МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XIV МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КОМП'ЮТЕРНІ СИСТЕМИ
ТА МЕРЕЖНІ ТЕХНОЛОГІЇ

13-14 квітня 2023 року

Київ 2023

УДК 004.7(043.2)

Збірник тез доповідей XIV Міжнародної науково-практичної конференції «Комп'ютерні системи та мережні технології» (CSNT-2023), м. Київ, 13–14 квітня 2023 р., Національний авіаційний університет. – К.: НАУ, 2023. – 172 с.

В процесі доповідей здійснено обмін новими ідеями, отриманими теоретичними і практичними результатами наукових досліджень в області інформаційних технологій. Обговорено сучасний стан ІТ галузі в Україні та світі, перспективні напрямки розвитку інформаційних технологій. Для науковців, викладачів, аспірантів, студентів, співробітників наукових установ та ІТ компаній. Матеріали подані мовою оригіналу (українська, англійська). Редакційна колегія зберегла авторський текст без істотних змін, звертаючись до коректування в окремих випадках.

Відповідальність за достовірність матеріалів несуть автори.

Рекомендовано до видання вченою радою Факультету комп'ютерних наук та технологій Національного авіаційного університету (протокол № 1 від 10 березня 2023 р.).

Редакція не обов'язково поділяє думку автора. Відповідальність за достовірність фактів, цитат власних імен та іншої інформації несуть автори.

ЗМІСТ

УДК 531.266

В.К. Антонов, д.т.н.
Національний авіаційний університет, Київ

МЕТРИКА КОНТИНУУМВИМІРНОГО ПРОСТОРУ

Проблема багатовимірності простору є одною із провідних у формуванні нових фізичних уявлень про природу матеріального Всесвіту. Практична сторона питання полягає у виникненні нових ступенів свободи для формування непротирічних уявлень, що ведуть до конструктивного розуміння природи і приводять врешті до технологічного опанування все більш глибоких рівнів організації матерії. Повсякденний досвід привів до побудови уявлень про час і простір як обумовлених характером руху матерії, що спостерігається в експериментах і веде до наближених до дійсності узагальнень. При цьому кінцевовимірність часу і простору співставляється із кінцевістю поточної кількості відомих із експериментів характеристик матерії. Сучасні фізичні уявлення використовують розмірність простору, що дорівнює 11. Сподівання покладаються на нові покоління Адронних Колайдерів, в каналах прискорення яких частинки будуть ніби нізвідки з'являтись і зникати, що експериментатори трактуватимуть як рух матерії уздовж розмірності простору.

Висловлювання про багатовимірність простору неможливо спростувати. У пропозиції завжди є можливість «відступити» на позицію математичності істини, що існує за визначенням. Але і фізично спростування не може бути доведеним, оскільки завжди залишається можливість відтермінування доказів до побудови нового надпотужного прискорювача. Таким чином маємо щось типу «потенціальної презумпції» позитивного сприйняття.

Визнаною формою існування матерії є рух. За нашим припущенням різним формам руху відповідають свої властивості матерії [1]. Наприклад неспростовним є припущення по масу (інерцію) як зумовлену рухом уздовж розмірності простору. Також неможливо виключити динамічність розмірності простру як зумовленої рухом матерії – за аналогією із загальною теорією відносності.

У формуванні уявлень про час і простір можливо прокласти тренд уздовж робіт Галілея, Ньютона, Мінковського, Калуци, Гільберта, Ейнштейна, Логунова, багатьох сучасних розробників.

Ідея континуумвимірності відповідає сучасному стану спрямування дослідницьких зусиль світової наукової спільноти.

Але перша ж спроба оцінити континуумвимірний простір як метричний і тим означити його належне місце у фізичних уявленнях приводить до катастрофічних наслідків, подібно ультрафіолетовій катастрофі на початку розвитку квантової механіки. Постулювання метрики у вигляді квадратичної форми із обмеженими коефіцієнтами приводить до ситуації, коли в просторі не існує окремих точок, що були би не нескінченно віддаленими. Це приводить до неможливості будь яких подальших побудов.

Несподіваний вихід знаходимо в роботі [2]. Автори визначають відстань ρ між двома нескінченними послідовностями $x = (x_1, x_2, \dots, x_n, \dots)$ і $y = (y_1, y_2, \dots, y_n, \dots)$, що збігаються до нуля, за виразом

$$\rho(x, y) = \sum_{j=1}^{\infty} \frac{|x_j - y_j|}{2^j (1 + |x_j - y_j|)} \qquad (1)$$

В нашому випадку континууму складових конттинуумвимірних векторів суму замінимо на інтеграл, а в послідовностях координат задамо експоненційне загасання

$$\rho(x, y) = \int_{j=0}^{\infty} \frac{|x_j - y_j|}{2^j (1 + |x_j - y_j|)} dj \qquad (2)$$

$x^j = x^0 e^{-\alpha j}$, $y^j = y^0 e^{-\beta j}$,

$x^0 = const, y^0 = const, \quad \alpha > 0, \quad \beta > 0.$

Врешті одержали вирази (1) і (2), які задовольняють нас відсутністю розбіжності, якої ми і прагнули позбутися. Натомість набуваємо небажаної нетрадиційності у продовженні побудови рівнянь з диференціальної геометрії, умов руху по геодезичним.

Подальший аналіз полягатиме у виводі континуальних рівнянь уздовж класичної теорії поля, пошуку квантово-механічних рівнянь для континуального простору, опису континуальної моделі квантової заплутаності.

УДК 004.056.53

Н.В. Багнюк, к.т.н.,
К.Я. Бортник, к.т.н.,
Р.В. Боба
Луцький національний технічний університет, Луцьк

МАТЕМАТИЧНА ТРЕНОВАНА МОДЕЛЬ ДЛЯ АНАЛІЗУ ДАНИХ З ВИКОРИСТАННЯМ MACHINE LEARNING В УПРАВЛІННІ САЙТУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Аналіз даних є важливим завданням у різних сферах, зокрема у фінансах, охороні здоров'я та маркетингу. Алгоритми машинного навчання широко використовуються для аналізу даних завдяки їхній здатності навчатися на основі даних і робити прогнози. Продуктивність моделей машинного навчання залежить від кількох факторів, включаючи якість даних, вибір функцій і вибір алгоритмів [1].

Послідовність імплементації:

1. Збір даних: відстежування дій користувачів на сайті.
2. Перетворення даних: дані перетворюються в матрицю.
3. Розбиття даних: дані розбиваються на тренувальну та тестову вибірки.
4. Вибір моделі: вибираємо модель для рекомендацій на основі матричної факторизації, яка дозволяє розкласти матрицю на дві менші матриці.
5. Навчання моделі: застосовуємо алгоритм навчання для навчання моделі на тренувальній вибірці.
6. Тестування та оцінка: оцінюємо точність моделі на тестовій вибірці, використовуючи метрики.

Для рекомендаційних систем в електронній комерції використовуються різні методи machine learning, такі як матрична факторизація, рекурентні нейронні мережі та інші [2].

Для побудови рекомендаційних систем зазвичай використовуються відкриті набори даних, що містять інформацію про покупки, оцінки та відгуки користувачів. Перш за все, необхідно провести підготовку даних, яка включає в себе очистку, обрізку та стандартизацію даних. Наступним кроком є розбиття даних на тренувальну та тестову вибірки.

Далі вибирається модель для рекомендацій. Зазвичай використовуються алгоритми матричної факторизації, такі як

Singular Value Decomposition або Alternating Least Squares. Також можна використовувати deep learning моделі, такі як neural collaborative filtering, яка використовує Convolutional Neural Network для аналізу товарів та користувачів.

Після вибору моделі необхідно провести навчання моделі на тренувальній вибірці. Для цього застосовуються алгоритми навчання, такі як стохастичний градієнтний спуск, який забезпечує оптимізацію параметрів моделі.

Наступним кроком є тестування та оцінка точності моделі на тестовій вибірці. Це можна зробити за допомогою різних метрик, таких як середньоквадратична помилка (RMSE) або середній ранговий показник (MRR).

Після навчання моделі та її перевірки на точність можна розпочати використання її для створення рекомендацій.

Рекомендації на основі користувача передбачають рекомендації для конкретного користувача на основі його попередніх покупок та оцінок. Модель аналізує подібних користувачів та рекомендує товари, які були куплені або оцінені цими користувачами.

Рекомендації на основі товару передбачають рекомендації товарів, які можуть зацікавити користувача на основі подібних товарів, які він купував або оцінював. Модель аналізує подібні товари та рекомендує інші товари, які були куплені або оцінені користувачами, що купували подібні товари.

Однією з основних переваг моделей машинного навчання для рекомендаційних систем є те, що вони можуть бути покращені з часом. Коли користувач робить нові покупки або оцінки, модель може бути знову тренована з новими даними.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Лі К., Чен Т., Лю Ю. та Ма Ю. (2019). Collaborative filtering with social exposure: a modular approach based on graph convolutional networks. Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval, 425-434.

2.. Alpaydin, E. (2020). Introduction to machine learning (3rd ed.). MIT press.

УДК 004.056.53

Н.В. Багнюк, к.т.н.,
К.Я. Бортник, к.т.н.,
І.В. Домарацький
Луцький національний технічний університет, Луцьк

РОЗРОБКА МОБІЛЬНОГО ДОДАТКА НА ОСНОВІ БІБЛІОТЕКИ REDUX, ЯКИЙ ЗАБЕЗПЕЧУВАТИМЕ ОБРОБКУ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ

У сучасному світі мобільні додатки є невід'ємною частиною життя багатьох людей. Розробка мобільних додатків забезпечує зручний та швидкий доступ до інформації та послуг, сприяє збільшенню продуктивності та ефективності бізнесу.

Однак, для розробки якісного мобільного додатка, потрібно мати чітке розуміння процесу його розробки та використовувати сучасні технології та інструменти. У цьому контексті, тема дослідження є актуальною та має значний потенціал для покращення розробки мобільних додатків.

Для розробки мобільного додатку на основі бібліотеки Redux, який забезпечуватиме обробку та збереження інформації, поставлено наступні завдання:

- Розробка мобільного додатку за допомогою бібліотеки Redux.
- Проектування архітектури мобільного додатка.
- Реалізація мобільного додатка з використанням бібліотеки Redux.

Процес розробки мобільного додатка з використанням бібліотеки Redux побудовано з особливим акцентом на забезпеченні обробки та збереження інформації.

Розробка мобільних додатків передбачає використання сучасних технологій та інструментів. Одним з найпопулярніших фреймворків для розробки мобільних додатків є React Native. За його допомоги розробляють мобільні додатки для платформ Android та iOS з використанням JavaScript та React. React Native дозволяє швидко розробляти та тестувати додатки, а також забезпечує багатофункціональність та високу продуктивність.

Redux є бібліотекою для керування станом додатка в React. Вона дозволяє зберігати стан додатка у зручному для використання вигляді та керувати його змінами. Redux також забезпечує підтримку розширення додатка та забезпечує простий та

зрозумілий код [1].

Для розробки мобільного додатка на основі бібліотеки Redux, потрібно визначити функціональні вимоги до додатка. Основні функції додатка:

- Збереження інформації про користувача.
- Збереження інформації про певні об'єкти.
- Обробка та збереження даних з форм та інших елементів введення.
- Відображення списку об'єктів та детальної інформації про них.

Для розробки компонентів додатка використовуються стандартні компоненти React Native, а також власні компоненти, які забезпечуватимуть взаємодію з Redux. Кожен компонент містить відповідну логіку для обробки дій користувача та взаємодії з Redux [2].

Для забезпечення можливості збереження та отримання даних з зовнішніх сервісів використано бібліотеку Axios для взаємодії з API та Async Storage для збереження даних на мобільному пристрої користувача. Для розробки інтерфейсу користувача використані бібліотеки React Native Elements та NativeBase, які забезпечують широкі можливості для розробки красивого та зручного інтерфейсу. Дизайн додатка створено з урахуванням основних принципів Material Design.

Розглянуто тему розробки мобільного додатка на основі бібліотеки Redux. Також основні концепції та технології розробки додатків на платформі React Native, включаючи використання компонентів, редукторів та зовнішніх сервісів. Описані особливості розробки на основі бібліотеки Redux, яка забезпечує зручний та стабільний спосіб роботи зі станом додатка. Отже, розробка мобільного додатка на основі бібліотеки Redux є актуальною та перспективною темою для дослідження.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Edmondson, A. (2018). Building a React Native App with Redux in 2018. Retrieved September 21, 2021, from https://medium.com/@austinwade/building-a-react-native-app-with-redux-in-2018-f2ba36670e6c

2. React Native Redux. (2021). In Github. Retrieved September 21, 2021, from https://github.com/aksonov/react-native-redux

УДК 004.056.53

Н.В. Багнюк, к.т.н.,
О.М. Лінчук,
Д.І. Сичов
Луцький національний технічний університет, Луцьк

АЛГОРИТМІЧНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ АНАЛІЗУ СТАНУ ТА ФУНКЦІОНУВАННЯ РОЗПОДІЛЕНОЇ ГЕТЕРОГЕННОЇ МЕРЕЖІ

Проблема аналізу стану та функціонування розподіленої гетерогенної мережі вимагає від спеціалістів розробки алгоритмічного програмного забезпечення, що забезпечує моніторинг та оптимізацію роботи мережі. У цьому контексті, програмне забезпечення, яке розробляється за технічним завданням, повинно вирішувати ряд актуальних завдань:

Забезпечення постійного моніторингу розподіленої гетерогенної мережі для виявлення можливих проблем, спричинених аномаліями або зовнішніми вторгненнями [1].

- Реалізація алгоритмів для аналізу трафіку мережі, що дозволяє виявляти кореляційні, структурні та інваріантні ознаки, характерні для нормального функціонування мережі та можливих загроз.

- Розробка модульної архітектури програмного забезпечення, що дозволяє легко інтегрувати нові компоненти для моніторингу та аналізу різних аспектів функціонування мережі.

- Створення інтуїтивного інтерфейсу користувача, що допомагає адміністраторам мережі швидко отримати доступ до потрібної інформації про стан та функціонування гетерогенної мережі.

- Розробка системи резервного копіювання та контролю версій для забезпечення надійності програмного забезпечення та зберігання історії змін у параметрах мережі.

- Інтеграція з існуючими системами моніторингу і керування мережею, що дозволить спеціалістам ефективно використовувати програмне забезпечення в різних мережевих середовищах.

- Реалізація механізмів автоматичного адаптування алгоритмів програмного забезпечення до змін у мережі та нових видів загроз, що полегшує процес моніторингу та аналізу стану мережі.

Забезпечення можливості масштабування програмного забезпечення для використання в мережах різних розмірів та конфігурацій, враховуючи специфіку гетерогенних мереж.

- Розробка засобів для підтримки різних протоколів зв'язку і стандартів мережевого обладнання, що гарантує широку сумісність програмного забезпечення з різноманітним мережевим обладнанням.

- Проведення експериментів та випробувань програмного забезпечення в реальних мережевих середовищах для перевірки ефективності алгоритмів та виявлення можливих проблем.

Автори [2] пропонують метод виявлення аномалій у мережі, заснований на інваріантах подоби, який передбачає порівняння значень інваріантів реальних обчислювальних процесів з еталонними значеннями. Це дозволяє розробити автоматичний алгоритм виявлення аномалій. Виявлення аномалій здійснюється за допомогою дворівневої класифікації мережевої активності, яка включає класифікатори та метод опорних векторів для визначення класів атак [2].

Використання тензорної методології для аналізу мережевого трафіку дозволяє отримати додаткові знання про власні вектори та топологічну структуру тензорного поля [3]. Графічні відображення тензор-трафіку і їх векторні аналоги демонструють високу ефективність використання векторних аналогів тензор-трафіку для ідентифікації аномальних режимів мережі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. L. Gorjan, M. Vojkovic, and B. Jerman-Blazic, "A framework for the analysis and management of heterogeneous IoT-enabled network infrastructure," in 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS), 2018, pp. 1-6.

2. J. Fan, Q. Chen, H. Du, Y. Liu, and W. Li, "An Efficient and Privacy-Preserving Distributed Network Traffic Classification," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6.

3. L. R. Rodrigues, S. Kundu, F. A. Silva, A. M. Alberti, and M. C. R. Melo, "Adaptive network monitoring and management through intelligent data aggregation," in 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2019, pp. 104-112.

УДК 004.056.53

Н.В. Багнюк, к.т.н.,
О.М. Лінчук,
О.О. Шипулін
Луцький національний технічний університет, Луцьк

АВТОМАТИЗОВАНИЙ АНАЛІЗ ТРАФІКУ В МЕРЕЖІ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Автоматизований аналіз трафіку в мережі з використанням штучного інтелекту є одним з найважливіших напрямків розвитку сучасних мережевих технологій. Зі зростанням кількості підключених пристроїв та користувачів, а також розвитком нових технологій з'являються нові виклики, пов'язані з аналізом трафіку в мережі та його оптимізацією. Автоматизований аналіз трафіку з використанням штучного інтелекту може бути дуже корисним для розв'язання цих проблем.

Трафік мережі - це об'єм даних, які передаються через мережу в певний проміжок часу. Трафік може бути різного типу: мережевий, додатковий, відео, голосовий тощо. Аналіз трафіку дозволяє визначити обсяг даних, що передаються в мережі, а також виявити проблеми, пов'язані з його передачею.

Одним з ключових підходів до автоматизованого аналізу трафіку в мережі з використанням штучного інтелекту є застосування методів машинного навчання. Машинне навчання дозволяє створювати алгоритми, які можуть самостійно вивчати та аналізувати велику кількість даних, знаходити закономірності та здійснювати передбачення. Застосування методів машинного навчання в аналізі трафіку в мережі може допомогти вирішити такі завдання, як ідентифікація типу трафіку, виявлення аномального трафіку та визначення його джерела [1].

Автоматизований аналіз трафіку в мережі з використанням штучного інтелекту також може бути корисним для покращення якості обслуговування користувачів. Наприклад, застосування машинного навчання для аналізу трафіку може допомогти виявити патерни використання мережі користувачами та запропонувати оптимальні налаштування мережі для кожного користувача, що дозволить забезпечити кращу швидкість та якість обслуговування.

Крім того, використання алгоритмів машинного навчання та глибокого навчання дає змогу створювати більш точні та ефективні

системи для аналізу мережевого трафіку. Такі системи можуть навчитися розпізнавати певні типи трафіку, класифікувати його та виявляти аномальну активність [2]. Це дозволяє зменшити кількість помилок та збільшити точність виявлення проблем в мережі, що є особливо важливим для глобальних мереж з великою кількістю користувачів.

Проте, існують виклики та перешкоди, пов'язані з автоматизованим аналізом трафіку в мережі з використанням штучного інтелекту, такі як складність обробки великої кількості даних, необхідність постійного навчання моделей та недостатня точність передбачень. Враховуючи ці фактори, важливо розробляти та вдосконалювати методи та алгоритми автоматизованого аналізу трафіку з метою підвищення їх ефективності та точності [3].

У підсумку, автоматизований аналіз трафіку в мережі з використанням штучного інтелекту є перспективним напрямком досліджень у галузі мережевої безпеки та оптимізації мережі. Його застосування може допомогти вирішувати складні завдання та покращувати якість обслуговування користувачів. З метою подальшого вдосконалення методів автоматизованого аналізу трафіку необхідно проводити дослідження та використовувати нові технології.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Zhang, H. Automated Traffic Analysis for Security and Network Management Using Machine Learning / H. Zhang, L. Huang, Y. Liu, H. Zhang // Proceedings of the 16th ACM Conference on Computer and Communications Security. – 2009. – С. 217-226.

2. Han, G. Automated Network Traffic Analysis Using Deep Learning Techniques / G. Han, Y. Kim, S. Cho // IEEE Access. – 2019. – Т. 7. – С. 11494-11505

3. Zhang, B. DeepPacket: A Deep Learning Approach to Network Traffic Classification / B. Zhang, X. Xie, W. Yu, S. Jiang // Proceedings of the 2018 IEEE International Conference on Communications. – 2018. – С. 1-6.

УДК 510.635:004.891(045)

А.І. Вавіленкова, д.т.н.
Національна академія Служби безпеки України, Київ

МОНІТОРИНГ МЕРЕЖ З МЕТОЮ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Сьогодні для організації захисту комп'ютерних мереж від кіберзагроз здійснюється багато превентивних заходів, серед яких постійний моніторинг мережі та сканування портів [1]. Одним із програмних засобів, що дозволяє здійснювати тестування на проникнення – Kali Linux.

Обмін даними в мережі відбувається між двома процесами за певним протоколом. Для встановлення зв'язку потрібні: номер протоколу; дві IP-адреси (адреса хоста-відправника та адреса хоста-одержувача) для побудови маршруту між ними; два номери портів (порт процесу –відправника та порт отримувача).

В комп'ютерних мережах порт є кінцевою точкою зв'язку в операційній системі. В програмному забезпеченні це логічна конструкція, яка ідентифікує конкретний процес або вид послуг [2].

Мережевий протокол задає загальні правила взаємодії різноманітних програм, мережевих вузлів чи систем і створює таким чином єдиний простір передачі. Для того, щоб прийняти і обробити відповідним чином повідомлення, їм необхідно знати, як сформовані повідомлення і що вони означають. Прикладами використання різних форматів повідомлень в різних протоколах можуть бути встановлення з'єднання з віддаленою машиною, відправлення повідомлень електронною поштою, передача файлів.

Коли клієнт і сервер починають використовувати TCP, створюється віртуальний канал. Дані по цьому каналу можуть одночасно передаватися в обох напрямках. Один прикладний процес пише дані в TCP-порт, вони проходять по мережі, а інших прикладний процес читає їх зі свого TCP-порту. Для того, щоб клієнт міг звертатися до необхідного йому серверу, він повинен знати номер порту, за яким сервер очікує звернення до нього .

Nmap («Network Mapper») – це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки, розроблена для швидкого сканування великих мереж.

Вихідні дані ***Nmap*** – це список просканованих цілей з додатковою інформацією щодо кожної з них залежно від заданих опцій. Ключовою інформацією є «таблиця важливих портів» [3].

Найпоширеніші дії, що можна здійснити за допомогою утиліти ***Nmap***:

- здійснити сканування визначених IP-адрес: **nmap 172.27.157.151**;
- здійснити сканування цілей, список яких знаходиться у файлі *.txt, наприклад, **nmap –iL targets.txt;**
- реалізувати метод сканування TCP портів, якщо порт відкритий і прослуховується, то результат виконання буде успішним, тобто з'єднання буде встановлене, у протилежному випадку вказаний порт є закритим або доступ до нього заблоковано засобами захисту, виконується за допомогою ключа **nmap –sT 192.168.1.17;**
- реалізувати метод напіввідкритого сканування, оскільки повне TCP-з'єднання з портом сканування не встановлюється **nmap –sS 192.168.1.2;**
- реалізувати Ping-сканування для отримання інформації про активні хости в сканованій мережі **nmap –sn 192.168.1.17;**
- визначити операційну систему віддаленого хосту **nmap –O 192.168.1.17.**

У доповнення до таблиці важливих портів ***Nmap*** може надавати подальшу інформацію про цілі: перетворені DNS імена, припущення про операційну систему, типи пристроїв і MAC адреси.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Юхименко П. Глобалізація та політика національної безпеки. – підручник. – 2021. – 402 с.

2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

3. Вавіленкова А.І., Душкевич В.С., Лозниця Р.А. Види налаштувань безпеки комп'ютера: Proceedings of the V International Scientific and Practical Conference «Formation of perceptions of the structure of scientific methodology», 30-31 січня, 2023, – Відень, Австрія: InterSci. – 2023. – С. 47–50.

УДК 004.724.4

К.О. Вадурін,
А.Л. Перекрест, д.т.н.,
Д.В. Кухаренко, к.т.н.
Кременчуцький національний університет
ім. М.Остроградського, Кременчук

РОЗРОБКА ЗАГАЛЬНОЇ СТРУКТУРИ ІНФОРМАЦІЙНОГО ОБМІНУ МІЖ ОСНОВНИМИ БЕЗДРОТОВИМИ ДАТЧИКАМИ БІОМЕТРИЧНОГО КОМПЛЕКСУ

У попередніх роботах основна увага була зосереджена на описі інформаційного обміну між блоками всередині наручного бездротового датчика та нагрудного датчика-накопичувача, актуальною задачею при цьому залишається визначення структури інформаційного обміну пристроїв у межах біометричного комплексу, та визначення основних функцій взаємодії з зовнішніми системами обробки біометричної інформації.

Метою роботи є синтез структури інформаційного обміну у межах біометричного комплексу для визначення кількості функцій які необхідно реалізувати у програмному забезпеченні окремого елемента цієї системи.

Об'єктом дослідження є процес обміну інформацією у межах біометричного комплексу.

Предметом дослідження є розробка загальної структури інформаційного обміну між основними бездротовими датчиками біометричного комплексу.

Методи дослідження практичні: синтез структури інформаційного обміну між основними елементами біометричного комплексу.

Наукова новизна полягає в першій розробці структури інформаційного обміну між основними елементами біометричного комплексу, що з поміж інших передбачає декілька режимів обміну інформацією, залежно від комплектації розроблюваної системи.

У дослідженні [1] наведено опис структури та роботи комплексу діагностичних процедур. Автори пропонують використовувати програмно-апаратний комплекс «Психолот-1» для реабілітації на основі біологічного зворотного зв'язку. Однак пропонований пристрій призначений для дослідження простих зорово-моторних реакцій, що не в повній мірі дозволяє ідентифікувати фізичні та

психологічні стани досліджуваного суб'єкта. У статті [2] описується неінвазивна система моніторингу серцевого ритму та артеріального тиску. Продемонстрована система може записувати в реальному часі частоту серцевих скорочень та артеріальний тиск. Однак, запропоноване рішення не повністю дозволить здійснити ідентифікацію поточного стану оператора.

