ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

УДК 621.548:004.77.056 **doi: 10.32620/reks.2021.4.11**

І. І. ФУРСОВ, О. В. ШМАТКО

Національний технічний університет «Харківський політехнічний інститут», Україна

АНАЛІЗ СТАТИСТИЧНИХ ПОКАЗНИКІВ ДИСПЕРСІЇ, АСИМЕТРІЇ ТА ЕКСЦЕСУ ПРИ ВИЗНАЧЕННІ ПОРУШЕНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ ВІТРОВИХ ГЕНЕРАТОРІВ

Активне впровадження інтелектуальних систем, що тісно взаємодіють з фізичними процесами з метою для вирішення широкого спектру різноманітних завдань життєдіяльності людини, обумовлює підвищення актуальності аналізу ризиків, пов'язаних з функціонуванням таких систем. Подібні гібридні складні інтелектуальні системи відносять до класу кіберфізичних систем (КФС). Порушення безпеки КФС, викликані стороннім втручанням в інформаційний потік, здатні призвести до економічних збитків, екологічних загроз і загроз життю і здоров'ю людини. Значне зростання інцидентів порушення безпеки КФС вітрових генераторів обумовлює актуальність досліджень методів захисту подібних систем. ***Предметом*** *вивчення у статті є процес визначення порушень інформаційної безпеки КФС вітрового генератора на основі аналізу статистичних показників дисперсії, асиметрії та ексцесу вхідного параметру «Потужність», зібраного сенсорами КФС.* ***Метою*** *є розробка алгоритму визначення порушень інформаційної безпеки КФС вітрових генераторів з використанням методів аналізу статистичних показників дисперсії, асиметрії та ексцесу.* ***Завдання:*** *формалізувати процес визначення фальсифікованих даних у інформаційному потоці КФС; визначити переваги та недоліки існуючих методів забезпечення інформаційної безпеки КФС; визначити ступінь змін статистичних показників дисперсії, асиметрії та ексцесу вибірки параметру «Потужність» вітрового генератора при наявності дезінформації у інформаційному потоці; проаналізувати можливість доповнення та подальшого вдосконалення запропонованого алгоритму. Використовуваними* ***методами*** *є: аналіз статистичних показників дисперсії, асиметрії та ексцесу вибірки параметру «Потужність» вітрового генератора. Отримані такі результати: розглянуто загальні характеристики КФС та особливості функціонування КФС вітрового генератора, як об'єкта досліджень даної роботи; розроблено початковий алгоритм визначення порушень інформаційної безпеки КФС вітрового генератора на основі використання статистичних показників дисперсії, асиметрії та ексцесу; визначено факт штучної підміни даних параметра «Потужність» інформаційного потоку КФС вітрового генератора; запропоновано шляхи покращення розробленого алгоритму з використанням однофакторного дисперсійного аналізу, бутстреп-методів.* ***Висновки.*** *Наукова новизна отриманих результатів полягає у: розробці вдосконаленого алгоритму визначення факту фальсифікації даних у інформаційному потоці КФС на основі аналізу показників дисперсії, асиметрії та ексцесу; використанні статистичного методу при визначенні порушень безпеки КФС, аналізі недоліків існуючих методів визначення порушень безпеки КФС та можливості їх комплексного покращення. Також розглядаються питання можливості покращення розробленого методу та тестування методу у подальшому.*

Ключові слова: *інформаційна безпека; КФС; статистичні показники; дисперсія; асиметрія; ексцес.*

Вступ

Кіберфізичні системи являють собою складні інформаційні системи, що комбінують інформаційні процеси управління та фізичні процеси виробництва та взаємодії з навколишнім середовищем. Кіберфізичні системи стають все більш розповсюдженими та впроваджуються у великій кількості сфер життєдіяльності людини. Однією з властивостей кіберфізичних систем (КФС) є широкомасштабність, що означає використання великої мережі сенсорів, інформація з яких обробляється центром керування КФС. З огляду на це, питання захисту інформаційних потоків мережі КФС стає одним з найактуальніших на етапі проектування даних систем.

КФС доволі часто впроваджуються у рамках об'єктів критичної інфраструктури, зокрема, у сфері «розумних систем електропостачання» (РСЕ), забезпечення безпеки яких стає завданням регіонального або національного рівня. Об'єкти вітрових електростанцій дедалі частіше стають ціллю кібератак, що обумовлено зростаючим попитом на невичерпні ресурси енергії та значними капіталовкладеннями з боку держав у дану сферу енергетики [1]. Забезпе-

чення інформаційного захисту вітрових генераторів нівелює матеріальні збитки кібератак на них та пов'язані загрози безперебійного постачання електроенергії до споживачів, забезпечує стабільність розвитку даного сектора економіки держави.

Таким чином, **метою** даної роботи є розробка методу визначення порушень інформаційної безпеки КФС вітрового генератора з використанням статистичних показників дисперсії, асиметрії та ексцесу.

Проблеми безпеки КФС вітрових генераторів

Протягом останніх років кількість кібератак на об'єкти критичної інфраструктури неухильно зростає. За даними [2] кількість значимих кібератак складає 1120 випадків у 2020 році, з них до 40 % припадає на енергетичний сектор. Більшість атак на КФС обумовлені економічною зацікавленістю зловмисників та легкістю завдання прямих збитків навколишньому середовищу та життю чи здоров'ю людини у наслідок виходу з ладу частини системи електропостачання. «Розумні» системи електропостачання (РСЕ) є розвитком ідей інтеграції цифрових технологій у енергетичній сфері, та являють собою інтелектуальні мережі виробництва та розподілу відновлювальної або невичерпної енергії для потреб інфраструктури Smart-систем. Успішна кібератака на КФС вітрових генераторів здатна привести до серйозних економічних збитків, виходу з ладу вартісного обладнання, збоїв постачання електроенергії до кінцевого споживача. Серед чинників що обумовлюють підвищені вимоги до ефективності та надійності систем безпеки КФС вітрових генераторів, найбільш істотними є такі:

– велика кількість каналів інформації, дані яких обробляє КФС у процесі роботи;

– легкість фізичного втручання у інформаційний потік через незахищеність окремих частин КФС, протоколів передачі даних;

– загроза матеріальних збитків та здоров'я людини у випадку порушення інформаційної безпеки КФС.

Для початку аналізу проблем та методів забезпечення безпеки КФС вітрових генераторів, доцільно розглянути модель функціонування систем РСЕ з використанням вітрових генераторів, можливі шляхи втручання у систему та механізми дій зловмисника.

На рис. 1 наведено спрощену модель мережі РСЕ, що включає такі піддомени:

– піддомен енергопостачання;
– піддомен сервіс-провайдеру;
– піддомен розподілу електроенергії;
– піддомен споживачів;
– піддомен вимірювальних приладів.

