Том 12
Автоматизація, метрологія та інформаційні технології

УДК 004.41

Венцкайтес В.О., студент групи КН04-15-М
Науковий керівник: Селівьорстова Т.В., к.т.н., доцент кафедри інформаційних технологій та систем
(Національна металургійна академія України, м. Дніпро, Україна)

РОЗРОБКА СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАСОБУ ДЛЯ ДОСЛІДЖЕННЯ ЯКОСТІ ПЗ НА БАЗІ СТАНДАРТУ ГОСТ 28195

Швидке збільшення складності і розмірів сучасних комплексів програм при одночасному зростанні відповідальності виконуваних функцій різко підвищило вимоги з боку замовників і користувачів до їх якості та безпеки застосування. Випробуваним засобом забезпечення високої ефективності і якості функціонування програм і програмних комплексів є міжнародні стандарти, розроблені за участю представників провідних компаній галузі.

По мірі розширення додатків і збільшення складності інформаційних систем виділилися області, в яких помилки або недостатня якість програм можуть завдати шкоди, що значно перевищує позитивний ефект від їх використання.

Однією з найважливіших проблем забезпечення якості програмних засобів є формалізація характеристик якості і методологія їх оцінки. Для визначення адекватності якості функціонування, наявності технічних можливостей програмних засобів до взаємодії, вдосконалення і розвитку необхідно використовувати стандарти в області оцінки характеристик їх якості. Основою регламентування показників якості програмних засобів є міжнародний стандарт ГОСТ 28195 [1].

Показники якості являють собою ієрархічну багаторівневу систему, в якій показники вищих рівнів визначаються через показники нижчих рівнів. Тільки на останньому рівні оцінка значень показників здійснюється на основі інформації, що відноситься безпосередньо до програмного засобу [2].

Стандарт ГОСТ 28195 встановлює загальні положення щодо оцінки якості ПЗ: номенклатуру та застосовність показників якості по підкласів і за фазами життєвого циклу.

Основні завдання, які вирішуються при оцінці якості ПЗ [3]: планування номенклатури показників якості; планування рівнів показників якості; вибір методів контролю показників якості ПЗ; контроль значень показників якості; прийняття рішення про відповідність реальних значень показників якості встановленим вимогам.

Відповідно до стандарту методи визначення показників якості ПЗ розрізняються:

– за методами отримання інформації про показник: вимір, реєстрація, розрахунок, сприйняття людиною;

– за джерелами отримання інформації про ПЗ: безпосереднє спостереження за їх функціонуванням в процесі роботи (традиційний); обробка висновків експертів (експертний).

Для реалізації ГОСТ 28195 розроблено спеціалізований програмний засіб, що реалізує визначення якості програмного засобу, на підставі експертних висловлювань та метрик.

Перелік посилань

1. ГОСТ 28195-89 «Оценка качества программных средств. Общие положения».

2. Роговцев А.М. Математические нечеткие подходы к контролю качества / А.М. Роговцев // Измерительная техника. – 2009. – №3. – С. 18-19.

3. Yaremchuk N. Evalustion of a complex quality index using numerical and verbal ordinal scale / N. Yaremchuk, O. Redyoga // Восточно-европейский журнал передовых технологий. – 2014. – ½ (67). – С. 58-62.

УДК 622.1:622.271

Власов В.С., аспірант кафедри програмного забезпечення комп'ютерних систем
Науковий керівник: Алексєєв М.О., д.т.н, професор, декан факультету інформаційних технологій
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

МЕТОДИКА ТРИВИМІРНОГО МОДЕЛЮВАННЯ ДЕФОРМАЦІЇ ЗЕМНОЇ ПОВЕРХНІ, ЯКА ПІДРОБЛЕНА ГІРНИЧИМИ РОБОТАМИ В УМОВАХ ШАХТ ЗАХІДНОГО ДОНБАСУ

Для прийняття рішень з прогнозування і мінімізації гідро-екологічних ризиків при закритті шахт Західного Донбасу планується розробити автоматизовану систему геолого-маркшейдерського забезпечення, що дозволяє визначати площі затоплених ділянок шахтних полів та обсяг між деформованою земною поверхнею і дзеркалом води. Для розробки цієї автоматизованої системи запропоновано методику тривимірного моделювання деформації земної поверхні при виїмці вугільних пластів на шахтах ПрАТ «ДТЕК Павлоградвугілля».

