УДК 004

О.Дзюбинський, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ВИЯВЛЕННЯ НЕСПРАВНОСТІ ЕЛЕМЕНТІВ ЦИФРОВИХ ПРИСТРОЇВ

У статті розроблено програмне забезпечення, яке призначено для системи виявлення несправності елементів цифрових пристроїв. Метою розробки є дослідження та програмна реалізація системи виявлення несправності елементів цифрових пристроїв. Об'єктом дослідження є процес виявлення несправності елементів цифрових пристроїв. Предметом дослідження є методи виявлення несправності елементів цифрових пристроїв. Методи дослідження базуються на методах системотехніки, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи виявлення несправності елементів цифрових пристроїв. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, виявлення несправності, цифрові пристрої

Постановка проблеми. Цифрові пристрої в даний час активно використовуються для Інтернету речей. Інтернет речей (IoT) отримав значне визнання і став новою парадигмою сенсорної взаємодії з фізичним світом в епоху Індустрії 4.0. Інтернет речей використовується в багатьох різноманітних програмах, які є частиною нашого життя та стають глобальними цифровими нервовими системами. Цілком очевидно, що в найближчому майбутньому сотні мільйонів людей і бізнесів з мільярдами матимуть розумні датчики та передові комунікаційні технології, і ці речі розширять межі існуючих систем.

Це призведе до потенційних змін у тому, як ми працюємо, навчаємося, впроваджуємо інновації, живемо та розважаємося. Гетерогенні розумні датчики в Інтернеті речей є незамінними частинами, які збирають необроблені дані з фізичного світу, будучи першим портом контакту.

Часто датчики в IoT розгортають або встановлюють у суворих умовах. Це неминуче означає, що датчики схильні до виходу з ладу, несправності, швидкого зношення, зловмисних атак, крадіжок і втручання. Усі ці умови змушують датчики в IoT видавати незвичайні та помилкові показання, які часто називають викидами. Значна частина поточних досліджень була проведена для розробки моделей викидів датчиків і виявлення несправностей виключно для бездротових сенсорних мереж (WSN), а адекватних досліджень у контексті IoT досі не проводилося.

Операційна структура бездротової сенсорної мережі значно відрізняється від операційної структури IoT, використання деяких існуючих моделей, розроблених для WSN, не може використовуватися в IoT для виявлення викидів і збоїв. Виявлення несправностей датчиків і викидів є дуже важливим в IoT для виявлення високої ймовірності помилкового зчитування або пошкодження даних, що забезпечує якість даних, зібраних датчиками.

Дані, зібрані датчиками, спочатку попередньо обробляються для перетворення в інформацію, а коли моделі штучного інтелекту (AI), машинного навчання (ML) далі використовуються IoT, інформація далі обробляється в програмах і процесах. Будь-які несправні, помилкові, пошкоджені показання датчиків пошкоджують навчені моделі, що, таким чином, створює ненормальні процеси або викиди, які значно відрізняються від нормальних поведінкових процесів системи.

У даній роботі представляємо вичерпний огляд виявлення несправностей датчиків, аномалій, викидів в Інтернеті речей і проблем. Обговорюються вичерпні рекомендації щодо вибору адекватної моделі виявлення викидів для датчиків у контексті IoT для різних програм.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи виявлення несправності елементів цифрових пристроїв.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи виявлення несправності елементів цифрових пристроїв.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем виявлення несправності елементів цифрових пристроїв.
– Дослідження системи виявлення несправності елементів цифрових пристроїв.
– Програмна реалізація системи виявлення несправності елементів цифрових пристроїв.

Об'єктом дослідження є процес виявлення несправності елементів цифрових пристроїв.

Предметом дослідження є методи виявлення несправності елементів цифрових пристроїв.

Методи дослідження базуються на методах системотехніки, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу

Інтернет речей є однією з ключових проривних технологій в епоху Індустрії 4.0 [1]. Існує зростаюча тенденція до використання Інтернету речей (IoT) у наукових та промислових спільнотах [1, 1]. Існує багато визначень, запропонованих для IoT, загалом, IoT можна описати як злиття різних технологій, які надають Інтернет-послуги та програми за допомогою електронних пристроїв, підключених до фізичних речей, з метою збору даних за допомогою різнорідних датчиків., для управління процесами [1].

