DOI: https://doi.org/10.32839/2304-5809/2020-9-85-25
УДК 004.49

Фурсов І.І., Шматко О.В.
Національний технічний університет
«Харківський політехнічний інститут»

ПИТАННЯ ВИЗНАЧЕННЯ ПОРУШЕНЬ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ

Анотація. Збільшення числа атак на кіберфізичні системи (КФС) виробничих процесів, запущених в критичній інфраструктурі, великий об'єм інформації, що надходить з тисяч пристроїв, якими обладнані сучасні КФС, і питання захисту таких даних на фізичному та інформаційному рівнях, створили потребу в нових стратегіях, адаптованих для виявлення сучасних загроз інформаційної безпеки подібних складних систем без перешкод в роботі самої інфраструктури інтелектуальних систем та нових підходів до визначення коректності роботи. Задачами даного звіту стали такі питання розв'язання завдань забезпечення інформаційної безпеки КФС а саме, огляд питань забезпечення інформаційної безпеки КФС, розробка алгоритму забезпечення інформаційної безпеки КФС, розгляд обраного методу виявлення порушень безпеки КФС основаного на аналізі самоподібності процесів, та його удосконалень, в рамках задач наукових досліджень.

Ключові слова: кіберфізичні системи, фрактальний аналіз, часові ряди, показник Херста, скейлингова функція, гомеостаз, само-подібність.

Fursov Ihor, Shmatko Alexandr
National Technical University "Kharkiv Polytechnic Institute"

ISSUES OF DETERMINING SECURITY BREACHES OF CYBER-PHYSICAL SYSTEMS

Summary. Critical infrastructure items can include enterprises, institutions, and organizations, regardless of their form of ownership, that may carry out activities and provide services in the energy, chemical, transport, information and communication technologies, electronic communications, banking and financial sectors, provide services in the areas of life support for the population, in particular in the areas of centralized water supply, sanitation, electricity and gas supply, food production, agriculture, and health care, can be municipal, emergency and rescue services, emergency services for the population, may included in the list of enterprises of strategic importance for the economy and security of the state. The increase in the number of attacks on cyber security systems (CPS) of production processes running in critical infrastructure, the large amount of information that comes from thousands of devices that are equipped with modern CPS, and the issues of protecting such data at the physical and information levels, have created the need for new strategies adapted to detect modern threats to the information security of such complex systems without interfering with the operation of the infrastructure of intelligent systems and new approaches to determining the correctness of work. The objectives of this report are the following questions of theoretical analysis and practical recommendations for solving the problems of ensuring information security of the CPS. We should review the subject area of information security issues of the CPS, analyze the models and methods of information systems for solving issues of ensuring information security of the CPS, perform development of an algorithm for providing a methodological information and software basis for supporting the information security of the CPS, consider of the selected method for detecting security violations of the CPS based on the analysis of self-similarity of processes, and its improvements, in the framework of scientific research tasks. In this work, the inspection and analysis of the security problems of CPS were performed. Methods for determining extraneous interference in the operation of cyberphysical systems were analyzed. The disadvantages of existing methods for determining violations of the CPS were considered. A number of scientific papers were analyzed on the topic of determining the violation of the stationary state of digital systems were reviewed. Criteria for selecting methods for ensuring the correct operation of cyberphysical systems were considered.

Keywords: cyberphysical systems, fractal analysis, time series, Hurst exponent, scaling function, homeostasis, self-similarity.

Постановка проблеми. Процес виявлення порушень безпеки складних кіберфізичних систем в різних варіантах реалізації пов'язаний із обробкою великої кількості вхідних параметрів, що обумовлено масштабністю подібних кіберфізичних систем та аналізу спектрів роботи подібних систем на фізичному або інформаційному рівнях. Інформаційною основою розв'язання завдань роботи є статистичний аналіз великих об'ємів даних, надходжених до кіберфізичної системи з сенсорів та детермінуючих стан її роботи в певний момент часу. З огляду на це, необхідними програмними системами, що підтримуватимуть проведення досліджень за тематикою забезпечення інформаційної безпеки кіберфізичних систем є пакети програм STATISTICA та Microsoft EXCEL.

Дані програмні засоби дозволяють проводити велику кількість необхідних статистичних розрахунків, кореляційний аналіз параметрів роботи кіберфізичних систем, побудову двохвимірних та трьохвимірних діаграм, робити регресійний аналіз вхідних параметрів, проводити аналіз часових рядів. Перевагами даних програмних засобів є простота організації роботи, докладна документація, досвід використання даних пакетів в подібних дослідженнях.

