КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2(14), 2021
ISSN 2663 - 4023
DOI: 10.28925/2663-4023.2021.14.8799
УДК 004.946.5.056

Чубаєвський Віталій Іванович
к.п.н., доцент,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Лахно Валерій Анатолійович
д.т.н., професор,
завідувач кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Ахметов Берік
доктор філософії, професор
Каспійський університет технологій та інженірингу імені.Ш.Есенова, м.Актау, Казахстан
ORCID ID: 0000-0003-2860-2188
lim4best@gmail.com

Криворучко Олена Володимирівна
д.т.н., професор,
завідувач кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Касаткін Дмитро Юрійович
к.пед.н., доцент,
доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0002-2642-8908
dm_kasat@ukr.net

Десятко Альона Миколаївна
доктор філософії,
доцент кафедри інженерії програмного забезпечення та кібербезпеки
Київський національний торговельно-економічний університет, м.Київ, Україна
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Литовченко Тарас Олексійович
аспірант кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, м.Київ, Україна
ORCID ID: 0000-0002-3869-367X
Ltmyjob28@nubip.edu.ua

ОПТИМІЗАЦІЇ РЕЗЕРВУ ОБЛАДНАННЯ ДЛЯ ІНТЕЛЕКТУАЛЬНИХ АВТОМАТИЗОВАНИХ СИСТЕМ

Анотація. Запропоновано алгоритми для нейромережевого аналізатора, задіяного у системі підтримки прийняття рішень (СППР) у ході вибору складу резервного обладнання (СРО) для інтелектуальних автоматизованих систем управління (ІАСУ) Smart City. Розроблено модель, алгоритми та відповідне програмне забезпечення для вирішення оптимізаційного завдання вибору СРО, здатного забезпечити безперебійну роботу ІАСУ як в умовах технологічних

збоїв, так і в умовах деструктивного втручання у роботу ІАСУ з боку атакуючих. Запропоновані рішення сприяють скороченню витрат на визначення оптимального СРО для ІАС на 15–17% порівняно з результатами відомих методів розрахунку. Наведено результати обчислювальних експериментів для вивчення ступеня впливу кількості виходів нейромережевого аналізатора на ефективність функціонування СРО для ІАСУ.

Ключові слова: Smart City; інтелектуальна автоматизована система управління; резерв обладнання; алгоритм; оптимізація.

ВСТУП

Сучасні міста є базовими точками розвитку економіки та людського капіталу. Оскільки центром уваги будь-якої цивілізованої держави є людина – все, що робиться у містах, робиться заради людей і для людей. Зі зростанням міського населення посилюється і вплив міст в економіці, а також їх роль у сучасному постіндустріальному світі. На етапі розвитку міста грають провідну роль загальному розвитку економік країн, як у локальному, і на національному рівнях. Саме у містах виробляється ключова частина валової внутрішньої продукції, формуються споживчі потреби та налагоджуються міжнародні зв'язки. Там сконцентровано основну частину населення багатьох провідних країн світу. В результаті розвитку інформаційних технологій (ІТ), усі великі міста почали розглядати можливості застосування потенціалу ІТ для спрощення систем управління муніципальною інфраструктурою, а також при застосуванні в інших сферах міського життя.

Як показує світова практика в процесі роботи складних інтелектуальних автоматизованих систем управління (ІАСУ), які керують багатьма процесами в Smart City (транспорт, освітлення, розподіл електричної енергії, безпека та ін.) неминуче виникають ускладнення або аварійні ситуації. Частково ці ускладнення чи аварійні ситуації виникають внаслідок порушення технологій експлуатації обладнання. Проте за останні роки багато порушень працездатності ІАСУ спричинені деструктивним втручанням комп'ютерних зловмисників (хакерів).

Апаратні засоби ІАСУ Smart City слід розглядати як складну технічну систему, в якій є велика кількість взаємозалежних елементів, компонентів та складових частин. У процесі експлуатації складових елементів та компонентів ІАСУ Smart City необхідно своєчасно виявляти та попереджувати потенційні відмови багатьох апаратних систем, наприклад, датчиків, сенсорів, камер відеоспостереження, мережевого обладнання тощо. Як правило, ще на стадії розробки таких складних систем, проектувальники закладають у їх конструкцію можливості для автоматичного відновлення працездатності багатьох елементів. Однак, така ситуація можлива далеко не завжди. Можливості щодо відновлення працездатності компонентів ІАСУ визначаються такими основними факторами як ресурси системи технічного забезпечення, ресурси працівників ремонтних служб, ресурси для транспортування резервного обладнання, топологія ІАСУ та її системи відновлення.

Як зазначає ряд досліджень [1-3] ІАСУ Smart City дедалі частіше стають об'єктами таргетованих атак [4, 5] та, відповідно, перелік кіберзагроз постійно зростає. Проблематика інформаційної безпеки (ІБ) при побудові Smart City стала однією з найбільш обговорюваних серед наукової спільноти [6, 7] та спеціалістів практиків [8]. Зростання кіберзагроз для ІБ Smart City призвело до того, що ризик виходу з ладу ІАСУ багатьох процесів Smart City, змусив задуматися про вузькі місця. Наприклад, ризики, пов'язані з тим, що цифрова і фізична інфраструктура Smart City неминуче

перетинається. Маштабним кібератакам можуть бути піддані будь-які системи управління Smart City. А ці системи, як правило, нерозривно пов'язані між собою.