У ході роботи було синтезовано загальну структуру інформаційного обміну між основними бездротовими датчиками біометричного комплексу, яку зображено на рис.1.

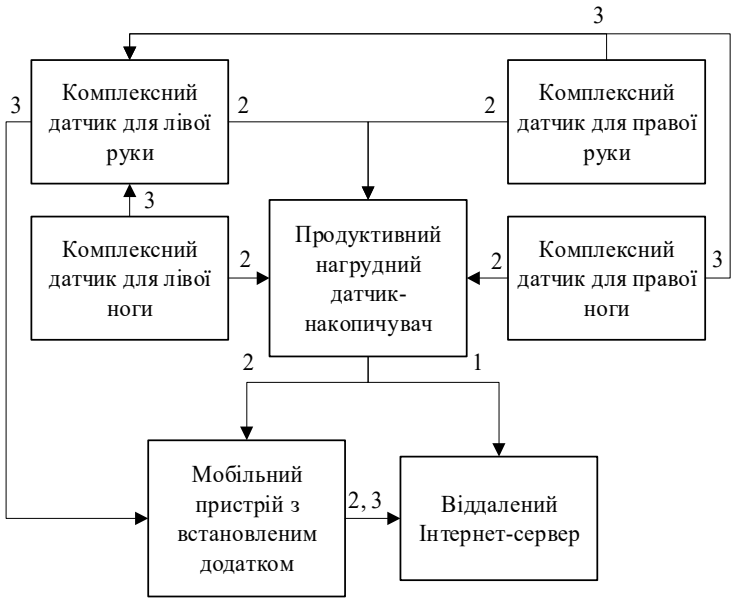


Рис.1. Загальна структура обміну інформацією у межах біометричного комплексу.

У структурі інформаційного обміну, що наведено на рис.1, передбачено такі сценарії:

1. Пряма віддача даних від нагрудного-датчика накопичувача до віддаленого Інтернет-серверу, що реалізується за допомогою GSM зв'язку.

2. Віддача нагрудним-датчиком накопичувачем отриманих від

інших бездротових датчиків системи даних до мобільного пристрою з встановленим додатком.

3. У третьому сценарії наведено роботу у ролі накопичувача даних комплексного датчика лівої руки, хоча у ролі накопичувача повинен виступати будь-який бездротовий датчик кінцівки та вільно віддавати оброблені дані до мобільного додатку.

Для усіх п’яти бездротових датчиків та їх інформаційних методів зв’язку з додатками та зовнішніми пристроями зв’язку має зберігатися тенденція до автономного функціонування, тобто у системі можуть спільно працювати п’ять датчиків, або чотири, або один опрацьовуючи лише власні показники.

У ході роботи було синтезовано структуру обміну інформацією у межах біометричного комплексу для моніторингу стану людини-оператора. Запропонована схема передбачає три основні сценарії обміну інформацією, програмна реалізація автоматичного переключення між якими дозволить значно облегшити використання різних конфігурацій біометричного комплексу як для наукових задач, так і для спорту та медицини.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Palagin O., Kurgaev O., Budnyk M., Chaikovsky I. Development of a Subsystem for Supporting a Complex of Diagnostic Procedures for the Information-Analytical System TISP. Cybernetics and Computer Technologies. 2021. 3. P. 86–102. (in Ukrainian) https://doi.org/10.34229/2707-451X.21.3.8.

2. Samartkit P., Pullteap S., Bernal O. A non-invasive heart rate and blood pressure monitoring system using piezoelectric and photoplethysmographic sensors. Measurement. 2022. 196. https://doi.org/10.1016/j.measurement.2022.111211.

УДК 004.386

К.О. Вадурін,
Д.В. Мосьпан, к.т.н.,
О.О. Юрко, к.т.н.
Кременчуцький національний університет
ім. М.Остроградського, Кременчук

РОЗРОБКА СТРУКТУРИ ІНФОРМАЦІЙНОГО ОБМІНУ У СХЕМІ НАРУЧНОГО БЕЗДРОТОВОГО ДАТЧИКА БІОМЕТРИЧНОГО КОМПЛЕКСУ МОНІТОРИНГУ СТАНУ ЛЮДИНИ-ОПЕРАТОРА

Людина-оператор, є складною психологічно-фізіологічною системою та вирішальним елементом у складі систем прийняття рішень. Задля моніторингу внутрішніх фізіологічних та психологічних параметрів людини-оператора, а також для визначення впливу ефективності нормалізуючих зовнішніх факторів актуальною задачею є розробка біометричного комплексу.

Метою роботи є розробка структурної схеми інформаційного обміну між блоками наручного бездротового датчика біометричного комплексу моніторингу стану людини-оператора.

Об’єктом дослідження є процес зняття, первинної обробки та обміну біометричною інформацією між блоками наручного бездротового датчика біометричного комплексу.

Предметом дослідження є розробка структурної схеми наручного бездротового датчика біометричного комплексу моніторингу стану людини-оператора.

Методи досліджень практичні: синтез структурної схеми наручного бездротового датчика біометричного комплексу моніторингу стану людини-оператора.

Наукова новизна полягає в удосконаленні структури інформаційного обміну між внутрішніми блоками наручного бездротового датчика біометричного комплексу та зовнішніми системами обробки інформації, що з поміж інших передбачає можливість динамічного автоматичного налаштування маршрутів збереження та обробки біометричної інформації.

З статті «Системи ідентифікації людської діяльності» [1], для подальшої роботи, можна підкреслити можливість використання

системи гіроскопу та акселерометру, для визначення напрямку руху кінцівок оператора стан якого діагностується. Знаючи розташування основних перемикачів на панелях, можна буде зберегти послідовність взаємодії оператора з ними, навіть без використання систем комп'ютерного зору та відео обладнання. Також, цікавість викликають проаналізовані методи класифікації ознак, що дозволить у подальшому здійснювати якісну обробку даних про положення та поточні дії оператора та робити невеликі прогнози майбутніх дій. У роботі «Рішення бездротової сенсорної мережі для моніторингу здоров'я пілотів легких літаків» [2] продемонстровано можливість використання бездротових технологій на легких літаках, що підтверджує можливість реалізації різних підходів для аналізу станів пілотів. При розробці запланованої інформаційної технології, планується використовувати обладнання іншого роду. Розроблена інформаційна технологія буде спрямований більше на аналізі стану саме пілота, без прив'язки до висоти польоту та льотних характеристик напряму, оскільки вона має інтегруватися в систему літака чи тренажера.

У ході роботи було синтезовано структуру інформаційного обміну у схемі наручного бездротового датчика біометричного комплексу моніторингу стану людини-оператора, як зображено на рис.1.

До складу системи мають входити чотири комплексні датчики кінцівок, причому функціонал усіх датчиків кінцівок має бути однаковим, тобто вони можуть бути взаємозамінними при діагностиці специфічних процесів на одній кінцівці.

Для обробки даних від датчиків та накопичення пакету показників, для подальшої відправки на обробку обов'язкове включення мікроконтролера-обробника.

Задля забезпечення зв'язку мікроконтролера-обробника з нагрудним датчиком-накопичувачем, мобільним пристроєм з встановленим додатком чи іншими датчиками у наборі передбачено використання інтерфейсу Bluetooth. Використання такого інтерфейсу бездротового зв'язку для комплексних датчиків кінцівок є обов'язковим задля мінімізації енергоспоживання.

При реалізації блоку живлення необхідно передбачати автономність бездротових датчиків, для чого всередині кожного

такого датчика має бути акумулятор з схемою заряду, або батарея та роз'єм для її швидкої заміни.

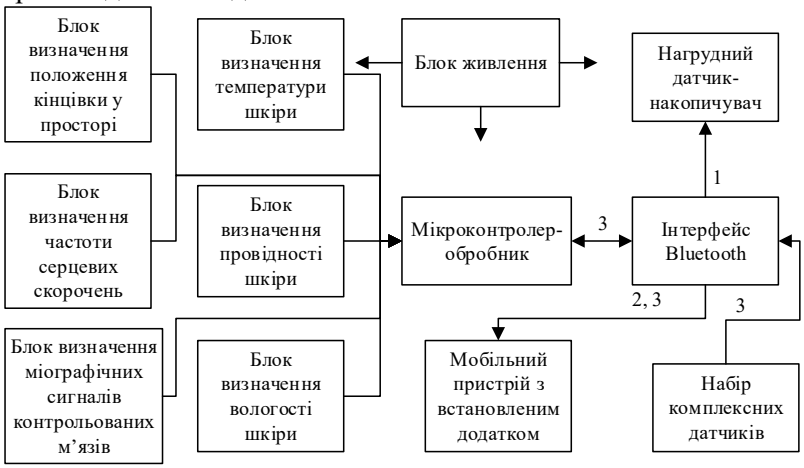


Рис.1. Синтезована структуру інформаційного обміну.

ВИСНОВОК. У ході роботи синтезовано структуру інформаційного обміну у схемі наручного бездротового датчика біометричного комплексу моніторингу стану людини-оператора. У подальшому планується реалізувати електричну принципову схему наручного бездротового датчика та програмне забезпечення з реалізованими алгоритмами для визначення оптимальних зовнішніх впливів для нормалізації стану людини-оператора.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Nweke H. F. et al. Data fusion and multiple classifier systems for human activity detection and health monitoring: Review and open research directions // Information Fusion. – 2019. – Т. 46. – С. 147-170.

2. Oliveira L. M. L. et al. A WSN solution for light aircraft pilot health monitoring // 2012 IEEE Wireless Communications and Networking Conference (WCNC). – IEEE, 2012. – С. 119-124.

УДК 004.386

К.О. Вадурін,
А.Л. Перекрест, д.т.н.,
Д.В. Кухаренко, к.т.н.
Кременчуцький національний університет
ім. М.Остроградського, Кременчук

РОЗРОБКА СТРУКТУРИ ІНФОРМАЦІЙНОГО ОБМІНУ У СХЕМІ НАГРУДНОГО ДАТЧИКА-НАКОПИЧУВАЧА БІОМЕТРИЧНОГО КОМПЛЕКСУ МОНІТОРИНГУ СТАНУ ЛЮДИНИ-ОПЕРАТОРА

Оскільки для моніторингу стану людини-оператора може використовуватися набір різних незалежних зовнішніх пристроїв, які можуть генерувати різнорідні дані використовуючи різні інтерфейси зв'язку, актуальною задачею є створення пристрою для систематизації, структурування, обробки та передачі даних до продуктивних систем обробки інформації. Перш за все, необхідно синтезувати внутрішню структуру інформаційного обміну такого пристрою. Функціонал такого пристрою передбачено реалізувати у нагрудному датчику-накопичувачі біометричного комплексу.

Метою роботи є розробка структури інформаційного обміну у схемі нагрудного датчика-накопичувача біометричного комплексу моніторингу стану людини-оператора.

Об'єктом дослідження є процес приймання, структурування та обміну біометричною інформацією між блоками нагрудного датчика-накопичувача.

Предметом дослідження є розробка структури інформаційного обміну у схемі нагрудного датчика-накопичувача біометричного комплексу моніторингу стану людини-оператора.

Методи досліджень практичні: синтез структури інформаційного обміну у схемі нагрудного датчика-накопичувача.

Наукова новизна полягає в удосконаленні інформаційного обміну у схемі нагрудного датчика-накопичувача за рахунок використання засобів для забезпечення зв'язку за інтерфейсами Bluetooth, Wi-Fi, GSM, що з поміж інших передбачає можливість динамічного автоматичного налаштування маршрутів збереження та обробки біометричної інформації.

У роботі з темою «Система визначення робочого навантаження пілота літака» [1] зазначається, що оцінка робочого навантаження

має велике значення для навчання уникненню людських помилок, особливо при використанні складних систем, які вимагають різних і паралельних видів діяльності. Надмірне робоче навантаження негативно впливає на ефективність роботи людини навіть у разі несприятливого результату. З проаналізованої роботи можна підкреслити актуальність пошуку системи, що дозволяє вимірювати температуру областей з швидкою регуляцією для отримання інформації про збільшення навантажень та стрес. Ідеї, що наводяться у дослідженні «Виявлення втоми у водіїв автомобілів і пілотів літаків за допомогою неінвазивних заходів» [2] реалізуються багатьма авторами, для моніторингу втоми у класах, на засіданнях та інше. Задля імплементації їх у розроблювану інформаційну технологію, потрібно розглянути можливість інтеграцій мікрокамер у шоломи чи окуляри пілотів, оскільки їх обличчя завжди закриті окулярами. Ідея здається збитковою для реалізації, хоча при побудові прототипу мобільного енцефалографа та інтеграції його у шолом, значно не вплине на кінцеву вартість інформаційної технології.

У ході роботи було синтезовано структуру інформаційного обміну у схемі нагрудного датчика-накопичувача.

Мікроконтролер-обробник продуктивного датчика, повинен мати аналогічні, або кращі, з точки зору продуктивності та кількості наявної пам’яті, параметри у порівнянні з іншими бездротовими датчиками комплексу, оскільки серед його функцій є попереднє формування з отриманих даних посилок та їх надсилання кінцевим пристроям-обробникам.

Зв’язок мікроконтролера-обробника з нагрудним датчиком-накопичувачем, мобільним пристроєм з встановленим додатком чи іншими датчиками у наборі передбачено використання інтерфейсу Bluetooth. Використання такого інтерфейсу бездротового зв’язку для комплексних датчиків кінцівок є обов’язковим задля мінімізації енергоспоживання.

Для забезпечення можливості вибору інтерфейсу зв’язку датчика-накопичувача з кінцевими пристроями обробниками, залежно від поставленої задачі моніторингу, необхідно реалізувати незалежну роботу мікроконтролера-обробника з інтерфейсами Wi-Fi, Bluetooth та GSM-зв’язком. Структура нагрудного-датчика накопичувача зображена на рис.1.

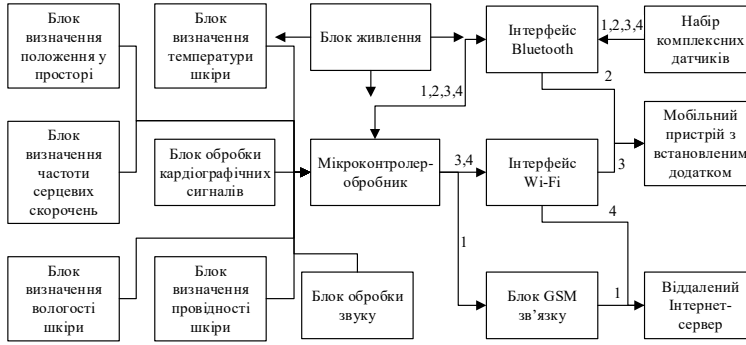


Рис.1. Синтезована структура інформаційного обміну нагрудного датчика-накопичувача.

У ході роботи синтезовано структуру інформаційного обміну між внутрішніми блоками нагрудного датчика-накопичувача та зовнішніми системами обробки даних інформаційної технології моніторингу стану людини-оператора. У подальших дослідженнях планується синтезувати електричну принципову схему нагрудного датчика-накопичувача, а також реалізувати програмне забезпечення для його роботи як у складі біометричного комплексу, так і з пристроями сторонніх виробників.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Alaimo A. et al. An aircraft pilot workload sensing system // European workshop on structural health monitoring. – Springer, Cham, 2021. – С. 883-892.

2. Hu X., Lodewijks G. Detecting fatigue in car drivers and aircraft pilots by using non-invasive measures: The value of differentiation of sleepiness and mental fatigue // Journal of safety research. – 2020. – Т. 72. – С. 173-187.

УДК 004.75

К.О. Вадурін,
А.Л. Перекрест, д.т.н.,
Д.В. Кухаренко, к.т.н.
Кременчуцький національний університет
ім. М.Остроградського, Кременчук

СТРУКТУРА ІНФОРМАЦІЙНОЇ СИСТЕМИ ОБРОБКИ ДАНИХ ОТРИМАНИХ ВІД БІОМЕТРИЧНОГО КОМПЛЕКСУ ДЛЯ МОНІТОРИНГУ, ПРОГНОЗУВАННЯ ТА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЛЮДИНИ-ОПЕРАТОРА

Наразі є актуальною задачею моніторинг стану людини-оператора у реальному часі. Для того щоб ефективно здійснювати зняття, первинну обробку, структурування обмін та збереження біометричних даних людини-оператора необхідно синтезувати спеціалізовану інформаційну систему обробки даних, яка передбачала б різні сценарії використання, комплексність біометричного комплексу та побажання як звичайного побутового користувача, так і вимоги дослідника.

Метою роботи є синтез структури інформаційної системи обробки даних отриманих від біометричного комплексу, для подальшої реалізації маршрутизації інформації за заданими у програмному середовищі налаштуваннями.

Об’єктом дослідження є процес обміну інформацією у межах інформаційної системи моніторингу стану людини-оператора.

Предметом дослідження є структура інформаційної системи обробки даних отриманих від біометричного комплексу.

Методи дослідження практичні: синтез структури інформаційного обміну в межах системи обробки даних отриманих від біометричного комплексу.

Наукова новизна полягає в удосконаленні структури інформаційного обміну в межах системи обробки даних отриманих від біометричного комплексу, що у порівнянні з іншими передбачає налаштування вибору маршруту обробки даних для забезпечення інтересів усіх потенційних користувачів біометричних комплексів.

Виходячи з аналізу літератури за цим напрямком визначено, що статті [1] дослідники розробили переносний пристрій на основі

високочутливих датчиків тиску, для моніторингу пульсу. Такий пристрій, за умови його мініатюризації, можна використати у ролі одного з датчиків для реалізації поставленої задачі комплексного моніторингу біологічних показників людини, але він не є комплексним рішенням топології інформаційної системи, що може включати велику кількість датчиків. У статті [2], описується медична система, що базується на основі GSM-модуля та здатна вимірювати насиченість крові киснем, частоту серцевих скорочень, частоту дихання. Недоліком цієї системи є її габарити, оскільки електронна схема пристрою розділена на декілька модулів, що є збитковим, реалізація одноплатної чи двоплатної схеми значно зменшить розміри та вагу пристрою.

У ході роботи було синтезовано структуру інформаційної системи обробки даних від біометричного комплексу, яку зображено на рис.1.

Рис.1. Структура інформаційної системи обробки даних від біометричного комплексу.

Синтезована структура передбачає наступні сценарії обміну даними:

1. Надсилання даних від біометричного комплексу до користувацького додатку, який в свою чергу надсилає дані до центрального серверу.

2. Відправку даних від біометричного комплексу до користувацького додатку, далі до користувацького серверу та до центрального серверу.

3. Надсилання даних від біометричного комплексу до користувацького сервера та центрального сервера.

4. Відправка даних від біометричного комплексу до професійно-

орієнтованого додатку та центрального сервера.

5. Віддачу даних від біометричного комплексу до професійно-орієнтованого додатка, професійно-орієнтованого сервера та центрального сервера.

6. Віддача даних від біометричного комплексу до професійно-орієнтованого сервера та центрального сервера.

7. Віддача інформації від біометричного комплексу до користувацького додатка, професійно-орієнтованого сервера та центрального сервера.

8. Пряма віддача даних від біометричного комплексу до центрального сервера.

При реалізації програмного забезпечення, для кожного елементу системи обробки даних, планується реалізувати можливість автономної роботи протягом певного часу з можливістю накопичення даних для їх подальшої синхронізації з центральним сервером, а також функцію автоматичної побудови маршруту.

У ході роботи синтезовано структуру інформаційної системи обробки даних від біометричного комплексу, за якою у подальшому планується реалізувати комплексну інформаційну технологію моніторингу, прогнозування та підтримки прийняття рішень людини-оператора у галузі пілотування, спорту та медицини.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Wang S., Zhang Z., Chen Z., Mei D., Wang Y. Development of Pressure Sensor Based Wearable Pulse Detection Device for Radial Pulse Monitoring. Micromachines. 2022. 13(10). p. 1699. https://doi.org/10.3390/mi13101699.

2. Kumar S., Akash K., Sumit Kumar J. GSM Based Embedded Medical Critical Care Signal Monitoring System. International Journal of Trend in Scientific Research and Development. 2019. 3(4). P. 1527–1555. URL: https://www.ijtsrd.com/papers/ijtsrd25126.pdf.

УДК 519.852.61

К.О. Вадурін,
Д.В. Мосьпан, к.т.н.,
О.О. Юрко, к.т.н.
Кременчуцький національний університет
ім. М.Остроградського, Кременчук

СИНТЕЗ АЛГОРИТМУ ВИКОРИСТАННЯ СИМПЛЕКС-МЕТОДА ДЛЯ ПОШУКУ ОПТИМАЛЬНОЇ КОМБІНАЦІЇ ЗОВНІШНІХ ФАКТОРІВ ДЛЯ НОРМАЛІЗАЦІЇ СТАНУ ЛЮДИНИ-ОПЕРАТОРА

Представляючи людину-оператора складною фізіологічно-психологічною системою, можна розглянути можливості для нормалізації її стану за допомогою декількох різних методів. Уже було синтезовано загальний еволюційний алгоритм для оптимізації комбінації та інтенсивності зовнішніх впливів на людину-оператора. Аналогічно, актуальною задачею є розробка алгоритму симплекс-метода нормалізації стану людини оператора, щоб забезпечити можливість усестороннього аналізу можливих комбінацій зовнішніх впливів та визначення оптимального підходу доцільного для реалізації на базі біометричного комплексу моніторингу стану людини-оператора.

Метою роботи є синтез алгоритму застосування симплекс метода для оптимізації зовнішніх впливів на людину-оператора.

Об’єктом дослідження є процес підбору оптимальної комбінації та інтенсивності значень зовнішніх впливів для нормалізації стану людини-оператора.

Предметом дослідження є синтез алгоритму використання симплекс-метода для пошуку оптимальної комбінації зовнішніх факторів для нормалізації стану людини-оператора.

Методи дослідження. Теоретичні: постановка проблеми використання симплекс-методу для визначення оптимальної комбінації зовнішніх впливів та їх інтенсивностей для нормалізації стану людини оператора. Практичні: синтез алгоритму використання симплекс-методу.

Наукова новизна полягає в удосконаленні алгоритму симплекс-метода для визначення оптимальних комбінацій та інтенсивностей зовнішніх впливів для нормалізації стану людини-оператора, що у порівнянні з іншими застосуваннями симплекс-методу спрямоване

на керування процесами різної природи.

Дослідники використовуються симплекс-метод для різних задач: для оптимізації індексу комфорту у будівлях на основі адаптивної нейро-фаззі інференційної системи [1]; для відправки інформації до слухової кори людини з використанням функціональної магнітно-резонансної томографії, керованої локалізації розсіяного джерела [2]; для оптимізації траєкторії руху промислових роботів [3]. Але у жодній, з проаналізованих праць, симплекс метод не використовувався для нормалізації стану людини оператора.

У ході роботи було синтезовано алгоритм використання симплекс-методу для визначення оптимальної комбінації та концентрації зовнішніх впливів, для нормалізації стану людини-оператора, набір яких може змінюватися відповідно до поточного стану дослідження. Розроблений алгоритм зображено на рис.1.

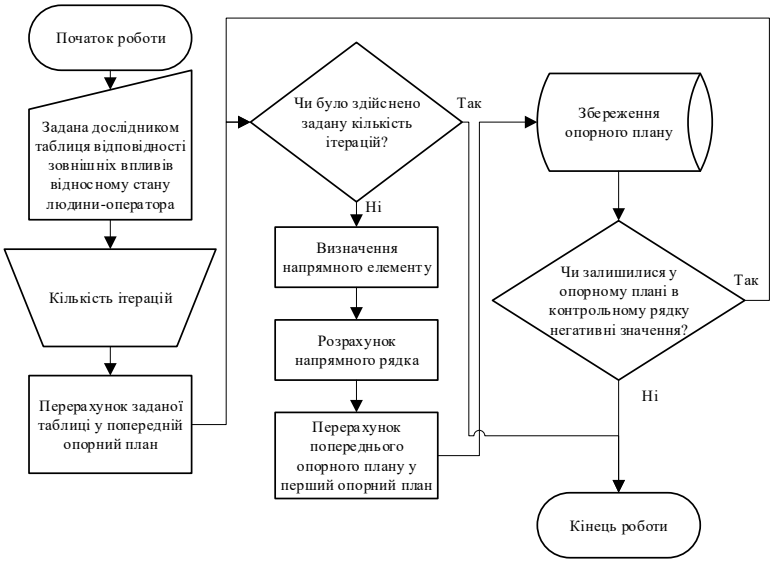


Рис.1. Синтезований алгоритм симплекс-методу.

За синтезованим алгоритмом симплекс методу, користувач має ввести відому таблиці зовнішніх впливів та їх відносну цінність для нормалізації стану людини-оператора, а також кількість ітерацій розрахунку. Далі, відбувається перерахунок класичної таблиці у попередній опорний план, за яким можливо розрахувати перший опорний план. Для визначення напрямного елемента відбувається

пошук мінімального значення серед значень останнього рядка значень попереднього опорного плану. За знайденим мінімальним значенням знаходиться напрямний елемент. Найменше отримане значення зберігається у вектор, разом з його координатами у межах поточного плану. Далі відбувається формування напрямного рядка та за методом трикутника відбувається перерахунок первинного у перший опорний план. Потім відбувається заміна попереднього опорного плану останнім і процес повторюється.