На основі аналітичного огляду робіт дослідників І.В. Котенко, Є.Ю. Павленка, та даних досліджень реальних кібератак [1; 7], встановлені такі проблеми забезпечення інформаційної безпеки кіберфізичних систем:

1) проблема створення методу виявлення порушень інформаційної безпеки (далі – ІБ) кібер-

фізичних систем, що забезпечує інваріантність до типу атак і способу їх реалізації. На даний час, процес виявлення різних типів деструктивних впливів на КФС вимагає істотних часових і обчислювальних витрат;

2) проблема створення методу, стійкого до кількості атак. Число можливих векторів атак на КФС і способів реалізації їх атак стає тим більше, чим складніше організована система. Інтеграція КФС з промисловістю та критичними галузями діяльності людини, робить такі КФС бажаною метою для атаки зловмисників;

3) проблема виявлення сучасного вірусного програмного забезпечення, направленого на порушення роботи КФС будь-якої конфігурації. Використання зловмисниками складного вірусного програмного забезпечення, створює труднощі зі своєчасним виявленням порушень в роботі КФС;

4) проблема створення методології динамічного захисту для забезпечення стійкості функціонування КФС в умовах кібератак. Існуючі методи захисту ІБ КФС направлені, передусім, на виявлення атаки, а не на стабілізацію її роботи після кібератаки, при цьому не розглядається питання відновлення параметрів КФС для забезпечення адекватності її роботи та збереженні функціональної стійкості [1];

5) проблема аналізу допустимих відхилів параметрів роботи системи в стаціонарному стані, для більш коректного визначення типу порушень роботи КФС, викликаних природними чинниками чи стороннім втручанням в її роботу.

Аналіз останніх досліджень та публікацій. В останні десятиріччя в світі відбулися інциденти порушення безпеки великих об'єктів критичної інфраструктури, в ході яких збій в роботі кіберфізичних систем ставив під загрозу здоров'я, безпеку і благополуччя не тільки окремих людей, а й цілих націй. На даний час відбулося близько сотні значних кібератак на об'єкти інфраструктури, та з кожним роком, згідно досліджень, їх кількість зростає. Кількість незначних випадків викрадення даних може сягати декількох тисяч в день [2].

Кіберфізичні системи (КФС) інтегрують фізичні та інтелектуальні компоненти при виконанні певних виробничих процесів. З огляду на збільшення кількості кіберфізичних систем в усіх критичних галузях інфраструктури, збільшенням можливостей шкідливого впливу на подібні системи шляхом фізичної чи інформаційної атаки на її компоненти, постає питання огляду предметної області забезпечення інформаційної безпеки подібних систем та обумовлюється актуальність роботи.

Ступінь інтернет-активності як організацій, так і окремих осіб значно збільшився, що сприяє зростанню числа потенційних напрямків атак. Крім того, в якості об'єкту атаки може виступати цілий ряд фізичних та інтелектуальних компонент складних кіберіфізичних систем. Загрози стають все більш витонченими. Вірусне програмне забезпечення вдосконалюється та вже має можливість функціонувати автономно. Процес порушень інформаційної безпеки кібкрфізичних систем, стає критично важливим для функціонування державного апарату та бізнесу у світовому масштабі. В даний час спостерігається тенденція до повернення вже відомих типів загроз, вдосконалених за допомогою сучасних технологій програмування, що відкриває нові горизонти в сфері виявлення та аналізу загроз.

23 грудня 2016 року компанія Ernst & Young представила звіт про готовність компаній світового рівня протистояти кібератакам та недостатніх інвестиціях в розвиток напрямів по боротьбі з кіберзлочинами, відсутності планів усунення негативних наслідків таких атак.

Звіт підготовлений за результатами дослідження в області інформаційної безпеки «Шлях до кіберустійкості: прогноз, захист, реагування» (Path to cyber resilience: Sense, resist, react) за 2016 рік.

В опитуванні брали участь 1735 підприємств з різних країн і галузей промисловості. Згідно з дослідженням, половина опитаних (50%) не здатні, на їхню думку, виявити ретельно підготовлені кібератаки – найбільший рівень не впевненості з 2013 року – за рахунок нестачі інвестицій в засоби виявлення кіберзагроз для прогнозування наслідків атаки, а також за рахунок відсутності механізмів безперервного моніторингу, роботи операційних центрів інформаційної безпеки (Security Operation Center, SOC) і механізмів активного захисту.