Зростання кількості та складності сценаріїв проведення кібератак призвело до того, що і так досить складна архітектура ІАСУ має потребу в доукомплектації різноманітними системами захисту інформації (СЗІ). Ландшафт кіберзагроз для ІАСУ, що змінився за останнє десятиліття, у тому числі у Smart City, породив необхідність визначення оптимального складу резервного обладнання, включаючи і СЗІ. Зауважимо, що в міру ускладнення архітектури ІАСУ обчислювальна складність пошуку оптимального складу резерву обладнання (СРО) теж зросла. Навіть висококваліфіковані експерти не завжди здатні оперативно проаналізувати усі змінні для такого класу завдань та видати обґрунтовані, підкріплені відповідними розрахунками рекомендації щодо побудови надійної архітектури ІАСУ.

Як показує практика для будь-якої ІАСУ, доцільно сформувати резерв, зокрема, і на випадок виходу обладнання з ладу внаслідок технологічних збоїв або кібератак. Вихід із роботи, наприклад, серверного обладнання або комутаційного вузла, виведе з ладу всю ІАСУ Smart City. Як показано в роботах [9, 10], всі сучасні рішення для ІАСУ обов'язково передбачають можливості створення резервного складу обладнання.

Вище наведені аргументи визначають релевантність пошуку нових моделей та методів для вирішення задачі з оптимізації складу резервного обладнання для ІАСУ Smart City. Причому акцент у вирішенні цієї оптимізаційної задачі повинен бути на її алгоритмізації з подальшим переведенням рішення в кібернетичну площину, коли оптимальний варіант можна знайти задіявши потенціал інтелектуальних систем підтримки прийняття рішення (далі СППР).

Постановка проблеми.

Розробка алгоритму для нейромережевого аналізатора, задіяного у системі підтримки прийняття рішень (СППР) у ході вибору складу резервного обладнання (СРО) для інтелектуальних автоматизованих систем управління (ІАСУ) Smart City

Аналіз останніх досліджень і публікацій. Вихід з ладу багатьох компонентів ІАСУ Smart City, наприклад, таких важливих як серверне та комунікаційне обладнання, джерела безперебійного живлення, СЗІ тощо. навіть на короткий час - втрати для бізнес-процесів Smart City. Слід зазначити, що при виявленні передаварійних ситуацій, наприклад, спричинених деструктивними діями атакуючої сторони або просто через технологічні збої в ході експлуатації ІАСУ для Smart City, розмірність простору ознак досить велика. Крім того, межі між класами різних типів аварійних ситуацій, які передбачають необхідність резерву обладнання для ІАСУ, у більшості ситуацій є нечіткими. Питанням мінімізації розмірності простору ознак при виявленні передаварійних станів обладнання ІАСУ для Smart City та при виявленні вторгнень присвячено чимало робіт. Наприклад, у роботах [11-14] показано, що застосування моделей, побудованих на байесівській класифікації [11, 12], та методах кластерного аналізу [13, 14] для вирішення завдання розпізнавання потенційно передаварійних ситуацій в ІАСУ, недоцільно через неточність отриманих висновків . Як показано в роботах [15, 16], для вирішення подібного класу задач краще задіяти штучні нейронні мережі (ШНМ). Наприклад, ШНМ прямого поширення. Як алгоритм навчання таких мереж можна застосувати алгоритм зворотного поширення помилки [17]. У роботах [18, 19] запропоновані математичні моделі на навчання ШНМ. Порівняно з іншими підходами, викладеними, наприклад, у роботах [20, 21], застосування ШНМ забезпечує універсальність алгоритму навчання.

ISSN 2663 - 4023

Зауважимо, що застосування алгоритму зворотного поширення помилки для навчання багатошарової ШНМ дасть можливість побудувати нейромережевий аналізатор для оптимізації СРО для ІАСУ Smart City та класифікації передаварійних ситуацій на об'єктах інформатизації, зокрема, що виникають через деструктивні дії атакуючої сторони.

Мета статті. Розробка алгоритмів для нейромережевого аналізатора (НА) для підвищення ефективності формування складу резервного обладнання для ІАСУ для Smart City, що дозволить скоротити час на ліквідацію аварійних ситуацій, а також знизити витрати на резервне обладнання, що забезпечує усунення відмов в ІАСУ для Smart City.

Для досягнення мети дослідження необхідно вирішити такі завдання:

- розробити нові алгоритми для СППР та НА аварійні ситуації під час вирішення оптимізаційної задачі вибору складу резервного обладнання для ІАСУ Smart City;
- провести обчислювальні експерименти для вивчення ступеня впливу кількості виходів НА на ефективність вибору складу резервного обладнання для ІАСУ Smart City.

МЕТОДИ І МОДЕЛІ ДОСЛІДЖЕННЯ

Введемо такі позначення:

U_{ij} – питоме збільшення резервних елементів i – го типу для j – го контуру ІАСУ для Smart City; m – кількість елементів для заданого типу обладнання ІАСУ для Smart City; t_r – час, витрачений на відновлення роботи ІАСУ для Smart City після аварійної ситуації, викликаної технологічними або іншими причинами; t_d – час, витрачений на доставку резервного обладнання до певного контуру ІАСУ для Smart City; t_p – час, витрачений ремонт; t_i – час, витрачений на поповнення резерву для елементів i – го типу; R – кількісний склад резерву обладнання відновлення роботи ІАСУ для Smart City; C – вартість СРО; C_d – вартість доставки резервного устаткування складу; C^0 – вартість серійного зразка обладнання для контуру ІАСУ для Smart City; k – номер кроку у процесі пошуку оптимального СРО; δ_{ij} – збільшення резервних елементів i – го типу для j – го контуру ІАСУ для Smart City.

Проблематиці обґрунтування кількісного складу резервного обладнання (СРО) для забезпечення поточних ремонтів ІАСУ Smart City не приділялося належної уваги. Хоча забезпечення відновлення працездатності як окремих контурів, так і ІАСУ для Smart City в цілому, необхідно розглядати як невід'ємну складову ефективної експлуатації ІАСУ. Завдання оптимізації складу СРО можна, наприклад, розглянути прийнявши як базовий критерій мінімальну вартість СРО.