Автор [3] виділяє такі основні частини мережі РСЕ:

– віддалені термінали (Remote Terminal Unit, RTU) для вводу службової інформації;

– інтелектуальні електронні маршрутизатори (ICS) для зв'язку операторів зі SCADA;

– SCADA-системи та система енергетичного менеджменту (Energy Management System, EMS);

– системи узгодження електрогенерації з регіональними комунікаційними організаціями;

– піддомен електропостачання (отримання інформації від сенсорів і вимірювальних приладів) для обміну з піддоменом сервіс-провайдерів (через оператора зв'язку із забезпеченням прийнятного

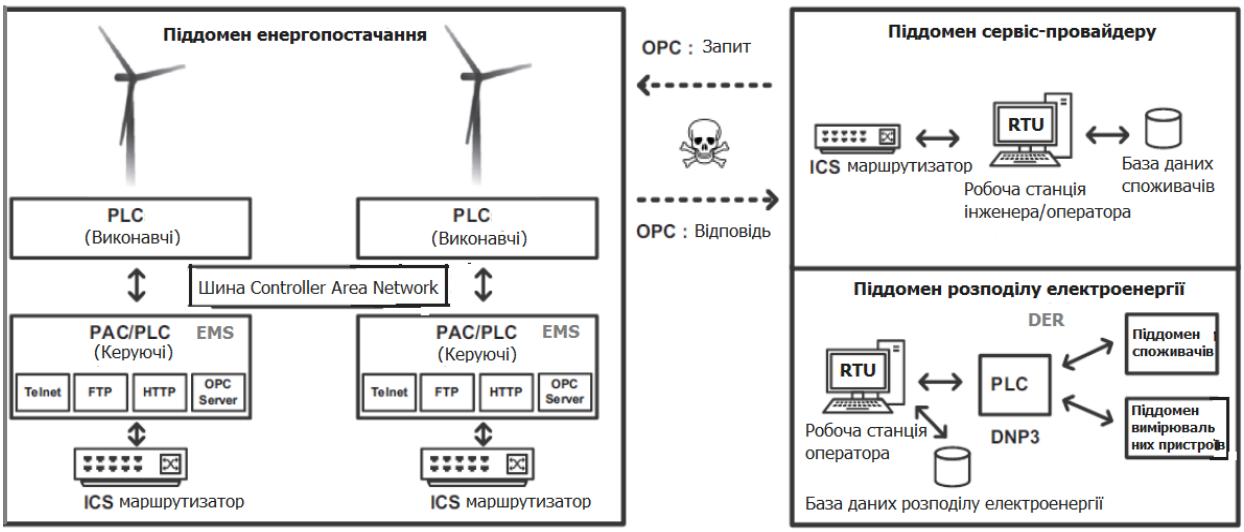


Рис. 1. Спрощена модель РСЕ

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

рівня кіберзахисту) доповнення, підготовки звітів і накопичення інформації;

– територіально-розподілені сенсори та вимірювальні прилади для роботи з розподіленими енергетичними ресурсами (Distributed Energy Resources, DER);

– OPC – являє собою набір прийнятих специфікацій, що забезпечують універсальний механізм обміну даними в системах контролю і управління. Більшість протоколів передачі даних добре задокументовані, зловмисник має доступ до нюансів роботи сполучних мережевих пристроїв. Фізичний доступ до ліній комутації мережевих пристроїв, зазвичай доступний для зловмисника.

– бази даних споживачів та розподілу електроенергії.

Автор [3] виділяє такі типи загроз «розумних» мереж електроспоживання, об'єктами яких є вітрові електростанції:

– загрози безпеки рівня платформ PCE;
– загрози безпеки рівню додатків;
– загрози мережевого рівня;
– загрози термінальних пристроїв.

У роботі [3] зазначено, що активи платформ, які підтримують сервіси PCE, належать сервіс-провайдеру. Вони включають систему керування енергоресурсами (EMS), системи керування даними вимірювальних пристроїв (MDMS). Виділено такі загрози безпеки для платформ PCE:

– атаки типу DDoS. Розподілена атака відмови в обслуговуванні (DDoS) являє собою зловмисну спробу порушення нормальної роботи цільового сервера чи мережі, за допомогою переповнення трафіку мережі запитами від мережі скомпрометованих комп'ютерних систем [4].

– зараження вірусним програмним забезпеченням. Хакери активно використовують вірусне програмне забезпечення типу «Trojan» та «Worm» для отримання контролю за віддаленими електронними пристроями. «Trojan» — тип вірусного програмного забезпечення, що приховує справжню мету своєї діяльності за допомогою механізмів маскування. Даний тип комп'ютерного вірусу активно використовують зловмисники при атаках на КФС, зокрема вітрових електростанцій. З метою проникнення до цільового пристрою, вірус використовує такі засоби, як приховане завантаження, використання уразливостей, завантаження іншим шкідливим кодом або методи соціальної інженерії [5].

– розкриття і модифікація інформації, що обробляється і зберігається в сервісній платформі.

– розкриття і модифікація операційних даних, оброблюваних і збережених в сервісній платформі.

Сервіс-провайдер може передавати інформацію про використані сервісні послуги клієнтів через клієнтський термінал або інше мережеве обладнання (наприклад, через Інтернет) на рівні додатків PCE.

Загрози безпеки рівня додатків:

– несанкціоноване розкриття персональних даних клієнтів;

– несанкціоноване розкриття та модифікація інформації про використання електроенергії;

– несанкціоноване розкриття службової (сервісної) інформації.

Мережеві активи також стають об'єктом атак оскільки включають маршрутизатори, комутатори та ін..

Кожна частина інформаційної системи може бути скомпрометована, та є потенційною ціллю зловмисників, з огляду на важливість операційних даних та потоку даних сенсорів КФС, якими оперує центр управління енергосистеми. Фізичний доступ до електронних компонентів систем передачі даних вітрових генераторів обумовлюється масштабністю мережі КФС. Отримавши доступ до будь якого віддаленого терміналу керування, маршрутизатору та ін., зловмисник ініціює роботу шкідливого коду. Можливим сценарієм дій зловмисника є вимагання коштів від власників енергетичної компанії у обмін на розблокування обладнання. У разі відмови, можливе віддалене виконання команд, що призводять до повного виходу з ладу обладнання вітрового генератора [6].

Таким чином, було розглянуто основні структурні частини мережі PCE вітрових генераторів, зазначено основні шляхи втручання зловмисників у мережу.

Аналіз робіт на тему безпеки КФС вітрових генераторів

У таблиці 1 наведено результати огляду методів безпеки КФС вітрових генераторів, та інфраструктури PCE, що були детально розглянуті у джерелах [6 – 9].

За результатами огляду літератури було визначено основні методи визначення загроз безпеки КФС:

– ймовірнісно орієнтована ациклічна графова модель;

– методи ресамплінгу;

– модель на основі SMT-обчислень.