Незважаючи на наявні інвестиції, 86% респондентів визнають, що їх служба кібербезпеки не відповідає повною мірою потребам організації.

Майже дві третини (64%) респондентів не мають спеціальних програм збору і аналізу інформації про кіберзагрози, або обмежуються несистемними заходами в цій області. Що стосується виявлення вразливостей, більше половини (55%) не мають у своєму розпорядженні відповідними технічними засобами і можливостями, або ж такі кошти використовуються нерегулярно, від випадку до випадку.

Більше половини (57%) респондентів відповіли позитивно на питання про інциденти порушень інформаційної безпеки в компанії. Майже половина (48%) вважають найбільшою вразливістю своєї організації застарілі засоби контролю, особливості архітектури інформаційної безпеки. Фізичні збитки при порушенні технологічних процесів оцінюються більше ніж викрадення даних [3].

Таким чином, на основі вищезгаданих загроз безпеки кіберфізичних систем, зростаючої кількості кібератак, нових викликів інформаційної безпеки промислових систем, пов'язаних зі розповсюдженням мережевих технологій та удосконаленням вірусного програмного забезпечення, в рамках досліджень даної роботи було обумовлено актуальність розробки виявлення методу виявлення порушень інформаційної безпеки складних кіберфізичних систем, стійкого до стратегій та типів атак, універсального до типів кіберфізичних систем.

Методи виявлення атак на кіберфізичні системи, як правило, пов'язані з обробкою часових рядів та великих об'ємів даних, проте в різних публікаціях описані різні методи виявлення порушень безпеки кіберфізичних систем. Далі опишемо основні дослідження по тематиці виявлення загроз кіберфізичних систем.

Наявні роботи з тематики забезпечення інформаційної безпеки кіберфізичних систем пропонують різні підходи до розробки методу виявлення порушень роботи кіберфізичних систем. Підходи визначення атак на кіберфізичні систе-

ми, запропоновані в сучасних наукових статтях, включають в себе:

1) методи забезпечення ІБ на основі використання мікроконтроллерів, розглянуті в роботах автора І.В. Котенко. Дані методи ефективні в при заздалегідь обумовленій архітектурі КФС, проте наведено мало посилань на дослідження подібних методів на практиці, відсутні обґрунтування універсальності даного методу;

2) методи аналізу великих об'ємів даних, наведений в роботах автора М.А. Полтавцевої, розглядає теоретичні аспекти визначення порушень роботи КФС;

3) метод визначення порушень роботи КФС на основі мультифрактального аналізу, наведений в роботах Є.Ю. Павленка. Даний метод визначення порушень нормальної роботи КФС має широкий перелік застосувань та практику використання. Аналіз вхідних параметрів не наведено;

4) метод визначення атак на КФС з використанням нейронних мереж, автора Л.В. Сухостат. Даний метод застосування методів глибоких нейронних мереж до процесу розпізнавання атак на кіберфізичні системи добре зарекомендував себе при визначенні втручань в роботу КФС різного типу та різних типах атак. Проте універсальність методу обмежена, що обумовлено складністю навчання нейронних мереж та варіативністю атак.

В цілому, описані та досліджені методи виявлення порушень роботи КФС мають недоліки, пов'язані з недостатньою ефективністю методів при великій варіативності типів атак та різнорідності типів КФС, економічною складовою впровадження методів в реальних КФС, відсутністю механізмів відновлення параметрів роботи КФС при атаках на них, та відсутністю аналізу впливів на КФС, спричинених природними факторами, що обумовлює подальші дослідження даної тематики.

Виділення невирішених раніше частин загальної проблеми. Відомо значне число робіт, присвячених забезпеченню інформаційної безпеки кіберфізичних систем, в яких проаналізований сучасний стан проблем безпеки та методи визначення кібератак на інформаційні системи, збереженню стійкості і коректності функціонування таких систем, дослідження ефективності методів забезпечення інформаційної безпеки кіберфізичних систем. До них відносяться роботи Л.В. Сухостат, П.Д. Зегжди, І.Б. Саєнко, І.В. Котенко, Ю.С. Васильєва, Д.В. Бірюкова, А.С. Міщенко, І.В. Красова, Р. Сенгера. Ряд робіт присвячений застосуванню саморегульовоного управління складних систем. Серед них – роботи Ю.М. Горського, І. Геростатопулоса, Л.Г. Тсслінова, В.В. Курейчика, Є.Ю. Павленко, однак питання застосування методів оцінки допустимих відхилів вхідних параметрів кіберфізичних розглянуто недостатньо у вищезгаданих роботах і потребує детального аналізу, що буде обумовлено в даній роботі.