Залежність для вирішення прямого оптимізаційного завдання для визначення СРО можна записати так:

$$C^0_{\sum CPO} = \sum_{i=1}^{N} C_i \cdot R_i^{opt} = \min_{(R_i,\dots R_N)} \sum_{i=1}^{N} C_i \cdot R_i \,, \quad ' \qquad (1)$$

при обмеженнях $SP(R_1,\dots R_N) \geq SP^0$,

ISSN 2663 - 4023

де N – кількість типів запасних частин (ЗЧ) для ІАСУ для Smart City;

$C_1,...,C_N$ – вектор вартості ЗЧ;

$R_1,...,R_N$ – оптимальний комплект ЗЧ;

SP^0 – нормативне значення критерію достатності ЗЧ для ІАСУ Smart City.

У результаті розробки методики визначення оптимального резерву запасного устаткування ИАСУ для Smart City застосовувався ієрархічний принцип. Відповідно до цього принципу для відновлення працездатності одного контуру ІАСУ можна використовувати два підходи. Перший – локальне розташування резервного устаткування. Наприклад, для автоматизованої системи управління міським транспортом, резервне обладнання розташовують безпосередньо в ситуаційному центрі управління роботою транспорту. Це дозволяє оперативно усувати наслідки аварійних ситуацій і забезпечує швидку заміну обладнання, що вийшло з ладу. Другий підхід – складське зберігання групового запасу резервів устаткування. Якщо в контурах ІАСУ експлуатуються однотипні вироби, наприклад, комутатори, маршрутизатори, камери відеоспостереження тощо, можна створити груповий запас резервного обладнання. Він доступний для всіх контурів ІАСУ Smart City, хоча територіально кожен із цих контурів може бути розташований досить далеко. Наприклад, Smart системи для управління охороною здоров'я або освітою розумного міста територіально не розташовують поруч із системами управління міським транспортом або розподілом електроенергії

Відповідно, відновити працездатність ІАСУ Smart City можна застосувавши два описані вище підходи.

Пропонується оптимізувати систему СРО для ІАСУ Smart City, прийнявши за основу наведений внесок кожного елемента в середній час, витрачене на відновлення працездатності ІАСУ Smart City в цілому.

Було розроблено відповідний ітераційний алгоритм, який може бути задіяний у обчислювальному ядрі СППР (Рис. 1, а, б, в). Алгоритм включає три підалгоритма.

У першому випадку див. рис. 1.а можна знайти наближене рішення оптимізаційної задачі. Для випадку, якщо задані обмеження на вартість СРО для ІАСУ Smart City.

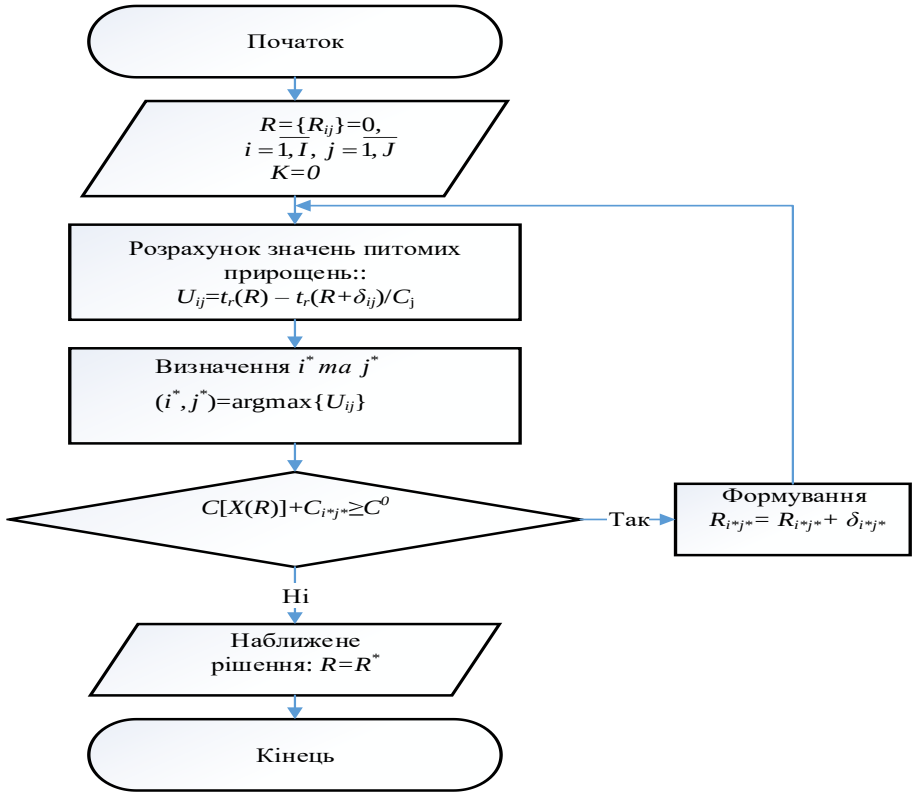
Для підвищення працездатності ІАСУ Smart City у складі модуля СППР щодо формування оптимального СРО було запропоновано задіяти нейромережевий аналізатор (НА) (Рис. 2). Даний НА дозволяє аналізувати дані про відмови обладнання ІАСУ Smart City за контурами і в подальшому використовувати ці дані для оптимізації СРО для контурів ІАСУ Smart City. Таким чином, НА є джерелом додаткових даних, що стосуються оцінювання працездатності ключового обладнання ІАСУ Smart City. Застосування НА дозволить удосконалити стратегії формування СРО та скоротити витрати на підтримку ІАСУ Smart City у робочому стані.