IoT використовуються в багатьох додатках у різних сферах, від моніторингу навколишнього середовища, охорони здоров'я, сільського господарства та виробничих секторів [5, 6, 7]. Інтернет речей еволюціонував від простого зв'язку та точки зв'язку для отримання даних фізичних об'єктів до комплексних інтелектуальних систем, які здатні збирати величезні обсяги даних і контролювати різні процеси для максимізації прибутку для організацій і окремих осіб.

IoT виявився продуктивною технологією в багатьох секторах, таких як промисловість, громадські та наукові кола. Останнім часом Інтернет речей став головною темою досліджень у більш широкій дослідницькій спільноті. Наразі глобальний ринок Інтернету речей досяг 9,1 мільярда доларів США, і, згідно з [8, 9], зведений річний темп зростання (CAGR) зростатиме на 40% до 2024 року. За оцінками, до року У 2020 році в середньому кожна людина матиме сім комунікаційних пристроїв на основі IoT [10].

В автомобільній промисловості до 2020 року понад 23,6 мільйонів автомобілів матимуть доступ до Інтернету. Згідно зі звітом Verizon [11], очікується, що глобальний ринок Інтернету речей зросте з прогнозованими темпами на 17% і досягне 1,3 трильйона доларів США.

У сфері сільського господарства до 2020 року очікується, що послуги цифрового точного сільського господарства на основі IoT досягнуть 4,5 мільярдів доларів США [12]. Здатність IoT здійснювати моніторинг у режимі реального часу та відносна простота використання відкрили для дослідників цілий новий діапазон використання IoT у багатьох програмах.

Компендіум датчиків на місці, вбудованих у пристрої IoT, є основними компонентами, які збирають цінні необроблені дані. Правильна робота датчиків у пристрої IoT відіграє життєво важливу роль у загальній продуктивності системи та залежних процесів,

додатків [13]. Датчики IoT часто розгортаються в суворих умовах; однак гарантувати правильну роботу датчика та передбачити несправності досить складно. Крім того, датчики в IoT зазвичай є найдешевшими електронними компонентами, які зазвичай схильні до несправностей.

Несправний датчик створює пошкоджені дані або помилкові зчитування або суперечливу інформацію на пристрої IoT [14]. Коли IoT обробляє ці пошкоджені дані датчиків, загальна продуктивність системи IoT знижується, що робить її неточною та ненадійною. Нещодавно зростаюча тенденція автоматизації багатьох процесів, як-от автономне керування транспортними засобами для зменшення кількості аварій, підкреслює важливість правильної роботи датчиків, які працюють у системі.

Оскільки системи IoT працюють безперервно, генеруючи великі обсяги мультимодальних даних, забезпечення точної роботи датчиків в IoT є критично важливим, тому має бути точний процес моніторингу для перевірки поведінки та продуктивності датчиків в IoT. Крім того, цей процес моніторингу датчиків має бути автоматизованим, масштабованим і достатньо гнучким, щоб використовувати його для потокової передачі необроблених даних, створених численними датчиками, вбудованими в пристрій IoT.

Відомо, що цей процес моніторингу, який зазвичай називають виявленням викидів датчика, виявляє будь-яку аномалію чи відхилення в показаннях датчика, і зазвичай це один із ключових процесів, що впливає на якість даних, зібраних датчиком. Останнім часом у дослідницьких спільнотах виявлення викидів викликає великий інтерес [15, 16, 17, 18].

Однак значна частина поточних досліджень щодо виявлення викидів стосується бездротових сенсорних мереж (WSN), а також широко використовується для виявлення шахрайства, порушень безпеки мережі, відстеження цілей, моніторингу навколишнього середовища та здоров'я.

Однак не було проведено адекватних досліджень щодо виявлення викидів датчиків у контексті IoT. Унікальні характеристики IoT у порівнянні з WSN показують, що традиційні методи виявлення викидів не застосовуються безпосередньо до IoT. Зазвичай IoT – це компендіум кількох подібних датчиків, вбудованих як одиниця, здатна виробляти величезні обсяги просторово-часових даних із малою затримкою, на відміну від WSN [19].

Коли є помилкові дані, створені одним типом датчика в межах IoT, спричинені збоєм або несправністю одного датчика з пари, ідентифікація несправного датчика, щоб зробити дані, надані цим датчиком, надлишковими в режимі реального часу, дозволяючи при цьому дані, створені вторинним подібним неушкодженим датчиком, відіграють важливу роль у правильному функціонуванні пристрою IoT.