Сучасні атаки на кіберфізічні системи відбуваються одночасно на декількох рівнях – від незаконного втручання в системні компоненти на фізичному рівні, до експлуатації інформаційних вразливостей на рівні комп'ютерної мережі та датчиків контролю роботи кіберфізичних систем. При цьому самі атаки стають складними, багатокроковими і розтягнутими в часі, а також враховують особливості системи та її інфраструктуру.

Об'єктом дослідження є кіберфізичні системи, процес визначення несанкціонованого вторгнення в дані системи на основі характеристик самоподібності процесів, що в них відбуваються.

Предмет досліджень – моделі та методи визначення атак на кіберфізичні системи.

Мета роботи – аналіз та вибір найбільш універсального, інваріантного до типу атак методу визначення коректності роботи КФС.

Задачами даної роботи є огляд питань теоретичного аналізу і практичних рекомендацій:

1) огляд предметної області питань забезпечення інформаційної безпеки КФС;

2) аналіз моделей та методів інформаційних систем для вирішення питань забезпечення інформаційної безпеки КФС;

3) розгляд обраного методу виявлення порушень безпеки КФС, заснованого на аналізі самоподібності процесів, та його удосконалень, в рамках задач наукових досліджень.

Виклад основного матеріалу. Кіберфізичні системи (КФС) інтегрують фізичні та інтелектуальні компоненти при виконанні певних виробничих процесів. З огляду на збільшення кількості кіберфізичних систем в усіх критичних галузях інфраструктури, як було зазначено у вступі, збільшенням можливостей шкідливого впливу на подібні системи шляхом фізичної чи інформаційної атаки на її компоненти, постає питання огляду предметної області забезпечення інформаційної безпеки подібних систем та обумовлюється актуальність досліджень даної предметної області.

За результатами експерименту, наведеному автором Л.В. Сухостат [4; 9] комбінація автоенкодеру та мережі глибокого навчання показала кращі результати виявлення атак ніж метод логістичної регресії та метод виявлення атак на основі згорткових нейронних мереж. Точність навчання пропонованого методу досягла 68.5%, що є високим показником зважаючи на варіативність класів атак.

Метод розпізнав 7 окремих підкласів атак та нормальний стан системи, на відміну від інших методів.

Проте, описаний вище метод не враховує різнорідність вхідних параметрів, відсутній аналіз застосовності методу при більшій кількості атак, та зазначається складність навчання методу при великій кількості варіацій вхідних критеріїв навчання. Отже, запропонований в роботі автора Л.В. Сухостат метод має недоліки при розв'язанні складної задачі визначення атак на кіберфізичні системи, через які даний метод не обирається як пріоритетний для виконання завдань даної наукової роботи.

У дисертаційній роботі автора Е.Ю. Павленко, за тематикою забезпечення інформаційної безпеки кіберфізичних систем запропоновано метод забезпечення інформаційної безпеки КФС на основі принципу гомеостазу [5].

Зазначається, що КФС являють собою замкнуту систему, що реалізує деяку цільову функцію (наприклад, функцію автоматичного очищення води, реалізованої в кілька взаємопов'язаних етапів). Наявність цільової функції системи обумовлює періодичність процесів, що в ній відбуваються.

Оскільки реалізовані КФС процеси є періодичними, робиться висновок про те, що потоки даних,

генерованих приладами КФС, як то сенсори параметрів навколишнього середовища, являють собою періодичні часові ряди, що володіють властивістю самоподібності, що доведено в роботах низки вітчизняних та закордонних авторів, (І.В. Мельник, О.І. Шелухін та ін.). Таким чином, пропонується оцінка самоподібності таких часових рядів, що дозволить зробити висновок про коректність роботи системи чи порушення в її роботі.

За результатами аналізу робіт Е.Ю. Павленка, І.В. Мельника, Л.О. Кіріченко було обрано фрактальні методи оцінки само подібності, для розв'язання наявних проблем існуючих методів визначення порушень безпеки КФС:

1. Фрактальні методи.