Як критерій оптимізації прийнятий наступний параметр:

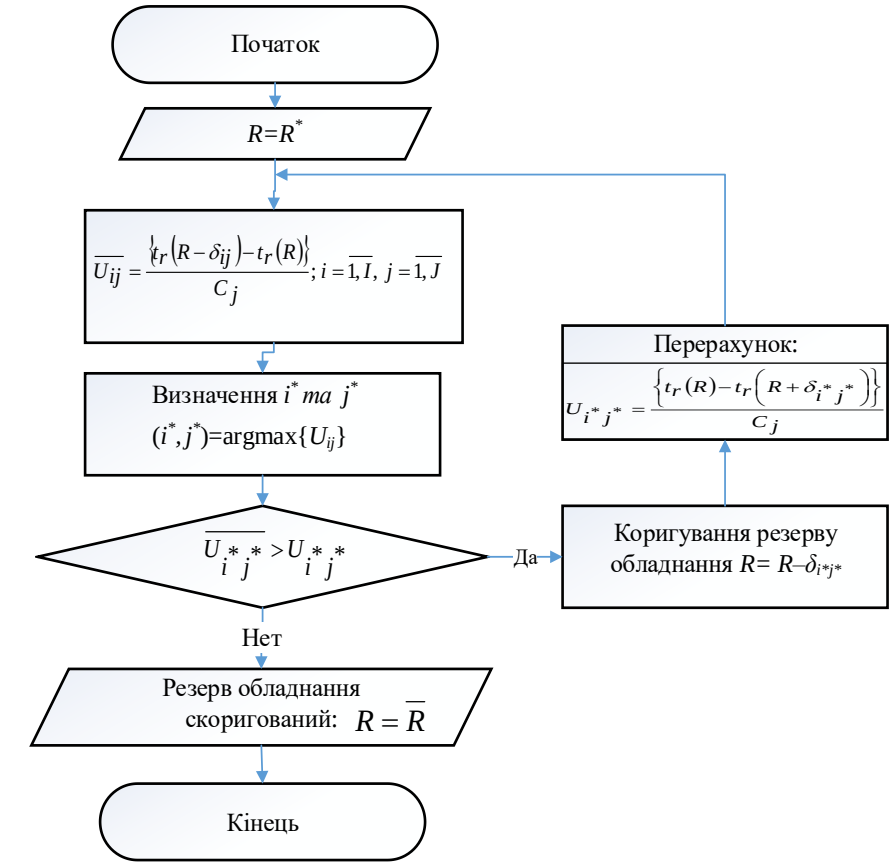
$$E = E_{ex} + E_{st} + E_s + E_{tr}, \tag{2}$$

Де $E_{ex}, E_{st}, E_s, E_{tr}$ – відповідно, витрати на експлуатацію обладнання ІАСУ, простой; зберігання СРО на складах; транспортування СРО.

ISSN 2663 - 4023

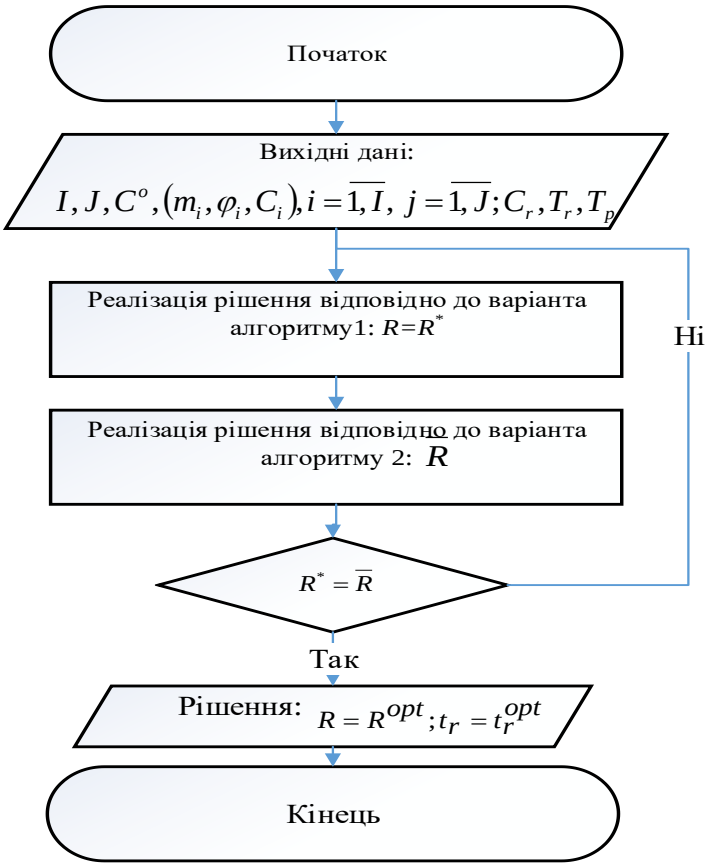


а)



б)

ISSN 2663 - 4023



в)

Рис. 1. Блок схема алгоритму для формування резерву обладнання для ІАСУ Smart City