Одною з основних умов методики тривимірного моделювання є висока точність кінцевих результатів досліджень, яка обумовлена можливими значними обсягами затоплення деформованої земної поверхні. При цьому, навіть незначна похибка в обчисленнях може привести до значних економічних втрат при прийнятті рішень щодо мінімізації гідро-екологічних ризиків, які виникають.

На підставі аналізу різних моделей, що використовують при моделюванні для вирішення поставленого завдання, були прийняті інтерполяційна та поліноміальна моделі.

Вихідною інформацією для побудови поверхонь є контрольні точки з координатами X, Y, Z. У нашому завданні це координати гирла розвідувальних свердловин, виїмкових полів і цілків, відмітки гирл розвідувальних свердловин, рівня ґрунтових вод, поверхні вугільних пластів, данні потужності вугільних пластів, що виймаються.

Інтерполяційна модель дозволила побудувати стовпчикову і каркасну модель поверхні землі, яка підроблена гірничими роботами.

Для побудови поліноміальної моделі в тривимірному просторі $z = f(x, y)$ використовували запропонований професором Зеленським А.С. алгоритм [1].

Розроблена методика тривимірного моделювання з використанням інтерполяційної та поліноміальної моделей деформації земної поверхні при виїмці вугільних пластів на шахтах ПрАТ «ДТЕК Павлоградвугілля» дозволила розробити програмне забезпечення. За допомогою розробленої програми з метою автоматизації прийняття рішень по мінімізації гідро-екологічних ризиків планується виконати моделювання і визначення площі та обсягів затопленої земної поверхні. Це дуже актуальна проблема при закритті шахт ПрАТ «ДТЕК Павлоградвугілля».

Перелік посилань

1. Зеленский А.С. Автоматизация геолого-маркшейдерского обеспечения в информационной системе управления рудным карьером / А.С. Зеленский, С.В. Баран, В.С. Лысенко. – Кривой Рог: Издательский центр ГВУЗ «КНУ», 2012. – 362 с.

УДК 004.942

Хрипливий А.Л., студент групи КН04-15-М
Кліщ С.М., аспірант кафедри інформаційних технологій та систем
Науковий керівник: Селівьорстова Т.В., к.т.н., доцент кафедри інформаційних технологій та систем
(Національна металургійна академія України, м. Дніпро, Україна)

ОСОБЛИВОСТІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ WEB-ДОДАТКУ НА PYTHON ДЛЯ ДОСЛІДЖЕННЯ СТАНУ ПЕРСОНАЛЬНОГО КОМП'ЮТЕРА В РЕАЛЬНОМУ ЧАСІ

В даний час віддалений моніторинг комп'ютера і контроль над його використанням стає все більш затребуваним. На ринку з'являються програми, які мають розширені функції віддаленого спостереження за робочими станціями користувачів, що дозволяють системним адміністраторам на підприємствах відстежувати мережеву активність співробітників в режимі реального часу, а також перевіряти конфігурацію встановлених пристроїв та програмного забезпечення на підключених до локальної обчислювальної мережі комп'ютерах, повністю контролюючи віддалені ПК без необхідності залишати своє постійне робоче місце [1,2].

Метою роботи було розробити програмну реалізацію додатку для збору частот процесора в реальному часі. Програмне забезпечення повинно мати веб інтерфейс, бути кросплатформеним, забезпечувати моніторинг необмеженої кількості хостів та експорт контрольних показників для подальшого їхнього аналізу засобами Matlab.

В роботі було використано робочу станцію Ubuntu 20.04 із встановленим Python. Для віртуалізації було застосовано гіпервізор другого типу VMware Workstation, який дозволяє користувачу встановлювати та адмініструвати віртуальні машини. У підготовленому віртуальному оточенні було використано 5 віртуальних машин (рисунок 1).

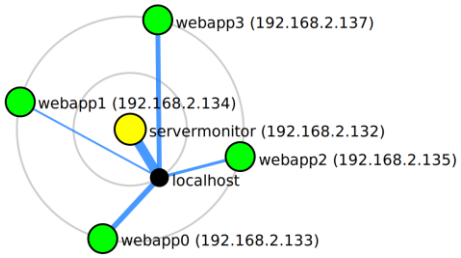

Рисунок 1 – Топологія віртуального мережевого оточення

Навантаження на процесори отримували із використанням команди hping3, після цього формувався масив даних, який аналізувався засобами Matlab. Був проведений аналіз отриманого часового ряду та встановлені його тенденції на базі показника Харста. Отримані результати можуть бути застосовані при плануванні мережевої інфраструктури в залежності від очікуваного навантаження на процесор.