До фрактальних методів відноситься розрахунок показника Херста – *H*. Даний параметр вказує на ступінь самоподібності процесу. Значення параметру *H* близьке до одиниці, вказує на фрактальні властивості процесу. Показник Херста обчислюється за допомогою *R* / *S* статистики (так звана статистика нормованого розмаху). При цьому обчислюється розмах ряду – *R*, за формулою 1, та стандартне відхилення *S* за формулою 2.

$$R = \min_{1\le u\le N}\sum_{i=1}^{u}(x_i - X_{cp}) - \min_{1\le u\le N}\sum_{i=1}^{u}\left(x_i - X_{cp}\right) \qquad (1)$$

$$S = \sqrt{\frac{1}{N}\sum_{i=1}^{u}\left(x_i - X_{cp}\right)^2} \qquad (2)$$

де – середнє арифметичне ряду спостережень за *N* періодів.

Показник Херста *H* можна розрахувати за формулою 3:

$$H = \log\frac{R/S}{\log(\alpha N)}, \qquad (3)$$

де α – задана константа, α > 0. Застосування коефіцієнта Херста для оцінки самоподібності даних, генерованих компонентами КФС, описано в роботах [5].

Низький показник *H* вказує на відсутність властивості самоподібності, і як висновок – на наявність кібератаки.

Показник Гельдера. Даний показник також використовують для визначення самоподібності як фрактальної властивості процесів, беручи до уваги що підпроцес володіє властивостями процесу в цілому та зміна в структурі роботи підпроцесу впливає і на зміну роботи цілого процесу.

Мультифрактальні властивості відображають мультифрактальний спектр Лежандра та показник Гельдера, зміна з плином часу якого дозволяє відслідкувати зміни у властивостях перебігу процесу, як то порушення роботи в наслідок стороннього втручання в роботу системи [5].

Графічно мультифрактальний процес відображається у вигляді мультифрактального спектра Лежандра (рис. 1).

Лівій частині спектра відповідають ділянки часового ряду з глобальними (значними) відхиленнями, а правій – з локальними (незначними) відхиленнями [5].

Спостереження за змінами мультифрактальних властивостей досліджуваного процесу дозволить виявити порушення в його стаціонарній роботі, що може бути викликано кібератакою на КФС та її компоненти.

Зміна мультифрактальних властивостей може проявлятися зі зміною таких показників спектру:

1. Ширини спектру – $width_{right} = \alpha_{max} - \alpha_0$;
2. Висоти його правої та лівої гілок – $height_{left} = f(\alpha_0) - f(\alpha_{min})$ та $height_{right} = f(\alpha_{0max}) - f(\alpha_0)$.

Метрика, оцінююча ширину спектра, раніше вже застосовувалась для виявлення мережевих атак, та добре зарекомендувала себе для виявлення атак на КФС, проте кількість метрик даного методу може бути збільшена, для досягнення більшої інваріантності до видів кібератак на КФС.

2. Спектральні методи.

Для оцінки того, чи є даний процес довгостроково залежним в спектральній області, використовують поняття спектральної щільності. Тоді слабо стаціонарний часовий ряд має довгострокову залежність, коли виконується умова 4:

$$f(\lambda) \sim C_f|\lambda|^{-\beta}, \lambda \to 0, \qquad (4)$$

Спектральна щільність $f(\lambda)$, розраховується за формулою 5.

$$f(\lambda) = \frac{\sigma^2}{2\pi}\sum_{k=-\infty}^{\infty} p(k)e^{ik\lambda} \qquad (5)$$

Спектральна щільність дозволяє відобразити зв'язок процесів з довгостроковою залежністю та самоподібних процесів.

Описаний в роботі Павленка Є.Ю. на тему забезпечення безпеки кіберфізичних систем на основі принципу гомеостазу метод визначення самоподібності процесів кіберфізичних систем добре досліджений в роботах вітчизняних авторів, універсальний до типів кіберфізичних систем, інваріантний до кількості атак та добре зарекомендував себе в практичній сфері визначення кібератак. Проте метод має недоліки