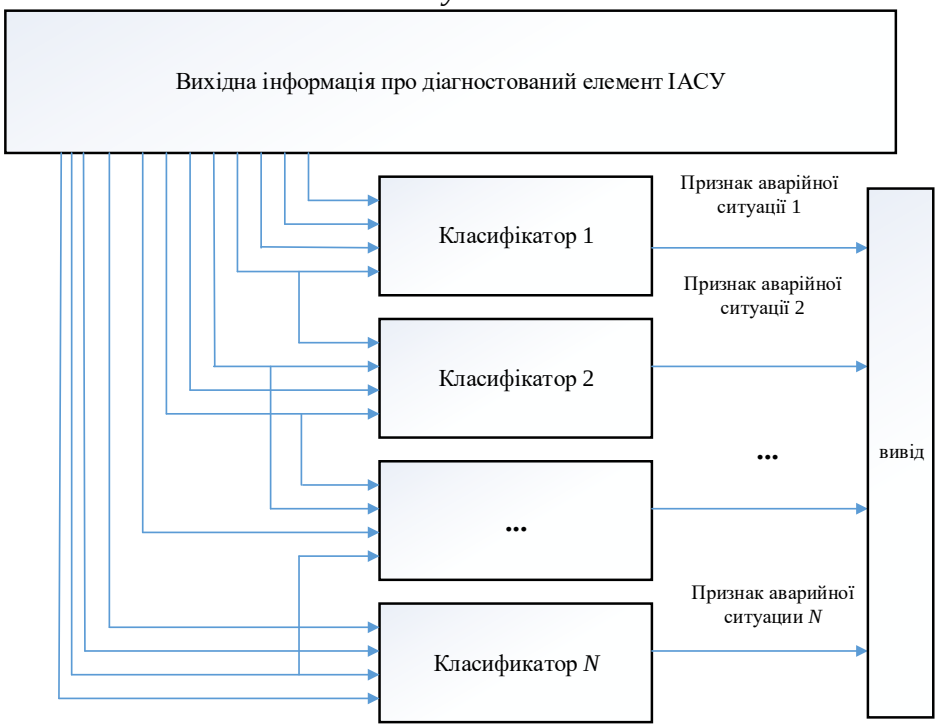


Рис. 2. Схема нейромережевого аналізатора, задіяного у складі СППР під час вибору СРО для ІАСУ Smart City

Розроблені моделі та відповідні алгоритми для НА, що застосовується в ході вирішення задачі оптимізації СРО для ІАСУ для Smart City, були реалізовані в прототипі модуля СППР.

ОБЧИСЛЮВАЛЬНИЙ ЕКСПЕРИМЕНТ

Даний прототип модуля СППР дозволяє у зручному для адміністратора ІАСУ Smart City графічному інтерфейсі виконати аналіз варіантів розв'язання задачі з оптимізації СРО для ІАСУ Smart City залежно від переліку передаварійних станів, виявлених за допомогою НА під час моніторингу роботи ІАСУ для Smart City.

Розроблений модуль дозволяє переглядати діагностичні повідомлення для визначення складу резервного обладнання для ІАСУ, а також, базові рекомендації та способи їх усунення.

Експериментальні дослідження розробленого модуля СППР проводилися для двох напрямів розвитку ІАСУ для Smart City. Перше – розумний транспорт. Друге – розумна освіта.

Працездатність модуля СППР перевірялася в ході оцінювання СРО АСУ для низки транспортних підприємств м. Києва, які впровадили елементи загальноміської інформаційної системи SEA Smart City. Для другого напряму експериментальні дослідження проводились на базі Національного університету біоресурсів та природокористування України, Єсенівського університету м. Актау Казахстан, Київського національного торговельно-економічного університету. Зазначені університети обрані як бази експериментального дослідження, оскільки активно розвивають Smart технології в навчанні, орієнтовані на: гнучке навчання в інтерактивному освітньому середовищі; швидку адаптацію студентів до навколишнього середовища, що стрімко змінюється; вільний доступ до освітнього контенту всього світу та ін.

Обчислювальні експерименти для оцінювання ефективності спільного застосування модуля СППР у ході оптимізації СРО для ІАСУ для Smart City та НА для розпізнавання аварійних ситуацій проводилися для різних стратегій експлуатації обладнання контурів ІАСУ (Рис. 3). На Рис 3. показані розрахункові залежності наведених витрат для різних стратегій експлуатації ІАСУ транспортним підприємством та АСУ університетів.

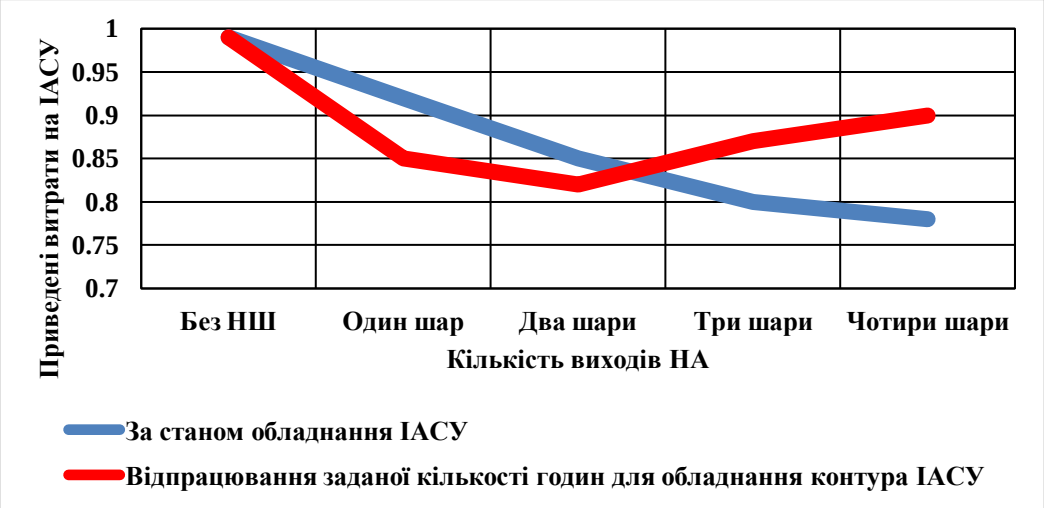


Рис. 3. Розрахункові залежності наведених витрат для різних стратегій експлуатації ІАСУ та кількості шарів у НА

ISSN 2663 - 4023

При цьому, в ході обчислювального експерименту, задіяно різну кількість нейронів у вихідному шарі.

На рисунку 4 показані залежності кількості ітерацій у процесі навчання НА від кількості нейронів та кількості шарів НА.