У ході роботи синтезовано алгоритм симплекс-методу, за яким буде створено модель програми у середовищі Mathcad для пошуку оптимальної комбінації інтенсивності вхідних впливів для нормалізації стану людини-оператора. У подальшому планується порівняння використання симплекс-методу з еволюційним алгоритмом для нормалізації стану людини-оператора.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Alizadeh, R., Dadashi, R., Sharifi, M., and Mashinchi, M. (2015). Multi-objective optimization of a thermal comfort index based on the adaptive neuro-fuzzy inference system and simplex algorithm. Energy and Buildings, 106, pp. 47-56. doi: 10.1016/j.enbuild.2015.07.003.

2. Ruchkin, D.S., Canolty, R.T., and Krusienski, D.J. (2018). Targeted information delivery to human auditory cortex using functional magnetic resonance imaging-guided sparse source localization. Human Brain Mapping, 39(12), pp. 4837-4850. doi: 10.1002/hbm.24331.

3. Han, X., Jiao, R., Li, X., and Wang, Y. (2020). An adaptive simplex algorithm for trajectory optimization of industrial robots. Journal of Intelligent and Fuzzy Systems, 39(1), pp. 735-744. doi: 10.3233/JIFS-179332.

УДК 004.421.2

К.О. Вадурін,
Д.В. Мосьпан, к.т.н.,
О.О. Юрко, к.т.н.
Кременчуцький національний університет
ім. М.Остроградського, Кременчук

СИНТЕЗ ІНТЕРПРЕТАЦІЇ ЕВОЛЮЦІЙНОГО АЛГОРИТМУ ДЛЯ НОРМАЛІЗАЦІЇ ФІЗІОЛОГІЧНО-ПСИХОЛОГІЧНОГО СТАНУ ЛЮДИНИ-ОПЕРАТОРА

Людина-оператор, протягом свого робочого часу, може перебувати у великій кількості різних фізіологічно-психологічних станах викликаних як зовнішніми впливами, так і внутрішніми процесами. Для конкретної ідентифікації зовнішніх впливів, внутрішніх процесів та їх наслідків для людини-оператора необхідно провести окремі комплексні дослідження з застосуванням експертних оцінок та залученням великої кількості людей різних професій. Для проведення цих досліджень, а також для виявлення дії зовнішніх впливів спрямованих на нормалізацію стану людини-оператора, за рахунок використання еволюційних алгоритмів у підборі оптимального значення зовнішніх впливів, доцільно розробити власну інтерпретацію еволюційного алгоритму, який потім можна було б швидко налаштовувати виходячи з вимог дослідження.

Метою роботи є створення власної інтерпретації еволюційного алгоритму з можливістю швидкого налаштування до вимог досліджень.

Об’єктом дослідження є процес підбору оптимальних значень зовнішніх впливів для нормалізації стану людини-оператора.

Предметом дослідження є синтез інтерпретації еволюційного алгоритму для нормалізації фізіологічно-психологічного стану людини-оператора.

Методи дослідження. Теоретичні: постановка проблеми використання еволюційного алгоритму для визначення оптимального співвідношення зовнішніх впливів для нормалізації стану людини оператора. Практичні: синтез інтерпретації еволюційного алгоритму.

Наукова новизна полягає в удосконаленні базової версії еволюційного алгоритму для застосування з безліччю вхідних

аргументів та функціями пристосованості різної складності.

Еволюційні та генетичні алгоритми уже широко використовуються для оптимізації дози ліків з використанням нечіткої системи висновків [1], для реалізації концепцій фармакогенетики та фармакогеноміки у індивідуальному підході для визначення оптимальної дози ліків [2], для визначення індивідуальної сприйнятливості до застосованих засобів на основі фармакогенетики в клінічній практиці [3]. Але у дослідженнях не наведено конкретних методів, за допомогою яких можливо визначати вплив та конкретний набір засобів для нормалізації стану людини.

У ході роботи було синтезовано алгоритм еволюційної моделі підбору параметрів до функції пристосування, що може змінюватися відповідно до поточного стану дослідження, який зображено на рис.1.

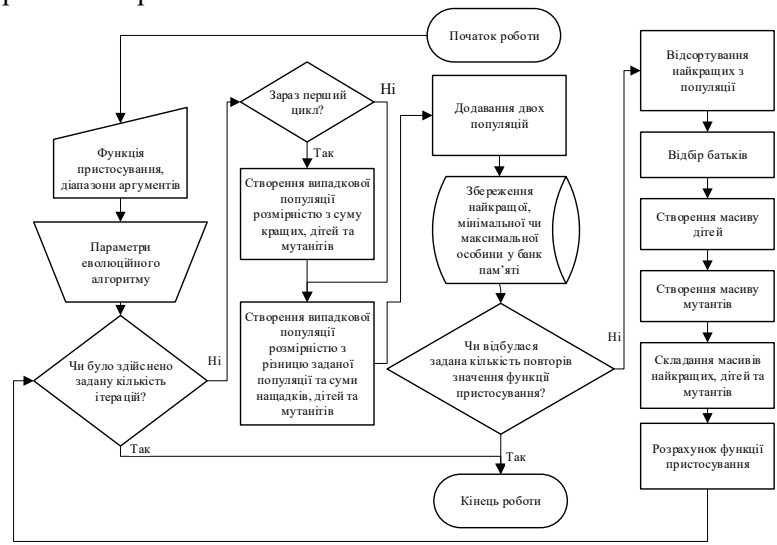


Рис.1. Синтезований еволюційний алгоритм.

За синтезованим алгоритмом, користувач має ввести функцію пристосування та налаштування еволюційного алгоритму, а також діапазон можливих значень аргументів. Далі, у першому циклі, створюється випадковий масив з розмірністю у задану кількість дітей, мутантів та найкращих екземплярів популяції. Потім відбувається створення масиву з кількістю особин що залишилася

задана за умовою, до цього елементу алгоритму відбувається перехід після кожної ітерації. Далі два масиви особин додаються та піддаються сортуванню та визначенню особини з максимальним значенням функції пристосування. Далі відсортовуються особини з найкращим значенням функції пристосування, обираються батьки, формуються масиви найкращих з ітерації, дітей та мутантів, які утворюють новий масив. Потім відбувається збільшення лічильника ітерації та процес продовжується до досягнення стоп умови, досягнення максимума значення лічильника ітерації чи заданої кількості повторів максимального значення функції пристосування.

У ході роботи синтезовано еволюційний алгоритм необхідний для створення програми у середовищі Mathcad для пошуку оптимальної функції пристосованості для визначення оптимальної комбінації інтенсивності вхідних впливів для нормалізації стану людини-оператора.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Subramanyam J., Ravi Kumar V. Optimization of drug dosage using genetic algorithm and fuzzy inference system. Journal of Advanced Research in Dynamical and Control Systems, 10(02), pp. 1424-1434. Available at: https://www.jardcs.org/abstract.php?id=1484.

2. Patrício A.F., Ribeiro L.C., de Melo Rodrigues V. Pharmacogenetics and pharmacogenomics: concepts and applications in drug safety and efficacy. Einstein (Sao Paulo), 19, eRW6213. Available at: https://doi.org/10.31744/einstein_journal/2021RW6213.

3. Liao J.G., Hsu K.L., Wang C.H. Personalized drug dosing using pharmacogenetics: current status and the future. Clinical and Translational Science, 14(1), pp. 8-18. Available at: https://doi.org/10.1111/cts.12877.

УДК 004.942:620.179.18:621.643.8

О.А. Владимирський, д.т.н.,
І.А. Владимирський, к.т.н.
Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, Київ

ОСОБЛИВОСТІ КОРЕЛЯЦІЙНОГО МЕТОДУ ПОШУКУ ВИТОКІВ ТА СПОСОБИ ЇХ ВРАХУВАННЯ

Даний метод, заснований на обробці сигналів з поверхні трубопроводу, поряд з так званим акустичним методом, заснованим на обробці сигналів з поверхні ґрунту над трубопроводом, на сьогоднішній день є найефективнішими та найпоширенішими при пошуку витоків на підземних трубопроводах. Проте умови пошуку витоків дуже різноманітні. Від їхнього врахування залежить достовірність результатів течешукання.

Взаємна кореляційна функція (ВКФ) чутлива до потужних джерел акустичних завад, механічно пов'язаних із трубопроводом - до шумів від сопел елеваторів у теплових мережах, від не до кінця відкритих або закритих засувок, від протікань у сальникових компенсаторах, від насосів, тощо. Не дивлячись на те, що джерела цих перешкод можна залишити за межами ділянки між датчиками, такі "позамежні завади", залежно від своєї потужності, частково або повністю "осліплюють" датчики течешукача, внаслідок чого максимум ВКФ може не відповідати витоку. Через чутливість ВКФ до подібних завад, перед застосуванням течешукача доцільно переконатися в тому, що основний шум, наприклад в теплову камеру, надходить саме з боку діагностованої ділянки трубопроводу, тобто саме від шуканого витоку. Найбільш просто це робиться шляхом порівняння рівнів шуму у різних точках на трубопроводі всередині даної теплової камери за допомогою акустичного течешукача або віброметра з цифровою індикацією. Спеціально для цього призначений течешукач А-10Т розробки ІПМЕ ім. Пухова НАНУ.

ВКФ чутлива до місць встановлення вібродатчиків. На рис.1 представлені ВКФ, отримані для однієї і тієї ж ділянки теплової мережі з установкою датчиків в одних і тих теплових камерах. Відмінність лише у позиції одного з двох датчиків, відстань між

позиціями 2,4 м. Більш виразної, якісної ВКФ відповідає і більша точність визначення координати витоку. Тому, для точного визначення місця витоку настійно рекомендується проводити 2-4 обчислення ВКФ при різних позиціях датчиків, що відрізняються один від одного не менше ніж на 0,5 м [1].

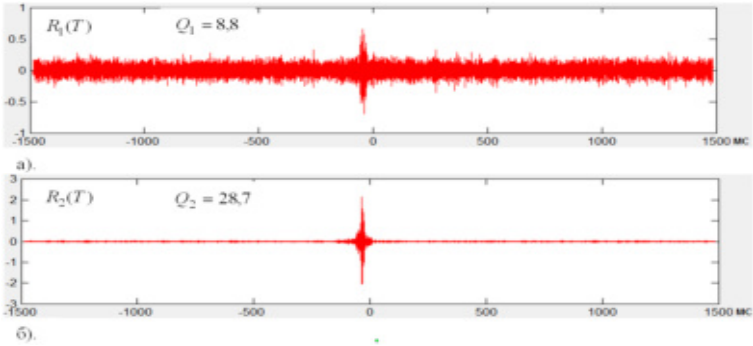


Рис.1. Вигляд ВКФ, обчисленої за сигналами з різними позиціями датчиків на трубопроводі.

У багатьох випадках ВКФ може мати розмитий, неоднозначний вид з різних причин. Значно підвищити достовірність визначення координати витоку дозволяє розроблений авторами спосіб, що полягає у цілеспрямованій просторово-частотній селекції ВКФ, сформованій найбільш потужними вібросигналами витоку із відомою швидкістю [2].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Патент на корисну модель № 144444; G01M 3/24, G01M 3/18, F17D 5/02. Владимирський О.А., Владимирський І.А. Параметричний кореляційний спосіб визначення координат витоків трубопроводів. Публікація відомостей 25.09.2020, Бюл. №18.

2. Владимирський О.А., Владимирський І.А. Кореляційні параметричні методи визначення координат витоків підземних трубопроводів// Електрон. моделювання, 2021, 43, № 3. – С. 3-17.

УДК 004.942 : 620.179.18 : 621.643.8

О.А. Владимирський, д.т.н.,
І.А. Владимирський, к.т.н.,
Г.В. Анфімова, к.г.н.,
І.П. Криворучко,
С.М. Дяченко
Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, Київ

СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАСОБІВ ДІАГНОСТИКИ ТА ПЕРІОДИЧНОГО КОРОЗІЙНОГО МОНІТОРИНГУ ПІДЗЕМНИХ ТРУБОПРОВОДІВ ТЕПЛОВИХ МЕРЕЖ

Значний знос підземних трубопроводів тепло і водопостачання міст України з одного боку і економічна неможливість провести масштабні оновлення трубопроводів, які відпрацювали регламентний термін експлуатації, з іншого боку породжують проблему інструментального визначення ділянок трубопроводів з фактичним критичним зносом для їх оновлення у першу чергу. Аналогічна технічна проблема актуальна для країн найбільших мегаполісів Північної Америки, Європи та інших регіонів.

Основним проявом зносу підземних трубопроводів міських теплових мереж є витоки, породжені корозійним стоншенням стінок трубопроводів. Тому показником зносу, який потребує інструментального визначення, є ступінь цього стоншення за віссю трубопроводу.

З відомих на даний момент технічних рішень, приладів і методик для оцінки стану металу стінок трубопроводів, можна виділити наступні: ультразвукова система WAVEMAKER Guided Ultrasonics Ltd (Великобританія) [1-2]; система безперервного моніторингу ЕМА ІЕЗ ім. Є.О. Патона НАН України [3-4]; Комплекти Каскад, Курсор, Вектор; спеціалізовані прилади магнітометричного неруйнівного контролю ТОВ "Энергодиагностика"; Системи внутрішньотрубної діагностики виробництва Inspector-systems (Німеччина), Центру технічної діагностики "Діаскан", ТОВ “НВЦ “ВТД” і багато інших. З різних причин всі перераховані вище засоби не дозволяють вирішити проблему дистанційного визначення координат та оцінки ступеня корозійного стоншення стінок трубопроводів розгалужених

міських теплових мереж з охопленням ділянок довжиною не менше 200 м у робочих режимах без виведення їх з експлуатації, в умовах наявності численних інженерних комунікацій, без необхідності виконання об'ємних земляних робіт.

Найбільш перспективним для вирішення задачі дистанційного діагностування теплових мереж можна вважати застосування низькочастотних віброакустичних методів. Низькочастотні вібросигнали від спеціальних генераторів поширюються уздовж трубопроводів на достатньо значну відстань для їх надійної реєстрації у наявних місцях доступу до трубопроводів для їхнього застосування у якості носіїв ознак корозійних стоншень підземних трубопроводів. Зазвичай наскрізні дефекти в трубопроводах тепломереж виникають в результаті розвитку і поглиблення в метал локалізованої у просторі групи каверн, деякі з яких формують свищі. Інші, різні за величиною каверни, у сукупності, створюють області стоншення металу зі своїми резонансними властивостями. Проблема з інтерпретації результатів в складній завадовій обстановці вирішується шляхом використання параметричних кореляційних методів [5-7]. Для практичного вирішення цього завдання у ІПМЕ ім. Г.Є. Пухова НАН України розроблено та випробувано експериментальну систему активно-пасивного корозійного моніторингу на базі створеного багатоканального розподіленого вздовж трубопроводу на сотні метрів реєстратора акустичних сигналів трубопроводів РАСТР-1. Результати випробувань підтверджують високу ефективність такого рішення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Alleyne D. N., Lowe M. J. S. and Cawley P. The reflection of guided waves from circumferential notches in pipes. ASME J. Applied Mechanics. 1998. Vol. 65. Pp. 635-641.

2. Demma A., Alleyne D., Pavlakovic B. Testing of Buried Pipelines Using Guided Waves. 3rd MENDT - Middle East Nondestructive Testing Conference & Exhibition (27-30 November, 2005, Bahrain, Manama) [Електронний ресурс]. URL: http:// www.ndt.net. (Дата звернення 04.03.2021).

3. Недосека С. А., Недосека А. Я. Диагностические системы семейства "ЕМА". Основные принципы и особенности

архитектуры (обзор). Техническая диагностика и неразрушающий контроль. 2005. № 3. С. 20-26.

4. Недосека А.Я., Недосека С.А., Яременко М.А. Непрерывный мониторинг магистральных газопроводов и газокомпрессорных станций методом акустической эмиссии. Техническая диагностика и неразрушающий контроль. 2011. № 4. С. 3-13.

5. Владимирский А. А., Владимирский И. А., Криворучко И. П., Савчук Н. П. Разработка модернизированной системы низкочастотного диагностирования состояния трубопроводов РАСТР-1М. Моделювання та інформаційні технології (збірник наукових праць ІПМЕ ім. Г.Є. Пухова НАН України). 2017. Вип. 78. С. 40-45.

6. Владимирський О. А., Владимирський І. А. Науковий твір "Методика диагностического обследования трубопроводов тепловых сетей, находящихся в эксплуатационных режимах, с применением регистратора акустических сигналов РАСТР-1. Свідоцтво про реєстрацію авторського права на службовий твір №95280 від 13.01.2020р. Україна. ІПМЕ ім. Г.Е.Пухова НАН України.

7. Владимирський О. А., Владимирський І. А. Організація мобільного просторово - розподіленого, синхронізованого збору акустичних даних про стан підземних трубопроводів. Збірник тез доповідей XIII міжнародної науково-практичної конференції CSNT 2021, "Комп'ютерні системи та мережні технології". М. Київ. 15-17 квітня 2021 р.

УДК 519.9

А.М. Воронін, д.т.н.,
А.С. Савченко, д.т.н.
Національний авіаційний університет, Київ

ВЕКТОРНА ОПТИМІЗАЦІЯ АРХІТЕКТУРИ НЕЙРОМЕРЕЖЕВИХ КЛАСИФІКАТОРІВ

Важливим різновидом систем штучного інтелекту є нейромережеві класифікатори. Вони застосовуються для технічної та медичної діагностики, класифікації різноманітних інформаційних джерел та ін.

Кількість нейронів вхідного шару $p_0 = n$ визначається розмірністю вхідного вектора ознак та не підлягає змінам. Аналогічно, кількість нейронів вихідного шару $p_{q+1} = m$ визначається числом областей (класів), на які ділиться простір ознак і є постійним. Кількість же обробних (прихованих) шарів q і число нейронів у кожному з них $p_1, p_2, ..., p_q$ становлять поняття **архітектури** нейронної мережі і можуть бути аргументами (незалежними змінними) при її оптимізації. Аргументами оптимізації архітектури нейронного класифікатора є кількості нейронів у кожному з обробних шарів, що становлять вектор незалежних змінних $p = \{p_j\}_{j=1}^{q}$. Від вибору архітектури p залежить якість функціонування нейронного класифікатора.

Одним із критеріїв є ймовірність помилки класифікації. Представимо його як кількість помилок класифікації $e(p)$, віднесене до загальної, досить великої кількості випробувань: N:

$$f_1(p) = \frac{e(p)}{N}.$$

Гранично допустиме значення помилки мережі має бути відоме з фізичних міркувань і задано як обмеження $f_1(p) \le A_1$.

Другий критерій характеризує час, необхідний для навчання нейронної мережі при даної архітектурі p. Спостерігається тісна кореляція між таким часом та сумарною кількістю нейронів у

прихованих шарах класифікатора. Тому представимо цей критерій у вигляді

$$f_2(p) = \sum_{k=1}^{q} p_k \ .$$

Гранично допустиме значення другого критерію визначається допустимим часом навчання нейронної мережі та визначається як обмеження $f_2(p) \le A_2$.

Допустима область аргументів оптимізації задається паралелепіпедним обмеженням

$$P = \{p | 0 \le p_k \le P_u, k \in [1, P_u], u \in [1, q]\},$$

де P_u – максимальна кількість нейронів в u -му шарі.

Обидва критерії є суперечливими, невід'ємними, мінімізованими та обмеженими. В наявності всі передумови для використання як цільової функції скалярної згортки критеріїв за *нелінійною схемою компромісів* [1].

Таким чином, вираз для задачі оптимізації архітектури нейронного класифікатора має вигляд

$$p^* = \arg\min_{p \in P} \left[\frac{A_1}{A_1 - e(p)/N} + \frac{A_2}{A_2 - \sum_{k=1}^{q} p_k} \right].$$

Здійснення викладених етапів векторної оптимізації дозволяє без безпосередньої участі особи, що приймає рішення, визначити архітектуру нейромережевого класифікатора, при якій системно ув'язуються суперечливі критерії ефективності його функціонування, а отримана архітектура є компромісно-оптимальною.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Воронін А.М., Зіатдінов Ю.К., Климова А.С. Інформаційні системи прийняття рішень: Навчальний посібник. – К.: НАУ, 2009. – 136 с.

УДК 004.23

В.І. Воронцов
Національний авіаційний університет, Київ

ОГЛЯД ФОРМАТУ POSIT

Posit арифметика - це новий тип даних, який розроблений як альтернатива float арифметиці стандарту IEEE754. Основна відмінність у формуванні числа posit перед float полягає у тому, що число posit має змінну довжину дробової частини (мантиси), а також з'являється додаткове поле режиму числа, яке теж має змінну довжину. Лише поля знаку та експоненти мають фіксоване значення, визначається в залежності від реалізації.

Формат числа posit:

MSB (старший розряд) LSB (молодший розряд)

Sign (S, знак)	Regime (R,режим)	Exponent (E,експонента)	Fraction (F,дробова частина)
1 біт	rs бітів	es бітів	n-rs-es-1 бітів

Стандарт posit диктує наступний розмір поля експоненти:

$$es = \log_2 \frac{n}{2^3} \quad , \qquad (1)$$

де n – кількість бітів.

Мінімальний розмір числа у форматі posit складає 8 біт.

Мантиса має ті ж властивості, що й в типі float, проте можливо що біти режиму заповнять весь допустимий простір і буде отримано пусту мантису, тобто її значення дорівнює 0. Також існує ціла частина – так званий віртуальний біт, який завжди рівний одиниці.

Оскільки при розмірі формату 8 біт, експонента буде нульовою, за множник будуть відповідати біти режиму. Біти режиму – це послідовність однакових знаків, яка закінчується знаком протилежної величини. Таким чином можна зрозуміти де закінчилось поле режиму та почалась експонента. Знаючи фіксовану довжину експоненти, можна дізнатись де починається дробова частина.

У табл. 1. відображена розшифровка бітів режиму в число k.

Таблиця 1.

Розшифровка бітів режиму в число k

R	**k**	**R**	**k**
10	0	01	-1
110	1	001	-2
1110	2	0001	-3

Поле режиму дає досить специфічне значення для числа загалом. Саме режим визначає додатній або від'ємний степінь числа, а експонента грає менш впливову роль, регулюючи певний діапазон значень, обмежений її бітами. Для визначення значення режиму використовується наступна формула:

$$Regime = useed^k \quad (2)$$

$$useed = 2^{2^{es}} \quad (3)$$

В даному випадку кількість біт експоненти визначає базис режиму, який підноситься у степінь k, що отриманий з режимних бітів.
Залежність базису режиму (useed) від кількості біт експоненти показано в таблиці 2.

Таблиця 2

Залежність базису (useed) від кількості біт експоненти (es)

es	0	1	2	3	4
useed	2	4	16	256	65536

Таким чином, posit-число можна порахувати за наступною формулою:

$$x = (-1)^S \times useed^k \times 2^e \times \left(1 + \sum_{i=1}^{fn-1} b_{fn-1-i} 2^{-i}\right), \quad (4)$$

де fn – кількість бітів дробової частини, b – певний біт дробової частини, e – значення експоненти.

В posit арифметиці існує лише один режим округлення: округлити до найближчого, прив'язати до найближчого парного, таке, яким є за замовчуванням режим округлення для IEEE 754. Якщо програміст або користувач відчуває потребу в інших трьох режимах, які підтримуються float (округлення вниз, округлення вгору, округлення до нуля), це означає, що програма вимагає числа valid (режим точного числа у стандарті posit, являє собою діапазон між 2 значеннями), а не posit або, можливо, просто правильного інструменту налагодження.

Проаналізуємо переваги та недоліки формату posit.

До переваг відноситься:

1. динамічний режим полів, який дозволяє досягнути кращої точності в певному діапазоні;
2. простота апаратної реалізації;
3. відсутність понять переповнення або втрати значимості;
4. мала кількість виключень, а саме NaN (не є числом), нескінченність, underflow;
5. переповнення ніколи не відбувається, окрім випадку 1/0;
6. на відміну від float, має лише 1 значення NaN, коли у float їх кількість може досягати 9 квадрильйонів;
7. підтримка доповняльного коду, що дозволяє виконувати порівняння чисел формату posit як знакові цілі числа;
8. єдина система правил округлення.

Недоліки:

1. в деяких випадках доведеться виконувати додаткові операції віднімання для порівняння чисел;
2. на сьогодняшній день немає апаратної реалізації у комерційних продуктах;
3. формат числа недостатньо досліджений відносно float чисел.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Posit Standard Documentation. URL: https://posithub.org/docs/posit_standard.pdf (дата звернення: 28.03.2023).

2. Posit lookup table. URL: https://posithub.org/widget/lookup (дата звернення: 28.03.2023).

УДК 004.045(043.2)

В.П. Гамаюн, д.т.н.
Національний авіаційний університет, Київ

КОНТРОЛЕЗДАТНІСТЬ РОЗРЯДНО-ЛОГАРИФМІЧНИХ КОДІВ

Представлення даних в засобах комп'ютерної техніки та інформатики є базовим при реалізації обробки, Контролездатність також складає необхідну частину практичних характеристик разом зі швидкістю, діапазоном та іншими.

Основні положення розрядно-логарифмічного кодування даних полягають у застосуванні спеціальних кодів для позначення розрядів цифрових операндів, які не є нульовими, тобто значущих розрядів:

$$\text{Операнд } A = \text{Арл} = \{ N_1\ N_2\ N_3\ N_4\ ,,,,,,,N_Q\}$$

Кожен код значущого $N_i = (a_i\ p_i \neq 0)$ обчислюється як логарифм від кількості, яка визначається цим розрядом: $N_i = \log_2 a_i\ p_i = i$. Таке кодування є однозначним та виконується без функціонального перетворення.