Методологія дослідження

Методологія дослідження була поділена на три основні етапи. Під час первинного етапу інформацію щодо необхідності виявлення несправностей датчиків, помилок аналізували за допомогою систематичного огляду літератури та консультацій з галуззю та компаніями, які пропонують продукти на основі Інтернету речей на ринку. На другому етапі було проведено критичний аналіз для розуміння етимологічних відмінностей між IoT і WSN, пов'язаних із збоями та помилками датчиків. Після визначення функціональних і робочих відмінностей датчиків між IoT і WSN, на останньому етапі відповідна література була ретельно переглянута, щоб отримати викиди датчиків і методи виявлення несправностей, які підходять для IoT.

Відмінності між IoT та бездротовими сенсорними мережами

У цьому розділі визначено та розглянуто декілька суттєвих відмінностей між IoT та бездротовими сенсорними мережами (WSN). Значна частина досліджень була проведена для розробки моделей викидів датчиків і виявлення несправностей виключно для WSN, однак адекватних досліджень у контексті IoT досі не проводилося. Оскільки бездротові сенсорні мережі та їх операційна структура значно відрізняються від операційної системи IoT, деякі з існуючих моделей, розроблених для WSN, не можна використовувати в IoT для виявлення викидів і збоїв [10, 11, 12].

IoT існує та працює на вищому рівні, ніж WSN. Зобразимо WSN як підмножину IoT, оскільки WSN є технологічною структурою, яка часто використовується в системі IoT для збору даних фізичних явищ у реальних умовах. На відміну від WSN, IoT мають менше проблем, пов'язаних із збоями в мережі, дефіцитом живлення або збоями вузлів тощо. Однак IoT матиме власний набір унікальних проблем (як обговорювалося в розділах вище), де лише кілька типів можна використовувати існуючі методи виявлення викидів і несправностей.

Викиди в контексті IoT

У контексті Інтернету речей викид датчика зазвичай відомий як нерегулярність або розбіжність у поведінці датчика під час процесу каталогізації певних параметрів або подій у порівнянні з його попередньою поведінкою чи показаннями. Не існує стандартного обмеженого визначення викидів датчика.

Джерела викидів датчиків в IoT.

– Внутрішні помилки датчика. Цей тип помилки пов'язаний із неправильними показаннями або вимірюваннями, отриманими від несправного датчика, вбудованого в пристрій IoT. Оскільки датчики є електронними компонентами, вони часто раптово виходять з ладу та припиняють працювати без будь-яких ознак погіршення продуктивності [16, 17, 18]. Цей вид збою датчика передає або відсутність показань, або нульові показання до алгоритму обробки даних у системі IoT [13]. Деяка література визначила цей тип несправності датчика як «бінарну несправність».

– Події датчика: оскільки датчик розгортається для збору даних у сценаріях або подіях реального світу, існує ймовірність безпрецедентної зміни події, спричиненої малоймовірними ситуаціями, які серйозно впливають на датчик, спричиняючи тим самим викиди. Наприклад, система IoT із кількома датчиками, які відстежують рівень температури та вологості на фермі, якщо хробак повзе на один із датчиків, фермер отримуватиме показання про те, наскільки хробак вологий і теплий, ці свідчення будуть неефективними для і перешкоджає роботі всієї системи моніторингу IoT.

– Періодичні помилки датчика: остання категорія несправності датчика – це періодичні помилки, які в основному викликані спорадичними подіями, такими як крадіжка, зловмисна атака та втручання в роботу датчика [19, 10, 11]. Ситуація, коли незакріплений роз'єм у датчику або в іншому місці сенсорного обладнання також може призвести до того, що датчик періодично створює розріджені дані для алгоритмів обробки даних [12].

Несправності датчиків і моделі виявлення викидів для IoT

Виявлення збоїв датчика та ідентифікація викидів у контексті IoT почали привертати значну увагу дослідницького співтовариства. Загалом існує п'ять макрокласів методів автоматичного виявлення викидів датчиків і несправностей, які можна використовувати в контексті IoT.

У цьому розділі обговорюються методи виявлення несправностей датчиків і викидів для IoT на основі таких дисциплін, як методи на основі статистики, методи на основі найближчого сусіда, методи машинного навчання та штучного інтелекту, методи на основі кластеризації та методи на основі класифікації техніки.