Перелік посилань

1. Удаленный мониторинг компьютера [Електронний ресурс] // ALP Group – Режим доступу до ресурсу: https://alp-itsm.ru/interesting/udalennyij_monitoring_kompyutera/.
2. Индикаторы технического анализа в Timing Solution: Hurst Exponent [Електронний ресурс] – Режим доступу до ресурсу: https://timing-solution.livejournal.com/56355.html.

УДК 004.056

Литвак Ю.В. студентка гр.125м-19-1
Науковий керівник: Войцех Сергій Іванович, ст. викл. кафедри безпеки інформації та телекомунікацій.
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

ДЕСТРУКТИВНИЙ ВПЛИВ ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЕННЯ НА ТЕХНІЧНІ ЗАСОБИ ОБРОБКИ ІНФОРМАЦІЇ

Електромагнітні завади можуть призводити до порушення цілісності та доступносты інформації, що обробляється технічними засобами прийому, обробки, збереження та передачі інформації (ТЗПІ). Це створює загрозу інформаційній безпеці об'єктів інформаційної діяльності (ОІД) та може призвести до суттєвих збитків.

ВСТУП

Електромагнітні завади — електромагнітне збурення, яке погіршує характеристики обладнання, каналу передавання чи системи [1].

Електромагнітна завада (електромагнітна перешкода) — небажане фізичне явище або вплив електричних, магнітних або електромагнітних полів, електричних струмів або напружень зовнішнього або внутрішнього джерела, яке порушує нормальну роботу технічних засобів або викликає погіршення їх технічних характеристик і параметрів [2].

Під час радіоелектронної боротьби застосовується навмисний електромагнітний вплив, спрямований на ОІД, тобто створюється перешкода.

КЛАСИФІКАЦІЯ ЗАВАД

За походженням завади поділяються на природничі та штучні.

1. Природничі завади:
- Космічні шуми, реліктове випромінювання;
- Радіовипромінювання Землі й об'єктів Сонячної системи;
- Атмосферні завади Землі.

2. Штучні завади:
- Навмисні – створюється формуванням середовищ з метою забезпечення умов для витоку інформації з обмеженим доступом.
- Ненавмисні – утворюються зазвичай в результаті виникнення полів і середовищ їх поширення
- Індустріальні або промислові завади – випромінювання промислових машин, побутових електроприладів тощо;
- Контактні завади – завади, що виникають внаслідок перехідних процесів;
- Станційні завади – завади від інших радіоелектронних засобів: радіостанцій, радіолокаторів тощо [2].

За способом формування розрізняють активні та пасивні завади.

1. Активні – завади, що створюються енергією джерел завад (генераторів або ретрансляторів);

2. Пасивні – завади, що створюються розсіюванням енергії електромагнітних хвиль об'єктами або середовищами.

За структурою випромінювання завади поділяються на Неперервні та Імпульсні:

1. Неперервні – завади, модульовані за амплітудою, частотою (фазою) або шумовою напругою;

2. Імпульсні – завади у вигляді серій не модульованих або модульованих радіоімпульсів [3].

Завади розрізняють як модульовані (за амплітудою, частотою або фазою), так і немодульовані (синусоїдальні або шумові).

ТЕХНІЧНІ ЗАСОБИ СИЛОВОГО ДЕСТРУКТИВНОГО ВПЛИВУ ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЕННЯ

Будь-яка інформаційна система може бути атакована за допомогою бездротових технічних засобів силового деструктивного впливу електромагнітних імпульсів на такі елементи системи, як бездротові і провідні лінії зв'язку, системи електроживлення та заземлення, безпосередньо на електронні елементи різних блоків.

Високочастотні електромагнітні засоби силового впливу (магнетрони, лазери на вільних електронах, генератори тощо) є найбільш впливовими і зручними у застосуванні. Особливість генераторів полягає в тому, що вони мають широку смугу та працюють в міліметровому діапазоні з високим ККД (десятки відсотків).

В технічних засобах, які використовують для випромінювання електромагнітних коливань застосовують спеціальні антенні системи, від ефективності яких багато в чому залежать оперативно-технічні характеристики всього комплексу силового впливу [4].