Для кожного числа операнд існує форма представленні у комп'ютерних засобах наступним чином зібраних у наступний формат:

$$\text{Sign A .}\ Q\ ,\ N_1\ N_2\ N_3\ N_4\ ,,,,,,,N_Q$$

де Sign A знак числа у двійковій системи числення .

Q - кількість значущих одиниць у двійковому операнді,

$N_1\ N_2\ N_3\ N_4\ ,,,,,,,N_Q$ масив розрядно-логарифмічних кодів (кодів значущих одиниць)/

Розглянемо формат РЛ числа: незвичним є параметр Q, так как інші параметри зустрічаються у відомих структурних одиниць обробки – векторах, масивах та інше. Кількість значущих одиниць є унікальним параметром бо відображає саме точне представлення Нуля =0 – таким чином немає значущих одиниць у числі і таке число має зчалення нуль. Дозволяє реалізувати стиснену форму для операнда – Два коди можуть представити число великого розміру для обробки. Наприклад

+ 10000000000000000000000000000000001 = +2.10101.0. де 10101 та 0 коди значущих одиниць.

Такий параметр є зручним при оцінці арифметичних операцій з точки зору штучного інтелекту:

-контроль ділення на нуль;
- нулевій результат при множенні;
-апріорний результат при додаванні та відніманні;
- порівняння з нулем.

Арифметичні операції для розрядно-логарифмічних операндів мають особливості наступного характеру. Так як: $N_i = \log_2 a_i p_i = i$. Тобто значення кодів пов'язані зі значенням логарифму то для однокодових операцій маємо наступні закони виконання:

Додавання $N_i + N_j = N_i N_i$, якщо $N_i > N_o$
$_j$ якщо $N_i + 1$ якщо $N_i = N_i$

По таких законах маємо алгоритми повнрозрядної обробки для розрядно-логарифмічних кодів.

Контролездатність таких алгоритмів є початковою темою у дослідженнях по розрядно-логарифмічному кодуванню. Саме параметр є головним при побудові алгоритмів безпомилкових виконань арифметичних операцій у комп'ютерних засобах. За початкову гіпотезу приймається, що правильним виконанням, операції є правильна кількість кодів у результаті. Таке значення параметра обчислюється додатковим програмно-апаратним забезпеченням, яке (гіпотетично) працює надійно. Така апаратура повинна працювати надійно та швидко, паралельно з основною процесорною частиною,

Щоб до завершення операції мати значення параметра Якщо значення співпадають, операція виконана безпомилково. Виконання умов гіпотез залежить від розподілення кодів значущих одиниць у розрядно-логарифмічних операндах.

Розглянемо такі умови при додаванні. Операнд А має масив де найменший код більше ніж найбільший код Операнда В – при такому випадку коди не перехрещуються та результат складається з суми Q=QA+QB – це найпростіший варіант,

Інший варіант коли коди операндів мають загальні значення

$N_1\ N_2\ N_3\ N_4$,,,,,,,,N_{QA}
$N_1\ N_2\ N_3\ N_4$,,,,,,,,N_{QB}

Пропонується наступна процедура для обчислення параметра

1. Викреслюється коди однакових значень- формується масив переносів

2. Формуються групи кодів, на які впливає перенос

3. В таких групах визначається значення суми, а також значення з вірогідним переносом у таку групу. Всі групи працюють паралельно.

4. Визначаються всі параметри по кожній групі Q та їх загальна кількість Q1+Q2+Q3+….

Розглянемо приклад

A= + QA=9. 17. 16.15.14.13.12.9.8.4.
та B=+QB=7. 16. 15. 6.5.4.3.2.

Формуємо масив переносів

A=17 14.13.12.9.8. B= 6.3.2.
P 17. 16.(16) (8) 5.

де в дужках зазначенні вірогідні переноси.

По першій групі маємо результат 18.16.; друга група 14.13.12.9.8.; третя група 6.5.3.2.

Після загальних обчислень Q1+Q2+Q3 маємо Q1+Q2+Q3=11 , що є правильним значенням параметру кількості значущих одиниць суми A та B.

Такий підхід може бути застосовано для всіх операцій для розрядно-логарифмічних кодів, що підтверджує контролездатність останніх.

УДК 004.274:004.056

С.Я. Гільгурт, д.т.н.
Національний авіаційний університет, Київ

ТЕХНІКА ВПОРЯДКУВАННЯ ПАТЕРНІВ ДЛЯ АНАЛІЗУ ТЕХНІЧНИХ ХАРАКТЕРИСТИК РЕКОНФІГУРОВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

У зав'язку зі сталим зростанням мережевого трафіку та кількості кібератак програмна реалізація засобів технічного захисту інформації вже не відповідають вимогам щодо їх швидкодії. Реконфігуровні рішення (на базі ПЛІС) поєднують продуктивність спецпроцесорів і гнучкість програмного забезпечення, тому все частіше використовуються для побудови таких засобів [1].

Схеми апаратного множинного розпізнавання патернів, яке здійснюється в системах технічного захисту інформації на базі сигнатурного (найбільш точного) підходу до розпізнавання, потребують методів кількісної оцінки їх технічних характеристик. Властивості словнику патернів, що входять до складу бази даних сигнатур, мають важливе значення при реалізації таких систем, тому для їх побудови необхідні техніки поводження з патернами.

Подамо множину патернів, що мають розпізнаватися сигнатурною системою захисту інформації, у наступному вигляді:

$$P = \left\{ p_1,\ p_2,\ p_3, \ldots\ p_k, \ldots\ p_\sigma \,\middle|\, \sigma, \Omega, m_{\min}, m_{\max}, \delta, \mu, \mu_z, \nu \right\},$$

де $p_1, p_2, p_3, \ldots p_k, \ldots p_\sigma$, – власне набір патернів, σ – кількість патернів в наборі, Ω – загальна кількість символів в наборі патернів, m_{min} – довжина найкоротшого патерну в наборі, m_{max} – довжина найдовшого патерну в наборі, δ – функція розподілу довжин, μ – перша функція самоподоби, μ_z – перша часткова функція самоподоби, ν – друга функція самоподоби. Патерни p_k є фіксованими послідовностями символів, код кожного з котрих належить до певного алфавіту Σ.

В якості основи подальших розрахунків запропоновано наступну техніку впорядкування патернів у наборі. Відсортуємо всі патерни в множині P за зростанням довжини, як наведено на рис. 1. Складені з квадратів стовпчики зображають рядки символів.

Назвемо *пакетом* сукупність патернів однакової довжини, не звертаючи уваги, як впорядковані патерни всередині сукупності.

Введемо індекс j таким, що співпадає з довжиною патернів в пакеті: $j = m_{min}, m_{min+1}, m_{min+2}, \ldots m_j, \ldots m_{max}$, де m_{min} – довжина найкоротшого патерну, m_{max} – довжина найдовшого патерну, причому кожне наступне значення цього індексу обов'язково на одиницю більше за попереднє, тобто в нумерації немає пропусків.

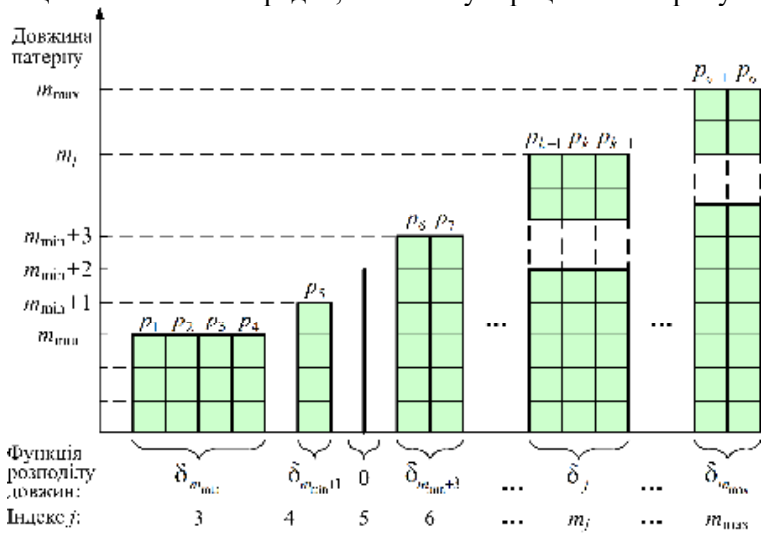


Рис.1. Техніка впорядкування пакетами однакової довжини.

Тоді довжина кожного патерну в наборі співпадатиме з індексом його пакету: $m_j = j$. *Функцію розподілу довжин* δ як залежність від індексу j визначимо рівною кількості патернів у відповідному пакеті: $\delta(j) = \delta_j$. За допомогою цієї функції можна зручно обчислити кількість ненульових пакетів ξ та загальну кількість символів Ω в наборі. Функції самоподоби дозволяють в різний спосіб кількісно оцінювати надмірність словнику патернів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Hilgurt S. A Concise Review of FPGA-Based Hardware Solutions for Network Intrusion Detection. Proceedings of the 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T'2021). – 2021. – Vol. 36. – IEEE, Kharkiv, Ukraine. – P. 164-168.

УДК 004.056.53

В.В. Горіна,
Я.В. Вовкотруб,
І.В. Радченко
Національний авіаційний університет, Київ

ТЕХНОЛОГІЇ РОЗРОБКИ ВЕБ-ЗАСТОСУНКУ КОМЕРЦІЙНОГО ПРИЗГАЧЕННЯ

Розробка веб-застосунків комерційного призначення передбачає використання сучасних технологій та інструментів програмування, а також дотримання принципів проектування користувацького інтерфейсу, що забезпечує зручне та ефективне взаємодію користувача з додатком. Ключовими аспектами технології розробки веб-застосунку є забезпечення безпеки та надійності системи, а також швидкого та ефективного доступу до інформації для кінцевих користувачів. Для досягнення цих цілей необхідно використовувати передові методи розробки програмного забезпечення, що дозволяють розробникам швидко та ефективно реалізовувати вимоги користувачів та забезпечувати якість продукту.

Як і розробка будь-якого застосунку, створення веб-сайту це комплексна задача, яка потребує чіткого планування і реалізації окремих модулів процесу розробки. Основні етапи розробки веб-застосунку включають наступні кроки:

1. Збір вимог: на цьому етапі визначаються потреби користувачів та бізнес-вимоги до проекту. Розробник повинен зрозуміти, які функції та можливості повинен мати веб-застосунок, щоб відповідати потребам користувачів та бізнесу.
2. Проектування: на цьому етапі створюється дизайн веб-застосунку та визначається архітектура проекту. Розробник повинен зрозуміти, як будуть взаємодіяти різні компоненти системи, які технології та інструменти використовуватимуться.
3. Розробка: на цьому етапі розробляється код веб-застосунку. Розробник повинен використовувати передові методи розробки програмного забезпечення та дотримуватися стандартів та правил кодування.
4. Тестування: на цьому етапі перевіряється, чи відповідає веб-застосунок вимогам, чи працює коректно та чи забезпечується безпека даних. Розробник повинен проводити різні види тестування, такі як функціональне, інтеграційне та навантаження.

5. Реліз: на цьому етапі веб-застосунок готовий до релізу та випуску на ринок. Розробник повинен забезпечити встановлення та налагодження веб-застосунку на серверах та забезпечити його підтримку та обслуговування.

6. Підтримка: на цьому етапі розробник повинен забезпечувати підтримку та обслуговування веб-застосунку, виправляти помилки та вдосконалювати його функціональність відповідно до потреб користувачів.

Розробка веб-застосунків є дуже поширеною в IT-індустрії. Веб-застосунки застосовуються у багатьох сферах, таких як електронна комерція, фінанси, медіа, соціальні мережі, блоги, державні та некомерційні організації, наукові та дослідницькі установи та багато інших. Деякі з найбільш поширених веб-застосунків включають:

- Системи управління контентом (Content Management Systems - CMS), такі як WordPress, Drupal та Joomla.
- Електронні магазини, такі як Amazon, eBay та Alibaba.
- Соціальні мережі, такі як Facebook, Twitter та LinkedIn.
- Онлайн-банкинг, такий як Chase, Bank of America та Wells Fargo.
- Онлайн-медіа, такі як The New York Times, CNN та BBC.

Веб-розробка стала доступнішою завдяки зростанню ресурсів та інструментів для розробки, в тому числі відкритих джерел, таких як фреймворки та бібліотеки.

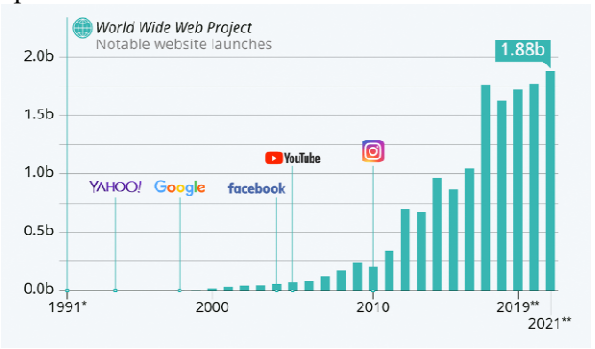


Рис. 1. Кількість веб-застосунків

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *How Many Websites Are There? by Martin Armstrong, Aug 6, 2021 (https://www.statista.com/chart/19058/number-of-websites-online/).*

УДК 004.056.53

[1]В.В. Горіна,
[1]К.О. Ільченко,
[2]М.Р. Ніколюк
[1]Національний авіаційний університет, Київ
[2]НТУУ "КПІ ім. І.Сікорського", Київ

ВИКОРИСТАННЯ SWOT-АНАЛІЗУ В УПРАВЛІННІ ПРОЄКТАМИ

SWOT-аналіз є однією з ключових методик управління, яка допомагає визначити сильні та слабкі сторони проекту, а також можливості та загрози, що можуть виникнути в майбутньому. Цей аналіз важливий для успішного планування та реалізації проектів, оскільки дозволяє виявити проблеми та ризики, які потрібно вирішувати, а також визначити конкурентну перевагу та стратегію розвитку проекту.

Методика SWOT (Strengths, Weaknesses, Opportunities, Threats) - це інструмент стратегічного аналізу, який допомагає оцінити сильні та слабкі сторони проекту, а також можливості та загрози зовнішнього середовища. SWOT-аналіз може бути корисним інструментом для розробки стратегії, планування проекту, а також для вирішення проблем [1].

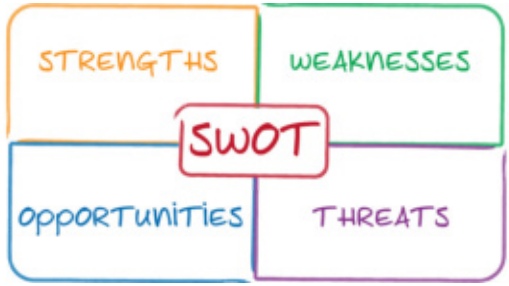


Рис. 1. Етапи SWOT-аналізу

SWOT-аналіз проводиться у 4 етапи:

- Оцінка сильних сторін (Strengths) - на цьому етапі слід з'ясувати, що робить проект успішним та чим він відрізняється від конкурентів. Сильні сторони можуть включати у себе високу якість продукту або послуги, сильну команду розробників, високу популярність у цільовій аудиторії та інші переваги.

- Оцінка слабких сторін (Weaknesses) - на цьому етапі слід з'ясувати, що потребує покращення в проекті, що заважає досягненню успіху. Слабкі сторони можуть включати у себе відсутність достатнього фінансування, відсутність висококваліфікованих спеціалістів, нестабільність управління та інші проблеми [2].

- Оцінка можливостей (Opportunities) - на цьому етапі слід з'ясувати, які можливості можуть бути використані для розвитку проекту. Можливості можуть включати у себе зростання ринку, з'явлення нових технологій, зміну політичної ситуації та інші.

- Оцінка загроз (Threats) - на цьому етапі слід з'ясувати, які загрози можуть виникнути та як їм протистояти. Загрози можуть включати у себе зміну законодавства, конкуренцію, зміну економічної ситуації, технічні проблеми та інші.

У висновку хотілося б зазначити, що SWOT-аналіз є потужним інструментом для планування та управління проектами, оскільки він дозволяє визначити сильні та слабкі сторони проекту, а також можливості та загрози, що можуть виникнути в майбутньому. Цей аналіз допомагає вирішити ряд проблем, таких як визначення стратегії, виявлення проблем та слабкі місця проекту, визначення конкурентної переваги та визначення ризиків.

SWOT-аналіз також допомагає підвищити ефективність управління проектами, дозволяє зробити правильний вибір при прийнятті рішень та дозволяє забезпечити успішну реалізацію проекту.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Jenei T. SWOT analyses of geothermal investment projects – case studies. International Review of Applied Sciences and Engineering. 2012. Vol. 3, no. 2. P. 97–103. URL: https://doi.org/10.1556/irase.3.2012.2.2 (date of access: 04.04.2023).

2. PEST and SWOT Analyses. Marketing Briefs: A Revision and Study Guide. 2012. P. 33–37. URL: https://doi.org/10.4324/9780080511085-12 (date of access: 04.04.2023).

УДК 004.056.53

В. В. Горіна,
Є. В. Негодюк
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ КВАНТОВОЇ ФІЗИКИ В КРИПТОГРАФІЇ ТА ЗАХИСТІ ДАНИХ

На сьогодення Інтеренет не тільки став необхідною складовою нашого життя, але й значно полегшив нашу повсякденну діяльність та забезпечив доступ до багатьох ресурсів та інформації.. Однак разом з цими плюсами він несе в собі вагому загрозу, а саме: втрату даних та використання їх зловмисниками для своїх корисливих цілей. Тому у сучасному світі важливим питанням є захист даних. Одним із найбільш поширених методів захисту є криптографічні протоколи, що використовують математичні алгоритми для захисту даних перед їх передачею, таких як RSA, AES і DES. Ці алгоритми шифрують дані за допомогою ключа, що генерується за певними правилами, і призначені для того, щоб зберегти інформацію в секреті, коли вона пересилається через відкриті мережі.

Проте, з появою квантових комп'ютерів стало очевидним, що ці алгоритми можуть бути легко розшифровані. Квантові комп'ютери здатні до швидкого розв'язування проблем, які займали кілька років для класичного комп'ютера, таких як факторизація великих простих чисел. Це вказує на те, що квантовий комп'ютер може легко розшифрувати дані, зашифровані звичайними алгоритмами.

Одним з підходів до розв'язання цієї задачі є застосування квантової криптографії, яка використовує властивості квантових частинок для створення безпечних криптографічних ключів та захисту передачі даних. Популярний метод квантової криптографії - це квантовий ключовий обмін (QKD). Він базується на використанні квантових властивостей світла, щоб створити безпечний криптографічний ключ між сторонами комунікації. Ключовим моментом у QKD є те, що при спробі перехоплення сигнального стану зі сторони зловмисника, він змінюється в результаті принципу невизначеності Гейзенберга.

Однією з основних переваг QKD є безумовна безпека, яку він забезпечує. Тобто квантовий ключ, який створюється в процесі

QKD, не може бути скомпрометований віддаленою стороною, навіть якщо він володіє найсучаснішими комп'ютерами та алгоритмами. Це відрізняє QKD від традиційних методів криптографії, які можуть бути підірвані сучасними комп'ютерами з високим рівнем обчислювальної потужності та складними алгоритмами. Це означає, що навіть якщо зловмисник отримує доступ до зашифрованих даних, не можна розшифрувати їх без квантового ключа. Таким чином, QKD забезпечує високий рівень безпеки для захисту конфіденційної інформації.

Недоліками QKD є технічна складність та високі витрати на системи розгортання. Використання квантової технології для створення безпечних ключів вимагає спеціального обладнання, яке є досить складним у виготовленні та вимагає спеціальної експертизи для його обслуговування. Процес QKD вимагає прямої видимості між приладами, що означає, що він не підходить для захисту даних на великій відстані.

Отже, розвиток квантової криптографії має значний потенціал у майбутньому, він забезпечує безумовну безпеку, що робить її привабливою для захисту даних у важливих сферах.Одним із напрямів розвитку квантової криптографії є підвищення ефективності. Іншим напрямком розвитку квантової криптографії є пошук нових методів захисту даних на основі квантової фізики, таких як квантова стеганографія, квантове шифрування та інші. Ці методи можуть забезпечити додатковий рівень безпеки та конфіденційності даних. Крім того, квантова криптографія може бути використана для захисту від майбутніх квантових комп'ютерів, які здатні розгадувати складні криптографічні алгоритми, які сьогодні використовують. Квантова криптографія може стати елементом забезпечення безпеки майбутнього квантового Інтернету.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Nielsen, Michael A. ta Chuang, Isaac L. "Quantum enumeration and quantum information",Cambridge University Press, 2010.

УДК 004.056.53

В.В. Горіна,
І.В. Радченко,
Я.В. Вовкотруб
Національний авіаційний університет, Київ

ПЕРСПЕКТИВИ РОЗРОБКИ ВЕБ-САЙТУ КОМПАНІЯМИ ДЛЯ ВЛАСНОГО БІЗНЕСУ

Розробка веб-сайту для власного бізнесу стає все більш популярним серед компаній, які хочуть підвищити свою онлайн-присутність і привернути нових клієнтів. Інтернет став важливим інструментом для підприємств, які хочуть збільшити своє охоплення аудиторії і розширити свій бізнес.

В Україні популярність розробки веб-сайтів компаніями для власного бізнесу зростає з кожним роком.

Згідно з дослідженням, проведеним компанією InMind, у 2021 році більшість підприємств в Україні (понад 80%) мають веб-сайт, і лише 18% не мають своєї онлайн-присутності. Також варто зазначити, що серед компаній, які мають веб-сайти, вище всього представлені підприємства малого та середнього бізнесу.

За даними досліджень, більше 60% малих і середніх підприємств (МСП) мають власний веб-сайт. Також, великі компанії все частіше інвестують у свої веб-сайти для поліпшення користувацького досвіду та підвищення продажів.

Розробка веб-сайту дозволяє компаніям показати свій бренд, продукти та послуги у світлі, з якого вони хочуть їх бачити. Крім того, веб-сайт дозволяє залучати нових клієнтів, розширювати аудиторію та збільшувати продажі.

Популярність розробки веб-сайту компаніями для власного бізнесу можна пояснити такими факторами:

1 Зручність: Веб-сайти доступні для перегляду у будь-який час та з будь-якого пристрою, що забезпечує зручність для користувачів та збільшує охоплення аудиторії.

2 Конкурентність: У сучасному світі, наявність веб-сайту допомагає підприємству конкурувати з іншими гравцями на ринку.

3 Збільшення продажів: Розробка веб-сайту дозволяє компанії залучати нових клієнтів, що збільшує продажі та доходи.

4 Поліпшення бренду: Веб-сайт є важливим елементом брендингу та маркетингу компанії.

Застосування альтернативних рішень може мати деякі негативні наслідки, зокрема:

1 Невідомість: Альтернативні рішення можуть бути менш відомими, що може призвести до ризику з використанням менш надійних або неякісних продуктів або послуг.

2 Компатибельність: Альтернативні рішення можуть бути менш сумісними з існуючими програмними засобами або ж апаратними рішеннями, що може привести до проблем з їх взаємодією.

3 Вартість: Альтернативні рішення можуть бути дорожчими або неможливими для довготривалого використання внаслідок високих витрат на підтримку і технічну підтримку.

4 Непевність: Альтернативні рішення можуть бути менш стабільними або менш прогресивними, що може призвести до того, що вони не зможуть задовольнити всі потреби бізнесу.

5 Безпека: Альтернативні рішення можуть мати менші заходи безпеки, що може призвести до ризику злому даних або інших кібератак.

6 Невизначеність: Альтернативні рішення можуть мати невизначені проблеми, які можуть виникнути в процесі роботи з ними, або невідомі наслідки при їх використанні.

Варто зазначити, що не всі альтернативні рішення мають негативні наслідки, і більшість рішень мають свої переваги та недоліки, які повинні бути ретельно вивчені перед прийняттям рішення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Андрушкевич З.М. Інтернет-маркетинг у соціальних мережах. Вісник Хмельницького національного університету. Економічні науки. 2014, No 2, Т. 1. С. 163-166.

УДК 004.42

М.М. Гузій, к.т.н.,
А.О. Старостенко
Національний авіаційний університет, Київ

ІНФОРМАЦІЙНА СИСТЕМА ВИБОРУ АРХІТЕКТУРНИХ ПАТЕРНІВ ЗА КРИТЕРІЯМИ ЯКОСТІ ВЕБ-ДОДАТКІВ

Вплив глобальної комп'ютерної мережі Інтернет на сучасний світ характеризується проникненням IT в усі сфери людського життя. Присутність в Інтернеті сьогодні є неохідною складовою виробництва, бізнесу, освіти, медицини. Веб-застосунки є специфічними програмними продуктами з точки зору розпізнавання середовища користувача, управління комунікаціями, вимог тестування, питань безпеки, інтерфейсу, функціонального дизайну і життєвого циклу.

Архітектура веб-додатку належить до основних факторів, які необхідно враховувати при проєктуванні для забезпечення якості програмного продукту. Організація *IEEE* визначає архітектуру як «фундаментальну організацію систем, втілену в їх компонентах, їхні зв'язки один з одним і середовищем та принципах керування проєктуванням і еволюцією». Дослідження архітектурних патернів проєктування необхідно для визначення вимог якості веб-додатків та прийняття архітектурно-проєктних рішень.

Мета дослідження - розробити інформаційну системи вибору архітектурних патернів за критеріями якості веб-додатків стандарту *ISO* 9126-1.