У цілому, перелічені вище методи забезпечення інформаційної безпеки КФС вітрових генераторів ураховують лише певну частину параметрів роботи системи. Проаналізовані методи не надають інформації про динаміку змін параметрів системи. Також не надаються рекомендації щодо динамічного реагування на фальсифіковані дані. Для розробки ефек-

Таблиця 1

Аналіз методів забезпечення безпеки КФС

Роботи з визначення методів забезпечення безпеки	Досліджені методи забезпечення інформаційної безпеки КФС	Аналіз роботи та результатів досліджень
«Bayesian Network Model for Accessing Safety and Security of Offshore Wind Farms» Ramirez-Agudelo O.H., Köpke C., Sill Torres F. [6]	Баєсова мережа (ймовірнісно орієнтована ациклічна графова модель)	Розглянута у роботі [6] модель інформаційної безпеки та функціонування КФС вітрових генераторів враховує цілий ряд критеріїв безпеки, таких як контроль персональних даних, адекватність даних сенсорів, людський фактор, за якими можливо визначити статус надійності та стабільності роботи системи. Розглянута модель дозволяє аналізувати загальне значення стану безпеки КФС вітрових генераторів, таких як дотримання вимог експлуатації, стан та охорона навколишнього середовища, запобігання нещасним випадкам та вірогідність кібератаки на систему. Розроблена модель на 20% збільшує точність розрахунку збоїв у системі, надає представлення системи у вигляді взаємозв'язків критеріїв безпеки.
«Power Grid Reliability Evaluation Considering Wind Farm Cyber Security and Ramping Events» Wu H., Liu J., Cui M., Liu X., Gao H. [7]	–	У роботі [7] розглянуто основні наслідки кібератак на вітрові електростанції. Аналізуються миттєва та довготривала недосконала типи атак: – миттєва атака в найгіршому випадку і довгострокова недосконала атака призводять до суттєвих наслідків для енергосистеми в різних часових масштабах. – частота відмов вітряної турбіни, що зазнала довготривалих недосконалих атак, швидко зростає, а її термін служби скорочується майже на 20%. – період пікового навантаження є вразливим для енергосистеми. Надійність системи виграє від інтелектуального керування темпів змін напруги, що знижує вплив кібератак.
«Zero-Dynamics Attack on Wind Turbines and Countermeasures Using Generalized Hold and Generalized Sampler» Kim D., Ryu K., Back J. [8]	Методи ресамплінгу	У роботі [8] розглядаються питання протидії атакам типу ZDA та не розглядаються інші варіанти атак. Для визначення факту стороннього втручання у інформаційний потік КФС вітрового генератора використовуються методи ресамплінгу, створення штучних вибірок на основі базової, для виявлення неадекватних змін вибірки. Метод дозволяє виявляти фальсифіковані значення лише за певним, чутливим до змін навколишнього середовища, параметром системи.
«Cyber Threat Analysis Framework for the Wind Energy Based Power System» Datta A., Ashiqur Rahman M. [9]	Модель на основі SMT-обчислень	У роботі [9] наведені переваги використання запропонованого SMT-методу, що базується на задачах виконуваності логічних формул. Завдяки запропонованому методу досягається урахування великої кількості варіантів загроз для КФС вітрових генераторів, наводиться теоретичні графіки росту складності обчислень при збільшенні числа турбін вітрових генераторів у рамках від 200 до 400 одиниць. Зазначено збільшення числа векторів атак на мережу вітрових генераторів при збільшенні числа турбін та більший ризик втрат електроенергії у випадку атаки на комплекс вітрових генераторів.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

тивного методу визначення порушень інформаційної безпеки КФС вітрових генераторів, доцільно використовувати комплекс змінних, поведінка яких з плином часу підкоряється певному закону, що заздалегідь відомий лише фахівцям безпеки та проектувальникам КФС. Даний факт не був досліджений у роботах [6–9], також заслуговує додаткової уваги, та пропонується до розгляду у рамках дослідження застосування статистичних методів для визначення фальсифікованих даних у інформаційному потоці КФС вітрових генераторів. Окремо слід зазначити роботи [10, 11], присвячені питанням оцінки вірогідності атак на Web-додатки та мережі передачі даних, на основі використання дерев атак та нечітких обчислень. Підходи зазначені у роботах [10, 11] з певною модифікацією зручно використовувати для оцінки вірогідності атак на КФС вітрових генераторів, у разі використання системою безпеки КФС методу, розглянутого у даній роботі.

З метою удосконалення існуючих методів визначення атаки на інформаційний потік КФС, при постійному ускладненні сценаріїв та стратегій атак зловмисника, у даний роботі пропонується статистичний метод визначення порушень безпеки КФС вітрових генераторів. Даний метод недостатньо висвітлений у сучасних джерелах, присвячених кібербезпеці, у той же час активно застосовується при моделюванні змін окремих параметрів КФС, з метою прогнозування окремих станів КФС та навколишнього середовища та оптимізації роботи КФС [12]. Таким чином, статистичний метод пропонується використати для визначення дезінформації у інформаційному потоці КФС вітрового генератора, за допомогою кількісної оцінки та порівнянні окремих статистичних параметрів при нормальному стані системи та у стані порушення безпеки.

Як правило, оптимальну комбінацію факторів, що суттєво впливають на результуючу ознаку КФС, визначають експериментально, шляхом зміни комбінації вхідних параметрів. У випадку багатокомпонентної системи, така стратегія призведе до суттєвих матеріальних або часових втрат. Виникає проблема розробки таких моделей, які сприяли б швидкому визначенню ключових факторів, що слугували б індикаторами втручань у інформаційних потік КФС

Будь яке втручання у інформаційний потік КФС залишає за собою цифровий слід, а саме:

– аномальні значення параметрів навколишнього середовища;

– різкі коливання параметрів що надходять до КФС;

– відсутність зміни параметрів з плином часу.

На основі сукупності перелічених вище ознак пропонується розробити комплексний метод дослідження інформаційного потоку на дезінформацію. Задачами роботи є огляд об’єкту досліджень, аналіз загроз РСЕ, аналіз та дослідження використання статистичних показників дисперсії, асиметрії та ексцесу параметру «Потужність» КФС вітрового генератора, що складатимуть частину загального алгоритму статистичного аналізу інформаційного потоку КФС на дезінформацію та аналіз можливості подальших досліджень статистичних методів у області визначення атак на КФС.

Опис об’єкта досліджень

Існує велика кількість КФС, аналіз інформаційного потоку яких можна застосувати для розв’язку задачі виявлення порушень безпеки КФС. Інформація, зібрана мережею сенсорів КФС, являє собою сукупність масивів даних різних параметрів роботи обладнання та даних стану навколишнього середовища. У рамках даної роботи було розглянуто визначення дезінформації у системі КФС **вітрового генератора**, що є частиною розумної електромережі Smart Grid, основним завданням якої є інтелектуальний підхід до виробітку та розподілу виробленої електроенергії між «розумними» споживачами.

КФС вітрового генератора оброблює дані стану навколишнього середовища, для налаштування та коректного функціонування фізичних компонент установки. Інформація про стан навколишнього середовища та параметри роботи вітрового генератора була зібрана та надана до вільного доступу ресурсом [13].

Інформаційний потік КФС вітрового генератора представлений такими даними сенсорів, як: продуктивна потужність (далі, «Потужність»), швидкість вітру, коефіцієнт передачі енергії, кут вітру.

Кожен з розглянутих параметрів відповідає певному впливу навколишнього середовища на виробіток електроенергії або стану компонент фізичної установки КФС вітрового генератора. Більш детальні моделі можуть включати більше параметрів, таких як нагрів турбін, що зменшує ККД установки, показники коливань башти та турбіни, що негативно впливають на ефективність роботи, установки та ресурс її роботи. Проте дані параметри не змінюють основний підхід до забезпечення безпеки інформаційного потоку, для аналізу достовірності даних, що надходять до КФС, тому приймаються надлишковими у рамках даного дослідження.