Статистичні методи

Методи, засновані на статистиці, були першими алгоритмами, використаними багатьма дослідниками для виявлення несправностей датчика та виявлення викидів. У цій техніці дані від датчиків моделюються за допомогою стохастичного розподілу. Точки даних від датчиків можна визначити як викиди або помилки, коли ймовірність екземпляра даних, згенерованого цією моделлю, дуже низька.

Ця техніка використовує попередні вимірювання датчика для наближення та створення моделі точної поведінки датчика. Однак щоразу, коли реєструється нове вимірювання від того самого датчика, ця точка даних потім порівнюється з моделлю, щоб перевірити, чи нова точка даних статистично несумісна з моделлю. Якщо модель несумісна з показаннями нового датчика, вона позначається як викид або помилкове вимірювання.

Підхід, заснований на статистичному вікні, зазвичай допомагає зменшити кількість

помилкових спрацьовувань помилок і викидів. Фільтр низьких і високих частот є прикладом основного статистичного методу, який класифікує показання датчиків як несправності або аномалії на основі розробки середнього значення попередніх вимірювань і визначення того, наскільки відрізняються нові показання.

Статистичний метод, заснований на просторово-часовій взаємозалежності даних датчиків, запропонований Hida та ін. [10]. Ця техніка здебільшого використовує два статистичні тести для локального виявлення викидів, щоб зробити прості процеси агрегування більш надійними. Статистичні моделі мають відношення до кількісних наборів даних реального значення або, принаймні, є розподілом кількісних даних, який потрібно перетворити на відповідне числове значення для чисельної обробки. Оскільки складність і обсяг даних датчиків зростає (як це зазвичай буває у випадку IoT), ця модель потребує більше часу для обробки, щоб перетворити складні дані.

Методи найближчого сусіда

Техніка на основі найближчого сусіда є широко використовуваною технікою для аналізу точок даних датчиків щодо найближчих сусідів. По суті, метод найближчого сусіда для виявлення несправності датчика та викидів явно спирається на поняття близькості. Техніка найближчого сусіда працює, покладаючись на відстані між вимірюваннями даних датчиків, щоб відрізнити ненормальні показання від правильних. Коефіцієнт локального викиду (LOF) – це відомий алгоритм визначення найближчого сусіда [13], який приписує помилку або оцінку викиду кожному показанню датчика на основі кількості вимірювань навколо його k-найближчих сусідів і кількості вимірювань навколо показання датчика. Показання датчика з вищими балами позначаються як аномалії.

Методи штучної нейронної мережі

Нейронні мережі та нечітка логіка є останніми підходами для виявлення несправностей датчиків і викидів у контексті IoT. Техніка нейронної мережі є логічною моделлю, яка надає комплексну ідею, яка допомагає в процесі прийняття рішень шляхом аналізу всього набору даних датчика [14, 15]. У той час як техніка нечіткої логіки дозволяє перехідні значення (наприклад, правильно/неправильно, так/ні, високий/низький) для розмежування стандартних/правильних показань датчика. В Інтернеті речей підхід нечіткої логіки може бути використаний для покращення прийняття рішень, покращення вибору голови кластеризації, покращення безпеки мережі та агрегації даних, ефективної обробки маршрутизації, протоколів MAC, якості обслуговування та, зрештою, ефективного виявлення несправностей датчиків і викидів.

Кластерні методи

Кластерний аналіз [16] є популярним підходом у спільноті інтелектуального аналізу даних, який групує пов’язані екземпляри даних у кластери подібної поведінки. Шляхом поділу даних на кластери подібних точок даних від датчиків, у яких кожен кластер даних містить точки даних, які схожі одна на одну та відрізняються від точок даних в інших групах кластерів. Цей підхід є підмножиною методів близькості. Початкові показання датчиків спочатку використовуються для створення кластерів, а потім нові вимірювання датчиків, призначені для невеликих і віддалених кластерів даних, або вимірювання датчиків, які знаходяться дуже далеко від центроїда основного кластера, позначаються як ненормальні показання.

Методи, засновані на класифікації

Методи, засновані на класифікації, є важливими точними методами інтелектуального аналізу даних і машинного навчання. Метою методів класифікації є ідентифікація моделі класифікації (названої класифікатором) за допомогою набору визначених точок даних датчиків (точки навчання), а потім класифікація незрозумілих екземплярів даних в одну з вивчених груп (нормальних/викидних).