Використання в нових технологіях фазованих антенних решіток дозволяє впливати відразу на декілька об’єктів.

Незважаючи на застосування спрямованих антен, потужний електромагнітний імпульс діє при атаці об'єкта на всі електронні компоненти в межах зони електромагнітного впливу і на всі контури, утворені зв'язками між елементами обладнання. Виводи транзисторів, конденсаторів, мікросхем і т. д. представляють собою «антени» для електромагнітних полів високої частоти [5,6].

Використання широкосмугових технічних засобів силового деструктивного впливу може призвести до значних порушення роботи технічних засобів прийому, зберігання та обробки інформації, знищення записів на магнітних носіях і т. п.

Тому, вдосконалення методів та засобів протидії деструктивному електромагнітному впливу сьогодні набуває додаткової актуальності.

Перелік посилань

1. Постанова КМ від 24.06.2009р. №679 "Про затвердження Технічного регламенту радіообладнання і телекомунікаційного кінцевого (термінального) обладнання"

2. Національна електронна бібліотека (Електрон. ресурс) / Основні причини виникнення взаємних завад та їх вплив на роботу на ТЗПІ/ Спосіб доступу: URL: https://studfile.net/preview/5368629/

3. Міночкін Д.А., к.т.н./Збірник наукових праць ВІТІ НТУУ „КПІ” № 1 – 2012/ Використання адаптивних антенних решіток для підвищення завадозахищеності систем радіозв'язкув складних завадових умовах

4. Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://supermegayo.ru/compterr/28.html. - Загол. з екрана

5. Національна електронна бібліотека (Електрон. ресурс) / Спосіб доступу: URL: http://supermegayo.ru/compterr/28.html. - Загол. з екрана

6. Перелік засобів загального призначення, які дозволені для забезпечення технічного захисту інформації, необхідність охорони якої визначено законодавством України від 10.09.2020.

УДК 004.056
Омелаєнко А. Г., студентка гр. 125м-19-1
Науковий керівник: Войцех Сергій Іванович, старший викладач кафедри безпеки інформації та телекомунікацій
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

МЕТОДИ ПОБУДОВИ КРИПТОГРАФІЧНИХ КОНСТРУКЦІЙ, СТІЙКИХ ДО ЗАГРОЗИ ЗАСТОСУВАННЯ КВАНТОВИХ ОБЧИСЛЕНЬ

Розглянуто можливості квантових обчислень. Зроблено порівняльний аналіз існуючих криптосистем. Наведені методи побудови нових криптографічних конструкцій.

Квантовий комп'ютер – обчислювальний пристрій, який для виконання своїх процесів використовує закони квантової фізики та об'єкти мікросвіту (фотони, іони, електрони).

Головні явища, які використовує квантовий комп'ютер — квантова суперпозиція та квантова заплутаність [1].

Квантові обчислення можуть бути застосовані у таких напрямах:

—Фінансове прогнозування;

—Економічна оптимізація;

—Моделювання хімічних реакцій (створення нових лікувальних препаратів);

—Моделювання взаємодії часток на атомарному рівні (відкриття нових фізичних явищ) (аналог адронного колайдера);

—Машинне навчання (навчання нейромереж);

—Квантові сенсори (метрологія, медицина, геодезія);

—Квантові комунікації (квантова телепортація);

—Квантова криптографія;

—Зведення експоненційно складних задач до поліноміального класу складності.

На відміну від класичних (лінійних) комп'ютерів, які оперують бітами, квантові комп'ютери для своїх обчислень використовують квантові біти або кубіти. Головною відмінністю і перевагою кубітів перед бітами — здатність перших перебувати у декількох станах (0 та 1) одночасно (принцип суперпозиції). За принципом суперпозиції [2], до вимірювання квантова система перебуває у ймовірнісному стані своїх можливих значень (тобто у кожен проміжок часу система може знаходитися в якомусь стані з деякою ймовірністю).

Можливості квантових комп'ютерів, які становлять загрозу для сучасної криптографії:

—вирішення деяких експоненційно-складних математичних задач за поліноміальний час, зокрема проблеми факторизації великих чисел (при умові, що на ньому можна буде реалізувати алгоритм Шора), що є загрозою для сучасних асиметричних криптосистем, таких як RSA, EIGamal, DiffieHellman, еліптична криптографія (Elliptic-curve cryptography (ECC));

—квадратичне зменшення часу пошуку в неупорядкованих базах даних (або ж метод грубої сили) (при можливості реалізації алгоритму Гровера), що є загрозою для симетричних криптосистем з недостатньо великим ключем шифрування; модулювання різних наукових систем, яке не може бути створене силами лінійних (неквантових) обчислень.

