделями.

У той же час, працівники з Home Security Heroes наводять статистику, як швидко ШІ зламує паролі, а саме: 51% паролів були зламані менш ніж за хвилину; 65% – менше ніж за годину; 71% – менш ніж за добу; 81% – менш ніж за місяць. Ця статистика говорить про те, що для створення надійного паролю потрібно створити нейромережу.

Глобальне дослідження трьох університетів (Стенфорда та національних університетів Сінгапура та Гонконгу) довело, що ШІ здатний читати думки людей, аналізуючи мозкову активність і на основі цих даних нейромережа генерувала зображення з точністю до 84%, аж до текстури та кольорів. Дослідники дійшли висновку у тому, що сканування мозку дає достатньо інформації, щоб машина отримувала точне уявлення, що думає людина.

Людство стоїть на порозі серйозних загроз, які може становити штучний інтелект. І навіть заклики тисяч експертів, в тому числі Маска, про призупинку навчання нейромереж, що перевершують GPT-4, як мінімум на півроку, навряд чи допоможе, оскільки така пауза не може бути прийнята швидко, оскільки вона вимагає впершу чергу, об’єднання зусиль урядів всіх країн.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kizzee K. Cyber Attack Statistics to Know in 2023. URL: https://parachute.cloud/cyber-attack-statistics-data-and-trends/.
2. Ahola M. The Role of Human Error in Successful Cyber Security Breaches. URL: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches.
3. On scientific understanding with artificial intelligence / M. Krenn at al. URL: https://www.nature.com/articles/s42254-022-00518-3.

Olena Ogir,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Research officer,
lenaogir@gmail.com

Oksana Tsurkan,
G.E. Pukhov Institute for Modelling in Energy Engineering of NASU,
Junior researcher,
otsurkan24@gmail.com

REVOLUTIONIZING ENERGY SECURITY WITH ELECTRON PROJECT TECHNOLOGIES

The electricity grid is one of the most complex systems ever built. It is an interconnected network of power plants, transformers, transmission lines, and distribution networks. The electricity grid is vital for the functioning of modern society, as it powers everything from homes and businesses to hospitals and critical infrastructure. However, it is also vulnerable to cyber threats, such as cyberattacks, data breaches, and other malicious activities. These threats can cause outages, disrupt operations, and undermine the stability of the grid. Despite the importance of the electricity grid, it is also a significantly vulnerable system due to its complexity, age, and interconnectivity. In recent years, there has been a growing concern about the potential for cyberattacks targeting the electricity grid. These threats can range from simple phishing emails to sophisticated attacks that result in widespread power outages, disrupt operations, and cause significant economic and social disruptions.

A cyberattack on the electricity grid can take many forms, including the installation of malware, ransomware, and other malicious software targeting critical control and monitoring systems. These attacks can potentially cause safety issues by disrupting the operation of protective devices that prevent overloading and short-circuiting of the grid's components. Furthermore, attackers can manipulate the grid's data to mislead operators and engineers, causing further damage to the grid [1]. Therefore, government agencies, regulators, and electricity utilities are taking steps to secure the grid against cyber threats. They are investing in advanced technologies, such as Intrusion Detection Systems (IDS), cyber threat intelligence tools, and smart grids, that can detect and respond to potential cyber threats more effectively. In addition, they are developing security policies, procedures, and guidelines aimed at protecting the grid's critical infrastructure from cyber threats. Despite the advances in technology and security measures, the electricity grid remains vulnerable to cyber threats. Therefore, continued investments in robust infrastructure and cybersecurity measures are essential to maintain the reliability and stability of this vital system.

The Electron project is a research initiative that aims to address these issues by delivering a new-generation Electric Power and Energy System (EPES) platform. The project is funded by the EU H2020 SU-DS04-2018-2020 program, and it brings together leading researchers and experts from different countries and disciplines. The new-generation Electric Power and Energy System (EPES) platform is an advanced

software platform that integrates cutting-edge technologies to enhance the efficiency, reliability, and sustainability of energy systems. It provides a comprehensive suite of tools and services for monitoring, controlling, and optimizing energy systems, and enables real-time data analytics and predictive modeling to support decision-making.

The EPES platform leverages a wide range of technologies, including machine learning, artificial intelligence, Internet of things (IoT) devices, blockchain, and cloud computing, to provide an integrated solution that addresses the complex challenges facing modern energy systems. It enables utilities and energy providers to streamline their operations and reduce costs, while ensuring reliable and resilient energy supply to customers. One of the key features of the EPES platform is its ability to integrate energy storage systems, renewable energy sources, and demand response programs into the grid, enabling dynamic management of energy supply and demand. This helps to reduce peak demand and optimize energy usage, as well as improve the efficiency of the grid [2].

The EPES platform also offers advanced analytics capabilities, including data visualization and real-time performance monitoring, which enable utilities and energy providers to identify and address inefficiencies, and optimize their operations to reduce costs and improve customer service.

Generally, the new-generation Electric Power and Energy System (EPES) platform represents a major step forward in the development of sustainable, efficient, and resilient energy systems that can meet the needs of today's society.

The main objective of the Electron project is to develop a resilient and secure EPES that can withstand cyber, privacy, and data attacks. The project seeks to achieve this goal by developing innovative solutions and technologies that combine advanced cybersecurity, data analytics, and artificial intelligence (AI) capabilities. Another innovation of the Electron project is the development of a secure and privacy-aware communication infrastructure [3]. The EPES platform will use advanced cryptographic protocols, such as blockchain and homomorphic encryption, to protect the confidentiality, integrity, and authenticity of data exchanged between different EPES components. The platform will also use privacy-preserving techniques to ensure that sensitive information, such as personal and financial data, is not leaked or misused.

The Electron project also aims to enhance the resilience of EPES against natural disasters, physical attacks, and other external threats. The project will develop innovative sensors, monitoring systems, and control algorithms that can detect and mitigate the impact of these events on the EPES infrastructure. The project will also develop advanced simulation and modeling tools that can help engineers and operators to design and test EPES architectures and scenarios under different conditions.

In conclusion, the Electron project represents a significant milestone in the field of EPES and cybersecurity. The project aims to deliver an innovative and resilient EPES platform that can empower the energy system’s resilience against cyber, privacy, and data attacks. It is a collaborative and interdisciplinary effort that involves experts from different domains and regions. The project’s results will benefit not only the energy sector but also other critical infrastructure sectors that rely

on electricity, such as transportation, healthcare, and telecommunications. The Electron project is an excellent example of how research and innovation can contribute to improving the resilience and security of critical infrastructures.

REFERENCES

1. Middleton B. A History of Cyber Security Attacks: 1980 to Present. New York : Auerbach Publications, 2017. 253 p. DOI: https://doi.org/10.1201/9781315155852

2. Towards Enabling Secure and Real-time Exchange of CTI data for EPES Infrastructures. URL: https://electron-project.eu/blog/towards-enabling-secure-and-real-time-exchange-of-cti-data-for-epes-infrastructures/.

3. ELECTRON architecture. URL: https://electron-project.eu/blog/electron-architecture/.

Сушко Сергій Володимирович,
ІПМЕ ім. Г.Є. Пухова НАН України,
молодший науковий співробітник, к.т.н.,
sergii.sushko@gmail.com

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

ОПТИМІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ЗНИЖЕННЯ ЕНЕРГОСПОЖИВАННЯ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

Анотація. Оптимізація програмного забезпечення тривалий час використовувалась як засіб покращення заздалегідь визначених параметрів програмного забезпечення. Найчастіше параметром оптимізації були час виконання програмного забезпечення та пам'ять програм. Проте також оптимізація може бути корисною в контексті енергоспоживання апаратно-програмного комплексу, на якому виконується оптимізована програма. Через зниження кількості арифметичних операцій, операцій вводу-виводу та зниження використання зовнішньої пам'яті знижується водночас кількість і частота перемикання транзисторів процесору, контролера пам'яті та власне пам'яті. Отже, оптимізація деяких прикладних параметрів комп'ютерних програм може впливати на енергоспоживання та енергоефективність обчислень.

Розглядаючи кібербезпеку енергетики як сукупність безпеки її складових частин, постає вимога безпеки до програмного забезпечення, що є частиною енергетики. Головні вимоги до програмних засобів в енергетиці є надійність та функціонування у повній відповідності до технічних вимог. Також достатньо часто ставиться вимога гарантованого виконання обчислень в заздалегідь визначений час. Саме в цьому і є зиск від використання оптимізованого програмного забезпечення, що дозволяє виконувати вимоги з мінімальним використанням наявних ресурсів.

Зважаючи на різноманіття існуючих методів та засобів оптимізації програмного забезпечення, виникає практичне питання які саме методи оптимізації та їх параметри потрібно використовувати в кожному конкретному випадку. Загалом існують десятки основних методів оптимізації та сотні варіацій [1]. Також суттєвою проблемою є те, що частина оптимізаційних методів приховується від користувача. Так, більшість компіляторів мають багато налаштувань оптимізації, проте безпосередньо логіка роботи оптимізаційних методів не викладена.