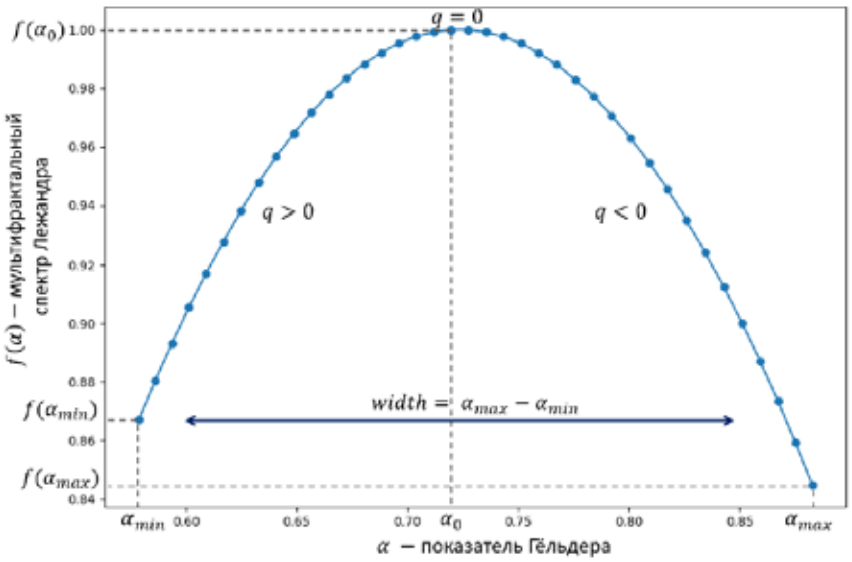

Рис. 1. Мультифрактальний спектр Лежандра

Джерело: [5]

пов'язані з відсутністю аналізу впливів варіацій вхідних параметрів та аналізі допустимих меж відхилень вхідних параметрів .

Стохастичний процес *X(t)* є статистично самоподібним, якщо $a^{-H}X(at)$, володіє тими ж статистичними характеристиками другого порядку, що і *X(t)*. Довгострокова залежність означає повільне (гіперболічне) спадання в часі автокореляційної функції випадкового процесу.

При мультифрактальному аналізі самоподібності процесів на основі показника Херста, процес вважають самоподібним, при розрахованому коефіцієнті $0.5 < H < 1$, (ряд демонструє персистентну (трендостійку) поведінку). При $H = 0.5$ роблять висновок, що властивість самоподібності процесу втрачається [6].

Детальний алгоритм розрахунку коефіцієнта Херста наведений нижче:

1. Формується матриця зчитаних значень сенсорів кіберфізичної системи.

2. Оскільки випадковий процес не є стаціонарним, розраховуються значення математичного очікування та середнього квадратичного відхилення по всій вибірці:

$$M_N = \frac{1}{N}\cdot\sum_{k=1}^{N} X_k, S_N = \sqrt{\frac{1}{N}\cdot\sum_{k=1}^{N}\left(X_j - M\right)^2} \qquad (6)$$

3. По відомому значенню математичного очікування визначається інтегральне відхилення:

$$D_j = \sum_{k=1}^{j} X_k - j\cdot M, j = 1\ldots N. \qquad (7)$$

4. По значенням інтегрального відхилення визначається параметр змінності випадкового процесу R_N, котрий залежить від кількості елементів вибірки *N*:

$$R_N = \max_{1<j<N}\left(D_j\right) - \min_{1<j<N}\left(D_j\right), \qquad (8)$$

5. Далі, для довгострокової залежності визначається параметр Херста *H*.

$$H = \frac{\ln\left(\frac{R}{S}\right)}{\ln\left(\frac{N}{2}\right)}, \qquad (9)$$

Аналізуючи показник *H* роблять висновок про самоподібність процесів часових рядів.

На основі даного математичного апарату пропонується аналіз часових рядів параметрів роботи КФС на самоподібність, для визначення атаки на КФС.

Поліпшенням даного методу має стати аналіз допустимих відхилів вхідних параметрів $X_k \pm \varepsilon$, входження даних відхилень до інтервалів надійності, обґрунтованих статистичними критеріями результатів обробки великих даних часових рядів, що є результатом природних факторів (а не атак на КФС), що стане нововведенням в області визначень порушень роботи КФС, та застосування показника Гельдера, для більш точного виявлення порушень інформаційної безпеки кіберфізичних систем.

Показник Гельдера можна визначити виконуючи перетворення Лежандра для деякої функції *f(α)*.

$$f(\alpha) = \min_{q}\left(q\alpha - \tau(q)\right) \qquad (10)$$

Перетворення Лежандра (10) можна використати, для відтворення мультифрактального спектра по скейлинговому показнику $\tau(q)$. Якщо функція τ диференційована, то можна перейти до параметризації мультифрактального спектра в термінах $\tau(q)$:

$$f(\alpha) = q\tau'(q) - \tau(q) \qquad (11)$$

Прикладом аналізу реальних показників сенсорів, є аналіз фрактальних властивостей часових рядів показань приладів, пов'язаних із сонячною активністю наведений у роботі [6].