На рисунку 5 показані залежності, що характеризують ймовірність точності розпізнавання аварійних ситуацій та правильне формування СРО для ІАСУ від кількості нейронів та кількості шарів НА.

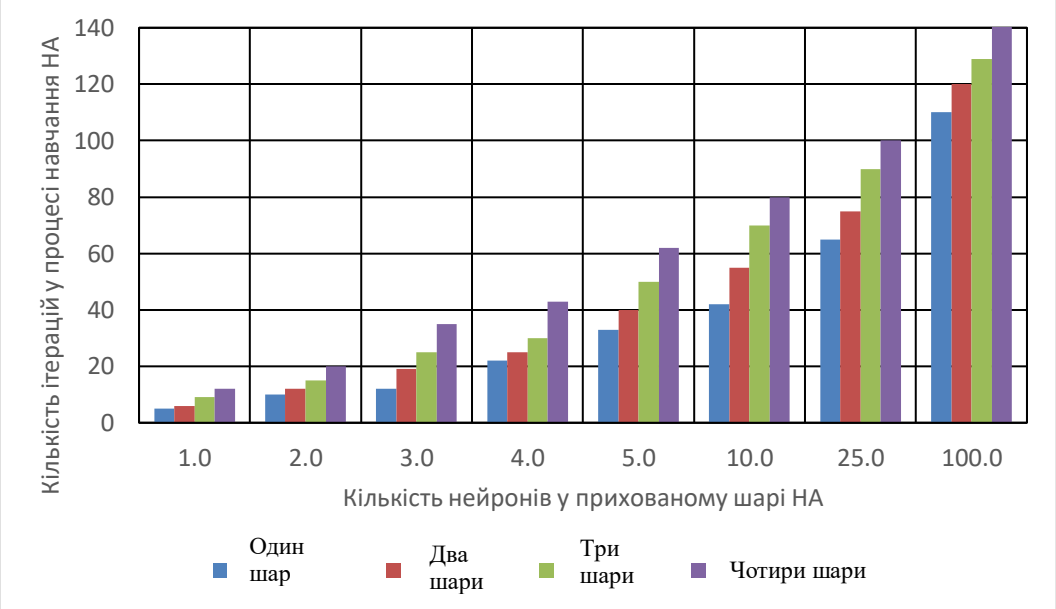


Рис. 4. Кількості ітерацій у процесі навчання НА від кількості нейронів та кількості шарів у НА

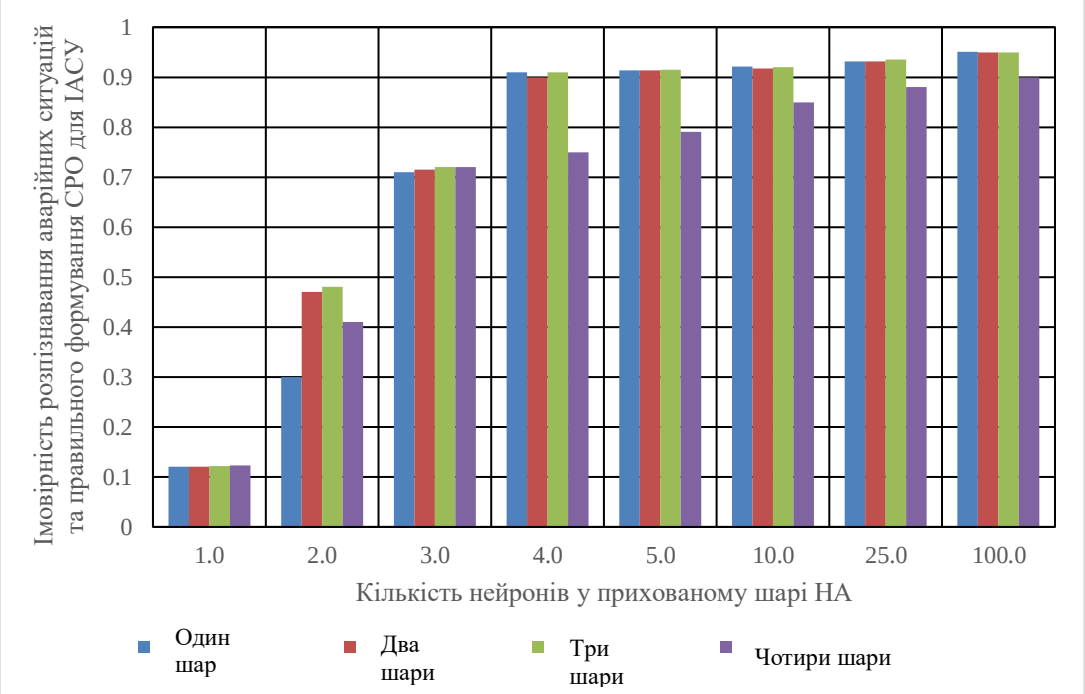


Рис. 5. Імовірність точності розпізнавання аварійних ситуацій та правильного формування СРО для ІАСУ від кількості нейронів та кількості шарів у НА

Як видно з отриманих графіків (Рис.3-5), найбільшого ефекту можна досягти у разі застосування стратегії експлуатації обладнання ІАСУ до вироблення заданої кількості годин. Розроблена СППР і НА можуть досить ефективно застосовуватися в процесі вирішення задачі вибору оптимального складу резервного обладнання, здатного забезпечити безперебійну роботу ІАСУ для Smart City як в умовах технологічних збоїв, так і в умовах деструктивного втручання в роботу ІАСУ Smart City з боку атакуючих. Пропоновані рішення сприяють скороченню витрат на створення складу резервного обладнання для ІАСУ для Smart City на 15-17% порівняно з результатами відомих методів розрахунку [22, 23].