Криптографічні системи в загальному випадку поділяються на симетричні, асиметричні та гібридні [3].

В симетричних криптосистемах шифрування і дешифрування даних виконується за допомогою одного і того ж секретного ключа. Асиметричні криптосистеми оперують двома типами ключів: закритим і відкритим.

Недоліки асиметричних криптосистем відносно симетричних:

– повільне шифрування та дешифрування даних;

– великий розмір ключа;

– залежність від властивостей обраної математичної задачі;

– чутливість до атаки виду «людина посередині».

– переваги асиметричних криптосистем перед симетричними:

– в асиметричних криптосистемах закритий ключ не передається, а зберігається виключно у свого власника;

– при лінійному збільшенні кількості користувачів, збільшення загального числа ключів також має лінійний характер.

На сьогоднішній день обмін секретними даними здійснюється з використанням обох криптосистем. Криптосистема, яка об'єднує у собі симетричну і асиметричну криптосистеми, називається гібридною (змішаною) криптосистемою. У таких системах симетричні ключі використовуються для шифрування повідомлень у межах одного сеансу (для нового сеансу генерується новий симетричний ключ), а для засекречення сеансових ключів використовуються довгострокові асиметричні ключі.

Сучасна асиметрична криптографія не є стійкою до загрози застосування потужних квантових обчислень. Необхідна розробка нових методів асиметричного шифрування [4].

Криптографічні конструкції, стійкі до квантових обчислень:

1. Симетрична криптографія.
2. Квантова криптографія.
3. Криптографія на основі решіток.
4. Мультиваріативна криптографія.
5. Криптографія на основі геш-функцій.
6. Криптографія на основі кодів.
7. Криптографія ізогінеї суперсингулярних еліптичних кривих.

Сучасна симетрична криптографія з великим ключем шифрування є квантовостійкою. Квантова криптографія – це спосіб симетричної криптографії, який вирішує проблему розподілу ключа і є стійким до квантових обчислень за рахунок повністю випадкової послідовності для створення ключа. Криптографія на основі решіток, мультиваріативна криптографія, криптографія на основі геш-функцій, криптографія на основі кодів, криптографія ізогінеї суперсингулярних еліптичних кривих – квантовостійкі асиметричні криптосистеми.

Перелік посилань

1.Amir Fruchtman, Iris Choi. Technical Roadmap for Fault-Tolerant Quantum Computing.Universityof Oxford. 2016. URL https://nqit.ox.ac.uk/sites/ files/2016-11/ pdf.

2. Принцип суперпозиції (квантова механіка). 2020. URL: https://uk.wikipedia.org/wiki

3. Брюс Шнайер. Прикладная криптография: 2-е издание, 2016. − 610 с.

4. Ю. І. Горбенко, Р. С. Ганзя. Аналіз шляхів розвитку криптографії після появи квантових комп'ютерів. 2014. URL:http://ena.lp.edu.ua/bitstream/ntb/27194/1/8-40-48.pdf.

УДК 004.056

Рахімова А.М. , студентка гр. 125м-19-1
Науковий керівник: Войцех С. І., старший викладач кафедри безпеки інформації та телекомунікацій
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

МЕХАНІЗМ ЗАХИСТУ RPL ПРОТОКОЛУ МАРШРУТИЗАЦІЇ ДЛЯ МАЛОПОТУЖНИХ МЕРЕЖ З ВТРАТАМИ

Швидке зростання Інтернету речей (IoT) відкрило нові можливості, а разом з тим створило нові вразливості та загрози критичній інформації. Таким чином, забезпечення захисту інформації під час передачі даних потребує додаткової уваги, так як атаки на протокол маршрутизації можуть мати критичні наслідки для мереж IoT.

Бездротові сенсорні мережі відіграють ключову роль у створенні IoT та дозволяють пристроям з обмеженими ресурсами підключатися до Інтернету та надавати послуги. З еволюцією IoT звичайні протоколи маршрутизації вже не можуть підтримувати постійно зростаючу кількість вузлів мережі. З цієї причини робочою групою Internet Engineering Task Force (IETF) спеціально для мереж з низьким енергоспоживанням та втратами (low power and lossy networks - LLN) розроблений протокол маршрутизації RPL (Routing Protocol for Low-Power and Lossy Networks) [1]. Протоколу набув популярності і став фактичним протоколом маршрутизації в Інтернеті речей.