На основі порівняльного аналізу існуючих архітектурних шаблонів проєктування веб-додатків проведено їх оцінку методами *SLR* за атрибутами якості, впливами, доменами. Для вибору патерну запропоновано аналітичну модель на основі мінімізації трудомісткості проєкту за методикою *COCOMO II.* В роботі розглянуто основні шаблони програмних архітектур *SOA, CQRS*, *VIPER, EDA* та *DDD*, проведено аналіз вимог якості веб-додатків за стандартом *ISO* 9126-1 та виконано формалізований опис вимог за методом *SQFD.*

Проведений аналіз проблеми дозволив визначити онтологію предметної області, модель комбінації архітектурного патерну та

необхідні тактики проєктування з урахуванням трудомісткісті проєктування системи за методикою *COCOMO II.*

Однією з фундаментальних концепцій специфікації архітектури програмного забезпечення є визначення необхідних рівнів вимірювання атрибутів якості програмного забезпечення (системних якостей). На основі глосарію термінів розробки програмного забезпечення *IEEE* якість програмних продуктів — це ступінь, до якої система, компонент або процес відповідають визначеним вимогам (таким як функціональність, продуктивність, безпека та ремонтопридатність) і ступінь, до якої система, компонент або процес відповідають потребам або очікуванням користувача. Опис модель якості стандарту *ISO* 9125-1 виконано за алгоритмом *SQFD*. Вимоги до веб-додатків мають суттєве значення для проєктування програм. За результатами *SLR* узагальнене поняття вимог не визначено, тому використано підходи дослідження [1].

Шаблони, орієнтовані на предметну область (наприклад комбінація "*CQRS*-мікросервіси", "*DDD*-клієнт/сервер"), можуть бути корисними для архітекторів програмного забезпечення та підтримати їх у визначенні початкового набору шаблонів на основі подібності між доменами веб-додатків та спостережуваними доменами на основі досвіду інших архітекторів.

Запропонована аналітична модель апробована на виборі базового шаблону архітектури та тактик проєктування для систем класу превентивного обслуговування на прикладі шаблону *DDD,* який має високий рівень модифікації та інтероперабельності системи. Отримані аналітичні залежності відносної оцінки трудомісткості можна використовувати для вибору архітектурно-проєктних рішень.

При прийнятті архітектурних рішень необхідно враховувати вплив шаблонів на атрибути якості. Простір рішень, з якого архітектор вибрає проєкт, є достатньо великим, тому архітекторам програмного забезпечення потрібні інструменти підтримки прийняття рішень [2]. За результатами дослідження розроблено інформаційну систему (ІС) вибору архітектурних патернів за критеріями якості веб-додатків стандарту *ISO* 9125-1.

В інформаційній системі для оцінки шаблонів використовується аналітична модель вибору на основі мінімізації трудомісткості проєкту (демовікно ІС представлено на рис.1).

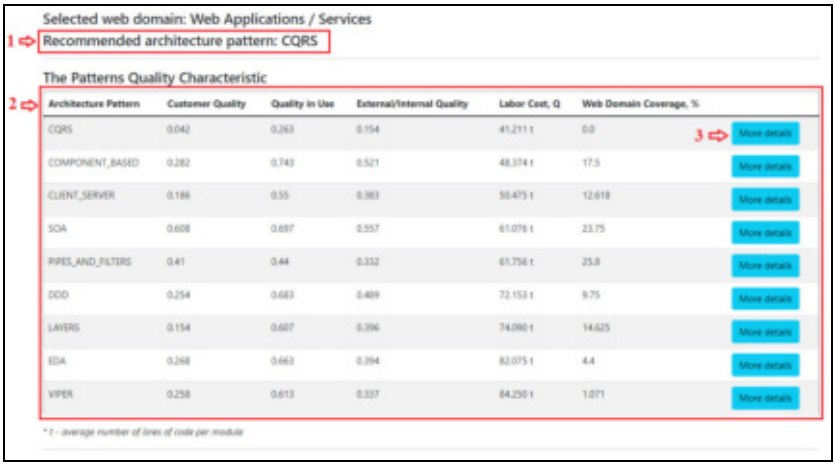


Рис. 1. Вікно ІС *«Architecture Pattern Analysis Information»*.

Програмний продукт *«Architecture Pattern Analysis Information»* дозволяє розробникам програмного забезпечення приймати архітектурно-проєктні рішення на основі відповідності архітектурного шаблону до вимог та критеріїв якості стандарту *ISO 9125-1.*

Результати досідження можна рекомендувати для розробки розширеної системи підтримки прийняття рішень архітекторів програмного забезпечення у пошуку та обгрунтуванні вибору комбінації шаблонів для створення програмної системи.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Харченко О.Г. Інструментальний засіб розробки та комунікацій вимог якості до програмних систем / О.Г. Харченко, В.В. Яцишин, І.Е. Райчев // Інженерія програмного забезпечення. 2010. №2. С.30-36.

2. Sabry A.E. Decision model for software architectural tactics selection based on quality attributes requirements / A.E. Sabry. Procedia Comput. Sci., 2015. Vol. 65. P. 422-431.

УДК 004.27;621.382

Ю.О. Гунченко, д.т.н.,
Л.Я. Мартинович
Одеський національний університет ім. І.Мечникова, Одеса

АЛГОРИТМ ПОБУДОВИ УНАРНИХ ТРІЙКОВИХ ФУНКЦІЙ

Трійкова логіка має ряд переваг порівняно з двійковою. Це такі, як природне представлення чисел зі знаком, коли не потрібно використовувати зворотній чи додатковий код або спеціальний знаковий біт; команда розгалуження по знаку в трійковій машині займає в два рази менше часу, ніж в двійковій; в тривходовому трійковому суматорі перенесення в наступний розряд виникає в 8 ситуаціях з 27, а в двійковому суматорі – в 4 з 8.

В двійковій логіці є всього 4 операції для одного аргумента, тобто унарних. У той же час в трійковій логіці їх 27. Наприклад, трійкова інверсія – унарна операція, яка міняє місцями два з трьох логічних станів: NOT– - інверсія, що міняє місцями 0 і +1; NOT - інверсія, що міняє місцями -1 і +1; NOT+ - міняє місцями -1 і 0.

Використовуючи універсальний пристрій, побудований на основі багатопорогового елемента багатозначної логіки [1], можна отримати усі 27 трійкових унарних операцій.

Таб. 1. Значення вихідних сигналів струмових перемикачів

Сума вхідних струмів	Вихідні сигнали струмових перемикачів			
terlev	СП1, СП2		СП3, СП4	
	$+R_1$	$+L_1$	$–R_1$	$–L_1$
–	0	+	–	0
0	+	0	–	0
+	+	0	0	–

Поєднуючи виходи СП1 – СП4 та константу, сформовану джерелом струму, можна отримати будь-яку трійкову унарну функцію. Реалізація трійкових унарних функцій здіснюється за допомогою наступного алгоритму:

1. Обираємо набір (№ в таблиці істинності) функції, який будемо реалізовувати першим: а) це не нульове значення («+» або «–»), якого в функції менше; б) кщо ненульових значень однакова кількість, то обираємо те, яке відповідає ненульовому вхідному аргументу («+» або «–»); в) кщо є і те, і інше, то обираємо будь-яке.

2. Обираємо RL-функцію, яка реалізує значення з п.1, незалежно

від отриманих значень при інших аргументах.

3. Обираємо набір (№ в таблиці істинності) функції, який будемо реалізовувати другим: а) це не нульове значення («+» або «–»); б) якщо два ненульових значення, то обираємо те, яке відповідає ненульовому вхідному аргументу («+» або «–»); в) інакше, обираємо те, що змінилось при виконанні п.2.

4. Обираємо RL-функцію (або її відсутність), яка реалізує значення з п.3 (можливо, їх буде дві, для компенсації дій функції з п.2). Якщо функція з п.4 змінює значення п.1: а) на нульове, то необхідно додати RL-функцію з п.2; б) інакше, необхідно додати RL-функцію з протилежним значенням у вибраному в п.1 номері функції з п.4.

5. Обираємо RL-функцію (або її відсутність), яка реалізує (або відповідним чином змінює) значення, що залишилось. Якщо функція з п.5 змінює значення п.1: а) на нульове, то необхідно додати RL-функцію з п.2; б)інакше, необхідно додати RL-функцію з протилежним значенням у вибраному в п.1 номері функції з п.5. Якщо функція з п.5 змінює значення п.3: а) на нульове, то необхідно додати RL-функцію з п.4; б) інакше, необхідно додати RL-функцію з протилежним значенням у вибраному в п.3 номері функції з п.5.

6. Оптимізація. Якщо в отриманому наборі функцій є такі, які в сумі дають константу («+1» чи «–1») на всіх наборах вхідних аргументів, то їх можна замінити на константу «+» або «–».

В результаті роботи методу, отримуємо таблицю, що демонструє, які виходи струмових перемикачів необхідно об’єднати та чи потрібно задіяти джерело струму, для того щоб синтезувати обрану функцію.

Висновок. В роботі запропоновано алгоритм побудови унарних трійкових функцій на основі універсального пристрою багатопорогового елемента багатозначної логіки. Даний алгоритм можна використовувати в якості основи для створення алгоритма побудови двомісних трійкових функцій

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Пат. UA 118735 Україна, МПК (2017.01) H03K19/00. Багатопорговий елемент багатозначної логіки / Гунченко Ю.О. Заявка 23.03.2017, опубл. 28.08.2017.

УДК 658.51.015

О.С. Гунько,
А.В. Антоненко, д.т.н.
Державний університет телекомунікацій, Київ

СИСТЕМА АВТОМАТИЗАЦІЇ SCADA

Автоматизація - це один з напрямків розвитку науки і техніки, який спрямований на використання систем управління, які не залучають людину до процесу або значно знижують рівень залучення та інтенсивність праці в роботі.

До основних переваг автоматизації можна віднести

- Збільшення обсягів виробництва та продуктивності
- Підвищення та передбачуваності якості
- Підвищення надійності

процесів і продукції

Ось кілька поширених застосувань автоматизації для підвищення продуктивності, якості та надійності. Основними недоліками автоматизації є наступні:

- Загрози безпеці
- Непередбачувані/надмірні витрати на розробку
- Високі витрати

SCADA (Supervisory Control and Data Acquisition - диспетчерський контроль і збір даних) - це програмний пакет, призначений для розробки систем, які збирають, обробляють, відображають і зберігають інформацію про об'єкти моніторингу та управління і працюють в режимі реального часу; системи управління, системи енергоменеджменту, системи моніторингу навколишнього середовища, наукові експерименти, автоматизація будівель тощо.

SCADA-системи мають багато переваг. В цілому, SCADA-системи допомагають оптимізувати виробництво і контролювати його відповідно до галузевих стандартів. Часто SCADA-системи також використовуються для усунення несправностей. Це пов'язано з тим, що технічне обслуговування стало важливим фактором забезпечення безперервного потоку виробництва без небажаних помилок.

Системи SCADA є життєво важливими для промислових організацій, оскільки вони допомагають підтримувати ефективність, обробляти дані для прийняття більш розумних

рішень, повідомляти про системні проблеми і скорочувати час простою.

Базова архітектура SCADA починається з програмованого логічного контролера (ПЛК) або віддаленого термінального пристрою (RTU). ПЛК і RTU - це мікрокомп'ютери, які взаємодіють з різними об'єктами, такими як заводське обладнання, HMI, датчики і кінцеві пристрої, і передають інформацію з цих об'єктів на комп'ютери, на яких запущено програмне забезпечення SCADA, розподіляють і відображають її, допомагаючи операторам та іншим співробітникам аналізувати дані і приймати важливі рішення.

Системи SCADA використовуються промисловими організаціями та державними і приватними компаніями для моніторингу та підтримки ефективності, розподілу даних для прийняття більш розумних рішень і повідомлення про проблеми системи для скорочення часу простою, оскільки системи SCADA можуть варіюватися від простих конфігурацій до великих і складних установок, вони можуть працювати в різних видах бізнесу, і системи SCADA є основою багатьох сучасних

- Енергетика
- Харчова промисловість
- Виробництво - нафта і газ, електроенергія
- Виробництво - транспорт
- Водопостачання - утилізація відходів
- Багато інших

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Learn all about SCADA systems: What is SCADA? | SCADApedia (scada-international.com)

2. What is SCADA? Supervisory Control and Data Acquisition (inductiveautomation.com)

3. What is SCADA System? - Basics of SCADA - InstrumentationTools

4. An Introduction to SCADA Systems - Technical Articles (allaboutcircuits.com).

УДК 658.51.014

О.С. Гунько,
А.В. Антоненко, д.т.н.
Державний університет телекомунікацій, Київ

МЕРЕЖЕВА БЕЗПЕКА. БРАНДМАУЕР НОВОГО ПОКОЛІННЯ

Коли потрібно захистити мережу, створюються брандмауери, щоб ускладнити зловмисникам доступ до внутрішньої мережі. Брандмауери можуть бути як апаратними, так і програмними. Використовуючи набір правил, брандмауер перевіряє та блокує трафік. Міжмережевий екран може сканувати як вхідний так і вихідний трафік.

У міру розвитку Інтернету їх потрібно було будувати з використанням нових методів безпеки для захисту мережі. Важливо відзначити це в моделі клієнт-сервер, яка є основною архітектурою сучасних обчислень. Мережевий захист, також відомий як брандмауер, можна включити в сучасний пристрій мережевої безпеки організації для включення політики безпеки та керування подіями (SIEM) і встановити на периметрі мережі організації для захисту від зовнішніх і внутрішніх загроз. Коли постачальник виявляє нову загрозу або виправлення, брандмауер оновлює набір правил для адресації постачальника. Основне призначення брандмауера – створити бар'єр між зовнішньою мережею та захищеною мережею. Брандмауер перевіряє всі пакети (фрагменти даних, призначені для передачі через Інтернет), які надходять або залишають захищену мережу. Після того, як інспектор завершить перевірку, брандмауер може відрізнити легітимні пакети від нелегітимних за допомогою попередньо встановленого списку правил. Ця пакетована форма інформації включає джерело, призначення та вміст. Вони можуть відрізнятися на кожному рівні мережі, як і правила. Брандмауери зчитують ці пакети та змінюють їх відповідно до правил, які вказують протоколу надсилати їх туди, куди вони повинні йти.

Брандмауер приймає лише вхідний трафік, на прийом якого він налаштований. Він розрізняє безпечний і зловмисний трафік і дозволяє або блокує певні пакети на основі попередньо визначених правил безпеки. Ці правила базуються на кількох аспектах, які вказують пакетні дані, наприклад джерело, адресат, вміст тощо.

Вони блокують трафік із підозрілих джерел, щоб запобігти кібератакам.

Існує декілька типів міжмережевих екранів залежно від методу фільтрації трафіку, структури та функцій: фільтрація пакетів, брандмауери з проксі-сервером, з перевіркою стану, брандмауери нового покоління.

Брандмауери наступного покоління - це брандмауери з глибокою перевіркою пакетів, які додають перевірку на рівні додатків, запобігання вторгненням та інформацію ззовні брандмауера, на додаток до перевірки та блокування портів/протоколів.

Цей брандмауер забезпечує розширене виявлення та усунення загроз. Співвідносячи мережеві події та кінцеві точки, можна виявити уникнення або підозрілу поведінку.

NGFW покращує фільтрацію пакетів і замість цього виконує глибоку перевірку пакетів (DPI). Подібно до фільтрації пакетів, DPI перевіряє кожен пакет на наявність IP-адрес джерела та призначення, портів джерела та призначення тощо. Вся ця інформація міститься в заголовках пакетів 3-го і 4-го рівнів.

NGFW блокує або дозволяє пакети в залежності від цільової програми; він робить це, аналізуючи трафік на 7-му рівні, рівні додатків. Традиційні брандмауери не мають такої можливості, оскільки вони аналізують трафік лише на рівнях 3 і 4.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/

2.https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall#:~:text=Firewalls%20prevent%20unauthorized%20access%20to,to%20secure%20a%20computer%20network

3. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

4. What is a next-generation firewall (NGFW)? | Cloudflare

УДК 004.94:518.5

Ю.Є. Добришин, к.т.н.,
С.М. Сидоренко
Національна академія Служби безпеки України, Київ

КЛАСИФІКАЦІЯ ДЕФЕКТІВ ПОШКОДЖЕНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ВНАСЛІДОК ВПЛИВУ КІБЕРАТАК

Задачею процесу дефектації пошкодженого програмного забезпечення, внаслідок впливу кібератак, є визначення дефектів, які потенційно можуть бути присутні у структурі програмного забезпечення. Рішення зазначеної задачі базується на необхідності встановлення основних типів дефектів, здійснення їхнього аналізу, в результаті чого створюються необхідні умови формалізації задачі дефектації.

Для досягнення мети необхідно розробити методику класифікації дефектів пошкодженого програмного забезпечення, формалізувати ознаки і основні поняття, що відносяться до дефектів, і в подальшому – запропонувати масиви технологічних кодів дефектів пошкодженого програмного забезпечення.

Питання класифікації дефектів пошкодженого програмного забезпечення розглядається багатьма авторами. Однак, існуючі системи класифікації недостатньо забезпечують можливість їх застосування для автоматизації процесу дефекації і потребують доопрацювання. Класифікація дефектів пошкодженого програмного забезпечення за певними ознаками, ускладнюється через вплив різноманітних факторів, які виникають внаслідок дії кібератак. Використання таких класифікаторів не забезпечує автоматизацію дефектації пошкодженого програмного забезпечення.

Авторами пропонується інша класифікація дефектів пошкодженого програмного забезпечення, в основу якої покладені зв’язки між пошкодженим програмним забезпеченням, можливими його дефектами та способами їх усунення.

Першим напрямком класифікації є визначення виду $\{v\}$ або характеру можливого дефекту. Наступним кроком класифікації є ділення дефектів по важливості $\{w\}$, наприклад основний і неосновний. Під основними розуміються дефекти, які обов’язково потребують перевірки. Відповідно, за їх наявності, програмне

забезпечення потребує відновлення. Неосновні дефекти дозволяють тимчасово використовувати пошкоджене програмне забезпечення.

Також, дефекти пошкодженого програмного забезпечення, можна класифікувати по їх значущості *{z}*. Наприклад, є дефекти, які не впливають на працездатність програмного забезпечення, а тому їх усунення необов'язкове. Існують дефекти, які усуваються шляхом незначного конфігурування програмного забезпечення. Якщо ж програмне забезпечення непрацездатне після пошкодження, дефекти усувати недоцільно. У цьому випадку необхідне переустановлення усього комплексу програмного забезпечення: системного, прикладного тощо.

Розробці заходів щодо усунення дефектів програмного забезпечення сприятиме і така ознака, як розподіл дефектів, виходячи з джерел їх виникнення *{d}*.

Знання причин появи дефектів дає можливість прогнозування необхідних заходів по усуненню кібератак та планування робіт щодо доопрацювання і використання засобів захисту програмного забезпечення.

На підставі викладеного та аналізу класифікаційних ознак дефектів пошкодженого програмного забезпечення розроблена структура технологічного коду дефекту, елементами якого є класифікаційні ознаки. $K_d = \{v, w, z, d\}$. Розроблений технологічний код є необхідним для автоматизації технологічного процесу дефектації пошкодженого програмного забезпечення, внаслідок впливу кібератак, а також вибору способів відновлення програмного забезпечення, автоматизації послідовності їх призначення та рішення інших питань щодо організації та технології захисту інформації у автоматизованих інформаційних системах та комплексах.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Литвиненко О. Є. Нечипорук О.П. Логіко-математичні методи діагностування складних систем: монографія. Київ: Артмедіа прінт, 2016. – 166 с.*

2. *Щербаков О.В. Луценко Є.С. Оцінка ефективності тестування програмного забезпечення на основі аналізу кількості та критичності знайдених дефектів. Системи обробки інформації. 2011. № 3. – С. 88 - 92.*

УДК 004.738 (043.2)

В.І. Дрововозов, к.т.н.,
Аль-Шаммарі Ахмед Аршед,
А.Б. Коцюр
Національний авіаційний університет, Київ

МЕТОДИКА МЕТАЕВРИСТИЧНОЇ ОПТИМІЗАЦІЇ КЛЮЧОВИХ ПАРАМЕТРІВ БЕЗПРОВОДОВИХ РАДІОМЕРЕЖ

Безпроводові мережі нових поколінь, призначені для підтримки різних видів трафіку, таких як голос, дані та мультимедіа, активно впроваджуються в сучасні складні та різнорідні інформаційно-комунікаційні системи. У цих мережах обмін даними між абонентами можна покращити завдяки високій якості зображень та відео, а доступ до інформації та послуг – за рахунок підвищення швидкості передачі даних, наскрізної якості сервісу (*End-to-End QoS*, *e2e QoS*) та зменшення рівня бітових помилок, заходів безпеки, урахування локації абонента, енергоефективності та новим гнучкими комунікаційним можливостям. Ці функції створюють нові можливості не тільки у виробничій та організаційній сферах, але і для постачальників контенту та послуг, що використовують ці мережі. Поставлені завдання розв’язуються за допомогою спеціальних модулів управління радіо ресурсами, адаптації та оптимізації на декількох рівнях стека протоколів моделі взаємодії відкритих систем (*Open System Interconnection Reference Model, OSI*).

Надання гарантій якості є важливою метою розробки безпроводових мереж. Різні методи можуть мати дуже різноманітні вимоги до якості щодо термінів передачі даних, міжкінцевої затримки та ймовірностей порушення, пов'язаних із затримкою. Наприклад, програми управління виробничим підприємством вимагають надійної та своєчасної доставки команд управління; отже, важливо гарантувати, що жоден пакет не втрачається чи затримується під час передачі пакету. Цей тип гарантій *QoS* зазвичай називають детермінованими або жорсткими гарантіями. З іншого боку, для більшості мультимедійних застосунків, включаючи відео телефонію, передачу мультимедіа та Інтернет-ігри, не потрібні такі суворі вимоги до якості *QoS*, тому що ці

застосунки мало чутливі до короткострокових порушень *QoS*. Цей тип гарантій *QoS* зазвичай називають статистичними або м'якими гарантіями.

Для безпроводових мереж, оскільки пропускна спроможність безпроводового каналу випадково змінюється з часом, спроба забезпечити детерміновану *QoS* (тобто з нульовою ймовірністю порушення *QoS*) призведе до надто консервативних гарантій. При цьому гарантована з імовірністю одиниця пропускна спроможність (без контролю потужності) дорівнює нулю.

Очевидно, що така консервативна гарантія недосяжна. За цими резонами в роботі розглядається статистична *QoS*. Для підтримки гарантій *QoS* запропоновано два загальні підходи.

Перший підхід – мережно-орієнтований. За таким підходом маршрутизатори, комутатори та центри збору даних у мережі повинні забезпечувати підтримку *QoS* для задоволення вимог щодо швидкості передачі даних, обмеженої затримки та втрати пакетів, що вимагаються програмними застосунками (наприклад, інтегровані сервіси або диференційовані послуги [1-3].

Другий підхід базується виключно на *End-to-End* (*E*2*E*) системі і не пред'являє жодних вимог до мережі. Зокрема, в *E*2*E* системах використовуються методи управління для досягнення максимальної якості на рівні застосунків без підтримки *QoS* на транспортному рівні. У цій роботі розглядається проблема забезпечення *QoS* з мережної точки зору. Для забезпечення гарантій *QoS* у безпроводових мережах архітектура мережі повинна містити такі компоненти: специфікація трафіку, маршрутизація *QoS*, контроль прийому викликів, характеристика безпроводових каналів, резервування ресурсів та планування пакетів. Схема мережі з архітектурною концепцією резервування *QoS* зображена на рис. 1.

Розподіл ресурсів зазвичай поєднується з контролем прийому запитів. Аналіз результатів пошуку маршруту на засадах *QoS* проводиться на маршруті, що складається з декількох транзитних ділянок і є оптимальним за критерієм мінімальної сумарної затримки. Розглянемо обґрунтування вибору методу оптимізації та результати роботи моделюючої програми.

Рис. 1. Мережна архітектура для резервування *QoS.*

Загальна мета процесу оптимізації полягає у визначенні маршруту з транзитними ділянками, що мають приблизно однакову пропускну спроможність із забезпеченням заявленої інформаційної цінності. Враховуючи співвідношення між функціями цінності інформації, суб'єктивними імовірностями та відповідними функціями корисності, введемо універсальну цільову функцію, вид якої визначається кількістю апріорної інформації про стан та параметри безпроводової мережі критичного застосування.

Розглянемо у якості одного з аргументів цільової функції надійність доставки даних r_d. Тоді компонент ультралінійної цільової функції $\Psi(r_d)$ матиме наступний вигляд:

$$\Psi(r_d) = \Psi\left[N_p, N_{lost}, \varepsilon, Route_i\right] = \Psi\left\{a\left[1-\left(\frac{N_p - N_{lost}}{N_p}\right)\right]^{\varepsilon}\left|\left(v_{pr}, Route_i\right)\right.\right\}; \quad (1)$$

$$0 \le \frac{N_p - N_{lost}}{N_p} \le 1, \ 1 \le \varepsilon \le 2,$$

де $Route_i$ – i-й маршрут доставки з M транзитними ділянками;

v_{pr} – кількість апріорної інформації про стан та параметри *i*-го маршруту. Без будь-якої втрати узагальненості можна вважати, що пропускні спроможності усіх ділянок мають один порядок, а в ідеалі є однаковими [1-3].

Строго кажучи, реальні аргументи цільової функції – затримка, надійність доставки та інші – приймають лише позитивні значення. Відповідно і цільова функція $\Psi(x_i)$ існуватиме лише у правому верхньому квадранті площини аргументів (x_i, ε), однак для розв'язку задачі оптимізації це не має принципового значення, оскільки при будь-яких величинах ε розглядається ультралінійна функція за модулем. Негативні значення аргументу на рис. 2 уведені лише для наочності представлення та спрощення алгоритмів стандартної задачі оптимізації стосовно конкретної проблеми, що розглядається у даному випадку.