Для формалізації та зручності роботи з підходами до оптимізації було створено декілька математичних моделей. Наприклад, у [2] описується

поліедральна модель, що перетворює тіло обчислювальних циклів на набір множин, нерівностей та кортежів. Така модель повністю абстрактно описує тіло циклу математичною мовою, а також дозволяє його змінювати через зміну математичного відображення. Також з'явились програмні засоби, наприклад Pluto [3], що в автоматичному режимі можуть виконувати деякі з оптимізаційних методів в автоматичному режимі, перетворюючи вихідний код в інший вихідний код.

У [4] та [5] автори використовують зазначений пакет Pluto для оцінки прискорення виконання тестових програм та зміни енергоспоживання при цьому. Використовуючи запропоновану оцінку енергоефективності, автори доводять, що використання розпаралелювання комп'ютерних програм в більшості випадків покращує енергоефективність обчислень, тобто для отримання того ж самого результату обчислень потрібно використати менше електричної енергії. Також авторами наводяться результати оптимізації методом розбиття на блоки. Цей метод також загалом позитивно впливає на енергоефективність обчислень. Також варто відзначити, що одночасне використання розпаралелювання та розбиття на блоки ефективно доповнює один одного.

Як висновок можна зазначити, що використання ефективних методів оптимізації окрім безпосередньо заданих цілей сприяє покращенню енергоефективності обчислень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Aho A., Lam M., Sethi R., Ullman J. Compilers, principles, techniques, and tools. Pearson Education, Inc., 2007. 1010 p.
2. Feautrier P., Lengauer C. The polyhedron model. *Encyclopedia of Parallel Computing*. Berlin : Springer, 2011. P. 1581–1592.
3. Bondhugula U. Effective Automatic Parallelization and Locality Optimization Using The Polyhedral model. The Ohio State University, 2010. 193 p.
4. Чемерис А. А., Сушко С. В. Исследование быстродействия и энергопотребления при автоматической оптимизации методами разбиения на блоки и распараллеливания для вычислений на платформе x64. *Моделювання та інформаційні технології*. 2017. № 80. С. 52–60.
5. Chemeris A., Lazorenko D., Sushko S. Influence of Software Optimization on Energy Consumption of Embedded Systems. *Green IT Engineering: Components, Networks and Systems Implementation*. Springer, 2017. P. 111–133.

Симонов Артем Андрійович
Державне підприємство «Державний науково-технічний центр з ядерної та радіаційної безпеки»,
начальник лабораторії,
aa_simonov@sstc.ua

КІБЕРЗАХИСТ ІНФОРМАЦІЙНИХ І КЕРУЮЧИХ СИСТЕМ АТОМНИХ ЕЛЕКТРОСТАНЦІЙ

Анотація. Забезпечення кіберзахисту інформаційних і керуючих систем атомних електростанцій є наразі критично важливою проблемою для України, з точки зору, як забезпечення ядерної та радіаційної безпеки, так і підтримання стабільності роботи об’єднаної енергетичної системи України. Першим етапом побудови дієвої структури забезпечення кіберзахисту, яка би враховувала світовий досвід, стала розробка та впровадження нормативного документа НП 306.2.237-2022 «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки».

Annotation. Cybersecurity assurance of instrumentation and control systems of nuclear power plants is currently a critically important issuefor Ukraine, both in terms of nuclear and radiation safety and keeping the stability of the unified energy system of Ukraine. The first step for establishing of the effective cybersecurity structure that takes into account international experience, was the development and implementation of theregulatory document NP 306.2.237-2022 «Requirements for cybersecurity of instrumentation and control systems of nuclear plants forassurance nuclear and radiation safety».

Проблема забезпечення кіберзахисту ядерних установок (ЯУ), зокрема атомних електростанцій (АЕС), стає все більш актуальною, оскільки регулярні атаки на об’єкти енергетичної інфраструктури України потребують впровадження відповідних заходів захистудля зниження вразливості ядерних об'єктів, зокрема, з погляду кіберзахисту.

Існує поширена думка про те, що АЕС «закриті» або повністю ізольовані від загальнодоступної мережі Інтернет і що це захищає їх від будь-яких кібератак. Безперечно фізична ізоляція мереж є необхідним та дієвим заходом захисту від кібератак. Треба завжди намагатись забезпечувати таку ізоляцію, але водночас необхідно впевнитися у реальній відсутності будь-яких шляхів доступу до ІКС АЕС із публічних мереж передачі даних, а також потрібно зважати на те, що фізичну ізоляцію мережі можна долати, наприклад, за допомогою портативних носіїв даних (як у випадку зі Stuxnet [1]), бездротового підключення до локальних мереж, безпосередніх дій інсайдерів, внесення програмних закладок на етапі розробки тощо.

Першим етапом забезпечення кіберзахисту є створення відповідної національної нормативної бази. Наразі в Україні ведеться масштабна робота з розвитку національної законодавчої та нормативної бази з кібербезпеки, зокрема введені в дію Закон України «Про основні засади забезпечення

кібербезпеки України» [2], постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [3] та рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» [4]. Зазначені документи встановлюють загальні вимоги до забезпечення кіберзахисту критичної інфраструктури України та передбачають гармонізацію і розвиток нормативної бази з урахуванням рекомендацій міжнародних стандартів і галузевої специфіки для врахування особливостей тааспектів роботи конкретних об'єктів, таких як АЕС.

Згідно з [2–4], для врахування галузевої специфіки та гармонізації з міжнародними стандартами і документами, у 2022 році в Україні введено в дію документ НП 306.2.237-2022 «Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» [5]. Під час розробки НП 306.2.237-2022 [5] були враховані рекомендації стандартів і документів міжнародних організацій, як-то Міжнародного агентства з атомної енергії (зокрема NSS No. 17-T [6], NSSNo.42-G [7], NSSNo.33-T [8]) та Міжнародної електротехнічної комісії (зокрема IEC 62645:2019 [9], IEC 62859:2016+AMD1:2019 CSV [10]), а також Комісії ядерного регулювання США (зокрема RG1.152 [11], RG 5.71 [12]).

НП 306.2.237-2022 [5] встановлює вимоги до кіберзахисту інформаційних і керуючих систем (ІКС) АЕС, їх компонентів і програмного забезпечення (ПЗ) зазначених систем, під час їх розроблення, впровадження, експлуатації та модифікації, з метою забезпечення ядерної та радіаційної безпеки, та регламентує:

1) вимоги до класифікації ІКС АЕС, їх компонентів і ПЗ, стосовно кіберзахисту, а саме встановлює критерії визначення рівнів кіберзахисту;

2) загальні принципи забезпечення кіберзахисту, такі як:

- політика кіберзахисту;
- глибокоешелонований кіберзахист;
- диференційований підхід до забезпечення кіберзахисту;
- загальні вимоги до забезпечення кіберзахисту;
- культура кіберзахисту;
- координація між кіберзахистом та функціями ІКС АЕС;

3) оцінювання та переоцінювання кіберзахисту ІКС АЕС і застосування ризик-інформованого підходу до оцінювання кіберзахисту діючих ІКС АЕС;

4) забезпечення кіберзахисту на усіх етапах життєвого циклу ІКС, їх компонентів та ПЗ, а саме на етапах:

- розроблення;
- впровадження;
- експлуатації;

5) вимоги до документів, що обґрунтовують кіберзахист (зокрема, до програм та планів кіберзахисту, документації розробників щодо кіберзахисту, плану реагування на кіберінциденти).

Впровадження НП 306.2.237-2022 [5] та реалізація його вимог направлена на підвищення кіберзахисту ІКС АЕС та побудову єдиної структури забезпечення кіберзахисту ІКС на АЕС України. Також впровадження

НП 306.2.237-2022 [5] сприяє подальшому розвитку нормативної та методичної бази, у якій будуть міститися більш детальні практичні методи забезпечення кіберзахисту ІКС АЕС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Falliere N., O'Murchu L., Chien E. W.32 Stuxnet Dossier. Version 1.4. Symantec Security Response. February 2011.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. С. 403.
3. Загальні вимоги 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,
4. Рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
5. НП 306.2.237-2022. Вимоги до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки : наказ Державної інспекції ядерного регулювання України від 22.03.2022 № 223. URL: https://zakon.rada.gov.ua/laws/show/z0395-22#Text.
6. Computer security techniques for nuclear facilities. IAEA nuclear security series No. 17-T (Rev. 1). Vienna : International Atomic Energy Agency, 2021. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf.
7. Computer security for nuclear security. IAEA nuclear security series No. 42-G. Vienna : International Atomic Energy Agency, 2021. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.
8. Computer security of instrumentation and control systemsat nuclear facilities: technical guidance. IAEA nuclear security series No. 33-T. Vienna : International Atomic Energy Agency, 2018. URL: https://www-pub.iaea.org/MTCD/ Publications/PDF/P1787_web.pdf.
9. IEC 62645:2019. Nuclear power plants. Instrumentation, control and electrical power systems. Cybersecurity requirements. URL: https://webstore.iec.ch/ publication/32904.
10. IEC 62859:2016+AMD1:2019 CSV. Nuclear power plants. Instrumentation and controlsystems. Requirements for coordinating safety and cybersecurity. URL: https://webstore.iec.ch/publication/64275.
11. Criteria for use of computer sinsafety systems of nuclear power plants. Regulatory guide1.152 Revision 3. Washington, DC : U.S. Nuclear Regulatory Commission, 2011. URL: https://www.nrc.gov/docs/ML1028/ML102870022.pdf.
12. Cybersecurity programs for nuclear facilities. Regulatory guide 5.71. Washington, DC : U.S. Nuclear Regulatory Commission, 2010. URL: https://www.nrc.gov/docs/ML0903/ML090340159.pdf.