Мережевий шлях будується у вигляді деревоподібної топології, що має назву спрямованих ациклічних графіків - DODAG (Destination Oriented Directed Acyclic Graphs) [1]. При побудові топології RPL використовується 4 типи контрольних повідомлень:

- DIS-повідомлення - використовується, коли новий вузол намагається приєднатися до мережі та запитує інформацію про топологію;
- DIO-повідомлення - використовується для налаштування та оновлення топології мережі;
- DAO-повідомлення - використовується для розповсюдження інформації “вгору”, від нижчих вузлів до кореневого (root) вузла;
- DAO-ACK-повідомлення - використовується в одноадресній комунікації у відповідь на повідомлення.

RPL будує DODAG на основі рангу вузлів (рис. 1). Ранг визначає відносне розташування вузлів відносно кореня DODAG.

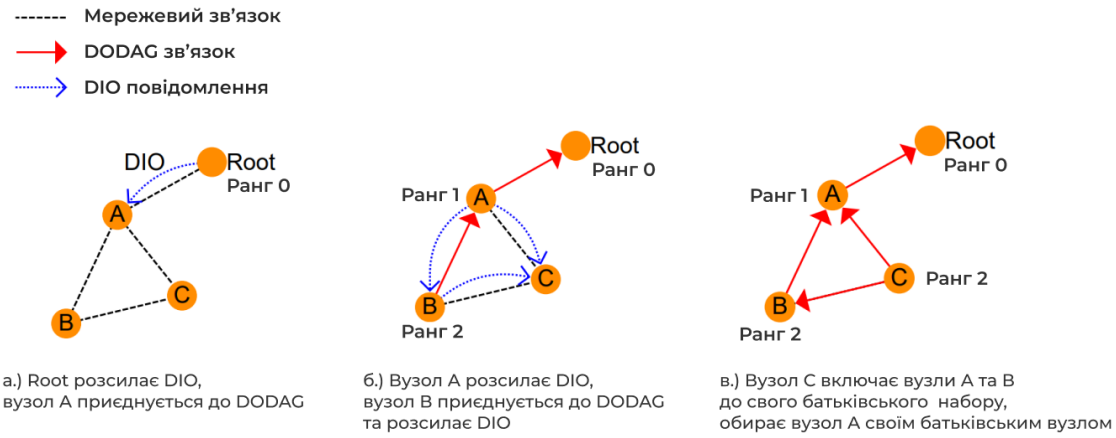

Рисунок 1 − Процес побудови DODAG

Root-вузол DODAG починає ініціалізацію RPL, періодично надсилаючи DIO повідомлення. Ці повідомлення містять усі необхідні параметри, що дозволяють навколишнім вузлам приєднуватися до DODAG. Отримавши кілька DIO, вузол приєднується до DODAG, створюючи список - так званий батьківський набір. Цей список містить адреси усіх можливих “батьків” - вузлів, що знаходяться ближче до кореневого пристрою. Серед батьківського набору він вибирає бажаного батька, тобто того, хто має найнижчий ранг. Після цього вузол обчислює власний ранг на основі батьківського рангу та цільової функції. Потім вузол може додатково рекламувати DODAG, розсилаючи власне DIO повідомлення [2].

Відповідно до специфікації [1] RPL протокол має три режими безпеки:

● “Незахищений” режим ("unsecured") - контрольні повідомлення відправляються без будь-яких механізмів захисту. Механізм захисту може бути присутній на канальному рівні.

● “Попередньо встановлений” режим ("preinstalled") - вузли, що приєднуються до екземпляра RPL, мають попередньо встановлені ключі, які дозволяють обробляти та генерувати захищені повідомлення RPL.

● “Автентифікований” режим ("authenticated") - вузли мають попередньо встановлені ключі, але даний ключ може використовуватися лише для приєднання вузла до DODAG. Приєднання автентифікованого екземпляра RPL як маршрутизатора вимагає отримання ключа від органу автентифікації. Процес отримання цього ключа виходить за рамки даної специфікації.