Задача пошуку оптимального маршруту в мережі з *N* вузлами та M транзитними ділянками докладно розглянута у нашій роботі [2] стосовно оптимізації наскрізної якості сервісу для безпроводової мережі. У строгому математичному сенсі задача максимізації функції корисності для безпроводової мережі критичного застосування є класичною задачею про потоки в мережі як різновид квадратичних задач розміщення. Тому не будемо її докладно розглядати, послався на вичерпні результати згаданої роботи [2].

Використання наближених методів і алгоритмів є на даний момент фактично єдиним способом вирішення проблеми. За останні роки запропоновані різноманітні евристичні та метаевристичні методи [1-3] отримання наближеного рішення квадратичної задачі про призначення: табу-пошук, імітація відпалу, генетичні алгоритми тощо. Не вдаючись до докладного порівняльного аналізу евристичних методів, оберемо метод табу-пошуку, як один із найбільш успішних методів, що застосовуються для розв'язання таких задач. Для прискорення роботи алгоритму застосовують спеціальні технології, отримані вітчизняними вченими [1-3]. На цілій серії задач отримані результати, які не поступаються, а часто перевершують результати найбільш успішних алгоритмів, що застосовуються для розв'язання квадратичної задачі про призначення.

У роботі [1] розроблений алгоритм розв'язання квадратичної задачі про призначення, заснований на класичній схемі з локальним пошуком для поліпшення отриманих рішень. Для прискорення роботи алгоритму застосована технологія локальної оптимізації з апостеріорною корекцією. Там же даний докладний опис алгоритму та наведені асимптотичні оцінки точності отриманих рішень. Відмічено, що точність отриманого рішення залежить не тільки від точності завдання вихідних даних, але і від детальності їх подання. Може трапитися, що при зайвій деталізації статистичних характеристик мереж виникнуть додаткові локальні мінімуми цільової функції, що призведе до підвищення ризику зациклення на одному з них. Ці питання носять системний характер. Основною проблемою деталізації подання вихідних даних є ризик зациклювання на локальних екстремумах цільової функції. Для згладжування цих екстремумів використаний алгоритм локальної апостеріорної оптимізації, заснований на методі дуального управління Фельдбаума: результати, отримані на поточному та на попередніх кроках пошуку, використовуються в якості початкових даних на наступних кроках. На рис. 2 та 3 показані графіки зміни перетину цільової функції f_c при локальній апостеріорній оптимізації різного порядку.

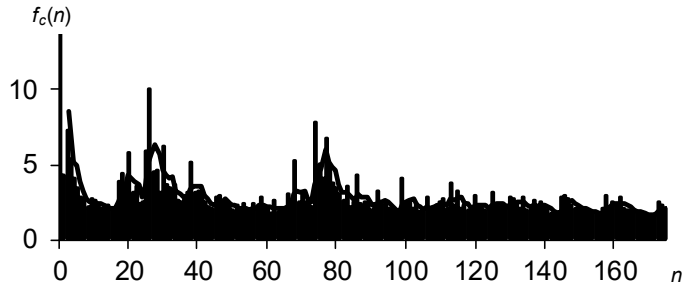


Рис. 2. Еволюція цільової функції без локальної апостеріорної корекції (лінійчатий графік) та з локальною апостеріорною корекцією по двох попередніх поточних даних.

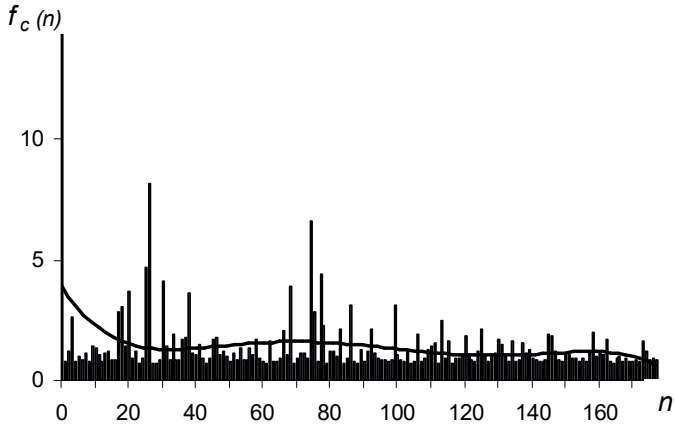


Рис. 3. Еволюція цільової функції без локальної апостеріорної корекції (лінійчатий графік) та з локальною апостеріорною корекцією по п'яти попередніх поточних даних.

Видно, що при накопиченні більшої кількості попередніх поточних даних локальні екстремуми згладжуються краще. Однак при цьому підвищується ризик пропуску глобального екстремуму.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Дрововозов В.І., Аль-Шаммарі Ахмед Аршед, Толстікова О.В., Водоп'янов С.В., Коцюр А.Б. Наскрізна якість сервісу безпроводових мереж з міжрівневою взаємодією. Проблеми інформатизації та управління. 2020. Вип. 63. С. 11–17.

2. Дрововозов В.І., Аль-Шаммарі Ахмед Аршед, Толстікова О.В. Оптимізація ключових характеристик безпроводових мереж з міжрівневою взаємодією. Проблеми інформатизації та управління. 2021. Вип. 67 (3). С. 16–27.

3. Gendereau M., Potvin J.-I. Handbook of Metaheuristic, 3rd ed. – Springer International Publishing AG, 2019. – 604 p.

УДК 004.738 (043.2)

В.І. Дрововозов, к.т.н.,
С.В. Водоп'янов, к.т.н.,
О.В. Толстікова, к.т.н.
Національний авіаційний університет, Київ

ЗАХИЩЕНІСТЬ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ У МЕРЕЖАХ ТРАНСПОРТНИХ ЗАСОБІВ

У результаті аналізу методів організації та забезпечення якості обслуговування в перспективних інформаційно-комунікаційних та комп'ютерних мережах критичного застосування виявлено, що основним проблемами для мереж є різнорідність мережного трафіку та перевантаження, які погіршують показники QoS. Запобігання перевантаженню реалізується шляхом побудови багаторівневої ієрархічної структури, але методи узгодження протоколів взаємодії автономних мережних сегментів потребують вдосконалення. Це у повній мірі відноситься і до інформаційно-телекомунікаційних систем залізничного транспорту [1].

Інформаційно-телекомунікаційні системи залізничного транспорту є гетерогенними за визначенням. В окремих сегментах комп'ютерних та телекомунікаційних систем залізниці обмін даними здійснюється через кабельні мережі.

Мережі залізничних станцій також мають змішану структуру з поєднанням проводового та безпроводового доступу. Вибір того чи іншого типу доступу обумовлюється міркуваннями пропускної спроможності, надійності та зручності встановлення з'єднань.

Безпроводовий сегмент посідає важливе місце в загальній структурі інформаційно-телекомунікаційних систем транспорту, зокрема, залізничного транспорту.

Окрім загальних проблем управління інформаційно-телекомунікаційними мережами, у безпроводових мережах досить гостро стоять проблеми захисту від несанкціонованих втручань та зовнішніх завад самого різного походження.

Безпроводова інформаційно-телекомунікаційну система (БП ІТС) залізничного транспорту. По суті, вона, як і інформаційно-телекомунікаційні системи повітряного транспорту, представляє собою систему критичного застосування, тобто систему, до якої пред'являються жорсткі вимоги стосовно швидкості опрацювання штатних та екстремальних ситуацій, захищеності від

несанкціонованих втручань та інших ключових параметрів ефективності.

Система критичного застосування (СКЗ) також лежать в основі організаційного управління авіаційним транспортом. Відмітимо тільки, що принциповою відмінністю авіаційного транспорту є те, що зовнішній обмін з іншими абонентами, що знаходяться як на землі, так і у повітрі, здійснюється виключно по безпроводовим каналам зв'язку. Не вдаючись до відмінностей авіаційного, залізничного та автомобільного транспорту, є загальні проблеми забезпечення їх глобальної ефективності.

Слід відмітити, що відбувається поступове нарощування апаратно-програмних засобів аж до створення апаратно-програмних комплексів, що виконують задані функції. Ця особливість СКЗ вимагає, щоб контроль ефективності також був безперервним.

Відмічені особливості інформаційних систем дозволяють сформулювати наступні рекомендації по проектуванню систем контролю та управління СКЗ.

1. Контроль представляє собою комплекс взаємозв'язаних заходів, які супроводжують процес створення системи від етапу проектування до здачі в експлуатацію.

На різних етапах створення СКЗ відкидаються або приймаються зразки комплектуючих елементів, варіанти структури системи, способи резервування, контролю і інші технічні рішення для досягнення головної мети – забезпечити на завершальному етапі створення системи необхідну ефективність.

2. Випробуванням на ефективність слід піддавати об'єкти, заздалегідь перевірені на функціонування. Ефективність авіаційних, залізничних та автотранспортних СКЗ – це властивість найкращої застосовності у критичних режимах.

3. До складу системи контролю включають різноманітні види і способи випробувань, що відповідають особливостям виробництва випробовуваних об'єктів.

4. Система контролю СКЗ за часом його проведення включає наступні основні етапи:

а) контроль апаратури і її елементів з метою отримання інформації про ефективність ключових елементів системи: власне

транспортних засобів, залізничних, повітряних та наземних автомобільних трас, диспетчерських систем тощо;

б) контроль апаратно-програмних комплексів та інформаційних систем в цілому;

в) уточнення оцінки ефективності системи за наслідками підконтрольної експлуатації системи і її частин у нештатних режимах.

5. Найдоцільнішим рішенням проблеми оцінки ефективності СКЗ в цілому є розрахунково-експериментальні методи, тобто поєднання натурних випробувань, розрахунків та імітаційного моделювання. У подальшому отримані оцінки підтверджуються, уточнюються або скасовуються на основі результатів випробувань достатньо репрезентативного об'єму.

6. Кожна СКЗ вимагає розробки своєї методики випробувань, що відображає її особливості, масштаб, область застосування.

Важливою проблемою є забезпечення захищеності ключових елементів, зокрема, інформаційно-комунікаційних та комп'ютерних мереж від несанкціонованого доступу.

Відповідно, і при загальному виборі конкретного мережного комутаційного, термінального і лінійно-кабельного обладнання необхідно враховувати безліч організаційних, технічних і економічних факторів.

У першу чергу, треба локалізувати та ізолювати протоколи обміну даними у сегментах мереж закритого, обмеженого та загального доступу. По суті, сучасні мережі, включаючи Інтернет, базуються на досить обмеженому списку ідей [2]:

– пакетний принцип передання даних та управління;

– адаптація довжини пакету до умов передачі (фрагментація/дефрагментація);

– інкапсуляція пакетів при переході від нижніх рівнів моделі *OSI* на верхні рівні та декапсуляція пакетів при переході від верхніх рівнів на нижні рівні;

– динамічна маршрутизація.

Із-за обмеженості об'єму даної роботи (детальне викладення методу наведене у роботі [2]) наведемо основні результати досліджень:

– для захисту мережних сегментів із закритим доступом від несанкціонованого проникнення (хакерської атаки на мережу,

перехоплення управління транспортним засобом) розроблено методи ізоляції протоколів закритого доступу від протоколів обмеженого та відкритого (загального) доступу;

– n статистичних показників повідомлень, зокрема, кількість вхідних та вихідних *IP, TCP, UDP* пакетів на інтервалі спостереження, час отримання та відправлення пакетів та ін., описуються n -мірною щільністю імовірності;

– щільності імовірності статистичних показників повідомлень у мережах закритого, обмеженого та відкритого доступу є параметрично несумісними, а відповідні коефіцієнти взаємної кореляції є величинами другого порядку малості;

– сукупності сигнатурних показників повідомлень у закритому доступі, у обмеженому доступі, у відкритому доступі та сигнатури атак представляють собою компоненти векторів, майже ортогональних одне одному, а їх векторні добутки – величини другого порядку малості;

– за результатами статистичного та сигнатурного аналізу фільтруються спроби як випадкового, так і навмисного несанкціонованого втручання до сегментів з закритим та обмеженим доступом [3].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Горбенко А.В. Методи та інструментальні засоби розробки комп'ютерних мереж інформаційно-управляючих систем критичного застосування. Автореферат. Канд. техн. наук. – Харків: Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут", 2004. – 20 с.

2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. - Pearson Education, Inc., Old Tappan, New Jersey, 2016. – 538 p.

3. Водоп'янов С.В. Методи побудови автономних комп'ютерних сегментів аеровузлової мережі. – Дис. канд. техн. наук. - К.: НАУ, 2018. – 164 с.

УДК 004.738.5(043.2)

О.В. Дубчак,
О.О. Левченко,
І.А. Кравчук
Національний авіаційний університет, Київ

АНАЛІЗ УРАЗЛИВОСТЕЙ ВЕББРАУЗЕРА

У 2022 р., за даними Державного центру кіберзахисту, зареєстровано перевишення кількості кіберінцидентів майже у три рази відносно 2021 р. Питання безпеки користувачів мережі Інтернет, що напряму залежить від програмного забезпечення, використовуваного для доступу до вебсайтів та їхнього перегляду – веббраузерів (ВБ), залишається пріоритетним, оскільки саме кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла у 18,3 та 2,2 рази відповідн [1].

Як відомо [2], ВБ є своєрідними «воротами», що надають доступ до мережі Інтернет, отже безпека ВБ є важливим критерієм захисту даних користувача від несанкціонованого доступу.

Станом на березень 2023 р., за даними StatCounter, найпоширенішим у світі ВБ є Google Chrome (64,8%), на другому місці Apple Safari (19,5%), далі - Edge (4,63%), Mozilla Firefox (2,93%), Samsung Internet (2, 57%) та Opera (2.33%). В Україні найпопулярнішим стабільно залишається Google Chrome (понад 66%), далі - Opera (12,97%), Safari (9,41%), Firefox — 4,48% та Samsung Internet — 1,78% [3].

Майже третина всіх ВБ містить критичні вразливості: Microsoft Internet Explorer і Edge – понад 40%;Google Chrome – майже 40%; Mozilla Firefox – 35%; Opera – 34%; Safari - майже 30%, відповідно до звіту дослідників Інтернет-безпеки щодо стану сучасних ВБ [4].

Причому, серед вразливостей ВБ найбільший відсоток припадає на ті, що спрямовані на отримання даних.

Користувачу важливо розуміти функціональність та можливості використовуваного ВБ - увімкнення за вмовчання деяких функцій ВБ може не тільки полегшити роботу, але й знизити рівень безпеки.

Серед конкретних особлививостей ВБ та пов'язаних з ними ризиків наявні наступні вразливості: ActiveX – технологія, що використовується Microsoft Internet Explorer у системах Microsoft

Windows; вразливості Java - успішні атаки вразливості можуть призвести до несанкціонованого доступу для читання даних, доступних для Java SE; вразливості JavaScript/VBScript – зловмисники можуть додавати значну кількість функцій та інтерактивності до вебсторінки; вебвідстеження – використовується для запам'ятовування і розпізнавання відвідувачів вебсайту.

Слід зауважити, що техніка вебвідстеження (ВВ) достатньо швидко розвивається останнім часом: І-е покоління приймає встановлені сервером ідентифікатори (файли cookie та evercookie); ІІ-ге покоління - відбиток браузера, ідентифікує пристрій на основі його унікальних конфігурацій (часовий пояс, системні шрифти, модулі до ВБ та їхні версії, журнал відвідувань, розширення екрану).

З одного боку, за допомогою ВВ можлива автентифікація користувачів, з іншого - ВВ може використовуватися для надання персоналізованих послуг. Причому, за умови, що надана послуга є небажаною, наприклад, небажана цільова реклама, таке ВВ становитиме порушення конфіденційності [5].

Отже, технологія ВВ багато в чому небезпечніше інших уразливостей ВБ, оскільки є підґрунтям загрози порушення конфіденційності даних користувача. Слід також зазначити, що захист від ВВ може бути проблематичним, оскільки неможливо дізнатися щодо наявності відслідковування дій користувача.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Звіт Державного центру кіберзахисту. [Електронний ресурс] - Режим доступу: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

2. What is a web browser? [Електронний ресурс]– Режим доступу: https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/

3. Статистичний звіт StatCounter [Електронний ресурс] - Режим доступу: https://gs.statcounter.com/browser-market-share/desktop-tablet-console/worldwide

4. Internet browser vulnerability and user security [Електронний ресурс] - Режим доступу:https://augustafreepress.com/news/internet-browser-vulnerability-and-user-security/

Yinzhi Cao. (Cross-)Browser Fingerprinting via OS and Hardware Level Features [Електронний ресурс]– Режим доступу: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf

УДК 004.738.5(043.2)

О.В. Дубчак,
О.О. Левченко,
Я.С. Мазур
Національний авіаційний університет, Київ

ЗАСОБИ ПРОТИДІЇ ВЕБВІДСТЕЖЕННЮ

Відповідно до результатів дослідження за 2022 р. приблизно 78% громадян України користуються послугами мережі Інтернет щоденно, а 82% - щотижнево [1]. Як відомо, у 2022 р. кількість подій інформаційної безпеки в категоріях «Шкідливий програмний код» та «Збір інформації зловмисником» зросла відповідно у 18,3 та 2,2 рази відносно показників попереднього періоду [2]. Загроза порушення конфіденційності має бути основним важелем обачливості користувачів під час відвідування глобальної мережі, оскільки необхідне програмне забезпечення містить веббраузери, однією із уразливостей яких є вебвідстеження.

Технологія вебвідстеження - відбиток браузера (ВБ), що є глобальним ідентифікатором, який робить його власника більш впізнаним на часто відвідуваних інтернет - ресурсах, багато в чому небезпечніше інших уразливостей веббраузерів. ВБ фіксує отриману ресурсом від браузера цілісну картину та ідентифікує користувача, навіть за умови внесення змін до налаштувань браузера. Пристрій позначається унікальною цифровою міткою у вигляді хеш-суми, знятої з налаштувань браузера. У результаті створюється база міток для ідентифікації користувачів, з якою під час наступного відвідування інтернет - ресурсу проводиться порівняння ВБ пристрою. За умови збігу відбувається однозначна ідентифікація [3].

Гарантовано дієві засоби захисту від зчитування ВБ наразі не розроблені, однак є способи, застосування яких дозволяє зменшити унікальність веббраузера: зміна налаштувань браузера; браузер Firefox з модифікованими налаштуваннями [4]; спеціалізовані розширення для браузера (Chameleon – модифікація значень User-Agent [5]; Canvasblocker – захист від збору цифрових відбитків з Canvas [6]; Canvas Defender – приблизно аналогічно Canvasblocker;[7] User-Agent Switcher – приблизно аналогічно Chameleon;[8] використовувати одночасно краще одне розширення); вимкнення Flash; вимкнення JavaScript; використання

Firefox із файлом user.js від ghacks; браузер Brave; Tor браузер без Tor Network; використання віртуальної машини; використання окремих пристроїв/браузерів [4].

У результаті проведеного аналізу заходів щодо зменшення унікальності веббраузера, одним з найоптимальніших визначено застосування спеціалізованих розширень, що дозволяють надати: різноманітність вибору; можливість налаштувати захист від ВБ на власний розсуд; зручний і зрозумілий інтерфейс (майже не потрібно стикатися з налаштуваннями безпосередньо браузера); можливість застосування до будь-якого браузера. Слід зазначити, спеціалізовані розширення часом можуть і не виправдати очікувань [4]. Також слід зауважити, що всі розширення захищають лише від одного параметру ВБ (для Chameleon і User-Agent Switcher - це User-Agent, а для Canvasblocker та Canvas Defender – відбиток Canvas) [5-8].

Висновок: найкраще рішення протидії ВБ-поєднання захисту від різних варіантів зчитування ВБ в одному розширенні (наприклад, захист від відбитка Canvas, WebGL, звукового відбитка, відстеження роздільної здатності екрану та апаратного відстеження).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Дослідження КМІС. [Електронний ресурс] - Режим доступу: https://www.ukrinform.ua/rubric-technology/3497671-blizko-78-ukrainciv-sodna-koristuutsa-internetom.html]*
2. *Звіт Державного центру кіберзахисту. [Електронний ресурс] - Режим доступу: https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit*
3. *Savannah Copland The Top Browser Fingerprinting Techniques Explained/ [Електронний ресурс] - Режим доступу: https://fingerprint.com/blog/browser-fingerprinting-techniques/*
4. *Septimiu-Vlad Mocan. Browser Fingerprinting and You (What It Is, How It Works, How It Violates Your Privacy, and What You Can Do) [Електронний ресурс. – Режим доступу: https://www.technadu.com/browser-fingerprinting/102454/*
5. *Chameleon [Електронний ресурс]– Режим доступу: https://github.com/sereneblue/chameleon.*
6. *CanvasBlocker [Електронний ресурс] – Режим доступу: https://github.com/kkapsner/CanvasBlocker*
7. *Canvas Defender [Електронний ресурс] /. – Режим доступу: https://addons.mozilla.org/uk/firefox/addon/no-canvas-fingerprinting/.*
8. *User-Agent Switcher [Електронний ресурс] – Режим доступу: https://addons.mozilla.org/en-US/firefox/addon/uaswitcher/?src=gitlab*

УДК 004.047(043.Я)

В.М. Єфимець, к.т.н.,
Д.М. Маршалок
Національний авіаційний університет, Київ

УЧБОВИЙ КОМП'ЮТЕРНИЙ КЛАСТЕР

В роботі досліджується учбовий комп'ютерний для вивчення дисципліни бакалаврського рівня.

Об'єднання процесорів в кластері є локальним, а між кластерами – глобальним. Для кластера актуальними є мінімізація міжкластерних обмінів. Формальне розв'язання цієї проблеми можливо звести до пошуку мінімального розрізу графа задачі G. Останній ділиться на шматки G_i, що відповідають підзадачам.

Для пошуку мінімального розрізу графа використовують послідовний алгоритм [1].

Приклад. Маємо граф задачі G, необхідно розрізати граф на l шматків.

Графу G відповідає квадратна матриця суміжності D, елементи якої визначаються так:

$$d_y = \begin{cases} m, \text{якщо вершина } a_i, a_j \text{-суміжні}, \\ 0, \text{якщо вершина } a_i, a_j \text{-несуміжні}. \end{cases}$$

Критерієм розрізу графа G є мінімальна кількість ребер U між шматками G_i. Підграф у шматку має максимальну кількість ребер. Деякі вершини графа G можуть попередньо бути закріпленими за шматками G_i.

Дві вершини графа називають суміжними, якщо існує ребро, що їх з'єднує. Число ребер, що інцидентні вершині a_i називають локальною ступінню $\delta(a_i)$ цієї вершини.

Послідовність кроків розрізання графа G:

1. Нехай перший шматок $G_1 = \{A_1, U_1\}$ починається з вершини a_ε.

2. Для визначення другої вершини шматка G_1 виділимо суміжні вершини a_ε в множині Γa_ε.

3. Визначимо відносні ваги $h(a_i) = \delta(a_i) - d_i$, що входять у множину Γa_ε. $\delta(a_i)$ – «локальний ступінь» вершини a_i. d_i – число

дуг, що з'єднують вершину a_i з вершинами графа G.

Процес продовжується до тих пір поки в G_1 не буде визначено задане число вершин.

Шматок G_1 відділяється з графа G, після чого виконується формування графа G_2. Першим його елементом буде вершина $a_\sigma \in Q$.

Структура учбового кластера $G_1 - G_3$ показана на рис.1. Кластер об'єднує процесори $П_1 - П_4$, які ототожнюються з підзадачами a_i.

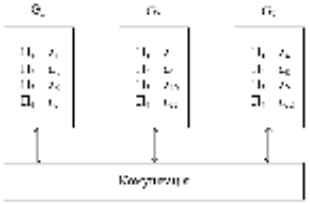


Рис.1. Кластерна КС.

Взаємозв'язки кластерів в комп'ютерній системі можуть бути подібними до зв'язків процесорів у кластері.

Розробка структури учбового кластера складається із послідовності кроків:

- на основі графа задачі G та матриці суміжності D формується граф G' – варіант завдання;
- визначаються шматки $G_1, G_2, ...$ та будується мінімальний розріз графа G' з урахуванням наявних або відсутніх заборонних вершин;
- з урахуванням топології кластера, числа та розмірів шматків $G_1, G_2, ...$ розробляється структура комп'ютерного кластера;
- для контролю відповідності мінімального розрізу графа задачі отриманого в домашньому завданні – розроблений додаток «Розрізання графу».

В досліджені використаний приклад задачі із роботи [1].

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Комп'ютерні системи. Лабораторний практикум для спеціальності 123 «Комп'ютерна інженерія». Київ, 2017. – 52 с.

УДК 004.056.53 (043.3)

І.А. Жуков, д.т.н.,
С.В. Балакін, к.т.н
Національний авіаційний Університет, Київ

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ АПАРАТНОЇ ТА ПРОГРАМНОЇ БЕЗПЕКИ АВІАЦІЙНИХ СИСТЕМ

Авіаційні системи є критично важливою інфраструктурою і потребують високого рівня безпеки для захисту від потенційних загроз. Безпека апаратного та програмного забезпечення є важливими компонентами забезпечення безпеки та надійності авіаційних систем [1].

Апаратна безпека стосується фізичного захисту пристроїв, які складають авіаційну систему. Сюди входять сервери, маршрутизатори, комутатори та інше обладнання, яке використовується для управління та експлуатації системи. Ось деякі з основних проблем апаратної безпеки в авіаційних системах:

1. Фізична безпека. Системи часто розташовані у віддалених районах, що робить їх уразливими до пошкодження.