Цей тип техніки потребує постійного оновлення для адаптації нових даних датчиків, які належать до нормального класу. У випадку IoT ця техніка класифікації адекватно підходить для виявлення несправностей і викидів, оскільки ця техніка прагне працювати за

загального припущення, що класифікатор можна дізнатися з наданої просторової функції для ідентифікації нормальних і викидних класів [17].

Щоб створити цю техніку, її необхідно розділити на два етапи: навчання та експеримент [18]. На етапі навчання методика спрямована на вивчення класифікатора з використанням доступних помічених навчальних даних, після чого слідує фаза експерименту, яка класифікує тестовий екземпляр як звичайний, викид або несправність датчика [19, 10].

Порівняння методів виявлення помилок і викидів для IoT

Незважаючи на те, що деякі дослідники нещодавно спробували досягти високої точності для досягнення високої точності, описані вище методи виявлення несправності сенсора та викидів для IoT, проте кожен із методів має Переваги та недоліки, як обговорюється нижче.

Статистичні методи

Переваги:

– Може ефективно ідентифікувати будь-які несправності датчиків і викиди в IoT після отримання правильної моделі розподілу ймовірностей.

– Несправності датчика та викиди можна виявити за допомогою часової кореляції. Будь-яка непередбачена зміна в розподілі даних негайно зменшує часові кореляції, тим самим виявляючи викиди.

Недоліки:

– Оскільки IoT часто використовуються в умовах реального життя, де часто немає попередніх знань про розподіл даних датчиків, параметричний статистичний підхід не є вигідним.

– Непараметричні статистичні моделі не підходять для IoT з великим об’ємом даних, які працюють у режимі реального часу.

– Часто є високі обчислювальні витрати на керування отриманими багатовимірними даними.

Методи найближчого сусіда

Переваги:

– Дуже просто застосувати до різних типів даних, створених різними датчиками в системі IoT.

– Можуть бути залишені без нагляду та в першу чергу потрібні для визначення відповідної міри відстані для наведених даних.

Недоліки:

– При використанні складних багатовимірних даних, створених IoT, вартість обчислень різко зростає.

– Масштабованість цих типів моделей викликає занепокоєння, особливо в контексті IoT.

– Часто дає високий коефіцієнт хибнонегативних результатів для виявлення несправностей датчика та викидів.

Методи машинного навчання

Переваги:

– Може використовуватися, коли датчики створюють погані, шумні та фрагментарні дані, оскільки властива поведінка цієї моделі узагальнює отримані точки даних.

– Існує обмежена потреба, іноді немає потреби, перенавчати модель, коли додаються нові дані датчика.

Недоліки:

– Модель потребує тонкого налаштування та моделювання, перш ніж її можна буде запустити в реальних умовах.

– Оскільки ця модель часто базується на правилах, якщо кількість змінних даних датчиків збільшується, це також експоненціально збільшуватиме кількість правил.

Кластерні техніки

Переваги:

– Після того, як кластери та нові точки даних буде вставлено в систему та перевірено на наявність помилок датчиків і викидів, модель можна легко адаптувати до інкрементної форми.

– Нагляд не потрібен.

– Дуже добре підходить для виявлення аномалії датчика на основі тимчасових даних IoT.

Недоліки:

– Це дуже дорого обчислювально під час роботи з багатовимірними даними датчиків для виявлення несправностей.

– Через високу обчислювальну вартість моделей він непридатний для датчиків із недостатнім ресурсом.

– Не вдається впоратися з будь-якими змінами в даних IoT.

Методи класифікації

Переваги:

– Ця модель не залежить ні від статистичної моделі, ні від оцінених параметрів даних.

– Забезпечує оптимальну, а іноді й максимальну ідентифікацію несправностей датчика та викидів.

– Може використовуватися на багатовимірних даних для виявлення викидів датчиків і несправностей.

Недоліки:

– Ця модель є обчислювально складною порівняно з кластеризацією та статистичними методами.

– Модель має навчитися отримувати нові точки даних.

Стратегії виявлення та ідентифікації несправності датчика

Автоматичне виявлення несправності датчика та автоматичну ідентифікацію можна виконати за допомогою трьох стратегій: стратегії мережевого рівня, однорідної стратегії та гетерогенної стратегії.

Стратегія мережевого рівня

Використовуючи керування на мережевому рівні та моніторинг мережевих пакетів, цей підхід виявляє будь-які збої датчиків [11, 12]. Датчики в системах IoT ефективно контролюють один одного, щоб виявити будь-які проблемні датчики. Цей підхід переважно використовує моделі Маркова для характеристики нормальної та ненормальної поведінки датчиків [13, 14].