До недавнього часу “попередньо встановлений” або “автентифікований” режими не були реалізовані в жодній операційній системі IoT. Нещодавно була представлена часткова реалізація даних функцій для Contiki [3]. Але в роботі була проведена оцінка лише накладних витрат, спричинених реалізацією механізму безпеки. Таким чином, механізму захисту протоколу потребує додаткового дослідження впливу різних мережевих атак.

Перелік посилань

1. RFC 6560 “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks”. Proposed standard. Internet Engineering Task Force (IETF). March 2012, 157p

2. Brandon Foubert “Cooperation between multiple RPL networks”. Networking and Internet Architecture, 2018, 43p.

3. Pericle Perazzo et al. “An Evaluation of the RPL Security Mechanisms for IoT Secure Routing”. University of Pisa, Department of Information Engineering, Pisa 56122, Italy, 2017, 12p.

УДК 004.942

Темчур В.О., студент групи КН901-14-1М
Наукові керівники: Селівьорстова Т.В., к.т.н., доцент кафедри інформаційних технологій та систем; Селегей А.С., к.т.н., доцент кафедри теорії металургійних процесів та хімії
(Національна металургійна академія України, м. Дніпро, Україна)

РОЗРОБКА СПЕЦІАЛІЗОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ДОСЛІДЖЕННЯ РУДНОГО НАВАНТАЖЕННЯ ДОМЕННОЇ ПЕЧІ

Завдання автоматизації математичних розрахунків і обчислень походить з витоків людської цивілізації, до появи перших рахункових пристроїв – абака, соробану та інших елементарних пристосувань. В наші дні практично всі інженерні розрахунки проводяться із застосуванням комп'ютерної техніки [1]. При цьому, сфера розробки інженерного програмного забезпечення відокремилася в окрему IT-індустрію, яка працює на стику різних науково-технічних знань і дисциплін – математики, фізики, електроніки, програмування. Цей міждисциплінарний підхід в повній мірі поєднує в собі ідеї STEM (science, technology, engineering, mathematics).

Рудне навантаження є одним з основних показників доменної плавки. Воно являє собою відношення маси залізорудної частини доменної шихти до коксової частини. Рудне навантаження змінюється вздовж радіуса колошника доменної печі. Даний розрахунок досить складний [2], тому розробка спеціалізованого програмного забезпечення для визначення завантаження доменної печі є актуальною задачею.

Методика визначення досить трудомістка і передбачає розбиття колошника на десять рівновеликих по площі кільцевих зон. Для визначення рудного навантаження в кожній радіально кільцевої зоні колошника необхідно знати кількість матеріалу і маси, що завантажується в неї. На сьогоднішній день відома інженерна методика для визначення рудного навантаження в кільцевій зоні. Вона являє собою теоретичний розрахунок траєкторії шихтових матеріалів, що засипають з лотка-розподільника безконусного завантажувального пристрою доменної печі. Однак зміна шихтових умов ведення доменної плавки викликає зміни траєкторії. Обчислення траєкторії є досить трудомістким процесом. У зв'язку з цим оперативно реагувати на зміну шихтових умовах при розрахунку рудної навантаження досить складно. Тому запропонована нова методика для визначення частинних і загальних рудних навантажень, заснована на показниках радарних датчиків рівня, розташованих на куполі колошника доменної печі. Запис рівнів засипання шихтових матеріалів дозволяє визначити їх об’єм. З огляду на насипну щільність даних матеріалів, можна обчислити фактичну масу. Знаючи ці параметри, неважко обчислити фактичне рудне навантаження доменної печі.

Розробку програмного додатку виконано із використанням C++ Builder. Додаток реалізує запропоновану Андрієм Селегеєм методику визначення рудного навантаження доменної печі, протестовану на даних, отриманих з радарів, що встановлені над колошником доменної печі. Розробка призначена для обробки статичних даних, проте її функціонал можливо гнучко пристосувати для обробки даних в реальному часі.

Перелік посилань

1. Артьомов В. Інженерні розрахунки і програми для інженерних розрахунків [Електронний ресурс] / Віталій Артьомов – Режим доступу до ресурсу: https://www.dystlab.store/index.php/uk/blog/80-longread/150-engineering-calculus-uk.

2. К вопросу создания информационной модели загрузки шихты в доменную печь / [А. Н. Селегей, В. И. Головко, М. А. Рыбальченко та ін.]. // Збірник наукових праць Національного гірничого університету. – 2017. – №52. – С. 272–278.