2. Атаки на ланцюги поставок: авіаційні системи покладаються на мережу постачальників, що робить їх уразливими до атак на ланцюги поставок.

3. Відсутність видимості: у багатьох випадках апаратне забезпечення безпеки в авіаційних системах не видно, що ускладнює виявлення потенційних загроз або атак. Відсутність видимості ускладнює впровадження та підтримку належних заходів безпеки.

5. Залежність від сторонніх компонентів. Авіаційні системи часто покладаються на сторонні компоненти, такі як сервери, маршрутизатори та комутатори, які можуть мати вразливості або бекдори.

Безпека програмного забезпечення, з іншого боку, стосується захисту програмного забезпечення та систем, які керують авіаційною системою. Важливі аспекти безпеки програмного забезпечення в авіації:

1. Практики безпечного кодування: авіаційне програмне забезпечення має бути розроблено та розроблено з використанням методів безпечного кодування. Це означає дотримання встановлених інструкцій і стандартів безпеки, таких як OWASP

Top 10, а також виявлення та усунення потенційних вразливостей безпеки під час процесу розробки.

2. Шифрування: шифрування використовується для захисту конфіденційних даних, які передаються через мережу, наприклад інформації про літаки та пасажирів. Шифрування гарантує безпеку даних і відсутність доступу для неавторизованих користувачів.

3. Виявлення та запобігання вторгненням: системи виявлення та запобігання вторгненням використовуються для виявлення та блокування несанкціонованого доступу до авіаційної системи. Ці системи відстежують мережевий трафік і можуть ідентифікувати потенційні загрози та атаки, допомагаючи запобігти порушенням безпеки [2].

4. Регулярні оновлення програмного забезпечення: регулярні оновлення програмного забезпечення та виправлення мають вирішальне значення для усунення вразливостей системи безпеки та забезпечення того, щоб система оновлювалася з найновішими протоколами безпеки.

5. Тестування безпеки: Регулярне тестування безпеки має важливе значення для виявлення вразливостей і слабких місць в авіаційній системі.

Безпека апаратного забезпечення є важливою для захисту фізичних компонентів від потенційних атак або вразливостей, тоді як безпека програмного забезпечення має вирішальне значення для захисту компонентів програмного забезпечення від потенційних атак або вразливостей. Особливості безпеки апаратного та програмного забезпечення в авіаційних системах включають заходи фізичної безпеки, резервування, шифрування, моніторинг, методи безпечного кодування, регулярні оновлення, тестування та аудит, контроль доступу та плани реагування на інциденти.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Farivarnejad, H., Rahimi, F., & Hashemi, M. (2019). A review of aviation cyber security issues and the role of the human factor in enhancing aviation cyber security. Safety Science, 120, 327-338.

2. Zhukov I. A., Balakin S.V. Detection of computer attacks using outliner. Науковий журнал «Молодий вчений». К.: 2016. № 9(36). С. 91-93.

УДК 629.056.6:043.2

Н.В. Журавель,
Б.І. Долінце

Національний авіаційний університет, Київ

ПІДВИЩЕННЯ ТОЧНОСТІ НАВІГАЦІЙНОГО СИГНАЛУ ЗА ДОПОМОГОЮ ФІЛЬТРУ КАЛМАНА

Існує велика кількість систем та алгоритмів фільтрації та корекції сигналів навігаційних засобів для отримання навігаційних даних вищої точності.

Більшість цих систем застосовують аналіз та використання надлишкової інформації, коли отримується один тип інформації з кількох різних джерел. Далі ця інформація проходить через схему корекції чи фільтрації і системи безпілотних літальних апаратів отримують сигнал необхідної точності.

Найпростішими та досить ефективними є системи із коректорами, які дозволяють знизити необхідну обчислювальну потужність, та через свою простоту побудову мають високу надійність.

Алгоритм неперервного оптимального фільтра Калмана об‘єднує розв’язання двох задач: спостереження та фільтрації [1].

Фільтр Калмана – це математичний алгоритм, який використовується для оцінки стану системи, коли система піддається невизначеності [2]. Алгоритм використовує серію вимірювань протягом певного часу, щоб оцінити стан системи, і він особливо корисний, коли система піддається впливу шуму або інших джерел невизначеності.

Він часто використовується в системах керування, де він використовується для оцінки стану системи та прийняття керуючих рішень на основі цієї оцінки [3].

По суті, фільтр Калмана працює за допомогою математичної моделі системи для прогнозування стану системи на основі попередніх вимірювань [4]. Потім прогнозований стан порівнюється з фактичним вимірюванням, а різниця між ними використовується для оновлення оцінки стану системи. Цей процес

повторюється з часом, причому оцінка стає точнішою, оскільки проводиться більше вимірювань [5].

Загалом, фільтр Калмана є потужним інструментом для оцінки стану системи, що піддається невизначеності, і він знайшов численні застосування в різних областях.

Таким чином роботу кожного кроку фільтра Калмана можна розділити на два етапи: прогноз і корегування. Етап прогнозу обчислює вектор стану, за його ж значенню на попередньому кроці роботи фільтра. На етапі коригування в алгоритм надходять дані поточних вимірювань, які використовуються для уточнення прогнозного значення вектора стану, і обчислення власне оцінки вектора стану динамічної системи.

Найбільш перспективним і високоточним є використання фільтру Калмана. Він дозволяє отримати найвищу точність навігаційного сигналу, але має особливості застосування і вимагає значних обчислювальних потужностей.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Vasyliev V., Dolintse B. Integration of Inertial and Satellite Navigation Systems with using Corrective Circuits and Filtering // Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), 2016 IEEE International Conference, 13-15 Oct. 2016, IEEE Conference Publications: 2016, pp. 275-278.

2. Single Simon, D. (2006). Optimal State Estimation: Kalman, H-infinity, and Nonlinear Approaches. John Wiley & Sons. ISBN: 978-0-471-70857-2.

3. Haykin, S. (2008). Kalman Filtering and Neural Networks. John Wiley & Sons. ISBN: 978-0-470-25388-3.

4. Särkkä, S. (2013). Bayesian Filtering and Smoothing. Cambridge University Press. ISBN: 978-0-521-76564-8.

5. Dolints B.I. Investigation of characteristics of an inertial-satellite navigation system with correctors in dynamic operating modes // Flight. Modern problems of science: XIII International. scientific practice. conf. students and young scientists, April 3-4, 2013: theses add. - K., 2013. - P. 123.

УДК 531.7

В.М. Ільченко, к.т.н.,
В.П. Квасніков, д.т.н.
Національний авіаційний університет, Київ

МЕТОД ВИМІРЮВАННЯ ГЕОМЕТРИЧНИХ РОЗМІРІВ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ ОПТИЧНИХ СИСТЕМ

Тенденція підвищення якості виробів, їх мікромініатюризація вимагає створення безконтактних засобів розмірного контролю із все більш високими технічними характеристиками. Використання оптичного випромінювання в інформаційних системах підвищує їх швидкодію, що дозволяє розв'язувати метрологічні задачі надзвичайно високої складності.

Основними вимогами до приладів розмірного контролю є висока точність, швидкодія, можливість контролю параметрів із складною просторовою поверхнею, а також надійність, гнучкість і сумісність з автоматизованими системами керування гнучких виробничих систем.

Інтелектуалізація в побудові робототехнічних вимірювальних комплексів пов'язана перш за все із створенням бази даних та бази знань для роботи експертної системи та отриманні вимірювальної інформації в реальному масштабі часу для гнучких виробничих систем.

У класі оптико-електронних вимірювальних пристроїв найбільш широку сферу застосування мають модульні пристрої, що складаються з набору універсальних вимірювальних та керуючих модулів. Це дозволяє в короткий термін створювати нові контрольно-вимірювальні пристрої під конкретну задачу гнучких виробничих систем з підвищенними метрологічними характеристиками.

Вимірювальний оптичний комплекс включає в себе оптичну систему, електромеханічний блок, електронний блок, оптико-електронну головку.

Оптичний метод дозволяє проводити тривимірний контроль геометричних розмірів, профілів та координат.

Одним з таких засобів є оптичні системи з відповідними високоточними давачами, створений на основі триангуляційного методу вимірювання.

Системи складаються з 4 базових модулів: оптико-механічного

модуля, електронного блоку, комп'ютера та спеціалізованого програмного забезпечення.

Час одного вимірювання висоти профілю незначний і становить 0,001-0,01 с. Така висока швидкодія систем, не потребує контакту з вимірюваною поверхнею, дозволяє робити вимірювання в ході руху без зупинок і забезпечити високу продуктивність вимірювань безпосередньо в ході технологічного процесу.

Цікавим є використання цифрової методики, яка дозволяє процес перетворення в цифрову форму здійснювати всередині оптичної головки. Основною перевагою методу є можливість використання субдискретизації, яка переводить процес вимірювання в область низьких частот. Ще однією перевагою субдискретизації є можливість уникнення використання високої частоти квантування. Згідно теореми Шеннона перетворення сигналу в цифрову форму вимагає частоти квантування по часу вдвічі більшої ниж ширина полоси частот сигналу.

З метою зниження похибки вимірювань була досліджена ефективність різних алгоритмів обробки вихідних сигналів оптичних давачів шляхом чисельного моделювання, а також в умовах їхньої реальної роботи з технічними поверхнями. Встановлено, що серед традиційних алгоритмів обробки найбільш оптимальним по точності і швидкодії є медіанний алгоритм, що забезпечує зменшення похибки в 2,5 рази.

Інформаційна оптико-електронна система включає в себе апаратно-програмний комплекс безконтактних вимірювань фактичних параметрів досліджуваних об’єктів зі спеціальним програмно-математичним забезпеченням і дозволяє здійснювати обробку результатів вимірювань в реальному масштабі часу, зберігання та передачу даних по комп’ютерній мережі автоматизованої системи керування підприємства.

УДК 004.45

О.Р. Іщук,
Н.А. Христинець, к.т.н.
Луцький національний технічний університет, Луцьк

СИСТЕМНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ДАНИХ В ОС WINDOWS

Резервне копіювання – це важлива процедура, яка дозволяє зберегти копію важливих даних у випадку їх втрати або пошкодження. ОС Windows має вбудовані засоби резервного копіювання, які дозволяють користувачам створювати резервні копії файлів та папок.

Для забезпечення максимальної захищеності даних, рекомендується використовувати додаткове програмне забезпечення для резервного копіювання, яке забезпечить більш гнучкі та розширені можливості. Перед створенням резервної копії, користувач повинен визначити, які дані необхідно зберегти, які джерела даних будуть включені та де буде зберігатися копія. Після створення резервної копії, рекомендується перевірити її на наявність помилок та забезпечити її безпечне зберігання. У наведеному фрагменті програмного скрипта з рисунку 1, організовано резервне копіювання у зазначену дату та час, що може бути ефективним у разі планування роботи з певною групою завдань.

```
if not exist D:\ exit
if not exist %bp% mkdir %bp%
@if exist %bp% echo Y|del %bp%

set folP=%date:~-4%.%date:~3,2%.%date:~0,2%_%time:~0,2%-%time:~3,2%-%time:~6,2%
"C:\Program Files\WinRAR\Rar.exe" a -r %bp%\%folP%.rar %sp%\*.*
```

Рис.1. Фрагмент програми резервного копіювання даних

Регулярне створення резервних копій - це важлива процедура, яка забезпечує збереження важливих даних в разі їх втрати або пошкодження. Використання хмарних сервісів для зберігання резервних копій є досить популярним способом забезпечення безпеки даних.

При використанні додаткового програмного забезпечення для резервного копіювання, рекомендується забезпечити його сумісність з ОС Windows та виконати його.

Опції резервного копіювання можуть відрізнятися залежно від версії ОС Windows, але в основному вони дозволяють зберігати дані на локальних дисках, зовнішніх пристроях, мережевих пристроях та хмарних сервісах.

Для резервного копіювання системи, можна використовувати засіб «Резервна копія та відновлення» у Панелі керування, який дозволяє зберігати образ всієї системи та налаштування.

Для відновлення даних з резервної копії, користувач повинен відкрити засіб резервного копіювання та вибрати пункт відновлення файлів. У разі втрати даних, резервна копія може бути останньою надією на їх відновлення, тому рекомендується виконувати резервне копіювання регулярно та забезпечити безпечне зберігання копій.

Для більшої ефективності та автоматизації процесу резервного копіювання, можна використовувати планувальник завдань, щоб регулярно створювати копії в задані часи.

Після виконання резервного копіювання, рекомендується перевірити відновлені файли та забезпечити їх правильне функціонування.

Отож, можна зробити висновки, що надійне резервне копіювання даних – це ключ до безпеки та надійності важливих даних, тому варто приділяти цьому питанню достатньо уваги та ресурсів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Що таке резервне копіювання даних, як його здійснювати, і де краще зберігати інформацію? [Електронний ресурс] // Урядовий кур'єр. – 2022. – Режим доступу до ресурсу: https://ukurier.gov.ua/uk/news/sho-take-rezervne-kopiyuvannya-danih-yak-jogo-zdij

2. Системне програмне забезпечення: навчальний посібник з дисципліни «Системне програмне забезпечення» для студентів базового напряму 6.050102 «Комп'ютерна інженерія»/ Укл.: І.В. Мороз, Л.О. Березко, О.Ю. Бочкарьов. – Львів: Видавництво Національного університету «Львівська політехніка», 2014. – 162 с.

УДК 004.451.44

А.В.Калюжняк
Запорізький національний університет, Запоріжжя

АЛЬТЕРНАТИВИ «МАРШИРУЮЧИХ КУБІВ» ДЛЯ ПОБУДОВИ ГЕОМЕТРИЧНИХ ОБ'ЄКТІВ

Проблема візуалізації поверхонь, які задані різними способами виникає у багатьох предметах математики, фізики, медицини, телебачення. На даний час одним із популярних методів зображення геометричних об'єктів, являється застосування алгоритмів з використанням апроксимації на трикутники, тобто тріангуляції. Під задачею розбиття на трикутники розуміється зображення поверхні заданої за допомогою функції трьох аргументів і фіксованого значення цієї функції – рівня. Розглядаючи методи рішення задач тріангуляції, необхідно виділити коміркові методи[1].

Алгоритм «Маршируючих кубів» являється комірковим методом візуалізації ізоповерхней в об'ємних даних. Основна задача реалізації полягає в тому, що ми можемо визначити воксель за значеннями пікселів у восьми кутах куба. Якщо один або кілька пікселів куба мають значення, менші за вказане користувачем ізозначення, а один або кілька мають значення, вищі за це значення, ми знаємо, що воксель повинен вносити певний компонент ізоповерхні. Визначивши, які грані куба перетинає ізоповерхня, ми можемо створити трикутні ділянки, які ділять куб між областями всередині ізоповерхні та областями поза нею. З'єднавши патчі з усіх кубів на межі ізоповерхні, ми отримаємо зображення поверхні. Даний алгоритм успішно застосовується для зображення геометричних об'єктів із використанням неявних функцій. Також існують інші коміркові методи побудови геометричних об'єктів такі як: метод Скелі, метод «Канейро» та «MT6».

Алгоритм Скелі, розроблений для побудови трьохмірних скалярних полів, заданих за допомогою функцій, визначених у кожній точці простору. Однак метод розбиття простору на комірки дає можливість використовувати цей алгоритм для зображення скалярних полів заданих на регулярній сітці.

Робота алгоритму Канейро, заснована на розбитті простору на трикутні піраміди, як і алгоритм «Маршируючі куби», він складається з двох етапів:

1. Розбиття простору на кінцеву множину комірок, пошук комірок, що перетинаються шуканою поверхнею.
2. Апроксимація поверхні у знайдених комірках.

Для порівняння методів можна використати порівняння за наступними критеріями:

1. Визначення кількості трикутників, що генеруються;
2. «якість» трикутників, що генеруються.

Незважаючи на можливе існування топологічної неточності в поверхні, яка генерується, алгоритм «Маршируючих кубів» широко використовується на практиці, так як ймовірність прояву помилок такого роду досить мала.

Наприклад, при візуалізації тестових поверхонь топологічна неточність жодного разу не виявилася. Алгоритм «MT6» запропонований як альтернативний алгоритм «Канейро»[2]. Основна відмінність цих двох методів в тому, що для алгоритму «MT6» відпадає необхідність зміни шаблонів прямо на дзеркальному і навпаки. Це досягається шляхом симетричного розбиття паралелепіпеда.

Далі проводиться тріангуляція поверхні в кожній комірці окремо. Причому кожна комірка розбивається на трикутники одним із заданих раніше способів, тобто значення координат для трикутників просто «підставляються» із заздалегідь заданої таблиці (Рис.1).

Для даних методів потрібно задати допустиму помилку застосування апроксимації, на основі якої обрати розмір комірки – трикутної піраміди.

При цій процедурі триангуляції комірки проводиться аналіз значення кожної функції у вершинах цієї комірки – тобто, визначається, які вершини знаходяться «всередині» поверхні, а які – «зовні». Отже, можна зробити висновок про достатність визначення функцій тільки у вершинах комірок [3].

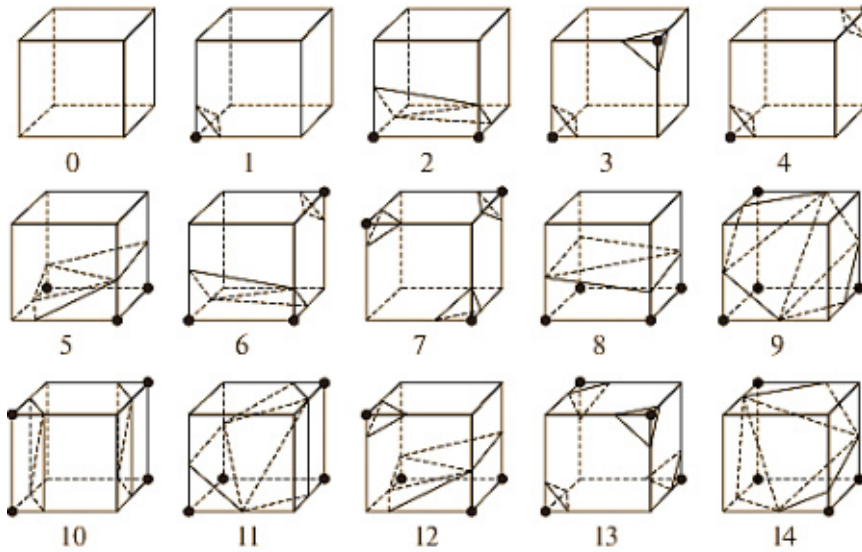


Рис. 1. Розбиття на поверхні.

Таким чином, при вирішенні прикладних завдань пов'язаних із візуалізацією геометричних об'єктів, краще всього використовувати алгоритм «Маршируючих кубів» у тому випадку, якщо важлива топологічна точність одержуваної поверхні. У протилежному випадку, можливе використання алгоритму «Канейро».

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Gong, F., Zhao, X.: Three-dimensional reconstruction of medical image based on improved marching cubes algorithm. In: 2010 International Conference on Machine Vision and Human-Machine Interface (MVHI), pp. 608–611. IEEE (2010)*

2. *Yang, X.D., Liu, B.H., Wang, Y.: Triangular surface reconstruction of CT images by using isosurface construction. In: 6th International Conference on e-Engineering and Digital Enterprise Technology, pp. 503–507 (2008)*

3. *Kai, Z., Lingzhong, F., HaiFang, L.: 3D reconstruction of brain atlas based on modified marching cubes algorithm. J. Comput. Appl. Softw. 33(4), 177–182 (2016).*

УДК 004.855.5

С.А. Качанов
Харківський національний університет ім. В.Каразіна, Харків

КЛАСТЕРИЗАЦІЯ І КЛАСИФІКАЦІЯ ЧАСОВИХ РЯДІВ

У сучасному світі обсяги даних постійно збільшуються, що потребує використання нових методів та підходів до їх аналізу. Часові ряди є важливим типом даних, який описує динаміку певних явищ в часі. Однак, аналіз часових рядів може бути складним завданням через їх високу динамічність та складні взаємозв'язки між даними.

Кластеризація і класифікація часових рядів є актуальними напрямками досліджень у багатьох галузях, таких як фінанси, медицина, промисловість, соціальні мережі, трейдинг тощо. Кластеризація та класифікація є важливими завданнями аналізу часових рядів, оскільки дозволяють групувати подібні ряди та класифікувати їх за певними критеріями.

Існує багато методів для кластеризації та класифкації часових рядів. У цій роботі зроблено короткий огляд найпопулярніших і найефективніших, за різними оцінками, з них.

Метод головних компонент (PCA) використовується для зменшення кількості змінних у даних шляхом перетворення даних на нові, які є лінійними комбінаціями початкових змінних. Він може бути використаний для кластеризації часових рядів за допомогою розрахунку власних векторів та значень, що відповідають найбільш значимим змінним.

Також досить популярним методом є стандартний кластерний аналіз. Кластерний аналіз використовується для групування часових рядів за схожістю. Метод кластерного аналізу використовується для визначення кількох кластерів, кожен з яких складається з часових рядів, які схожі між собою. Можуть бути використані різні метрики подібності, такі як Евклідова відстань, косинусна відстань, Мангеттенська відстань та інші.

Для аналізу та прогнозу часових рядів часто використовуються методи машинного навчання. Одним з найбільш ефективних методів є використання рекурентних нейронних мереж, зокрема, довго-короткочасної пам'яті (LSTM).

Нейромережа LSTM є спеціальним типом рекурентних нейронних мереж, який може ефективно працювати з даними, які мають довготривалу залежність. Це робить його досить ефективним для аналізу та передбачення часових рядів.

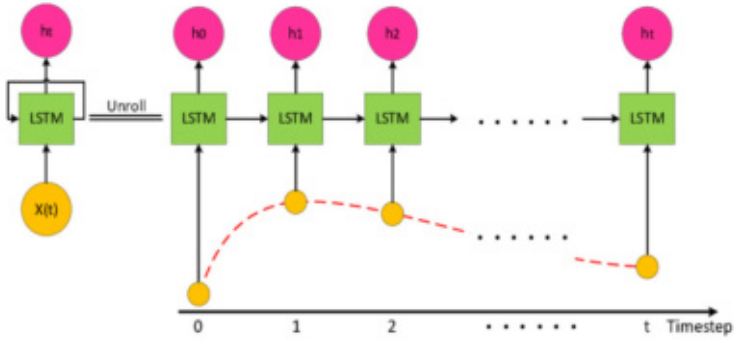


Рис.1. Схема використання LSTM при аналізі часових рядів

У LSTM мережі кожен нейрон має внутрішні стани, які зберігають інформацію з попередніх часових кроків. Це дозволяє мережі зберігати інформацію про довготривалу залежність між даними в часі. При використанні LSTM для аналізу часових рядів дані спочатку розбиваються на послідовності, що містять фіксовану кількість кроків. Кожна послідовність використовується для тренування мережі, яка використовується для передбачення наступних значень у часовому ряді.

Проведений порівняльний аналіз методів кластеризації і класифікації часових рядів показав, що універсальних методів не існує, кожен має свої переваги і недоліки, тому для конкретного набору даних необхідно використовувати різні підходи, методи та моделі машинного навчання.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. How to Develop LSTM Models for Time Series Forecasting [Електронний ресурс] – Режим доступу: www/ URL: https://machinelearningmastery.com/how-to-develop-lstm-models-for-time-seriesforecasting/ – Загол. з екрану

УДК 796.11.3:658

Н.О. Коваленко, к.пед.н.
Льотна академія Національного авіаційного університету, Кропивницький

ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ АРМ МЕНЕДЖЕРА В УПРАВЛІННЯ АЕРОПОРТОВИМ КОМПЛЕКСОМ

Для підвищення якості обслуговування споживачів послуг повітряного транспорту авіакомпаніям і особливо аеропортам необхідно постійно впроваджувати в організаційний процес забезпечення авіаперевезень передові інформаційні системи і технології.

Інформаційна система є складовою частиною виробництва і технології виконуваних робіт, фундаментом організації аеропортової діяльності, у тому числі обслуговування пасажирів. Відомо, що новітні системи автоматизованого управління ресурсами і пропускною спроможністю аеропорту базуються на інформаційних технологіях та автоматизації процесу управління.

Впровадження АРМ Забезпечення управління якістю послуг аеропортів – сукупність організаційних та економічних параметрів і показників, що забезпечують ефективне управління якістю послуг шляхом сучасної організації обслуговування пасажирів, реєстрації білетів, комп'ютерної технології проведення досмотру пасажирів, а також митного контролю; результатом чого є забезпечення розвитку технічної оснащеності процесу надання послуг, підвищення рівня якості, досягнення регулювання та зниження витрат, підвищення економічної ефективності від запроваджених заходів [1].

Одним із сучасних елементів автоматизації робочого місця менеджерів аеропортового комплексу та вдосконалення їх діяльності є впровадження BPMS-системи.

BPM АРМ програмне забезпечення аеропортового комплексу (англ. Business Process Management, управління бізнес-процесами) – концепція автоматизованого процесного управління аеропортовим комплексом, що розглядає управлінські процеси як особливі ресурси аеропорту, що безперервно адаптуються до постійних змін, і покладається на такі принципи, як зрозумілість і видимість бізнес-процесів в організації рахунок моделювання управлінських процесів з використанням формальних нотацій,

використання програмного забезпечення моделювання, симуляції, моніторингу та аналізу управлінських процесів, можливість динамічного перебудови моделей бізнес-процесів силами менеджерів та засобами програмних систем [2].

Вдосконалення АРМ менеджера та його управлінської діяльності за рахунок впровадження BPM-програмного забезпечення дозволить підвищити ефективність роботи аеропортового комплексу, збільшити прибутковість діяльності шляхом оптимізації та контролю.