Однорідна стратегія

Гомогенна стратегія використовує кілька датчиків одного типу для ідентифікації та виявлення будь-якого датчика в системах IoT, який має тенденцію демонструвати ненормальну поведінку [15]. Розміщуючи датчики того самого типу, які генерують подібні значення, просторово близько один до одного, цей підхід виявляє будь-яку некорельовану поведінку, таким чином дозволяючи виявити будь-який несправний датчик. Цей тип датчиків в основному використовує модель часових рядів з авторегресійною інтегрованою ковзною середньою (ARIMA) для порівняння прогнозованих вимірювань датчиків із звітними вимірюваннями датчиків [15, 16].

Гетерогенна стратегія

Гетерогенна стратегія має тенденцію поєднувати різні типи точок даних від датчика для виявлення несправності датчика [17, 18]. Стратегія стала популярною останнім часом із розвитком систем IoT із вбудованими датчиками різних типів. Ця стратегія виявляє збій датчика шляхом класифікації виходів датчиків, а потім навчання класифікатора ідентифікувати той самий набір точок даних на основі різних підмножин датчиків в одній системі IoT [19].

На рисунку 1 зображена структурна схема розробленої, в результаті виконання магістерського проектування системи.

Як видно з рисунка структурно система складається з наступних головних блоків:

– інтерфейс користувача;
– блок моделювання;
– блок діагностики;
– бази даних.

Розглянемо ці структурні блоки більш детальніше.

Найбільш великим структурним блоком є блок інтерфейсу користувача. Цей блок є дуже важливим, тому, що багато в чому, від інтерфейсу користувача залежить наскільки легко можна буде навчати користувача діагностиці цифрових схем.

Інтерфейс користувача складається з наступних структурних підблоків:

– меню користувача;
– панель інструментів;
– навігатор;
– графічне зображення елементів та мікросхем;
– візуалізація цифрових схем;
– візуалізація процесу діагностики, показів осцилографа та індикаторів.

Розглянемо блок діагностики.

Структурно він складається з наступних підблоків:

– блок формування та запуску тестуючи послідовностей;
– блок осцилографів, для зняття осцилограм з виходів та входів цифрової схеми;
– блок виявлення помилок та несправностей.