У процесі обчислювальних експериментів показано, що оптимальне число виходів дорівнює 2–3. Така кількість виходів забезпечує, у своїй зниження наведених витрат за створення резерву устаткування ІАСУ для

В результаті проведених експериментів встановлено, для практичного застосування доцільно вибрати структуру, яка складається з одного прихованого шару. Кількість нейронів у прихованому слід прийняти рівною кількості входів НА.

ПОДЯКИ

Робота виконана в рамках грантового дослідження АР08855887-ОТ-20 «Розробка інтелектуальної системи підтримки прийняття рішень у процесі інвестування у системи кібернетичної безпеки».

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропоновано: для оцінювання ефективності вибору складу резервного обладнання для ІАСУ Smart City, у тому числі комплексу складу СЗІ, застосовувати систему показників достатності.

Розроблено: модель, алгоритм та відповідне ПЗ для вирішення оптимізаційної задачі вибору складу резервного обладнання, здатного забезпечити безперебійну роботу ІАСУ для Smart City як в умовах технологічних збоїв, так і в умовах деструктивного втручання в роботу ІАСУ для Smart City з боку атакуючих. Пропоновані рішення сприяють скороченню витрат на створення складу резервного обладнання для ІАСУ Smart City на 15-17%, порівняно з результатами відомих методів розрахунку.

Проведено обчислювальні експерименти для вивчення ступеня впливу кількості виходів нейромережевого аналізатора на ефективність вибору складу резервного обладнання для ІАСУ Smart City. Також розглянуто різноманітні стратегії експлуатації резервного обладнання для ІАСУ для Smart City.

Показано, що оптимальна кількість виходів нейромережевого аналізатора дорівнює 2-3. Така кількість виходів забезпечує, у своїй зниження наведених витрат за створення резерву устаткування ІАСУ для Smart City у середньому 17–21%.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0305-0310). IEEE.

2 Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques. International Journal of Environmental Research and Public Health, 17(24), 9347.
3 Lee, J., Kim, J., & Seo, J. (2019, January). Cyber attack scenarios on smart city and their ripple effects. In 2019 International Conference on Platform Technology and Service (PlatCon) (pp. 1-5). IEEE.
4 Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. Machines, 9(4), 78.
5 Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of Urban Technology, 26(2), 47-65.
6 Ferraz, F. S., & Ferraz, C. A. G. (2014, December). Smart city security issues: depicting information security issues in the role of an urban environment. In 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (pp. 842-847). IEEE.
7 Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. Sustainability, 12(7), 2916.
8 Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y., & Han, Z. (2019). Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access, 7, 54508-54521.
9 Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946.
10 Hajian-Hoseinabadi, H. (2011). Impacts of automated control systems on substation reliability. IEEE Transactions on Power Delivery, 26(3), 1681-1691.
11 Weber, P., & Jouffe, L. (2006). Complex system reliability modelling with dynamic object oriented Bayesian networks (DOOBN). Reliability Engineering & System Safety, 91(2), 149-162.
12 Cai, B., Liu, H., & Xie, M. (2016). A real-time fault diagnosis methodology of complex systems using object-oriented Bayesian networks. Mechanical Systems and Signal Processing, 80, 31-44.
13 Kuhn, R., & Culhane, D. P. (1998). Applying cluster analysis to test a typology of homelessness by pattern of shelter utilization: Results from the analysis of administrative data. American journal of community psychology, 26(2), 207-232.
14 Maździarz, A. Alarm Correlation in Mobile Telecommunications Networks based on k-means Cluster Analysis Method. Journal of telecommunications and information technology, 2, 2018, pp.95-102. https://doi.org/10.26636/jtit.2018.124518
15 Bapiyev, I. M., Aitchanov, B. H., Tereikovskyi, I. A., Tereikovska, L. A., & Korchenko, A. A. (2017). Deep neural networks in cyber attack detection systems. International Journal of Civil Engineering and Technology (IJCIET), 8(11), 1086-1092.
16 Wang, G., Hao, J., Ma, J., & Huang, L. (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert systems with applications, 37(9), 6225-6232.
17 Cilimkovic, M. (2015). Neural networks and back propagation algorithm. Institute of Technology Blanchardstown, Blanchardstown Road North Dublin, 15, 1-12.
18 Wilamowski, B. M. (2009). Neural network architectures and learning algorithms. IEEE Industrial Electronics Magazine, 3(4), 56-63.
19 Prechelt, L. (1996). A quantitative study of experimental evaluations of neural network learning algorithms: Current research practice. Neural Networks, 9(3), 457-462.
20 Karayiannis, N. B., & Venetsanopoulos, A. N. (1993). Fast learning algorithms for neural networks. In Artificial Neural Networks (pp. 141-193). Springer, Boston, MA.
21 Tamp, N. V., & Tamp, V. L. (2016). Programma raspoznavaniya sostoyanij informacionno-vychislitel'noj seti na osnove nejronnoj seti s obratnym rasprostraneniem oshibok. Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM Nomer svidetel'stva: RU 2016660599.
22 CHEN, Mu-Chen; HSU, Chih-Ming; CHEN, Shih-Wei. Optimizing joint maintenance and stock provisioning policy for a multi-echelon spare part logistics network. Journal of the Chinese Institute of Industrial Engineers, 2006, 23.4: 289-302.
23 MOURONTE-LÓPEZ, Mary Luz. Optimizing the spare parts management process in a communication network. Journal of Network and Systems Management, 2018, 26.1: 169-188.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (14), 2021
ISSN 2663 - 4023

Vitaliy Chubaievskyi
Candidate of Political Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0001-8078-2652
chubaievskyi_vi@knute.edu.ua

Valery Lakhno
Doctor of Technical Sciences, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0001-9695-4543
lva964@gmail.com

Berik Akhmetov
PhD in Computer Sciences, Professor
Caspian University of Technology and Engineering named after Sh.Yessenov, Aktau, Kazakhstan
ORCID ID: 0000-0002-4377-0916
andriy.blozva@nubip.edu.ua