Удовенко Владислав Віталійович,
Європейський університет,
аспірант,
vudovenko@e-u.edu.ua

КІБЕРЗЛОЧИНИ: ЗАГРОЗА ДЛЯ ВСІХ І КОЖНОГО

Розслідування кримінальних правопорушень, що вчиняються в сфері комп'ютерної інформації, є досить актуальною в сучасному світі. З поширенням комп'ютерів та Інтернету кіберзлочинність стала однією з найбільш поширених форм злочинної діяльності.

Масштаб загроз інформаційному простору не обмежується кордонами однієї держави, оскільки сучасні глобальні комп'ютерні мережі охоплюють переважну більшість країн світу, що додатково сприяє різкому підвищенню кримінального комп'ютерного професіоналізму та високої мобільності злочинців. Тому своєчасним є дослідження та аналіз системи швидкозмінних високотехнологічних кібернетичних загроз, тактики взаємодії у сфері інформаційної безпеки, яка впливає на формування сталого розвитку суспільства, на функціонування механізмів протидії інформаційним загрозам з урахуванням сучасних реалій [1, с. 401].

Питання боротьби із кіберзлочинністю розглядали такі видатні вчені, як Дж. Арас, Г.П. Власова, О.Є. Користін, М.Ю. Літвінов, Р.В. Лук'янчук, В.В. Марков, М.А. Ожеван, Ю.М. Онищенко, О.В. Орлов, П.І. Пушкаренко, К.М. Рудой, Є.Д. Скулиш, В.Г. Хахановськийта інші. Слід зазначити, що більшість науковців досліджували проблему правового регулювання боротьби із кіберзлочинністю в різних аспектах. Отже, проблема боротьби з кіберзлочинністю стала настільки важливою, що її розглядають як науково-практичну і науково-методичну проблему.

Тривалий час ця сфера практично не була врегульована міжнародним правом, але нині вироблено низку норм, що мають за мету боротьбу з високотехнологічною злочинністю. Однак, наявне міжнародно-правове поле не достатньо ефективне, оскільки відсутня навіть єдність та одноманітність правового регулювання зазначеної сфери [2].

За останні роки кіберзлочинність стала значною загрозою для безпеки як держав, так і громадян, оскільки сучасне суспільство не може уявити свого життя без інтернету, комп'ютерів, смартфонів та інших технологічних пристроїв. Водночас швидкий розвиток технологій і залежність від цифрових систем створюють нові можливості для злочинців, які використовують цифрове середовище для вчинення злочинних дій.

Кіберзлочини мають широкий спектр прояву, від крадіжок даних та викрадення грошей до кібершпигунства та кібертероризму. Поряд з виникненням нових видів злочинів у сфері інформаційних технологій, практично будь-які злочини, такі як привласнення, крадіжка, шахрайства, злочини в банківській сфері, комп'ютерне шпигунство, комп'ютерні диверсії (у тому числі руйнування операційних систем, сповіщень та використання

комп'ютерних вірусів), комп'ютерний тероризм, крадіжку комп'ютерних послуг (зокрема, обчислювальних ресурсів), махінації та маніпулювання системою обробки даних, а також крадіжка фінансових засобів і підробка документів, порушення приватної або державної таємниці, протиправне копіювання програмних продуктів, яке порушує авторське та інші права [3, с. 59].

Кіберзлочинність – це вчинення злочину, що пов'язано з використанням комп'ютерних технологій, мереж Інтернет та інших електронних пристроїв.

Кіберзлочинність може мати різні форми прояву: від крадіжки конфіденційної інформації до кібертероризму та кібершантажу.

Відповідно до Конвенції про кіберзлочинність прийнято поділяти кіберзлочини на наступні види:

– правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до систем; нелегальне перехоплення інформації; втручання у дані та системи; виготовлення, розповсюдження та збут шкідливого програмного забезпечення та спеціальних пристроїв);

– правопорушення, пов'язані з комп'ютерами (комп'ютерне підроблення та комп'ютерне шахрайство);

– правопорушення, пов'язані зі змістом (вироблення, володіння, розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем);

– правопорушення, пов'язані з порушенням авторських та суміжних прав [4].

Водночас, кіберзлочини в залежності від наслідків та масштабу, можна поділити на дві категорії:

– кіберзлочини публічної дії, спрямовані на ураження комп'ютерних та інформаційно-комунікаційних систем державних органів, міжнародних організацій, великих підприємств, державних реєстрів, об'єктів критичної інфраструктури та інших;

– кіберзлочини індивідуальної дії, спрямовані на заволодіння майном або інформацією певної особи, групи осіб або підприємства [5].

На наш погляд, залежно від характеру вчиненого злочину, можна виділити такі види кіберзлочинів:

– крадіжка даних;
– шахрайство в Інтернеті;
– кібербулінг;
– кібертероризм;
– кібершантаж;
– хакерство та комп'ютерний злом.

У багатьох країнах світу були створені спеціальні органи, які займаються розслідуванням кіберзлочинів. В Україні цим займається Департамент кіберполіції ГУНП, що бере на себе функції з розслідування, запобігання та виявлення кіберзлочинів.

Кіберзлочинність є серйозною проблемою сучасного світу, що призводить до значних збитків для окремих осіб, компаній та держав. Важливо розуміти основні види кіберзлочинності та її наслідки для ефективної боротьби з нею.

Для зменшення кількості кіберзлочинів необхідно проводити постійну роботу з просвітницької та попереджувальної роботи, застосовувати сучасні методи боротьби з кіберзлочинністю використовувати різноманітні заходи, які включають в себе законодавчі акти, програми та ініціативи.

Отже, розслідування кіберзлочинів є важливою проблемою, яка вимагає використання спеціалізованих знань і навичок, оскільки вони часто включають складні технологічні аспекти та використання анонімних мереж та інструментів. Помилки, допущені при цьому слідчими і дізнавачами, здебільшого є наслідком їх незадовільної професійної підготовки саме для цього сегменту їх криміналістичної діяльності [6, с. 15].

Нині існує значна кількість програм та ініціатив, які мають на меті запобігання кібератакам та забезпечення кібербезпеки. Однак, важливо пам’ятати, що кіберзлочинність постійно зростає. Зокрема, з огляду статистичних даних Генеральної прокуратури України випливає, що станом на 31 грудня 2022 року у сфері інформаційних технологій обліковано 3 415 кримінальних правопорушень, в 2021 році їх було 3 310, а в 2020 році – 2298 [7]. Тому необхідно продовжувати розвивати та підтримувати високий рівень компетенції у галузі кібербезпеки. Також необхідно забезпечувати належний рівень фінансування органів, які займаються боротьбою з кіберзлочинністю.

Враховуючи це, можна стверджувати, що дослідження кіберзлочинності та розслідування її випадків є надзвичайно важливою справою в нашому сучасному світі, де кіберзлочинність стала однією з найбільш поширених форм злочинної діяльності. Подальше дослідження цієї проблеми та вдосконалення методів боротьби з кіберзлочинністю є важливим завданням для науковців, правоохоронних органів та спеціалістів у галузі кібербезпеки.

Висновок, який можна зробити, що в боротьбі з кіберзлочинністю важливо розвивати та підтримувати високий рівень компетенції у галузі кібербезпеки, а також забезпечувати належний рівень фінансування органів, які займаються боротьбою з цим явищем. Тільки таким чином можна ефективно захистити суспільство від кіберзлочинності та забезпечити безпеку в Інтернеті.

Отже, дослідження проблеми кіберзлочинності та розслідування її випадків є важливим кроком у забезпеченні кібербезпеки та боротьбі з кіберзлочинністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Харитоненко І. О. Феномен кіберзлочинності в сучасній кримінологічній теорії. *Часопис Київського університету права*. 2020. № 4. С.401–404.

2. Яцишин М. Ю. Проблеми уніфікації поняття кіберзлочинність у міжнародному праві URL: https://elib.institutemvd.by/bitstream/MVD_NAM/4631/1/Aleksey%20Ulyanov.pdf.

3. Ботвінкін О. В. Проблеми забезпечення національної безпеки в інформаційній сфері. *Юридичний журнал*. 2007. № 2. С. 59–60.

4. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

5. Кривенко К. Кіберзлочинність: актуальна судова практика. URL: https://biz.ligazakon.net/analitycs/209283_kberzlochinnst-aktualna-sudova-praktika.