Цільовою функцією роботи КФС вітрового генератора є функція потужності електроенергії. Параметр «Потужність» залежить від низки факторів, таких як сила вітру у районі роботи башти, кут вітру, коливання башти та ін.

Відповідно до формули для визначення потужності вітрового генератора необхідно мати таку інформацію [14]:

$$P = \frac{1}{2} \cdot A \cdot \rho_\alpha \cdot v^3, \quad (1)$$

де A – площа крил генератора,

ρ_α – густина повітря,

v – швидкість вітру.

Таким чином, для забезпечення певного рівня обсягу енергії, виробленої вітровим генератором, необхідно встановлювати вітровий генератор у місцевості, умови навколишнього середовища якої максимізуватимуть потужність генератора, тобто місцевості де превалюють сильні вітри.

У разі виникнення порушень інформаційної безпеки КФС вітрового генератора, спричинених діями хакера, існують такі варіанти розвитку подій:

1. Фальсифікація даних параметру «Потужність». Наслідок порушення безпеки – невірний розподіл потужності виробленої електроенергії, збитки споживачів електроенергії.

2. Фальсифікація даних навколишнього середовища з метою невірної конфігурації турбін генератора. Наприклад, при фальсифікації параметра «кут вітру», центр управління КФС приймає рішення про автоматичну зміну кута нахилу башти вітрового генератора, що призводить до втрат виробленої потужності.

3. Ввід у центр керування КФС шаблонів імітації нормального стану навколишнього середовища. При даному сценарії можливе завдання фізичної шкоди частинам вітрового генератора, у той час як центр керування отримуватиме фіктивні дані про нормальний стан системи. Кожен з описаних сценаріїв атак на КФС вітрового генератора включає етап підміни даних сенсорів.

Зловмисник має безліч шляхів виконання даної операції, від використання вірусного програмного забезпечення до перехоплення пакетів даних, що надходять від сенсорів КФС. Визначення факту даної підміни становить основну задачу роботи. Оскільки заздалегідь невідомо, яку стратегією порушень безпеки КФС використає зловмисник, постає питання розробки універсального до типів атак методу. Розроблений метод має включати аналіз окремих показників інформаційного потоку, динаміка змін яких є аномальною для даного стану системи. Ще однією особливістю розроблюваного методу має стати можливість порівняння прогнозованих значень параметрів навколишнього середовища із фактичними для подальшого висновку про наявність дезінформації у системі.

Алгоритм визначення загроз інформаційної безпеки КФС вітрового генератора включає такі кроки:

1. Збір даних параметрів «потужність», «сила вітру», «кут вітру», «коефіцієнт передачі» для нормального стану системи. Зібрані дані підтверджуються незалежними спостереженнями.

2. Формування звіту по описовим статистикам кожного із зібраних параметрів сценарію нормального стану системи.

3. Побудова графіків відповідності нормальному розподілу зібраних параметрів у нормальному стані системи.

4. Зміна стану системи, штучна фальсифікація значень окремих параметрів. Моделювання стану загрози інформаційної безпеки КФС.

5. Формування звіту по описовим статистикам кожного з параметрів для стану системи у випадку наявності дезінформації.

6. Побудова графіків відповідності нормальному розподілу зібраних параметрів системи у випадку наявності дезінформації.

7. Порівняння результатів, запис значень окремих описових статистик аналізованих параметрів та показників ексцесу та асиметрії, графіків відповідності нормальному розподілу.

8. Формування бази даних випадків атак на інформаційний потік. Формування значень відхилень описових статистик за якими проводиться подальші висновки щодо наявності дезінформації у інформаційному потоці КФС вітрового генератора.

На основі даного алгоритму пропонується виконувати пошук порушень безпеки КФС вітрового генератора.

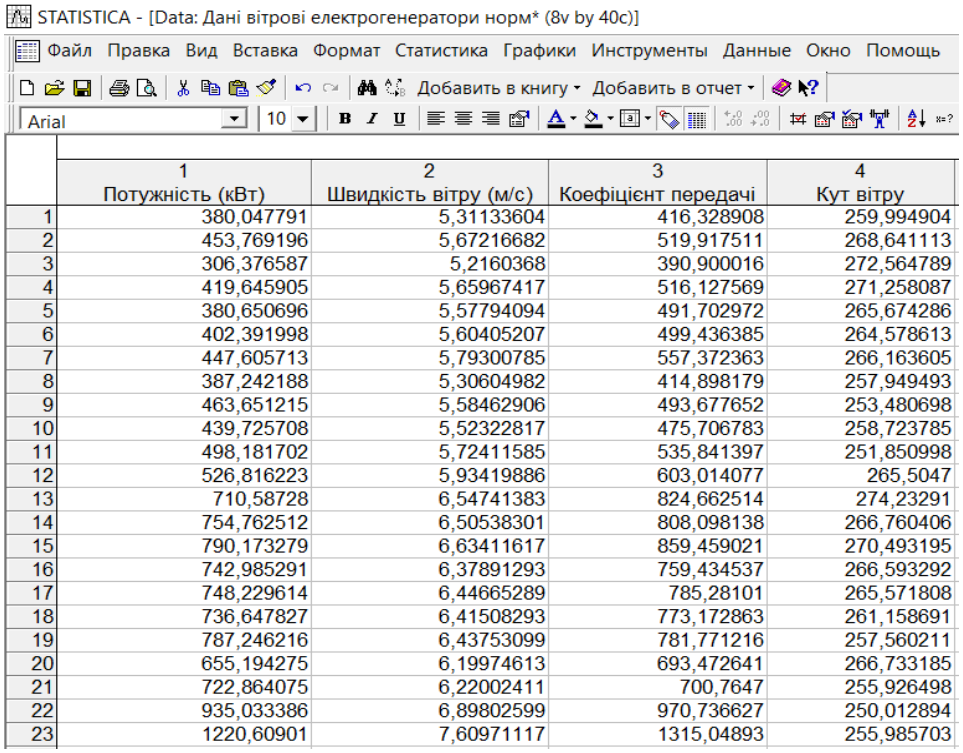
Вхідні дані нормального стану системи КФС вітрового генератора наведено на рисунку 2. При виконанні розрахунків використовувався програмний пакет STATISTICA 6.

Вхідний масив даних перевіряється на наявність дезінформації, що у випадку порушення інформаційної безпеки на об’єкті вітрового генератора, призведе до подальших збоїв роботи КФС.

Статистичні методи дозволяють дослідити відхил від нормальних значень досліджуваного параметру, у той же час аналіз має проводитись і для початкової вибірки. У якості критеріїв для оцінки змін у значеннях досліджуваних параметрів було обрано дисперсію, ексцес та асиметрію вибірки.