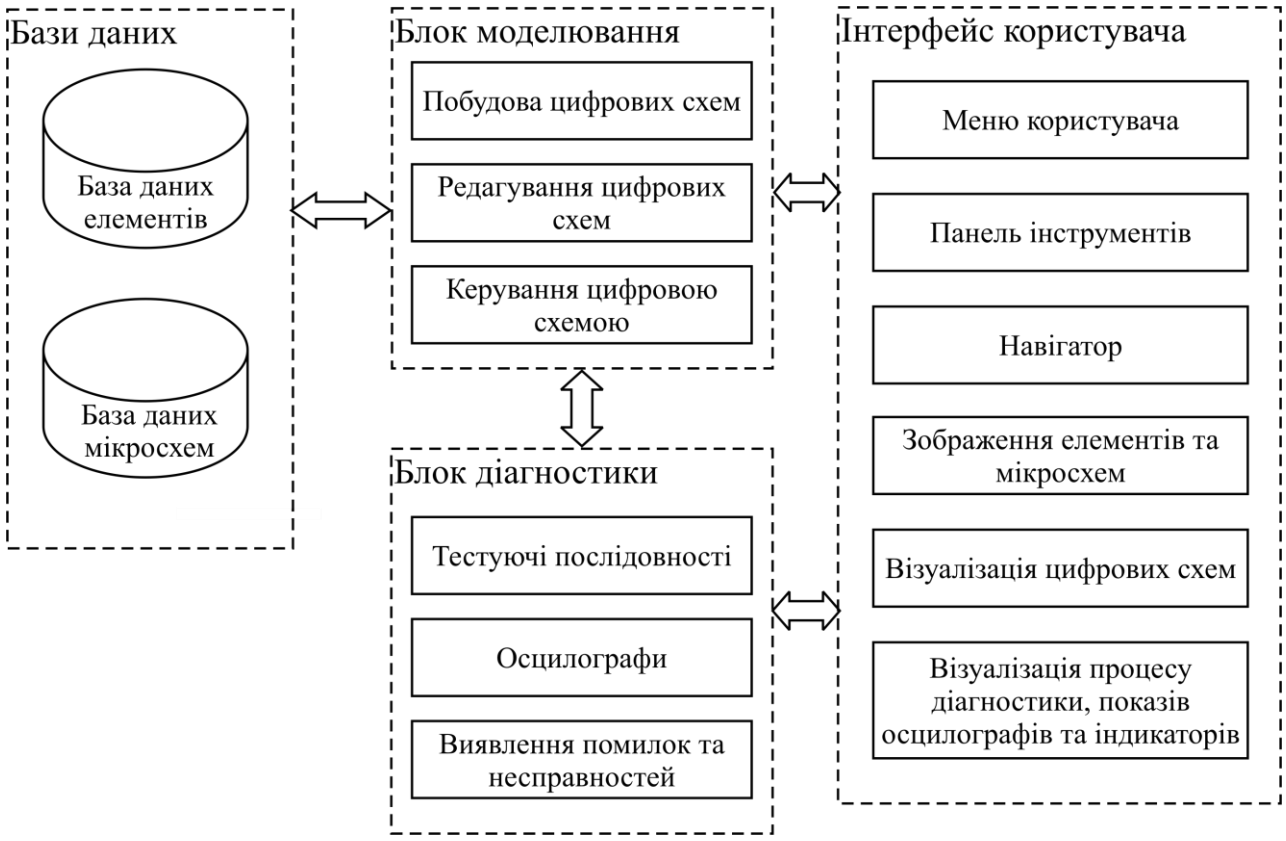

Рисунок 1 – Структурна схема системи

Перейдемо до розгляду блоку моделювання. Він складається з наступних структурних підблоків: побудова цифрових схем, де можно з наявних компонентів побудувати цифрову схему; редагування цифрових схем – для внесення змін у побудовану цифрову схему;

керування цифровою схемою, для відслідковування того, як проходять сигнали по цифровій схемі.

Розглянемо блок роботи з базою даних. Він складається з наступних підблоків: база даних елементів; база даних мікросхем.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів виявлення несправності елементів цифрових пристроїв. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем виявлення несправності елементів цифрових пристроїв; Досліджена система виявлення несправності елементів цифрових пристроїв; На основі отриманих результатів досліджень створена програмна реалізація системи виявлення несправності елементів цифрових пристроїв; Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання виявлення несправності елементів цифрових пристроїв. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kovalenko A.S. Information model and its element for displaying information on technical condition of objects of integrated information system / A.S. Kovalenko, A.A. Smirnov, A.V. Kovalenko, A.P. Dorensky // International Journal of Computational Engineering Research (IJCER). – India: Delhi, 1016. – Volume 6, Issue 1. – P. 21-27.
2. Кожанова А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / О.А. Смірнов, А.С. Кожанова, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 1013. – Вип. 6(113). – С. 255-257.
3. Коваленко А.С. Задачи распознавания ситуаций в ERP системах / А.В. Коваленко ., А.А. Смірнов, А.С. Коваленко // Системи обробки інформації. – Х.: ХУПС, 1014. – Вип. 4(120). – С. 161-164.
4. Коваленко А.С. Підсистема технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко, О.А.Смірнов, О.В. Коваленко // Системи озброєння і військова техніка.– Х.: ХУПС, 1014. – № 1(37). – С. 126-129.
5. Коваленко А.С. Анализ эффективности использования экспертной системы технической диагностики с традиционной структурой / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 1014. – № 2(38). – С. 106-108.
6. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 1014. – № 2(15). – С.154-157.
7. Коваленко А.С. Разработка структуры экспертной системы технической диагностики интегрированной информационной системы / А.С. Коваленко, А.А. Смирнов, А.В. Коваленко // Наука і техніка Повітряних Сил Збройних Сил України. – Харків: ХУПС, 1014. – № 2(15). – С.154-157.
8. Коваленко А.С. Структура системи технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Кіровоградського національного технічного університету / техніка в сільськогосподарському виробництві, галузеве машинобудування, автоматизація. – Кіровоград: Вид-во КНТУ, 1014. – Вип. 27. – С. 245-251.
9. Коваленко А.С. Дослідження будови інтегрованої інформаційної системи та її елементів / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 1014. – № 4(40). – С. 85-88.
10. Коваленко А.С. Розробка структури бази даних для обліку технічного стану елементів інтегрованої інформаційної системи з урахуванням вимог споживачів інформації / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи обробки інформації. – Х.: ХУПС, 1015. – Вип. 1(126). – С. 75-79.
11. Коваленко А.С. Обґрунтування набору даних для оцінки технічного стану інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС, 1015. – Вип. 1(42). – С.39-41.
12. Коваленко А.С. Експертна система технічного діагностування інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Системи озброєння і військова техніка. – Х.: ХУПС, 1015. – № 1(41). – С. 106-111.
13. Коваленко А.С. Удосконалення методу технічного обслуговування об’єктів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко, О.П. Доренський // Системи озброєння і військова техніка. – Х.: ХУПС, 1016. – № 2(46). – С. 109-114.
14. Кожанова А.С. Система технічної діагностики інтегрованих інформаційних систем – обґрунтування необхідності створення, визначення понятійного апарату та напрямів досліджень / А.С. Кожанова, О.А. Смірнов,