Olena Kryvoruchko
Doctor of Engineering Sciences, Professor, Head of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0002-7661-9227
kryvoruchko_ev@knute.edu.ua

Dmytro Kasatkin
Candidate of Pedagogical Sciences, Associate Professor, Associate Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0002-2642-8908
dm_kasat@ukr.net

Alona Desiatko
PhD in Computer Sciences, Associate Professor of Department of Software Engineering and Cyber Security
Kyiv National University of Trade and Economics, Kyiv, Ukraine
ORCID ID: 0000-0003-2860-2188
desyatko@knute.edu.ua

Taras Litovchenko
Graduate student of the Department of Computer Science and Networks
National University of Life and Environmental Sciences of Ukraine Kyiv, Ukraine
ORCID ID: 0000-0002-3869-367X
gusevbs@gmail.com

OPTIMIZATION OF EQUIPMENT RESERVE FOR INTELLECTUAL AUTOMATED SYSTEMS

Abstract. Algorithms for a neural network analyzer involved in the decision support system (DSS) during the selection of the composition of backup equipment (CBE) for intelligent automated control systems Smart City are proposed. A model, algorithms and software have been developed for solving the optimization problem of choosing a CBE capable of ensuring the uninterrupted operation of the IACS both in conditions of technological failures and in conditions of destructive interference in the operation of the IACS by the attackers. The proposed solutions help to reduce the cost of determining the optimal CBE for IACS by 15–17% in comparison with the results of known calculation methods. The results of computational experiments to study the degree of influence of the outputs of the neural network analyzer on the efficiency of the functioning of the CBE for IACS are presented.
Keywords: Smart City; intelligent automated control system; equipment reserve; algorithm; optimization

REFERENCES

1 Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th

Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0305-0310). IEEE.
2 Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks Detection in IoT-Based Smart City Applications Using Machine Learning Techniques. International Journal of Environmental Research and Public Health, 17(24), 9347.
3 Lee, J., Kim, J., & Seo, J. (2019, January). Cyber attack scenarios on smart city and their ripple effects. In 2019 International Conference on Platform Technology and Service (PlatCon) (pp. 1-5). IEEE.
4 Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity Risk Assessment in Smart City Infrastructures. Machines, 9(4), 78.
5 Kitchin, R., & Dodge, M. (2019). The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. Journal of Urban Technology, 26(2), 47-65.
6 Ferraz, F. S., & Ferraz, C. A. G. (2014, December). Smart city security issues: depicting information security issues in the role of an urban environment. In 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (pp. 842-847). IEEE.
7 Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. Sustainability, 12(7), 2916.
8 Wang, D., Bai, B., Lei, K., Zhao, W., Yang, Y., & Han, Z. (2019). Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access, 7, 54508-54521.
9 Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165, 106946.
10 Hajian-Hoseinabadi, H. (2011). Impacts of automated control systems on substation reliability. IEEE Transactions on Power Delivery, 26(3), 1681-1691.
11 Weber, P., & Jouffe, L. (2006). Complex system reliability modelling with dynamic object oriented Bayesian networks (DOOBN). Reliability Engineering & System Safety, 91(2), 149-162.
12 Cai, B., Liu, H., & Xie, M. (2016). A real-time fault diagnosis methodology of complex systems using object-oriented Bayesian networks. Mechanical Systems and Signal Processing, 80, 31-44.
13 Kuhn, R., & Culhane, D. P. (1998). Applying cluster analysis to test a typology of homelessness by pattern of shelter utilization: Results from the analysis of administrative data. American journal of community psychology, 26(2), 207-232.
14 Maździarz, A. Alarm Correlation in Mobile Telecommunications Networks based on k-means Cluster Analysis Method. Journal of telecommunications and information technology, 2, 2018, pp.95-102. https://doi.org/10.26636/jtit.2018.124518
15 Bapiyev, I. M., Aitchanov, B. H., Tereikovskyi, I. A., Tereikovska, L. A., & Korchenko, A. A. (2017). Deep neural networks in cyber attack detection systems. International Journal of Civil Engineering and Technology (IJCIET), 8(11), 1086-1092.
16 Wang, G., Hao, J., Ma, J., & Huang, L. (2010). A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering. Expert systems with applications, 37(9), 6225-6232.
17 Cilimkovic, M. (2015). Neural networks and back propagation algorithm. Institute of Technology Blanchardstown, Blanchardstown Road North Dublin, 15, 1-12.
18 Wilamowski, B. M. (2009). Neural network architectures and learning algorithms. IEEE Industrial Electronics Magazine, 3(4), 56-63.
19 Prechelt, L. (1996). A quantitative study of experimental evaluations of neural network learning algorithms: Current research practice. Neural Networks, 9(3), 457-462.
20 Karayiannis, N. B., & Venetsanopoulos, A. N. (1993). Fast learning algorithms for neural networks. In Artificial Neural Networks (pp. 141-193). Springer, Boston, MA.
21 Tamp, N. V., & Tamp, V. L. (2016). Programma raspoznavaniya sostoyanij informacionno-vychislitel'noj seti na osnove nejronnoj seti s obratnym rasprostraneniem oshibok. Svidetel'stvo o gosudarstvennoj registracii programmy dlya EVM Nomer svidetel'stva: RU 2016660599.
22 CHEN, Mu-Chen; HSU, Chih-Ming; CHEN, Shih-Wei. Optimizing joint maintenance and stock provisioning policy for a multi-echelon spare part logistics network. Journal of the Chinese Institute of Industrial Engineers, 2006, 23.4: 289-302.
23 MOURONTE-LÓPEZ, Mary Luz. Optimizing the spare parts management process in a communication network. Journal of Network and Systems Management, 2018, 26.1: 169-188.