Дані параметри є інформативними для аналізу наявності викидів, діагностування нестандартного поводження системи, проте слід зауважити, що дані параметри не можуть бути використані для визначення імітації нормальної роботи системи.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)



	1 Потужність (кВт)	2 Швидкість вітру (м/с)	3 Коефіцієнт передачі	4 Кут вітру
1	380,047791	5,31133604	416,328908	259,994904
2	453,769196	5,67216682	519,917511	268,641113
3	306,376587	5,2160368	390,900016	272,564789
4	419,645905	5,65967417	516,127569	271,258087
5	380,650696	5,57794094	491,702972	265,674286
6	402,391998	5,60405207	499,436385	264,578613
7	447,605713	5,79300785	557,372363	266,163605
8	387,242188	5,30604982	414,898179	257,949493
9	463,651215	5,58462906	493,677652	253,480698
10	439,725708	5,52322817	475,706783	258,723785
11	498,181702	5,72411585	535,841397	251,850998
12	526,816223	5,93419886	603,014077	265,5047
13	710,58728	6,54741383	824,662514	274,23291
14	754,762512	6,50538301	808,098138	266,760406
15	790,173279	6,63411617	859,459021	270,493195
16	742,985291	6,37891293	759,434537	266,593292
17	748,229614	6,44665289	785,28101	265,571808
18	736,647827	6,41508293	773,172863	261,158691
19	787,246216	6,43753099	781,771216	257,560211
20	655,194275	6,19974613	693,472641	266,733185
21	722,864075	6,22002411	700,7647	255,926498
22	935,033386	6,89802599	970,736627	250,012894
23	1220,60901	7,60971117	1315,04893	255,985703

Рис. 2. Вхідні дані роботи вітрового генератора зібрані з інтервалом 5 хвилин

На рисунку 3 наведено масив даних для випадку штучної зміни даних. Жовтим кольором позначені окремі значення параметрів, що були фальсифіковані.

Результати досліджень

Відповідно до отриманих результатів аналізу даних роботи КФС вітрового генератора, представлених на рисунку 4, визначено такі характеристики параметру «Потужність»:

1. Дисперсія параметру «Потужність» склала 129984,0 що є великим значенням з урахуванням нормального стану системи, подібні зміни параметру вказують на нерівномірність виробітку електроенергії через добові зміни швидкості вітру у районі турбіни.

2. Коефіцієнт асиметрії (Skewness) дорівнює 0,72, що вказує на відхил від нормального закону розподілу даної величини.

3. Ексцес (Kurtosis) дорівнює 0,06, що говорить про невелику кількість відхилень значень параметрів.

	1 **Потужність (кВт)**	2 Швидкість вітру (м/с)	3 Коефіцієнт передачі	4 Кут вітру
1	100	2,1	1	100
2	102,1	2,15	1	100
3	106,8999	2,1	2	120
4	108,0001	2,5	2	120
5	100	5,57794094	491,702972	265,674286
6	103	5,60405207	499,436385	264,578613
7	109	5,79300785	557,372363	266,163605
8	387,242188	5,30604982	414,898179	257,949493
9	100	5,58462906	493,677652	253,480698
10	100	5,52322817	475,706783	258,723785
11	110	5,72411585	535,841397	251,850998
12	526,816223	5,93419886	603,014077	265,5047
13	710,58728	6,54741383	824,662514	274,23291
14	754,762512	6,50538301	808,098138	266,760406
15	790,173279	6,63411617	859,459021	270,493195
16	742,985291	6,37891293	759,434537	266,593292
17	748,229614	6,44665289	785,28101	265,571808
18	736,647827	6,41508293	773,172863	261,158691
19	787,246216	6,43753099	781,771216	257,560211
20	820	6,19974613	693,472641	266,733185

Рис. 3. Штучно змінені дані у вхідному потоці

Descriptive Statistics (Дані вітрові електрогенератори)

Variable	Valid N	Mean	Mode	Minimum	Maximum
Потужність (кВт)	40	812,3462	Multiple	306,3766	1724,488
Швидкість вітру (м/с)	40	6,5261	Multiple	5,2160	8,376
Коефіцієнт передачі	40	855,9537	Multiple	390,9000	1752,200
Кут вітру	40	250,4392	Multiple	185,2734	274,233

Variable	Variance	Std.Dev.	Standard Error	Skewness	Kurtosis
Потужність (кВт)	129984,1	360,5331	57,00530	0,72293	0,061335
Швидкість вітру (м/с)	0,7	0,8406	0,13291	0,35250	-0,589440
Коефіцієнт передачі	123223,4	351,0319	55,50301	0,80940	0,167081
Кут вітру	464,3	21,5488	3,40716	-1,87315	3,610894

Рис. 4. Результати описових статистик параметру «Потужність» для нормального стану системи КФС вітрового генератора

Графік розподілу за нормальним законом параметру «Потужність», зібраного КФС вітрового генератора у стані без порушень інформаційної безпеки, надано на рисунку 5.

Результати розрахунку описових статистик дисперсії, асиметрії, ексцесу параметру «Потужність» вітрового генератора для стану фальсифікації даних наведено на рисунку 6.

Згідно результатів дослідження описової статистики для параметру «Потужність», для стану фальсифікації даних, отримали:

1. Дисперсія дорівнює 234133,2 що є більшим значенням ніж у дослідженні нормального стану системи, подібні зміни параметру вказують на нерівномірність виробітку розподілу параметру «Потужність» через можливе втручання у інформаційний потік.

2. Коефіцієнт асиметрії (Skewness) дорівнює 0,016, що вказує на відхил від нормального закону розподілу даної величини.

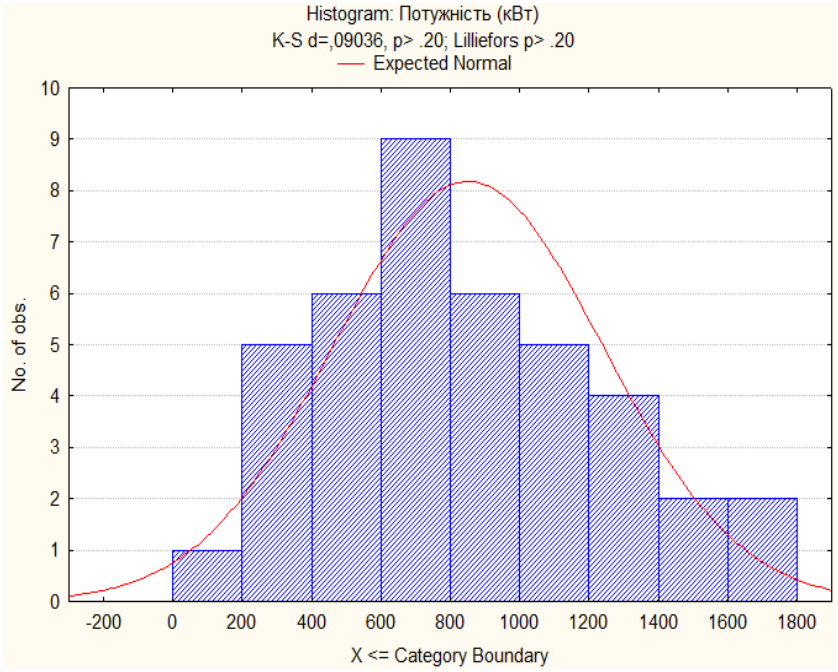


Рис. 5. Розподіл параметру «Потужність» за нормальним законом

Descriptive Statistics (Spreadsheet1)

Variable	Valid N	Mean	Median	Minimum	Maximum	Variance	Std.Dev.	Standard Error	Skewness	Std.Err. Skewness	Kurtosis
Потужність (кВт)	40	776,1685	788,7097	100,0000	1724,488	234133,2	483,8731	76,50705	-0,016901	0,373783	-0,857777

Рис. 6. Результати описових статистик параметру «Потужність» вітрового генератора для стану фальсифікації даних

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

3. Ексцес (Kurtosis) дорівнює –0,857, що говорить про велику кількість відхилень значень параметрів.