6. Бегма А. П., Ховпун О. С. Розслідування злочинів в ІТ-сфері. *Наукові праці Національного університету «Одеська юридична академія»*. Т. 28. 2021. С. 12–19.

7. Офіційний сайт Офісу Генерального прокурора. URL: https://new.gp.gov.ua/ua/posts/statistika.

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

Хоменко Олексій Антонович,
Інститут телекомунікацій і глобального інформаційного простору
НАН України,
аспірант,
oleksii.khomenko@icu-ng.org

СТАТИСТИЧНИЙ ПІДХІД ДЛЯ ОБРОБКИ ДАНИХ ТА ФОРМУВАННЯ ІНДЕКСІВ ПРО КІБЕРІНЦИДЕНТИ, КІБЕРАТАКИ, КІБЕРЗАГРОЗИ ТА ЗАХОДИ ПРОТИДІЇ

Завданням Стратегії кібербезпеки України [1] С. 3-19 передбачено розроблення методики збору кіберстатистики та щорічне оприлюднення статистичної інформації щодо кібератак, кіберінцидентів та заходів протидії за сферами відповідальності основних суб'єктів національної системи кібербезпеки на їх офіційних сайтах. Завданням Плану реалізації цієї стратегії [2] передбачено розроблення та затвердження методики збору кіберстатистики нормативно-правовим актом Адміністрації Державної служби спеціального зв'язку та захисту інформації України, а такою збирання та оприлюднення у відповідності до розробленої методики відповідних статистичних даних.

Станом на 01.05.2023 р. термін «кіберстатистика» є предметом гострих дискусій з нормативної та наукової точки зору. Ряд досліджень, зокрема [3], до кіберстатистики відносять:

- тенденції кібербезпеки;
- найбільші витоки даних і статистика зламів;
- статистика кіберзлочинності за типом атак;
- статистика відповідності та управління кібербезпекою;
- галузева кіберстатистика;
- статистика витрат на кібербезпеку;
- статистика зайнятості в сфері кібербезпеки;
- популярні загрози та тенденції загроз;
- вартість кіберзлочинності;
- моделі та засоби захисту;
- поширені типи кібератак;
- щоденна та щорічна кількість атак, частота атак;

У теорії статистики [4] під статистикою розуміють:

– кількісні дані, які характеризують визначену сторону суспільного життя;

– практичну діяльність державних установ, спрямовану на збір, обробку і аналіз даних про масові явища та процеси суспільного життя;

– науку, яка розробляє і впроваджує принципи і методи дослідження кількісних характеристик масових суспільних явищ.

Предметом статистичного вивчення (дослідження) є розміри і кількісні співвідношення масових суспільних явищ та закономірностей їх формування і розвитку в конкретних умовах простору та часу. Статистичні дослідження здійснюються за допомогою методів масового статистичного спостереження, статистичного зведення і групування, узагальнених статистичних показників, а також їх аналізу, викладення та інтерпретації.

До показників (індикаторів, параметрів, характеристик) масових суспільних явищ можуть буди віднесені, з певними обумовленнями, показники метаданих, індикатори безпеки, компрометації, загроз, заходи з протидії шкідливому впливу інші показники, пов’язані з даними технічного характеру.

Основні узагальнюючі статистичні показники:

– середні величини;
– відносні величини;
– показники варіації;
– показники динаміки;
– статистичні індекси;
– рейтинги.

Індекси дозволяють вивчати і аналізувати кількісні зміни і зіставлення складних сукупностей, що складаються з різнорідних та непіддатних підсумовуванню елементів.

Статистичний індекс (лат. index – узагальнюючий показник):

– спеціально сформований узагальнюючий статистичний показник, призначений для зіставлення (порівняння) незіставних явищ;

– відносна величина, яка характеризує зміну (співвідношення) складних явищ у часі, просторі або/також у порівнянні з планом, нормою чи стандартом.

Статистико-економічний індекс – статистичний індекс, призначений для дослідження та аналізу соціально-економічних та фінансово-економічних явищ. Основною мірою зіставлення незіставних економічних показників виступає ціна одиниці продукції (грошова міра споживчої вартості одиниці продукції).

Рейтинг – статистичний індекс, який зіставляє об’єкт індексування (рейтингування) з порядковим номером (натуральним числом) у переліку (списку). Часова та просторова залежність рейтингу визначається, як правило, описово.

Основні завдання статистичного індексування:

– визначення середніх змін складних, різнорідних або несумірних сукупностей у часі та у просторі;

– встановлення середніх характеристик (показників, індикаторів) складних явищ у часі та у просторі;

– визначення ролі окремих факторів (параметрів) в загальній зміні складних явищ у часі та у просторі;

– оцінювання ступеню (середнього ступеню) досягнення (виконання) планових (нормативних) показників по сукупності або по її частині.

Основні види статистичних індексів:

– індивідуальні (характеризують зміну одного елемента або однорідної сукупності);

– загальні (зведені) (характеризують зміну складного явища в цілому);

– групові індекси (субіндекси) (різновид загальних індексів, який вибірково охоплює групу елементів сукупності за спорідненими показниками);

– агрегатні (характеризують динаміку складного явища та дозволяють агрегувати (підсумовувати) і порівнювати елементи сукупності, які мають різні одиниці вимірювання за допомогою співвимірників (ваг)).

Основою підготовки даних в рамках статистичного підходу є визначення базисних параметрів, призначених для зіставлення незіставних статистичних показників. Базисні параметри статистичної сукупності формують систему базисних параметрів та є системоутворюючими для такої системи. Формування системи базисних параметрів вважається основним завданням системного аналізу статистичних систем.

Запропонована модель статистичної системи індексів про кіберінциденти, кібератаки, кіберзагрози та заходи протидії, базисними параметрами якої є:

– індикатори кіберінцидентів;

– індикатори кібератак;

– індикатори кіберзагроз;

– заходи кіберзахисту.

Набір базисних параметрів сформовано з урахуванням положень нормативних документів:

– Національна система оцінки кіберінцидентів CISA / CISA National Cyber Incident Scoring System (NCISS);

– Класифікація кіберінцидентів (Звіт про нові практики в регіоні ОБСЄ) / Cyber Incident Classification (A Report on Emerging Practices within the OSCE Region);

– NIST: Оцінка кіберризиків / NIST Cyber Risk Scoring (CRS);

– MITRE: показники кібервідмовостійкості, показники ефективності та оцінка / MITRE: Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring;

– ETSI GS ISI 00X Індикатори інформаційної безпеки / ETSI GS ISI 00X Information Security Indicators (ISI);

– ISO/IEC 27004:2016(E) Інформаційні технології — Методи безпеки — Управління інформаційною безпекою — Моніторинг, вимірювання, аналіз та оцінка;

– Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 06.10.2021 р. № 601.

Відповідні базисні параметри широко використовуються для формування глобальних індексів кібербезпеки [5]. Наведемо для прикладу один з можливих наборів базисних параметрів для кіберіндидентів:

Кіберінцидент		*Опис*
Клас	*Параметр*	
Образливий вміст	Спам	Небажана масова електронна пошта. Одержувач не надав дозволу на надсилання повідомлення, який можна перевірити, і що повідомлення надсилається як частина більшої колекції повідомлень, усі з яких мають функціонально порівняний вміст
	Шкідлива мова	Дискредитація чи дискримінація (кіберпереслідування, расизм, булинг, хейтинг, тощо)
	Дитина (сексуальне насильство)	Дитяча порнографія, пропаганда сексуального насильства
Шкідливий код	Вірус	Програмне забезпечення, яке навмисно встановлено без дозволу у систему із шкідливою метою. Для активації коду зазвичай необхідна взаємодія користувача
	Черв’як	
	Троян	
	ШПЗ	
	Номеронабирач	
	Руткіт	
Збір інформації	Сканування	Атаки, що надсилають запити до системи для виявлення слабких місць. Процеси тестування для збору інформації про хости, служби та облікові записи
	Сніфінг	Несанкціоновані спостереження та запис мережевого трафіку
	Соціальна інженерія	Збір інформації від імені людини нетехнічним способом (брехня, хитрощі, хабарі, погрози)

Формування набору (системи) базисних параметрів (індикаторів, показників) статистичних індексів про кіберінциденти, кібератаки, кіберзагрози та заходи протидії є першим основним етапом статистичного спостереження відповідних масових процесів. Наступними етапами спостереження є отримання статистичних, створення бази даних результатів статистичного спостереження та аналіз цих даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.
2. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» : Указ Президента України від 01.02.2022 № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/37/2022#Text.
3. Воттерс Е. 50 найпопулярніших статистичних даних, цифр і фактів з кібербезпеки, Computing Technology Industry Association (CompTIA). 27 Jan. 2023. URL: https://connect.comptia.org/blog/cyber-security-stats-facts.
4. Мармоза А. Т. Теорія статистики. 2-е вид. переоб. і доп. Київ : Центр учбової літератури, 2013. 592 с.
5. Худинцев М. М., Жилін А. В., Давидюк А. В. Світові індекси кібербезпеки: огляд та методики формування (Глобальний звіт / Каталог) / за заг. ред. М. М. Худинцев. Київ : Міжнародний університет кібербезпеки, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, 2021. 240 с.