Одним з приладів, що реагує на сонячну активність, є надлегкі крутильні ваги (КВ). З їх допомогою Ш. Кулон встановив закон взаємодії електричних зарядів, а Г. Кавендіш виміряв величину світової гравітаційної постійної.

У роботах українського науковця А.Ф. Пугача [6], вперше були проведені тривалі однорідні спостереження за поведінкою надлегких КВ, забезпечених автоматичною системою реєстрації даних. Показання КВ реєструвалися кожну хвилину. Часові ряди показників, знятих з крутильних вагів в експерименті роботи [6] наведено на рис. 2.

У роботі [6] проведено аналіз часових рядів, отриманих в різні періоди року, який показав наявність явно виражених мультифрактальних властивостей. На рис. 3 показані мультифрактальні спектри, отримані методом мультифрактального аналізу рядів дводобових спостережень (2880 значень), типові для лютого, травня та жовтня. Це дозволяє роботи висновки про сезонність та самоподібність процесів, що відбуваються у високих шарах атмосфери, на котрі впливає низка факторів.

При зміні параметрів стану системи, змінюються показники кривих Херста та Гельдера, зміщуються мультифрактальний спектр, змінюється ширина гілок спектра, мінімальне та мак-

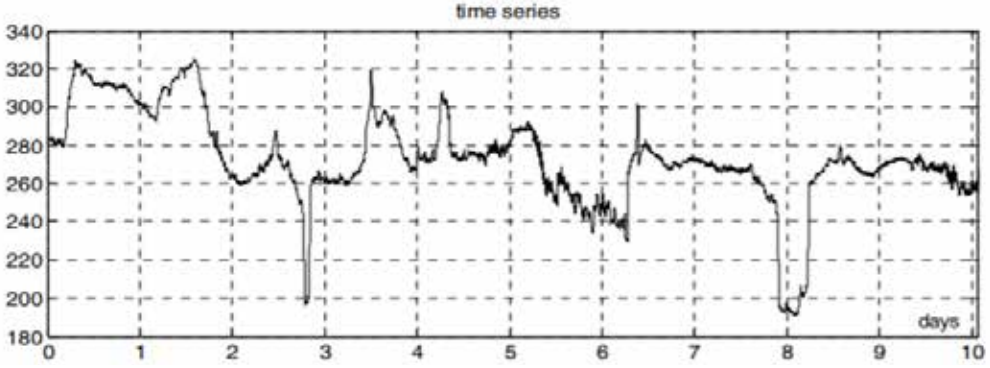

Рис. 2. Часовий ряд показників крутильних вагів

Джерело: [6]

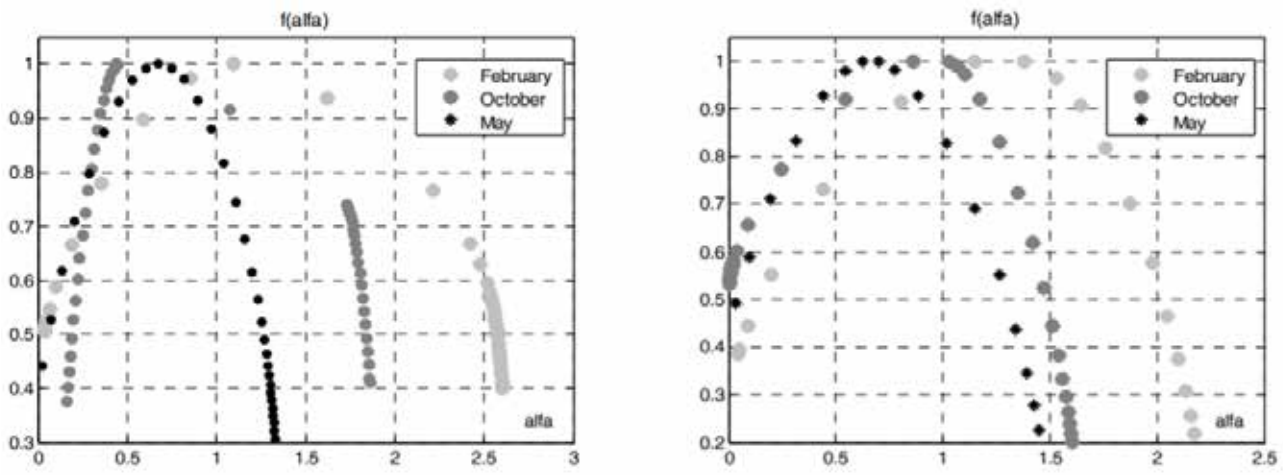

Рис. 3. Зміна фрактальних характеристик довготривалих процесів

Джерело: [6]

симальне значення α, що пропонується використовувати як критерій порушень нормальної роботи кіберфізичних систем.