Графік розподілу за нормальним законом параметру «Потужність», зібраного КФС вітрового генератора у стані фальсифікації даних, надано на рисунку 7.

Спостерігаємо відхилення від нормального закону розподілу та результатів розподілу параметру «Потужність» у стані на рисунку 5, а саме наявнять аномальної кількості значень у інтервалі 0–200 кВт, спричинені порушенням інформаційної безпеки КФС вітрового генератора, наявністю хибних даних у інформаційному потоці КФС, які є потенційно небезпечними для функціонування фізичних компонент КФС у майбутньому. Таким чином, спочтерігаємо результативнсть методу при виявленні загроз безпеки КФС вітрових генератоів, навіть при незначних обсягах викривлених даних, що у досліді склали 5 рядків із 40 записів, що дорівнює 12,5 %.

Отже, при порівнянні значень статистичних параметрів дисперсії, асиметрії та ексцесу параметру «Потужність» КФС вітрового генератора, спостерігаємо суттєве збільшення розглянутих показників у випадку порушення інформаційної безпеки, до 80% абсолютного значення показника при викривленні незначної частини вихідних даних (частина фальсифікованих рядків у процесі досліду склала 12,5%). Відхилення від закону нормального розподілу випадкових величин параметру «Потужність» вітрового генератора, також є індикатором наявності фальсифікованих даних у інформаційному потоці КФС. Таким чином, у ході досліджень було визначено факт штучної фальсифікації даних на основі кількісної оцінки зміни основних статистичних показників вибірки даних параметра «Потужність» вітрового генератора.

У цілому, запропонований метод надає можливість ідентифікації втручань у інформаційний потік вітрового генератора з високою вірогідністю, є альтернативою застосувань методів ресамплінгу та графових ациклічних моделей, запропонованих у роботах [5, 7], так як окрім виявлення факту фальсифікації даних, метод дозволяє аналізувати нормальний стан системи та динаміку змін досліджуваних параметрів, чисельно досліджувати взаємозв'язок змін окремих факторів. На базі статистичних методів можливе проведення факторного експерименту, прогнозування значень параметрів на основі регресійної моделі нормального стану системи та стану фальсифікації даних, що є областю подальших досліджень.

Висновки

Збільшення кількості атак на КФС енергетичного сектору, зокрема об'єкти вітрових електростанцій, обумовлює необхідність пошуку ефективних методів виявлення порушень безпеки даних складних інтелектуальних систем. Великі об'єми даних, що надходять до КФС з навколишнього середовища чи її фізичних компонентів, обумовлюють склад-

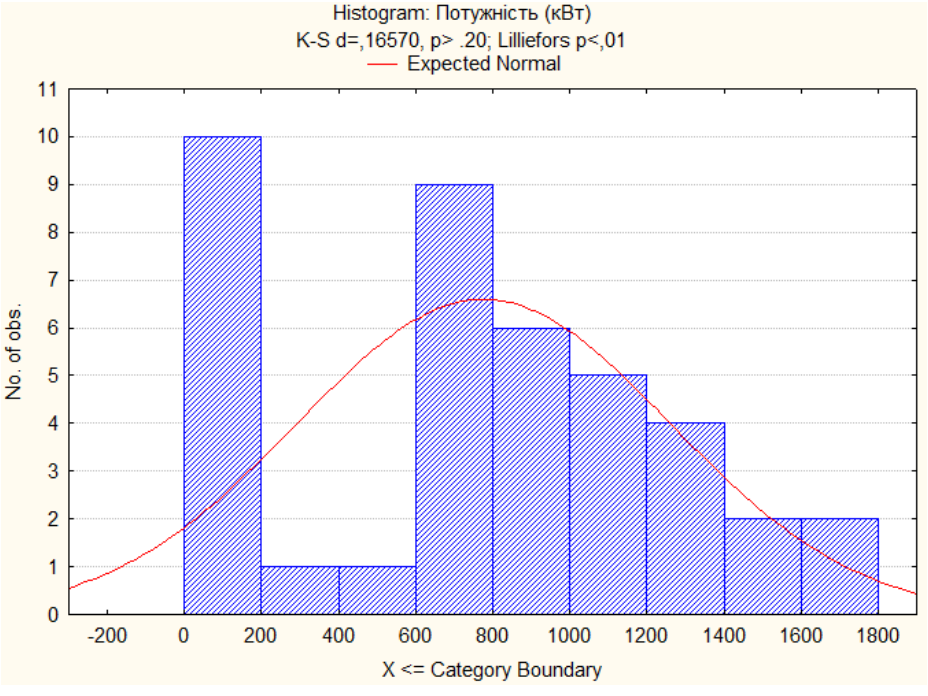


Рис. 7. Відповідність нормальному закону параметру «Потужність» для випадку фальсифікації даних

ність процесу визначення порушень інформаційної безпеки даних гібридних обчислювальних систем. Задачами роботи стали: огляд методів виявлення порушень інформаційної безпеки КФС, аналіз проблем захисту КФС вітрових генераторів, розробка алгоритму виявлення порушень безпеки КФС вітрових генераторів з використанням статистичного метода, виявлення змін статистичних показників дисперсії, асиметрії та ексцесу параметру «Потужність» КФС вітрового генератора у випадку фальсифікації даних. Використання статистичних методів недостатньо висвітлені у науковій літературі тематики визначення порушень безпеки КФС, проте математичний апарат даних методів знайшов широке застосування як при визначенні аномальних параметрів роботи об'єктів критичної інфраструктури, так і при прогнозуванні роботи складних фізичних та інтелектуальних систем.

За результатами роботи, у ході проведених досліджень, було виявлено суттєві зміни значень дисперсії, асиметрії та ексцесу, отриманими з розрахунку описових статистик вхідного параметру «Потужність» вітрового генератора.

Дисперсія параметру «Потужність» зросла з 129984 до 234133 тобто на 80%, коефіцієнт асиметрії змінився у межах від 0,72 до 0,016, ексцес у межах 0,06 до –0,857. Таким чином спостерігаємо суттєві зміни основних статистичних характеристик вибірки при наявності фальсифікації даних.

Дані зміни вказують на порушення стандартної поведінки системи, що не можуть бути викликані змінами навколишнього середовища, та є індикатором потенційного стороннього втручання у інформаційний потік, на що вказує ступінь зміни даних Однак, досліджувана вибірка даних, параметру «потужність», може бути досліджена окремо з допомогою подальших, удосконалених статистичних методів, для виявлення закономірностей змін окремих показників та побудови регресійної моделі. У майбутньому, метод визначення порушень інформаційної безпеки пропонується удосконалити застосуванням процедур одно факторного дисперсійного аналізу, для моделювання впливів окремих факторів на можливі суттєві зміни досліджуваного параметру «Потужність» вітрового генератора, статистичного бутстреп-аналізу, для більш точної оцінки зміни основних статистичних параметрів. Подальші удосконалення методу визначення порушень безпеки інформаційного потоку КФС можуть бути оцінені кількісно, можливе проведення повного факторного експерименту.