УДК 004(056.53+413.4)

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

Коженевський Сергій Романович,
ІПМЕ ім. Г.Є. Пухова НАН України,
головний інженер, к.т.н.,
serhiikozhenevskyi@gmail.com

ТИПОВИЙ ШАБЛОН ВПЛИВУ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ НА КОРИСТУВАЧІВ СОЦІОТЕХНІЧНИХ СИСТЕМ ВІДПОВІДНО ДО CAPEC

Анотація. Приділено увагу протидії впливу соціальної інженерії на користувачів соціотехнічних систем. Продемонстровано важливість розуміння їхніх уразливостей. Це досягнуто визначенням типового шаблону впливу соціальної інженерії відповідно до CAPEC. Його використання орієнтоване на встановлення способів виконання дій зловмисником і, як наслідок, підвищення обізнаності користувачів соціоінженерних систем.

Abstract. Attention is paid to counteracting the influence of social engineering on users of sociotechnical systems. The importance of understanding their vulnerabilities has been demonstrated. This is achieved by identifying a typical social engineering impact pattern in accordance with CAPEC. Its use is aimed at establishing ways of performing actions by intruder the and, as a result, increasing the awareness of users of social engineering systems.

Одним з важливих аспектів протидії впливу соціальної інженерії є розуміння уразливостей користувачів соціотехнічних систем [1]. Це досягається розробленням типових шаблонів, кожним з яких відображаються атрибути та способи діяльностей

вірогідних зловмисників [2, 3]. Такі відомості узагальнюються і представляються у загальнодоступних каталогах, наприклад [2], Common Attack Pattern Enumeration and Classification (CAPEC™). Тому визначення типового шаблону впливу соціальної інженерії на користувачів соціотехнічних систем відповідно до CAPEC є актуальним завданням.

Відповідно до CAPEC типовим шаблоном впливу соціальної інженерії описуються способи маніпулювання і експлуатування людей [2, 3]. Кінцевою метою таких діяльностей є виконання зловмисником дій та/або отримання доступу до конфіденційної інформації. Серед типових доменів впливу соціальної інженерії виокремлюються параметри запитів, ідентифікаційна інформація, місцезнаходження ресурсу, дії, цілісність коду програмного забезпечення, поведінка людини, метадані [2].

Типовим шаблоном впливу соціальної інженерії структурується інформація за встановленими критеріями [2, 3]. Насамперед описується особливість дії (діяльності) з боку зловмисника. В окремі категорії виокремлено вірогідність і серйозність впливу соціальної інженерії. Наприклад [2], підроблення ідентифікаційної інформації характеризується середніми вірогідністю і ступенем серйозності. Крім того встановлюються передумови та наслідки впливу соціальної інженерії, а також способи його пом’якшення.

Наприклад [2], типовим шаблоном маніпулювання поведінкою людини (зокрема, користувача соціотехнічної системи) визначається використання соціальним інженером психологічної схильності для вимагання інформації, маніпулювання або виконання потрібних дій. Така атака характеризується високою вірогідністю реалізування і середнім ступенем серйозності. Обумовлюється володінням соціальним інженером засобами і знаннями для спілкування з користувачем соціотехнічної системи. Їх застосування призводить до порушення основних властивостей інформації (конфіденційності, цілісності, доступності). Запобігання цьому можливе шляхом регулярного підвищення обізнаності користувачів соціотехнічних систем.

Отже, визначення типового шаблону впливу соціальної інженерії дозволяє зрозуміти уразливості користувачів соціотехнічних систем. У цьому випадку рекомендовано використання відомих практик, зокрема, CAPEC. Такі дії загалом дозволяють зосередити увагу на уразливостях користувачів соціотехнічних систем і, як наслідок, підвищенні їх обізнаності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мохор В. В., Цуркан О. В., Клименко Т. М., Яшенков В. П., Цуркан В.В. Різновиди екторів при аналізуванні вразливостей соціотехнічних систем до впливів соціальної інженерії. *Кібербезпека енергетики* : матеріали науково-практичної конференції (Київ, 28 травня 2021 р.). Київ, 2021. С. 44.

2. Common Attack Pattern Enumeration and Classification (CAPEC™). URL: https://capec.mitre.org/about/index.html (дата звернення: 02.05.2023).

3. Adversary Emulation Plans. URL: http://attack.mitre.org/resources/ adversary-emulation-plans/ (дата звернення: 02.05.2023).

УДК [004(056.53+413.4)::001.51]::303.732

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

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

Дорогий Ярослав Юрійович,
КПІ ім. Ігоря Сікорського;
доцент, д.т.н., доцент,
Argusyk@gmail.com

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

СИМБІОЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ СФЕРИ ЕНЕРГЕТИКИ

Анотація. Проаналізовано процес захищання інформації об'єктів критичної інфраструктури сфери енергетики. Виокремлено заходи забезпечення непорушності властивостей конфіденційності, цілісності та доступності. Продемонстровано форми співжиття окремих різновидів систем захисту інформації. Крім того акцентовано увагу на можливості їхнього інтегрування розробленням і впровадженням систем управління інформаційною безпекою.

Abstract. This analysis examines the process of protecting critical infrastructure objects in the energy sector. It emphasizes measures for ensuring confidentiality, integrity, and availability. The coexistence of different types of information protection systems is demonstrated, along with the potential for integrating them through the development and implementation of information security management systems.

Порушення енергозабезпечення призводить до завдання шкоди життєво важливим національним інтересам України. Запобігання цьому досягається операторами на об'єктовому рівні управління, зокрема, шляхом захищання інформації об'єктів критичної інфраструктури сфери енергетики [1]. Виконання даного завдання можливе розробленням і впровадженням та/або комплексної системи захисту інформації [2], та/або системи інформаційної безпеки [3], та/або системи управління інформаційною безпекою [2].

Характерною особливістю упровадження зазначених систем є орієнтованість на інформаційно-комунікаційну систему як об’єкт захищання інформації [2–4]. При цьому непорушність властивостей конфіденційності, цілісності та доступності може забезпечуватися розробленням і комплексних систем захисту інформації, і систем інформаційної безпеки, і систем управління інформаційною безпекою. Принциповою відмінністю щодо їхнього обирання є потреба в задоволенні вимоги щодо захищання державної таємниці, службової інформації, державних і єдиних реєстрів [2]. В такому випадку розроблення і впровадження комплексної системи захисту інформації на об’єкті критичної інфраструктури сфери енергетики є обов’язковою нормою [1, 2]. Водночас варто врахувати те, що при обиранні систем управління інформаційною безпекою захищається об’єкт критичної інфраструктури сфери енергетики загалом. Їхнім упровадженням допускається урахуванням норм і настанов вітчизняного законодавства [5], наприклад [2, 4], щодо розроблення комплексних систем захисту інформації і систем інформаційної безпеки. Крім того в технологічному аспекті виокремлюються заходи А 8.20 і А 8.21 зі захищання як мереж, так і мережевих сервісів [5].

Отже, захищання інформації об’єктів критичної інфраструктури сфери енергетики можливе шляхом або розроблення однієї з систем захисту інформації, або їх комбінування. Заразом впровадження системи управління інформаційною безпекою дозволяє урахувати як настанови щодо застосовності і комплексних систем захисту інформації, і систем інформаційної безпеки.

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.
2. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 №80/94-ВР. URL: https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80.
3. 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.
4. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53375.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. [Valid from 2022-10-25]. URL: https://www.iso.org/standard/2700.

Chaikin M.M.,
G.E. Pukhov Institute for Modeling in Energy Engineering NASU,
graduate student,
mchaikin@outlook.com

PROBLEMS OF ASSESSING THE STATE OF CYBERSECURITY OF CRITICAL INFRASTRUCTURE OBJECTS ACCORDING TO THE NIST CYBERSECURITY FRAMEWORK IN UKRAINE

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.

From the beginning of the military aggression, the occupiers showed a special interest in the capture and destruction of energy facilities. On February 24, 2022 the Kakhovskaya hydroelectric power station was captured. On 25 February, Russian troops blew up a gas pipeline near Kharkiv, Ukraine's second-largest city. On 2 March, 2022, Russia claimed to have taken control of the area surrounding the 5.7GW nuclear power plant in Zaporizhzhia, Europe's largest. In addition, during the period of autumn 2022 – spring 2023, the occupiers repeatedly launched rocket-bomb strikes specifically at energy facilities. At the same time, according to the analysis of the specialists of the ESET corporation, which works in close contact with the State Service for Special Communications and Information Protection of Ukraine, energy facilities were one of the priority targets of cyberattacks by the aggressor state [1].

Such activity of the enemy caused the accelerated modernization of requirements for the protection of critical infrastructure, including in cyberspace. At the beginning of last year, the state of regulatory regulation of cyber security issues was not fully determined. It is worth noting that the requirements for cyber security for critical infrastructure objects are described in the following legal documents:

- Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine [2];
- Law of Ukraine On information protection in information and communication systems [3];
- Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects [4];
- Law of Ukraine On Critical Infrastructure [5]

Law of Ukraine «About Critical Infrastructure» was entered into force on June 15, 2022 and finally defined a special body that will have to develop requirements for the protection of critical infrastructure and create a register of critical infrastructure objects – this body is State Service of Special Communications and Information Protection of Ukraine. 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.