Таким чином, в рамках подальших досліджень забезпечення безпеки КФС, пропонується застосування потужного апарату аналізу самоподібності процесів систем різної природи на основі визначення показників Херста та Гельдера, та визначення допустимих меж відхилень вхідних параметрів, для ефективного визначення атак на кіберфізичні системи та підвищення безпеки останніх, що обумовлено актуальністю даної роботи.

Питання оцінки впливу відхилень вхідних параметрів роботи методу визначення порушень роботи кіберфізичних систем на основі мультифрактального аналізу стало об'єктом подальших досліджень.

Описаний вище алгоритм визначення порушень безпеки є типовим для визначення порушень роботи кіберфізичних систем, став базою для пропонованого в розроблюваній роботі удосконаленого методу, що враховуватиме аналіз відхилень вхідних параметрів та робитиме коректування видачі алгоритмом звіту про виявлення порушень безпеки кіберфізичних систем.

Список літератури:

1. Котенко И.В. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров. *Вопросы кибербезопасности.* 2018. № 3(27). С. 29–36.
2. Самые громкие кибер-атаки на критические инфраструктуры. URL: https://habr.com/ru/company/panda/blog/316500/, 23.05.2020
3. Полтавцева М.А. Особенности применения технологий обработки больших данных в задачах обеспечения кибербезопасности. *Методы и технические средства обеспечения безопасности информации.* Санкт-Петербург : Изд-во политехнического университета, 2018. № 27. С. 4–7.
4. Сухостат Л.В. Обнаружение атак на киберфизические системы на основе глубокого обучения. Институт Информационных Технологий НАНА. Баку, 2018.
5. Павленко Е.Ю. Обеспечение информационной безопасности киберфизических систем на основе принципа гомеостаза. Дисс. на соискание ученой степени кандидата технических наук. Санкт-Петербургский политехнический университет Петра Великого. Санкт-Петербург, 2018. 183 с.
6. Кириченко Л.О. Радивилова Т.А. Фрактальный анализ реальных даннях. *International Journal "Information Content and Processing.* 2018. Volume 5, Number 2. Pp. 142–152.

References:

1. Kotenko, I.V. (2018). Kompleksnyy podkhod k obespecheniyu bezopasnosti kiberfizicheskikh sistem na osnove mikrokontrollerov [An integrated approach to ensuring the security of cyber-physical systems based on microcontrollers]. *Voprosy kiberbezopasnosti,* no. 3(27), pp. 29–36.
2. The loudest cyber attacks on critical infrastructures. URL: https://habr.com/ru/company/panda/blog/316500/
3. Poltavtseva, M.A. (2018). Osobennosti primeneniya tekhnologiy obrabotki bol'shikh dannykh v zadachakh obespecheniya kiberbezopasnosti [Features of the application of big data processing technologies in the tasks of ensuring cybersecurity]. *Metody i tekhnicheskiye sredstva obespecheniya bezopasnosti informatsii.* SPb.: Izd-vo politekhnicheskogo universiteta, no. 27, pp. 4–7.
4. Sukhostat, L.V. (2018). Obnaruzheniye atak na kiberfizicheskiye sistemy na osnove glubokogo obucheniya [Detection of attacks on cyber-physical systems based on deep learning] Institut Informatsionnykh Tekhnologiy NANA. Baku, 2018.
5. Pavlenko, E.Yu. (2018). Obespecheniye informatsionnoy bezopasnosti kiberfizicheskikh sistem na osnove printsipa gomeostaza [Ensuring information security of cyber-physical systems based on the principle of homeostasis]. PhD for the degree of candidate of technical sciences. St. Petersburg, 183 p.
6. Kirichenko, L.O., & Radivilova, T.A. (2018). Fraktal'nyy analiz real'nykh dannykh [Fractal analysis of real data]. *International Journal "Information Content and Processing*", vol. 5, no. 2, pp. 142–152.