М.П. Савченко, Д.М. Ізосімов, В.В. Мороз // Створення та модернізація озброєння і військової техніки в сучасних умовах: Тринадцята наук.-техн. конф., 5-6 вер. 2013 р., м. Феодосія: тези доп. – Феодосія: ДНВЦ, 1013. – С. 187-188.
15. Кожанова А.С. Визначення основних напрямків досліджень щодо створення системи технічної діагностики інтегрованих інформаційних систем / А.С. Кожанова, О.А. Смірнов, А.В. Челпанов // Проблемні питання розвитку озброєння та військової техніки Збройних Сил України: IV наук.-техн. конф., 16-20 груд. 2013 р., м. Київ: зб. тез. – Київ: ЦНДІ ОВТ ЗСУ, 1013. – С. 293.
16. Коваленко А.С. Обґрунтування необхідності створення систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Інформатика та системні науки : V Всеукр. наук.-практ. конф., 13–15 бер. 2014 р., м. Полтава : зб. тез. – Полтава: ПУЕТ, 1014. – С. 292-294.
17. Коваленко А.С. Створення систем технічної діагностики для автоматизації процесів керування в інтегрованих інформаційних системах / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку ІТ-індустрії: VI між нар. наук.-практ. конф., 17-18 квіт. 2014 р., м. Харків: зб. тез. – Харків: ХНЕУ, 1014. – С. 241.
18. Коваленко А.С. Визначення понятійного апарату та напрямів досліджень для синтезу систем технічної діагностики інтегрованих інформаційних систем / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комп'ютерне моделювання у наукоємних технологіях (КМНТ-2014): наук.-техн. конф. з міжнар. участю, 18-31 трав. 2014 р., м. Харків: зб. наук. праць. – Харків: ХНУ, 1014. – С. 190-193.
19. Коваленко А.С. Розробка структури бази даних інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Проблеми і перспективи розвитку ІТ-індустрії: VII міжнар. наук.-практ. конф., 17-18 квіт. 2015 р., м. Харків: зб. тез. – Харків: ХНЕУ, 1015. – С. 15.
20. Коваленко А.С. Дослідження елементів інтегрованої інформаційної системи / А.С. Коваленко, О.А. Смірнов, О.В. Коваленко // Комбінаторні конфігурації та їх застосування: XVII між нар. наук.-практ. сем., 17-18 квіт. 2015 р., м. Кіровоград: зб. тез – Кіровоград: КНТУ, 1015. – С. 5.

УДК 004

М.Жупило, магістр гр. КІ-21МЗ,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ ХМАРНИХ СЕРВІСІВ

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення конфіденційності даних хмарних сервісів. Метою розробки є дослідження та програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів. Об'єктом дослідження є процес забезпечення конфіденційності даних хмарних сервісів. Предметом дослідження є методи забезпечення конфіденційності даних хмарних сервісів. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення конфіденційності даних хмарних сервісів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

комп'ютерна інженерія, конфіденційність даних, хмарні сервіси

Постановка проблеми. Незалежно від того, чи виконуєте ви робочі навантаження в загальнодоступній хмарі, приватній хмарі, гібридній інфраструктурі чи мультихмарі з декількома хмарними провайдерами, вам потрібно дотримуватися правил обробки даних і гарантувати безпеку своїх даних.

Недотримання правил щодо даних і наступне порушення може призвести до грошових втрат і шкоди авторитету бренду. Щоб забезпечити захист даних у хмарі, ви можете застосувати різні методи, такі як шифрування, контроль доступу, захист кінцевих точок і моніторинг.