In 2021, the Administration of the State Service for Special Communications and Information Protection of Ukraine published Order No. 601 dated October 6,

2021, containing «Methodical recommendations on increasing the level of cyber protection of critical information infrastructure» [6]. Changes to this order, which were approved by the orders of the State Special Communications Administration dated 12.10.2021 No. 616 and dated 10.07, were published later. 2022 No. 343. These recommendations are developed taking into account the Framework for Improving Critical Infrastructure Cybersecurity issued in 2014 and updated in 2018 by the National Institute of Standards and Technology of the United States of America (NIST Cybersecurity Framework – NIST CSF) [7].

As a next step, on March 24, 2023, the Cabinet of Ministers of Ukraine adopted the Resolution on «Some issues of conducting an independent audit of information security at critical infrastructure facilities», which introduced a mandatory cyber security audit of critical infrastructure facilities every 2 or 3 years (depending on the category criticality) [8].

Since the State Service for Special Communications and Information Protection of Ukraine is responsible for the cyber protection of critical infrastructure objects, it can be stated that at the moment there are 3 different ways to confirm compliance with cyber security requirements, according to the 601st Order:

– Construction of a comprehensive information protection system with confirmed compliance (KSZI);

– Building an information security management system (ISMS);

– Audit for compliance with NIST CSF requirements and re-audit following implementation of recommendations.

In addition, it should benotedt hat some Ukrainian energy companies fall under the scope of regulation of the European Union in matters of cyber security. For example, the Ukrenergo company, as an operator of the dispatching and trunktransmission system, is part of the European network of electricitytransmission system operators, which unites 43 operatorsin 39 countrie sof the European continent – ENTSO-E (European Network of Transmission System Operators for Electricity), which has and develops its cybersecurity requirements – Network code on energy cybersecurity.

The recast of the Electricity Regulation (Regulation (EU) 2019/943) [9] 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. 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 for critical infrastructure components, a minimum protection level for energy system operators, a European energy cybersecurity maturity framework and supply chain risk management.

In January 2022, the European Network of Transmission System Operators for Electricity (ENTSO-E) announced the details of its new cybersecurity code. The Network Code on Cybersecurity (NCCS) is the first network code that will be developed according to the new rules established by the European Union on the internal market for electricity and is expected to enter into force by January 2024. The network code aims to set a European standard for the cybersecurity of cross-border electricity flows. It focuses on improving cybersecurity resilience through the

enhancement of threat decision and incident reporting and proposes various measures to improve cybersecurity resilience that are essential to preserving the continuity of the services. On January 14, 2022, the preparation of the draft document was completed [10].

At the same time, the State Service for Special Communications and Information Protection of Ukraine and the Cabinet of Ministers of Ukraine, with the activehelp of international partners, are working on updating Resolution No. 518 of the Cabinet of Ministers of Ukraine dated June 19, 2019 «On the approval of General requirements for cyber protection of critical infrastructure objects», which will lead to the acquisition of NIST CSF status is necessarily the standard for critical infrastructure facilities, instead of a recommendation status.This is a very important and timely step, as it will allow to synchronize the issue of cyber protection of critical infrastructure with the United States and implement a standard that was created specifically for critical infrastructure, as well as remove the variability of the choice of the approach by which to build cyber security at the objects of critical infrastructure.

The NIST Cybersecurity Framework is a widely used standard for managing and reducing cybersecurity risk. However, evaluating a critical infrastructure object according to this framework can present several challenges. Here are some potential problems:

1. Complexity: Critical infrastructure objects can be complex systems with many interconnected components and subsystems. Evaluating all of these components against the NIST Cybersecurity Framework can be a daunting task.
2. Limited scope: The NIST Cybersecurity Framework is primarily focused on cybersecurity risk management. However, critical infrastructure objects may face risks that go beyond cybersecurity, such as physical security, natural disasters, and human error. Evaluating only the cybersecurity aspect of an infrastructure object may not provide a complete picture of the risks it faces.
3. Lack of guidance: The NIST Cybersecurity Framework provides general guidance on cybersecurity risk management but does not provide specific instructions for evaluating critical infrastructure objects. As a result, organizations may struggle to know how to apply the framework to their specific infrastructure objects.
4. Limited metrics: The NIST Cybersecurity Framework provides a set of core metrics that can be used to measure cybersecurity risk management effectiveness. However, these metrics may not be applicable to all critical infrastructure objects or may not provide a complete picture of risk management effectiveness.
5. Evolving threats: Cybersecurity threats are constantly evolving, and the NIST Cybersecurity Framework may not always be able to keep up with the latest threats. As a result, organizations may need to supplement the framework with additional measures to ensure that their critical infrastructure objects are adequately protected.

Assessing the state of cybersecurity of critical infrastructure objects according to the NIST Cybersecurity Framework in Ukraine in the context of Russian military aggression may present additional challenges beyond the ones mentioned earlier. Here are some potential problems:

1. Increased threat level: The ongoing conflict with Russia increased the threat level for critical infrastructure objects in Ukraine. Cyber attacks used as a tool of warfare, making it even more important for organizations to assess their cybersecurity posture and take appropriate measures.

2. Limited access: Parts of Ukraine may be difficult to access due to the conflict, making it challenging for organizations to conduct cybersecurity assessments or receive support from experts in other regions or countries.

3. Limited resources: The ongoing conflict may divert resources away from cybersecurity, making it more difficult for organizations to implement the NIST Cybersecurity Framework or invest in cybersecurity measures.

4. Political interference: The conflict with Russia may also create political interference that could impact the implementation of the NIST Cybersecurity Framework. For example, political pressure may be applied to prioritize certain critical infrastructure objects over others, regardless of their actual risk level.

5. Uncertainty: The ongoing conflict may create a sense of uncertainty for organizations operating in Ukraine, making it more challenging to develop long-term plans or invest in infrastructure improvements. This uncertainty may also make it more difficult to attract and retain cybersecurity talent.

However, there are ways to address these problems, including:

1. Prioritizing cybersecurity: It is essential to prioritize cybersecurity for critical infrastructure objects, even in the midst of a conflict. This requires allocating adequate resources and investing in the necessary expertise to implement the NIST Cybersecurity Framework effectively.

2. Enhancing threat intelligence: Critical infrastructure organizations must have access to accurate and up-to-date threat intelligence to better understand the types of cyber attacks they may face. This information can help them tailor their cybersecurity measures to address specific threats.

3. Increasing collaboration: Collaboration between public and private organizations is essential for effective cybersecurity. In the context of Russian military aggression, this collaboration must include coordination with international partners to share best practices and identify emerging threats.One such example of ccollaborationis the program for assessing the state of cyber protection of 38 critical infrastructure objects according to the NIST Cybersecurity Framework, which is implemented in Ukraine with the support of the Project «Cybersecurity of Critical Infrastructure» of the United States Agency for International Development (USAID).

4. Adapting to changing conditions: In a conflict environment, conditions may change rapidly, and organizations must be prepared to adapt their cybersecurity measures accordingly. This requires a flexible approach that can quickly respond to new threats.

5. Investing in employee training: Employees are often the weakest link in cybersecurity. Organizations must invest in cybersecurity training to ensure that employees are aware of the risks they face and know how to respond to potential cyber attacks.

6. Overall, assessing the state of cybersecurity of critical infrastructure objects according to the NIST Cybersecurity Framework in Ukraine under the conditions of

Russian military aggression requires a comprehensive approach that prioritizes cybersecurity, enhances threat intelligence, increases collaboration, adapts to changing conditions, and invests in employee training. By addressing these challenges, organizations can better protect critical infrastructure and ensure the ongoing safety and security of Ukraine.

Overall, assessing the state of cybersecurity of critical infrastructure objects according to the NIST Cybersecurity Framework in Ukraine under the conditions of Russian military aggression requires a comprehensive approach that prioritizes cybersecurity, enhances threat intelligence, increases collaboration, adapts to changing conditions, and invests in employee training. By addressing these challenges, organizations can better protect critical infrastructure and ensure the ongoing safety and security of Ukraine.