Розглянутий статистичний метод, у порівнянні з наданими у оглядовій частині наукової літератури, методами забезпечення безпеки КФС вітрових генераторів, надає більше відомостей про інформаційний потік, потребує меншої величини вибірки даних для розрахунків, оскільки спирається на чутливі до змін показники дисперсії та асиметрії та є формалізованим та перспективним до подальших досліджень.

Література

1. Zabetian-Hosseini, A. Cyberattack to Cyber-Physical Model of Wind Farm SCADA [Text] / A. Zabetian-Hosseini, A. Mehrizi-Sani and C. Liu // IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, 2018. – P. 4929-4934. DOI: 10.1109/IECON.2018.8591200.

2. Медведская, Н. Статистика по кибербезопасности за 2020 год [Електронний ресурс] / Н. Медведская. – Режим доступу: https://10guards.com/ru/articles/2020-cybersecurity-statistics/. – 14.06.2021.

3. Костров, Д. «Умные сети электроснабжения» (smart grid) и проблемы с кибербезопасностью [Текст] / Д. Костров // Журнал Information Security/ Информационная безопасность. – 2014. – № 3. – С. 45-47.

4. What is DDoS attack? [Electronic resourse]. – Access mode: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. – 24.08.2021.

5. ESET Енциклопедія загроз. Троян [Електронний ресурс]. – Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/. – 24.08.2021.

6. Ramirez-Agudelo, O. H. Bayesian Network Model for Accessing Safety and Security of Offshore Wind Farm [Text] / O. H. Ramirez-Agudelo, C. Köpke, F. Sill Torres // Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. – Research Publishing, 2020. – P. 1756-1763. DOI: 10.3850/978-981-14-8593-0_5799-cd.

7. Power Grid Reliability Evaluation Considering Wind Farm Cyber Security and Ramping Events [Text] / H. Wu, J. Liu, M. Cui, X. Liu, H. Gao // Appl. Sci. – 2019. – Vol. 9, Iss. 15. – Article Id: 3003. DOI: 10.3390/app9153003.

8. Kim, D. Zero-Dynamics Attack on Wind Turbines and Countermeasures Using Generalized Hold and Generalized Sampler [Text] / D. Kim, K. Ryu, J. Back // Appl. Sci. – 2021. – Vol. 11, Iss. 3. – Article Id: 1257. DOI: 10.3390/app11031257.

9. Datta, A. Cyber Threat Analysis Framework for the Wind Energy Based Power System [Text] / A. Datta, M. Ashiqur Rahman // CPS-SPC'17. – 2017. – P. 81-92. DOI: 10.1145/3140241.3140247.

10. Тецкий, А. Г. Применение деревьев атак для оценивания вероятности успешной атаки Web-приложения [Текст] / А. Г. Тецкий // Радіоелек-

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

тронні і комп'ютерні системи. – 2018. – № 3(87). – С. 74–79. DOI: 10.32620/reks.2018.3.08.

11. Нечітка ієрархічна оцінка якості комплексних систем захисту інформації [Текст]/ І. В. Шелехов, Н. Л. Барченко, В. В. Кальченко, В. К. Ободяк // Радіоелектронні і комп'ютерні системи. – 2020. – № 4(96) . – С. 106–115. DOI: 10.32620/reks.2020.4.10.

12. Adeyanju, A. Theoretical Analysis of the Bladeless Wind Turbine Performance [Text] / Anthony Adeyanju, D. Boucher // Journal of Scientific Research and Reports. – 2020. – Vol. 26, Iss. 10. – P. 93–106. DOI: 10.9734/jsrr/2020/v26i1030325.

13. Erisen, B. Wind Turbine Scada Dataset. 2018 Scada Data of a wind turbine in Turkey [Electronic resource] / B. Erisen. – Access mode: https://www.kaggle.com/berkerisen/wind-turbine-scada-dataset. – 03.03.2021.

14. Wagner, H.-J. Introduction to wind energy systems [Text] / H.-J. Wagner // 5th course of the MRS-EMRS "Materials for Energy and Sustainability" and 3rd course of the "EPS-SIF International School on Energy". – 2017. – Vol. 148. – Article Id: 00011. – 16 p. DOI: 10.1051/epjconf/201714800011.

References

1. Zabetian-Hosseini, A., Mehrizi-Sani, A., Liu, C. Cyberattack to Cyber-Physical Model of Wind Farm SCADA. *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 4929-4934. DOI: 10.1109/IECON.2018.8591200.

2. Medvedskaya, N. *Statistika po kiberbezopasnosti za 2020 god* [Cybersecurity statistics for 2020]. Available at: https://10guards.com/ru/articles/2020-cybersecurity-statistics/. (accessed 14.06.2021).

3. Kostrov, D. «Umnye seti elektrosnabzheniya» (smart grid) i problemy s kiberbezopasnost'yu ["Smart power supply networks" (smart grid) and cybersecurity problems]. *Information security*, 2014, no. 3, pp. 45-47.

4. *What is DDoS attack?* Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. (accessed 24.08.2021).

5. *ESET Entsyklopediya zahroz. Troyan* [ESET Encyclopedia of threats. Trojan]. Available at: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/troyan/. (accessed 24.08.2021).

6. Ramirez-Agudelo, O. H., Köpke, C., Sill Torres, F. Bayesian Network Model for Accessing Safety and Security of Offshore Wind Farm. *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, Research Publishing, Singapore, 2020, pp. 1756-1763. DOI: 10.3850/978-981-14-8593-0_5799-cd.

7. Wu, H., Liu, J., Cui, M., Liu, X., Gao, H. Power Grid Reliability Evaluation Considering Wind Farm Cyber Security and Ramping Events. *Appl. Sci.* 2019, vol. 9, iss. 15, article id: 3003, DOI: 10.3390/app9153003.

8. Kim, D., Ryu, K., Back, J. Zero-Dynamics Attack on Wind Turbines and Countermeasures Using Generalized Hold and Generalized Sampler. *Appl. Sci.* 2021, vol. 11, iss. 3, article id: 1257. DOI: 10.3390/app11031257.

9. Datta, A., Ashiqur Rahman, M., Cyber Threat Analysis Framework for the Wind Energy Based Power System. *CPS-SPC'17*, Dallas, TX, USA, Nov. 3, 2017, pp. 81-92. DOI: 10.1145/3140241.3140247.

10. Tetskii, A. G. Primenenie derev'ev atak dlya otsenivaniya veroyatnosti uspeshnoi ataki Web-prilozheniya [Using attack trees to estimate the probability of a successful attack on a Web application], *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2018, no. 3(87), pp. 74–79. DOI: 10.32620/reks.2018.3.08.

11. Shelekhov, I., Barchenko, N., Kal'chenko, V., Obodyak, V. Nechitka iyerarkhichna otsinka yakosti kompleksnykh system zakhystu informatsiyi [Fuzzy hierarchical assessment of the quality of integrated information security systems]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, no. 4(96), pp. 106-115. DOI: 10.32620/reks.2020.4.10.