REFERENCES

1. A year of devastating cyber attacks in Ukraine: how threats attacked users and organizations. URL: https://www.eset.com/ua/about/newsroom/press-releases/malware/god-razrushitelnykh-kiberatak-v-ukraine-kak-ugrozy-atakovali-polzovateley-i- organizatsii/.
2. Law of Ukraine On the Basic Principles of Cybersecurity in Ukraine. URL: https://zakon.rada.gov.ua/laws/show/2163-19?lang=en#Text.
3. Law of Ukraine On information protection in information and communication systems, URL: https://zakon.rada.gov.ua/laws/show/80/94-вр?lang=en#Text (link is external).
4. Resolution of the Cabinet of Ministers of Ukraine On Approval of General Requirements for Cyber Protection of Critical Infrastructure Objects, URL: https://zakon.rada.gov.ua/laws/show/518-2019-п?lang=en#Text.
5. Law of Ukraine On Critical Infrastructure. URL:https://zakon.rada.gov.ua/laws/show/1882-20#Text.
6. Order No. 601 dated October 6, 2021 of Administration of the State Service for Special Communications and Information Protection of Ukraine «Methodical recommendations on increasing the level of cyber protection of critical information infrastructure», URL: https://cip.gov.ua/ua/news/nakaz-ad-2021-10-06-601.
7. NIST Cybersecurity Framework, URL: https://www.nist.gov/cyberframework.
8. Resolution of the Cabinet of Ministers of Ukraine «Some issues of conducting an independent audit of information security at critical infrastructure facilities». URL: https://www.kmu.gov.ua/npas/deiaki-pytannia-provedennia-nezalezhnoho-audytu-informatsiinoi-bezpeky-na-s257-240323.
9. Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0943&from=EN.
10. Network Code on Cybersecurity Drafting Status, URL: https://www.entsoe.eu/network_codes/nccs/.

Тяпкова Олександра Ігорівна,
ННІ права КНУ ім. Тараса Шевченка,
студентка,
alessandra.tpkv@gmail.com

ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ: РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ В ЕНЕРГЕТИЦІ ТА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Останні події в Україні та по всьому світу підкреслили важливість забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури, зокрема в енергетичному секторі.

Адже енергетична безпека є важливою складовою національної безпеки України, виступаючи стратегічною галуззю нашої економіки. Безперебійне функціонування енергетичного сектору є гарантією стабільних процесів, спрямованих на підтримання енергонезалежності та успішного розвитку України як європейської країни [1, с.495].

Енергетична безпека України є важливим компонентом національної безпеки та стратегічним сектором нашої економіки. Надійне функціонування енергетичного сектору є запорукою стабільних процесів, спрямованих на досягнення енергонезалежності та успішного розвитку України як європейської країни.

Зміни, які відбулися в зовнішньому та внутрішньому безпековому середовищі України, потребують негайних заходів для створення ефективної системи забезпечення кібербезпеки енергетичних об'єктів, яка є необхідною складовою національної безпеки.

З урахуванням розвитку інтелектуальних енергетичних систем стає все більш актуальною проблема забезпечення кібербезпеки в енергетиці, особливо враховуючи з'явлення нових загроз і прагнень політичного керівництва РФ дестабілізувати ситуацію в енергетичному секторі України.

Зміни, що сталися в зовнішньому та внутрішньому безпековому середовищі України, вимагають негайних заходів щодо створення ефективної галузевої системи забезпечення кібербезпеки енергетичних об'єктів, яка є важливою складовою національної безпеки [2, с.30]. У контексті розвитку інтелектуальних енергетичних систем зростає проблема забезпечення кібербезпеки в енергетиці, особливо з урахуванням появи нових гібридних загроз та прагнень політичного керівництва РФ дестабілізувати ситуацію в енергетичному секторі України.

Згідно зі статтею 6 Закону України "Про основні засади забезпечення кібербезпеки України", об'єкти енергетичного сектору можуть бути віднесені до категорії критичної інфраструктури.

Згідно з Постановою Кабінету Міністрів України від 23.08.2016 №563 "Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави", інформаційні системи енергетичного сектору включаються до переліку об'єктів критичної

інфраструктури держави з урахуванням негативного впливу на енергетичну безпеку держави або регіону, до якого можуть призвести кібератаки на такі системи [3, с.50].

Згідно зі згаданим вище Законом України, забезпечення кібербезпеки об'єктів критичної інфраструктури, включаючи енергетичний сектор, досягається за допомогою створення системи управління інформаційною безпекою (СУІБ) відповідно до міжнародного стандарту ISO/IEC 27001:2013 або за допомогою створення комплексної системи захисту інформації (КСЗІ) відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах".

Забезпечення кіберстійкості є надзвичайно важливим аспектом для енергетичних систем та об'єктів критичної інфраструктури, оскільки вони є потенційними цілями для кіберзлочинців. Розслідування кіберзлочинів в цих сферах вимагає спеціалізованого підходу та високої кваліфікації з боку фахівців [4, с.8].

Варто навести декілька ключових аспектів, які слід враховувати при розслідуванні кіберзлочинів в енергетиці та об'єктах критичної інфраструктури.

По-перше, створення спеціалізованих кібербезпекових команд. Енергетичні компанії та організації, відповідальні за об'єкти критичної інфраструктури, повинні мати власні команди кібербезпеки, які спеціалізуються на виявленні, розслідуванні та реагуванні на кібератаки. Ці команди повинні мати високу експертизу в галузі кібербезпеки та бути здатними швидко реагувати на інциденти.

По-друге, збір доказів. Розслідування кіберзлочинів вимагає збору великої кількості доказів. Це може включати аналіз логів систем, мережевих пакетів, файлів журналів, образів дисків тощо. Фахівці з кібербезпеки повинні мати доступ до відповідних інструментів та методик для збору та аналізу цих доказів.

Законодавством України, зокрема Законом 2149-IX, були внесені зміни до розділу XVI Кримінального кодексу України (ККУ), що стосуються відповідальності за кіберзлочини. Конкретно дві норми цього розділу були змінені. Згідно зі Законом "Про електронні комунікації" та вимогами іншого законодавства України у сфері кібербезпеки, термін "електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку" було замінено на "інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі".

Ці зміни відтепер враховуються у статті 361 ККУ. Однак залишається незрозумілим, чому термінологія була змінена лише частково. Назва розділу та інші статті з розділу, які також охоплюють поняття "кіберзлочини" не зазнали змін. Юридичні склади інших правопорушень, які також відносяться до цього розділу, залишилися без змін. Крім того, є й інші питання, на які не отримано чітких відповідей.

Наприклад, чому відповідальність за розповсюдження або збут шкідливих програм була посилена (частина 1 статті 361-1 ККУ), а санкції за збут або

розповсюдження інформації з обмеженим доступом залишилися без змін (частина 1 статті 361-2 ККУ).

Закон України № 2137-IX від 15.03.2022, що набрав чинності 22 березня 2022 року, впровадив ряд важливих змін з метою підвищення ефективності розслідування кіберзлочинів. Ось лише деякі з цих змін:

— Тепер може застосовуватися арешт до комп'ютерних систем або їх частин, якщо вони були отримані в результаті вчинення злочину, є засобом для його вчинення або необхідні для проведення експертного дослідження, а також якщо власник обмежує доступ до них (абз. 2 ст. 170 Кримінального процесуального кодексу (КПК)).

— Під час обшуку слідчий або прокурор можуть отримувати доступ до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку без попереднього дозволу, якщо інформація, яка на них зберігається, має значення для розкриття обставин злочину (абз. 2 ч. 6 ст. 236 КПК).

— Огляд комп'ютерних даних здійснюється шляхом відображення інформації, що міститься в них, у формі, зрозумілій для сприйняття (фотографії, відеозаписи тощо) (ч. 2 ст. 237 КПК).

— Вводиться нова розшукова дія - зняття показань технічних пристроїв, які можуть фотографувати, відеозаписувати або здійснювати записи, з метою отримання доказів, на підставі постанови слідчого або прокурора (ст. 245-1 КПК).

— Встановлення місцезнаходження радіообладнання (радіоелектронного засобу) тепер може здійснюватися за заявою його власника без необхідності дозволу слідчого.

Це показує системність підходів законодавця. Запропоновані механізми дозволяють ефективно втілити в життя задум щодо кримінально-правового забезпечення кібербезпеки, своєчасно перевести проаналізовані вище норми ККУ в реальні вироки для тих, хто підриває безпеку України та українців.

Таким чином, кібербезпека є життєво важливим фактором існування критичного та енергетичного комплексу та його складових. В сучасних умовах критично важливим є не лише запровадження новітніх технологій забезпечення енергоефективності, але й виконання завдання щодо захисту енергетичної системи від реальних та потенційних загроз у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ємельянов В.М., Бондар Г.Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. Публічне управління та регіональний розвиток. 2019. № 5. С. 493-523.

2. Мальцева І., Черниш Ю., Овсянніков В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. Кібербезпека: освіта, наука, техніка. 2021. № 12. Т. 4. С. 29-35.

3. С. Гончар, М. Комаров, «Методика оцінки кіберстійкості об’єктів критичної інфраструктури», Безпека соціально-економічних процесів в кіберпросторі: Всеук. наук.-практ. конф., 2019, Київ, 2019, С. 49-50.

4. Теленик С.С. Адміністративно-правове регулювання державної системи захисту критичної інфраструктури України: автореф. дис. …д-ра юрид. наук: спеціальність 12.00.07. Запоріжжя, 2021. 37 с.

Кириленко Владислав Миколайович,
ННІ права КНУ ім. Тараса Шевченка,
студент,
vlad2504368@gmail.com

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасному світі спостерігається формування інформаційного суспільства, що має значний вплив на суспільний розвиток. Україна активно бере участь у цьому процесі, сприяючи створенню єдиного світового ринку інформації та глобальній інформатизації. Інформаційний фактор відіграє важливу роль у відстоюванні державних інтересів як на внутрішньому, так і на міжнародному рівні.

Широкий та оперативний доступ до інформації є ключовим елементом управління процесами та інститутами. Розповсюдження новітніх систем обробки інформації та телекомунікацій є важливим аспектом інформатизації сучасного суспільства.

Одним з чинників, який сприяє забезпеченню інформаційної безпеки, є застосування технологій штучного інтелекту. Штучний інтелект є одним з провідних напрямів розвитку у всіх розвинутих країнах світу. Якщо Україна не приділятиме належної уваги проблемам штучного інтелекту, вона може втратити можливість здійснити технологічний прорив. Глобальний ринок технологій на основі штучного інтелекту буде розділений між конкуруючими країнами, що ускладнить розвиток держави в стратегічно важливих галузях економіки та сповільнить її прогрес.

Активний розвиток інформаційних технологій призводить до необхідності вивчення проблем інформаційної безпеки, таких як загрози для інформаційних ресурсів, різних засобів та заходів захисту, бар'єри для проникнення, а також вразливі місця в системі захисту інформації.

Переваги штучного інтелекту над людською роботою очевидні. Ця система виявляється значно більш уважною та прискіпливою до відбуваючихся процесів. Завдяки швидкості "самонавчання" нейронних мереж можна стверджувати, що вона здатна вчасно виявляти загрози (за умови правильного формулювання завдань для мережі) без конкуренції. На даному етапі розвитку штучний інтелект може не забезпечити необхідну реакцію на негативні процеси, але безумовно зможе це зробити [1, с.18].

Загалом, під інформаційною безпекою розуміють сукупність засобів, методів та процесів, які забезпечують захист інформаційних активів та гарантують збереження ефективності та практичної корисності технічної інфраструктури інформаційних систем, а також збереження та обробку відомостей, що містяться в таких системах.

Особливу важливість та актуальність в суспільних відносинах набуває використання штучного інтелекту у системі забезпечення інформаційної безпеки, оцінки та аналізу інформаційних загроз, а також практичного

застосування штучного інтелекту в контексті інформаційного опору з метою захисту територіальної цілісності України та суверенітету. Це є концептуальною основою діяльності суспільства.

У сучасних умовах глобалізації вважається, що інформаційна безпека є одним з найважливіших факторів, що забезпечують умови для реалізації національних інтересів та здатності держави подолати кризові ситуації при зовнішній агресії. Ефективні заходи щодо управління інформаційною безпекою з боку держави, як головного суб'єкта, можуть допомогти подолати загрози соціально-економічному та політичному життю країни. Сфера оборони та безпеки є головною галуззю у світі і зазнає серйозних змін через впровадження технологій штучного інтелекту, що впливає на баланс сил між державами.

Штучний інтелект, результат людської діяльності, може логічно мислити, керувати своїми діями та обґрунтовувати свої рішення, але не може коригувати їх при зміні умов. Він є високим досягненням технологічної цивілізації, складною системою взаємозв'язків та основою для створення інформаційних системних утворень. В найближчому майбутньому активне використання технологій штучного інтелекту та нанобіотехнологій може спричинити переформатування поведінки людей, зміну суспільних відносин та вплинути на особистісні характеристики.

Застосування штучного інтелекту в інформаційній безпеці має свої коріння у двох основних чинниках. По-перше, його використання є необхідним для швидкого реагування на кіберінциденти. По-друге, це пов'язано з нестачею кваліфікованих кіберзахисних спеціалістів.

На сьогоднішній день застосування штучного інтелекту в інформаційній безпеці значно розширилося. Глобальні компанії активно аналізують великі обсяги інформації в мережі, щоб виявити нові загрози або передбачити атаки нульового дня. Ці компанії використовують системи, які збирають великі масиви даних та застосовують технології штучного інтелекту для аналізу, виявлення закономірностей, кластеризації даних та прогнозування загроз. Без таких технологій обробка такого обсягу інформації є практично неможливою. Для цих цілей широко використовуються нейронні мережі та кластеризація.

Штучний інтелект – відносно новий термін для українського законодавця, тому однозначне правове визначення, а тим більше правове регулювання, наразі відсутні в чинному законодавстві.

При цьому Україна вже «заклала перший камінь» в розвиток та регулювання штучного інтелекту. Так, Розпорядженням Кабінету Міністрів України від 02 грудня 2020 р. № 1556-р було схвалено Концепцію розвитку штучного інтелекту в Україні[4].

Концепція визначає штучний інтелект як організовану сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми

роботи з інформацією та визначати способи досягнення поставлених завдань.

Штучний інтелект активно використовується відслідковуванні загроз, де на основі інформації, що зібрана з різних джерел, відкритих і закритих, прогнозуються загрози інформаційній безпеці. Таким чином, за останні двадцять років масштаб і застосування штучного інтелекту в сфері інформаційної безпеки значно збільшилися. Штучний інтелект виявляється ефективним помічником у захисті від кіберзагроз.

Ефективна стратегія інформаційної безпеки передбачає комплексний підхід, який охоплює п'ять ключових сфер: • Виявлення та аналітика загроз. • Безпека даних та додатків. • Управління ідентифікацією. • Безпека мережі та систем.

Україна активно реформує оборонно-промисловий комплекс, і важливою частиною цього процесу є впровадження інноваційних технологій штучного інтелекту. Відомо, що провідні країни світу вивчають та використовують можливості штучного інтелекту в оборонній сфері. Наприклад, компанія Thales Group, яка спеціалізується на цифровій ідентифікації безпеки, розробляє та виробляє інформаційні системи для авіакосмічних та військових галузей. Ці системи становлять потужну основу для швидкого та ефективного захисту критичної інфраструктури в різних секторах, таких як енергетика, хімічна промисловість, транспорт, екологія тощо. Thales Group сприяє забезпеченню інформаційної безпеки державних органів, приватних компаній та власників об'єктів критичної інфраструктури.

В системі інформаційної безпеки, основними типами штучного інтелекту є:

1) EDR (Endpoint Detection and Response) - це платформи, призначені для виявлення атак на робочих станціях, серверах та інших комп'ютерних пристроях (кінцевих точках) і негайної реакції на них. Використовуючи технології штучного інтелекту, продукти цієї категорії можуть виявляти невідомі шкідливі програми, автоматично класифікувати загрози та самостійно реагувати на них, передаючи дані в центр управління. Штучний інтелект приймає рішення на основі загальної бази знань, яка накопичується з великої кількості пристроїв. Деякі продукти цього типу також використовують штучний інтелект для розмітки даних на кінцевих точках та контролю їх переміщення, щоб виявляти внутрішні загрози.

2) NDR (Network Detection and Response) - це пристрої та аналітичні платформи, які виявляють атаки на мережевому рівні та дозволяють швидко на них реагувати. Використовуючи статистику та базу знань про загрози, продукти цього типу виявляють загрози в мережевому трафіку за допомогою штучного інтелекту та можуть автоматично реагувати на них, змінюючи конфігурацію мережевих пристроїв та шлюзів. Деякі продукти спеціалізуються на захисті хмарних провайдерів та їх інфраструктури. Додатковий сценарій використання штучного інтелекту в мережевому захисті полягає в аналізі поштового трафіку для виявлення фішингу.

3) SIEM (Security Information and Event Management) - це рішення, яке надає моніторинг інформаційних систем в реальному часі та аналізує події

безпеки, що надходять від мережевих пристроїв, засобів захисту інформації, IT-сервісів, інфраструктури систем та додатків, допомагаючи виявляти інциденти інформаційної безпеки. В таких системах накопичується великий обсяг даних з різних джерел, а використання штучного інтелекту дозволяє виявляти аномалії евристичними методами та зменшувати помилкові спрацьовування під час зміни моделей даних.

4) SOAR (Security Orchestration and Automated Response) - це системи, які дозволяють виявляти загрози інформаційній безпеці та автоматизувати реагування на інциденти. У рішеннях цього типу, на відміну від SIEM-систем, штучний інтелект допомагає не тільки проводити аналіз, але й автоматично реагувати на виявлені загрози відповідним чином та інші [2, 3].

Отож, у контексті інформаційної безпеки, штучний інтелект можна описати як програмне забезпечення, яке здатне аналізувати оточуюче середовище, визначати певні події та приймати самостійні заходи за необхідності. Штучний інтелект використовується для розшифрування закономірностей та виявлення аномалій, тому він може бути корисним інструментом для моніторингу загроз. Надійна стратегія інформаційної безпеки також допомагає захистити персональні дані населення, державні дані та алгоритми, що стає все більш важливим з поширенням нових моделей штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16–26.
2. Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. URL: https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-criticalinfrastructure
3. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA. Int. J. Cyber Warf. Terror. 2016. Vol. 6, pp. 1–16.
4. Розпорядження КМУ Про схвалення Концепції розвитку штучного інтелекту в Україні від 02.12.2020 року. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text

ЗМІСТ

МАТЕРІАЛИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»
31 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 № 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/