12. Adeyanju, A., Boucher, D. Theoretical Analysis of the Bladeless Wind Turbine Performance. *Journal of Scientific Research and Reports*, 2020, vol. 26, iss. 10, pp. 93-106. DOI: 10.9734/jsrr/2020/v26i1030325.

13. Erisen, B. *Wind Turbine Scada Dataset. 2018 Scada Data of a Wind Turbine in Turkey*. Available at: https://www.kaggle.com/berkerisen/wind-turbine-scada-dataset. (accessed 03.03.2021).

14. Wagner, H.-J. Introduction to wind energy systems. Ruhr-University Bochum, Energy Systems and Energy Economics, *5th course of the MRS-EMRS "Materials for Energy and Sustainability" and 3rd course of the "EPS-SIF International School on Energy",* 2017, vol. 148, article Id: 00011. 16 p. DOI: 10.1051/epjconf/201714800011.

Надійшла до редакції 28.07.2021, розглянута на редколегії 26.11.2021

АНАЛИЗ СТАТИСТИЧЕСКИХ ПОКАЗАТЕЛЕЙ ДИСПЕРСИИ, АСИММЕТРИИ И ЭКСЦЕССА ПРИ ОПРЕДЕЛЕНИИ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ ВЕТРОВЫХ ГЕНЕРАТОРОВ

И. И. Фурсов, А. В. Шматко

Активное внедрение интеллектуальных систем, которые тесно взаимодействуют с физическими процессами для решения широкого спектра различных задач жизнедеятельности человека, обусловливает повышение актуальности анализа рисков, связанных с функционированием подобных систем. Подобные гибридные сложные интеллектуальные системы относят к классу киберфизических систем (КФС). Нарушения безопасности КФС, вызванные посторонним вмешательством в информационный поток, способны привести к экономическим убыткам, экологическим угрозам и угрозам жизни и здоровью человека. Значительный рост инцидентов нарушения безопасности КФС ветровых генераторов обусловливает актуальность исследований методов защиты подобных систем. **Предметом** изучения в статье является процесс определения нарушений информационной безопасности КФС ветрового генератора на основе анализа статистических показателей дисперсии, асимметрии и эксцесса входного параметра «Мощность», собранного сенсорами КФС. **Целью** является разработка алгоритма определения нарушений информационной безопасности КФС с использованием методов анализа статистических показателей дисперсии, асимметрии и эксцесса. **Задачи**: формализовать процесс определения фальсифицированных данных в информационном потоке КФС; определить преимущества и недостатки существующих методов обеспечения информационной безопасности КФС; определить степень изменений статистических показателей дисперсии, асимметрии и эксцесса выборки параметра «Мощность» ветрового генератора при наличии дезинформации в информационном потоке. Проанализировать возможность дополнения и дальнейшего совершенствования предложенного алгоритма. Используемыми методами являются: анализ статистических показателей дисперсии, асимметрии и эксцесса выборки параметра «Мощность» ветрового генератора. Получены следующие **результаты**: рассмотрены общие характеристики КФС и особенности функционирования КФС ветрового генератора, как объекта исследований данной работы; разработан начальный алгоритм определения нарушений информационной безопасности КФС ветрового генератора на основе использования статистических показателей дисперсии, асимметрии и эксцесса; определено факт искусственной подмены данных параметра «Мощность» информационного потока КФС ветрового генератора; предложены пути улучшения разработанного алгоритма с использованием однофакторного дисперсионного анализа, бутстреп-методов. **Выводы**. Научная новизна полученных результатов заключается в разработке усовершенствованного алгоритма определения факта фальсификации данных в информационном потоке КФС на основе анализа показателей дисперсии, асимметрии и эксцесса; использовании статистического метода при определении нарушений безопасности КФС, анализе недостатков существующих методов определения нарушений безопасности КФС и возможности их комплексного улучшения. Также рассматриваются вопросы возможности улучшения разработанного метода и тестирования метода в дальнейшем.

Ключевые слова: информационная безопасность; КФС; статистические показатели; дисперсия; асимметрия; эксцесс.

ANALYSIS OF STATISTICAL INDICATORS OF VARIANCE, ASYMMETRY AND EXCESS IN DETERMINING INFORMATION SECURITY VIOLATIONS OF CYBERPHYSICAL SYSTEMS OF WIND TURBINES

I. Fursov, O. Shmatko

The active introduction of intelligent systems that closely interact with physical processes to solve a wide range of different tasks of human life increases the relevance of risk analysis associated with the functioning of such systems. Such hybrid complex intelligent systems belong to the class of cyberphysical systems (CPS). Violations of CPS security caused by outside interference in the information flow can lead to economic losses, environmental threats, and threats to human life and health. A significant increase in incidents of violation of the safety of CPS wind turbines determines the relevance of research on methods for protecting such systems. The **subject matter** of the study in the article is the process of determining violations of the information security of the CPS of a wind generator based on the analysis of statistical indicators of variance, asymmetry, and kurtosis of the input parameter "Power" collected by CPS sensors. The **goal** is to develop an algorithm for determining violations of the information security of the CPS using methods for analyzing statistical indicators of variance, asymmetry, and kurtosis. The **task**s to be solved are: to formalize the process of identifying falsified data in the information flow of the CPS;

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

to determine the advantages and disadvantages of existing methods for ensuring the information security of the CPS; to determine the degree of changes in statistical indicators of variance, asymmetry, and kurtosis of the sample of the "Power" parameter of the wind generator in the presence of misinformation in the information flow; to analyze the possibility of supplementing and further improving the proposed algorithm. The **methods** used are analysis of statistical indicators of variance, asymmetry, and kurtosis of the sample of the parameter "Power" of the wind generator. The following results are obtained: the general characteristics of the CPS and features of the functioning of the CPS of the wind turbine as the object of research of this work are considered; an initial algorithm for determining violations of the information security of the CPS of wind turbine based on the use of statistical indicators of variance, asymmetry, and excess is developed; the fact of artificial substitution of data for the parameter "power" of the information flow of the CPS of a wind turbine is determined; ways to improve the developed algorithm using one-factor variance analysis, bootstrap methods are proposed. **Conclusion**s**.** The scientific novelty of the results obtained consists of the development of an improved algorithm for determining the fact of data falsification in the CPS information flow based on the analysis of variance, asymmetry, and kurtosis indicators; the use of a statistical method for determining CPS security violations, analyzing the shortcomings of existing methods for determining CPS security violations and the possibility of their comprehensive improvement. The issues of the possibility of improving the developed method and testing the method in the future are also considered.

Keywords: information security; CPS; statistical indicators; variance; asymmetry; kurtosis.

Фурсов Ігор Ігорович – асп. каф. програмної інженерії та інформаційних технологій управління, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна.

Шматко Олександр Віталійович – канд. техн. наук, доцент кафедри програмної інженерії та інформаційних технологій управління, Національний технічний університет «Харківський політехнічний інститут», Харків, Україна.

Ihor Fursov – PhD student of the SEMIT Department of National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine,
e-mail: ihor.fursov@gmail.com, ORCID: 0000-0002-3597-4935.

Oleksandr Shmatko – Candidate of Technical Sciences, Associate Professor of the SEMIT Department of National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine,
e-mail: asu.spios@gmail.com, ORCID: 0000-0002-2426-900X.