Слід зазначити, що (BPM) має високий рівень впровадження серед регіональних, та аеропортів хабів, як метод управління, спрямований на досягнення основних переваг автоматизації, таких як економічна ефективність, швидший час виходу на ринок і покращене обслуговування клієнтів.

BPM – це сучасна цифрова система з кількох модулів, які дозволяють керувати робочими процесами компанії, контролюючи кожен із них і зменшуючи вплив людського чинника, шляхом впровадження АРМ управлінського персоналу різних рівнів [3]. BPM для АРМ можуть бути тиражованими або унікальними (замовними), створеними для окремого підрозділу аеропорту. Це визначає структуру продукту. Тиражовані BPM до певної міри універсальні та доступні, а замовні, вирізняються просунутою архітектурою.

Найчастіше у аеропортових комплексах для АРМ менеджерів замовляють індивідуальну розробку, тому що це дозволяє зробити інструмент для бізнесу під специфічні завдання, він обходиться дорожче, але його ефективність у рази вища за стандартні рішення, оскільки враховує специфіку діяльності та особливі потреби замовника.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Laudon K., Laudon J. Management Information Systems: Managing the Digital Firm. 9th ed. Prentice Hall, 2021. P.211.

2. Інститут автоматизованих технологій на повітряному транспорті [Електронний ресурс]. Режим доступу : http:www.iatvt.ru. Останній доступ: 2023.

3. Global Aviation Safety Roadmap. ICAO, 2023. 23 p.

УДК 681.12

[1]Є.В. Красовська, к.т.н.,
[2] О.Д. Красовський
[1]ВСП «Фаховий коледж інженерії, управління та землевпорядкування НАУ», Київ
[2]Національний авіаційний університет, Київ

СИСТЕМА ОХОРОННОЇ СИГНАЛІЗАЦІЇ З GSM КОМУНІКАТОРОМ

Захист приміщення – завдання, яке вирішується, за допомогою сучасних засобів, а саме охоронної сигналізації. Системи, що використовують GSM-зв'язок, дозволяють здійснити охорону будь-яких об'єктів, в тому числі і нетелефонізованих. Для організації GSM-сигналізації використовуються технічні засоби охорони: приймально-контрольний прилад, GSM-модуль, сповіщувачі, виконавчі пристрої, додаткове обладнання.

В якості сповіщувачів використовуються: охоронні сповіщувачі, датчики руху, пожежні сповіщувачі, сповіщувачі іншого призначення. Сповіщувачі можуть бути: світлові, звукові, комбіновані, мовні. Додаткове обладнання: зчитувач електронних ключів Touch Memory, безконтактних карт Proximity, кодонаборна панель, тривожна кнопка.

Структурна схема системи безпеки з GSM комунікатором (рис. 1) складається з: ІЧ/лазерного детектора, ІЧ датчика наближення, блоку виявлення вторгнень, мікроконтролера, панелі управління користувача, блоку живлення, GSM модему.

Рис. 1. Структурна схема системи безпеки з GSM комунікатором.

Коли система підключається до джерела живлення (рис. 2), вона переходить в режим очікування. Однак, коли клеми роз'єму J2

замкнуті, попередньо запрограмоване попередження автоматично передається на відповідний мобільний номер. Можна підключити будь-який блок виявлення вторгнення до вхідного гнізда J2. Активний низький рівень (L) на вивід 1 роз'єму J2 запускає систему безпеки.

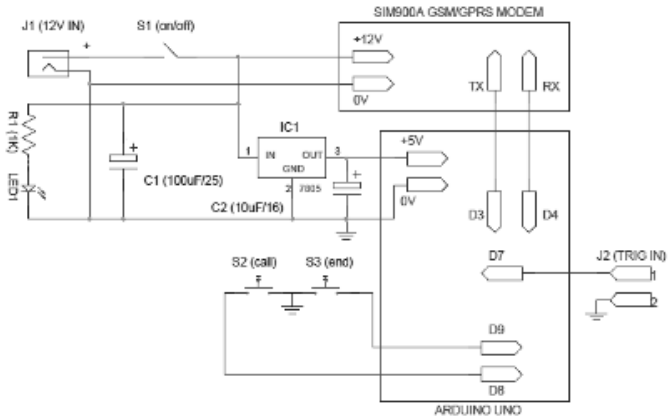


Рис. 2. Принципова схема системи безпеки з GSM комунікатором.

Для реалізації системи охоронної сигналізації з GSM комунікатором необхідні наступні компоненти: Arduino Uno, плата розширення GPRS і GSM для Arduino, ІЧ-датчик, пасивний звуковий модуль для Arduino, сирена-клаксон 12В, блок живлення 12В, пасивний звуковий модуль для Arduino, електронна 16-кнопкова клавіатура для Arduino.

Методами підвищення надійності оповіщення може бути: використання декількох SIM – карт: при неможливості відправити повідомлення з однієї карти, комунікатор перемкнеться на резервну; використання додаткових каналів передачі інформації: проводової телефонної лінії, TCP/IP-мереж.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Види охоронної сигналізації та принцип роботи системи [Електронний ресурс]. – Режим доступу: URL http://www.klaster-plus.ua/ua/stati-i-obzory/vidy-okhrannoi-signalizacii-i-princip-ikh-raboty/

УДК 004.9

Д.П. Кучеров, д.т.н.
Національний авіаційний університет, Київ

ІНТЕЛЕКТУАЛЬНА ТЕХНОЛОГІЯ УПРАВЛІННЯ БОРТОВИМ АВІАЦІЙНИМ КОМПЛЕКСОМ

Інформаційна технологія створення бортових інформаційних систем (ІС) передбачає умови організації обчислювального комплексу і формалізації знань про динаміку взаємодії літака із зовнішнім середовищем. Задачі аналізу і інтерпретації при функціонуванні бортових ІС визначають концепцію розробки інтелектуальних систем, заснованих на знаннях, безперервна зміна і удосконалення яких відбувається у процесі їх експлуатації. Особливості цих завдань складається в такому:

- аналіз альтернатив, прогноз розвитку ситуацій і прийняття рішень відбувається на основі даних динамічних вимірювань, математичних моделей і структурованої бази знань. Для забезпечення надійності оцінки ситуації і відпрацювання обґрунтованих рішень враховуються: реальна структура вітрового поля; особливості динаміки літака в ситуації, що розглядається;
- алгоритм і програмне забезпечення реалізується з врахуванням функціонування системи в режимі реального часу, враховуючи допустимий час реакції. Оцінка і прогноз динамічних характеристик літака основані на ефективному поєднанні традиційних методів аналізу поведінки літака в умовах тряски із нейромережевими алгоритмами перетворення вимірювальної інформації в умовах неповноти і невизначеності даних;
- база знань ІС в максимальному ступені пристосована до сприйняття фактичної інформації про поведінку літака на трясці при неперервній зміні динаміки об’єкта і зовнішнього середовища. Інтерпретація складних процесів і явищ, що визначають поведінку літака в умовах тряски, здійснюється на основі принципів оброблення інформації в мультипроцесорному обчислювальному середовищі. Динамічна модель бази знань працює спільно з графічним інтерфейсом, що забезпечує наочне відображення процесу розвитку ситуації, індикацію зовнішніх впливів і оперативної зміни сигналів управління на основі когнітивної парадигми.

Таким чином, моделі і об'єкти управління, що використовуються в бортових ІС нового покоління являють собою клас динамічних систем, стан яких неперервно змінюються в часі. Особливості поведінки літака у неперервному середовищі, що змінюється, визначають різні підходи, що поєднують традиційні методи і моделі аналізу і прогнозу динамічних ситуацій з новим математичним апаратом, що включає штучні нейронні мережі і генетичні алгоритми.

Концептуальні основи створення бортових ІС базуються на теоретичних принципах, що визначають архітектуру системи і рівні її управління. За основу прийняття рішень використовуються знання висококваліфікованих фахівців-експертів в предметній області, що розглядається, і увесь необхідних арсенал методів і засобів аналізу і інтерпретації знань. Поряд з традиційними математичними методами тут широко застосовуються досягнення штучного інтелекту і нові принципи функціонування ІС реального часу. Серед них важна роль належить принципу відкритості, що дозволяє забезпечити найбільш складні рівні ієрархічної структури системи – самоорганізацію і самонавчання. Використання цих принципів дозволяє ІС розуміти складні процеси взаємодії динамічного об'єкта із зовнішнім середовищем, моделювати власні дії, навчатися на власному досвіді.

Проблеми синтезу складних систем визначаються кардинальними змінами цілей поведінки систем і складається в безпосередньому врахуванні природних властивостей нелінійних об'єктів в процедурах синтезу, а також формуванні механізмів генерації зворотних зв'язків. Такий підхід дозволяє більш жорстко підходити до рішення проблеми аналітичного синтезу системи підтримки прийняття рішень щодо забезпечення безпеки літака в складних ситуаціях.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Protsenko O., Savchenko T., Myronenko M., Prikhodchenko O. Informational and extreme machine learning for onboard recognition system of ground objects. IEEE 11th Intern. Conf. on Dependable Systems, Services and Technologies (DESSERT). – 2020. Kyiv, Ukraine, P. 213-218.

УДК 004.75

І.О. Ліпко,
В.О. Капілевич
Центр воєнно-стратегічних досліджень Національного університету оборони України ім. І.Черняховського, Київ

АКТУАЛЬНІ ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ВЗАЄМОСУМІСНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ СКЛАДОВИХ СИЛ ОБОРОНИ УКРАЇНИ

Низкою стратегічних документів держави з оборонного планування визначені завдання щодо вирішення проблемних питань із реалізації воєнної політики України, а саме: досягнення взаємосумісності сил оборони з відповідними структурами держав – членів НАТО.

Так, відповідно до положень [1] в силах оборони України повинна бути розгорнута об'єднана мережа оборони, обмін інформацією в якій здійснюється відповідно до технічних та процедурних принципів та рівнів взаємосумісності НАТО.

Рядом концептуальних [2] документів Міноборони України визначено, що досягнення взаємосумісності з державами – членами НАТО забезпечується запровадженням у силах оборони України положень ініціативи НАТО FMN (Federated Mission Networking, Об'єднана мережа для проведення операцій).

Координація робіт із запровадження у силах оборони України ініціативи НАТО FMN здійснюється у рамках Трастового фонду НАТО з удосконалення системи командування, управління, зв'язку та обміну інформацією.

Вирішення технічних та процедурних питань взаємосумісності інформаційних систем досягається шляхом запровадження положень, які визначені у так званих "спіралях" FMN. Кожна "спіраль" являє собою визначений набір сервісів, які повинні бути взаємосумісними та реалізовані протягом 4 років.

У свою чергу, взаємосумісність інформації досягається шляхом використання об'єднаної моделі даних. В НАТО така модель розроблена у рамках Багатосторонньої програми взаємосумісності (Multi-Laterial Interoperability Program, MIP). З 01 липня 2022 року Керівною Радою MIP прийнято рішення щодо надання Україні статусу її асоційованого члена [5].

Досягнення взаємосумісності інформаційних систем складових

сил оборони передбачає вирішення наступного комплексу завдань:

адаптація положень документів (вимог, інструкцій тощо) ініціативи НАТО FMN в силах оборони України шляхом розробки відповідних військових публікацій та стандартів тощо;

розроблення, взаємосумісної із моделлю JC3IEDM, моделі даних сил оборони в якості основи для інформаційного обміну між інформаційними системами складових сил оборони та аналогічними системами держав – членів НАТО та їх партнерів;

проведення комп'ютерних навчань із визначення рівнів взаємосумісності інформаційних систем із подальшою участю у міжнародних навчаннях як під керівництвом НАТО, так і в двосторонніх навчаннях тощо.

Виконання другого завдання є найбільш ресурснозатратним що потребує залучення до розробки самої моделі як цивільних висококваліфікованих фахівців, так й подальших кроків із модернізації існуючих інформаційних систем.

Авторами визначено особливості взаємосумісності інформаційних систем і мереж за рахунок проведеного загального аналізу мереже-центричного та дата-центричного підходів (окреслених положеннями ініціативи НАТО FMN), які необхідно враховувати для досягнення взаємосумісності між партнерами у середовищі НАТО, а також серед складових сил оборони України, державних установ та некомерційних організацій.

В умовах воєнного стану, потреба мати інформаційну перевагу над ворогом набуває важливого значення для сил оборони України. Тому, щоб приймати ефективні рішення швидше ніж ворог, інформаційний обмін між партнерами національного та міжнародного рівнів стає пріоритетним напрямком. Виникла необхідність об'єднання на інформаційному рівні різнорідних систем та мереж, не пов'язаних між собою. Обумовлені можливістю ведення спільних операцій, держави-партнери НАТО розпочали розвиток спроможностей для набуття взаємосумісності між ізольованими та відокремленими елементами інформаційної інфраструктури оборонного призначення. Це призвело до появи мереже-центричного, а згодом і дата-центричного підходів, націлених на формування цілісної та пов'язаної між собою інфраструктури у єдине інформаційне середовище.

Практичне використання мереже-центричного підходу в

державах-членах НАТО пов'язано з можливістю вести інформаційний обмін між системами та мережами в середовищі НАТО завдяки наявності спільних мов обміну, які однозначно визначають (конкретизують) інформацію. Таку спільну мову визначає модель даних обміну інформацією, практичним прикладом використання якої є Модель Joint C3 (Command, Control, Communications) Information Exchange Data Model.

Використання вказаної моделі визначається Угодою зі стандартизації НАТО STANAG 5525, яка у Міністерстві оборони України запроваджена у якості військового стандарту.

Завдання із досягнення взаємосумісності інформаційних систем передбачає семантичну сумісність на основі загальної моделі даних обміну інформацією та механізму обміну даними із системами та мережами партнерів. В свою чергу, це охоплює велику кількість вимог до обміну інформацією (Information Exchange Requirements), які висуваються до окремих елементів інформаційної інфраструктури. Об'єднання таких вимог в модель даних надає змогу спільно використовувати загальні елементи даних.

Під семантичною сумісністю треба розуміти можливість інформаційних систем та мереж вести обмін інформацією, інтерпретуючи її одержувачу так само за змістом як і передбачав передавач. Однак для спільних та узгоджених дій, потрібно не тільки мати технічну можливість вести обмін такої інформації та інтерпретувати її спільною мовою, але й знати загальні процеси, що описують спільні та узгоджені дії між партнерами. Розуміння таких процесів передбачає використання об'єднаної моделі даних і формує технічні вимоги до механізмів обміну між системами та мережами партнерів. У зв'язку з тим, що при появі нових таких вимог, вони повинні бути враховані в оновленій моделі даних, стає важко підтримувати узгодженість сутностей та зв'язків між ними, відображену в описовій документації, а сама модель часто збільшується, що призводить до складності її розуміння, і як наслідок, до затримки в її впровадження.

Разом з тим, в положеннях ініціативи НАТО FMN йдеться про використання дата-центричного підходу, за допомогою якого фокус зміщується на важливість самих даних, які несуть більшу цінність та важливість ніж програмне забезпечення.

При такому підході інформаційну інфраструктуру потрібно

створювати навколо загальнодоступного сховища даних з фізичним або логічним доступом до нього.

На відміну від сховищ даних попереднього покоління, де дані використовувались в основному для загального статистичного аналізу, а метадані не враховувались взагалі, друге покоління сховищ даних вже відрізняється можливістю проведення динамічного аналізу даних. Це забезпечує баланс продуктивності навантаження та логічний доступ до даних, безперервно користуючись метаданими, які додатково описують (деталізують) фізично-збережені дані. Перспектива росту кількості даних та подальша обробка великих масивів даних, їх динамічне оновлення (зміна) свідчить про актуальність використання дата-центричного підходу при побудові інформаційної інфраструктури в інтересах сил оборони України.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 17.09.2021 № 473.

2. Концепція розвитку IT-інфраструктури Міністерства оборони України та Збройних Сил України, затверджена Міністром України 03.11.2021.

3. "Україна стала асоційованим членом програми технологічного співробітництва збройних сил країн НАТО", - Олексій Резніков [Електронний ресурс]. – Режим доступу: https://www.mil.gov.ua/news/2022/07/12/ukraina-stala-asoczijovanim-chlenom-programi-tehnologichnogo-spivrobitnicztva-zbrojnih-sil-krain-nato-oleksij-reznikov/.

4. Lasschuyt, Eddie, et al. How to make an effective information exchange data model or the good and bad aspects of the NATO JC3IEDM. TNO PHYSICS AND ELECTRONICS LAB HAGUE (NETHERLANDS), 2004.

5. Кірпічніков, Ю., et al. "Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб." Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського (2022): 68-75.

УДК 004.056.53

Ю.В.Лукаш
Національний авіаційний університет, Київ

ВИКОРИСТАННЯ НЕЙРОННОЇ МЕРЕЖІ РОЗПІЗНАВАННЯ ОБРАЗІВ ДЛЯ ПОБУДОВИ АСИСТЕНТУ ДЛЯ ВОДІЯ (ADAS) В СУЧАСНОМУ АВТОТРАНСПОРТІ

На сьогодні великого поширення набуває розвиток штучного інтелекту, нейромереж та їх практичне використання в різних сферах нашого життя. Зокрема такі системи активно створюються для забезпечення безпеки дорожнього руку, наприклад відслідковування порушень правил дорожнього руху, також для реалізації вдосконаленої системи допомоги водію (ADAS) в сучасних автомобілях і навіть для побудови автопілота.

ADAS включає в себе широкий набір різних помічників, які можуть використовувати цілий ряд апаратних засобів. Для автомобілів це зачасту – набір різних відео-камер, радари, лідари.

В рамках моєї роботи було обрано розглянути функцію попередження водія від аварії з іншими перешкодами. Такими перешкодами було визначено – легкові автомобілі, вантажні автомобілі, автобуси та пішоходи, які можуть переходити дорогу. Перелік цих категорій використано для побудови дата-сету з розміченими даними, на яких в подальшому проводилося навчання нейронної мережі.

Для класифікації і розпізнавання образів я обрав Deep Neural Network (dnn) OpenCV та зокрема модель YOLO, котру додатково навчав на створеному дата-сеті. Ця модель була обрана через те, що вона дає хороше співвідношення по якості виявлення об’єктів та швидкодії їх виявлення. Це співвідношення є надзвичайно важливим, тому що система повинна працювати в реальному часті з одним або кількома потоками відео і опрацьовувати якомога більшу кількість кадрів, в ідеалі всі кадри.

Для навчання було підготовлено, розмічено та використано дата-сет, який налічує 600 унікальних зображень, що містять шукані об’єкти для розпізнавання.

Аналіз параметрів моделі, яка стала результатом навчання на власному дата-сеті показав 41 mAP при швидкодії 87 FPS.

Такі показники є досить конкурентними порівняно з іншими

версіями моделей. Проте інші, загальнодоступні моделі, працюють з іншими категоріями та класами об’єктів, що не завжди дозволяє використовувати їх напряму для побудови ADAS системи.

В рамках роботи також було розроблено механізм підтвердження об’єктів на послідовності кадрів. ADAS система як правило використовує актуатор, щоб сповістити водія про небезпеку, ним може виступати звуковий чи світловий сигнал або візуалізація на екрані. То ж, для уникнення випадкового спрацювання модуля розпізнавання об’єктів було створено програмний модуль, який проводить додаткову обробку результатів роботи нейронної мережі по детекції. Він ідентифікував та порівнював виявлені об’єкти від кадра до кадру – і видавав підтвердження про виявлення небезпечного для зіткнення об’єкту лише після його кількаразового підтвердження.

Задачею даної роботи було реалізувати функціонал для обробки відео-потоку, успішного аналізу даних за допомогою самостійно навченої моделі, виявлення об’єктів, що можуть нас зацікавити та валідації знайдених об’єктів шляхом їх підтвердження, і за результатами такої обробки повідомлення водія про потенційну небезпеку.

Наступними кроками будуть покращення характеристик навченої моделі шляхом збільшення дата-сету та покращення швидкодії роботи нейронної мережі за рахунок використання спеціалізованих графічних процесорів з використанням CUDA.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. J. Redmon, S. Divvala, R. Girshick, and A. Farhad, "You only look once: Unified real-time object detection," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 2016, P. 779-788.

2. J. Redmon and A. Farhadi, "YOLO9000: Better, Faster, Stronger," in 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 2017, P. 6517-6525.

УДК: 004.738.5:004.056.53

А. В. Мельник, к.п.н.
Житомирський державний університет ім. І.Франка, Житомир

ОПТИМІЗАЦІЯ ЕФЕКТИВНОСТІ КЕШУВАННЯ В ІНФОРМАЦІЙНО-ОРІЄНТОВАНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ АНАЛІЗУ ТРАФІКУ І ВИКОРИСТАННЯ АДАПТИВНИХ АЛГОРИТМІВ

Інформаційно-орієнтовані мережі зазвичай містять велику кількість вузлів та ресурсів, що надають послуги, які користувачі можуть запитувати. Один із способів покращити продуктивність таких мереж - це використання кешування, що дозволяє зберігати копії даних вузла в локальній пам'яті та використовувати їх для задоволення майбутніх запитів. Проте, існує декілька факторів, які можуть погіршити ефективність кешування в інформаційно-орієнтованих мережах, таких як великий обсяг даних, що потребують кешування, нестабільність запитів, а також несприятливі зміни у мережі.

У літературі існує велика кількість адаптивних алгоритмів кешування, які дозволяють змінювати стратегію кешування в залежності від змінних умов мережі та даних. Розглянемо деякі з них:

1. Алгоритм кешування з часовими мітками (Time-based cache algorithm) Цей алгоритм використовує часові мітки для визначення того, коли дані востаннє використовувалися. Дані, які були використані нещодавно, зберігаються в кеші, а ті, які не використовувалися довший час, видаляються. Один з недоліків цього методу - він не враховує популярність даних, тому дані, які були запитані менше, можуть бути видалені надто рано.

2. Адаптивний алгоритм кешування LRU-K (Least Recently Used K) - цей алгоритм використовує історію використання даних для прийняття рішення про збереження або видалення даних з кешу. Він враховує не лише останній запит, а й K попередніх запитів. Це дозволяє покращити точність передбачення попиту на дані, зберігати більш популярні дані в кеші та видаляти менш популярні.

3. Адаптивний алгоритм кешування LFU-K (Least Frequently Used K) - цей алгоритм використовує історію використання даних для визначення їх популярності. Дані, які були запитані менше, видаляються з кешу, а більш популярні зберігаються. Аналогічно

до LRU-K, LFU-K враховує K попередніх запитів для точнішого визначення популярності даних.

4. Адаптивний алгоритм з попереднім прогнозуванням (Adaptive Pre-fetching algorithm) Цей алгоритм передбачає, які дані будуть запитані в майбутньому, та зберігає їх у кеші. Це дозволяє зменшити час на обробку запитів, оскільки запитані дані вже знаходяться в кеші. Однак, якщо прогнозування неправильне, це може призвести до зайвого використання пам'яті та зменшення ефективності кешування.

5. Адаптивний алгоритм з резервуванням (Adaptive Reservation algorithm) Цей алгоритм зарезервовує деяку кількість пам'яті для найбільш популярних даних та використовує LRU-стратегію для менш популярних даних. Це дозволяє зберігати найбільш важливі дані в кеші, тоді якщо пам'ять стає обмеженою, менш популярні дані будуть видалені першими. Однак, якщо популярність даних змінюється динамічно, то цей алгоритм може виявитися менш ефективним.

6. Алгоритм кешування зі змінним розміром кешу (Variable-size cache algorithm) Цей алгоритм дозволяє змінювати розмір кешу в залежності від популярності даних. Якщо деякі дані стають більш популярними, то розмір кешу збільшується, щоб зберегти ці дані. Це дозволяє ефективніше використовувати доступну пам'ять. Однак, цей алгоритм може бути витратним з точки зору обчислювальних ресурсів, оскільки потребує частого перерахування розміру кешу.

Кожен з цих алгоритмів має свої переваги та недоліки і вибір певного алгоритму залежить від конкретних умов та вимог до системи кешування.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Adaptive probabilistic caching technique for caching networks with dynamic content popularity URL: https://www.sciencedirect.com/science/article/abs/pii/S0140366418302925?via%3Dihub1 (дата звернення 12.03.2023)

2. Cache Replacement Algorithms: How To Efficiently Manage The Cache Storage URL: https://dev.to/satrobit/cache-replacement-algorithms-how-to-efficiently-manage-the-cache-storage-2ne1 (дата звернення 02.03.2023)

УДК 004.89

К.В.Мельник, к.т.н.,
С.В.Лавренчук, к.т.н.
Луцький національний технічний університет, Луцьк

ВИЯВЛЕННЯ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТКАМИ МЕТОДАМИ МАШИННОГО НАВЧАННЯ

Шахрайством з кредитними картками оцінюється в десятки мільярдів доларів. Наприклад, згідно звіту 2018 року Європейського центрального банку (ЄЦБ) [1], збитки від шахрайства з картками складає 1,8 мільярда євро в Єдиній європейській платіжній зоні (SEPA).

Структура шахрайства: 79% - це шахрайства за відсутності фізичної картки (CNP) (тобто платежів через Інтернет, поштою чи телефоном), 15% – транзакцій у момент здійснення - термінали продажу (POS), наприклад, особисті платежі в роздрібних магазинах або ресторанах, і 6% від транзакцій в банкоматах.

Загальний рівень шахрайства в карткових платіжках свідчить про важливість постійного моніторингу шахрайства та заходів безпеки з боку наглядачів карткових систем.

Для виявлення моделей шахрайства з кредитними картками необхідно здійснювати аналіз великих обсягів даних транзакцій. В останні роки саме алгоритми машинного навчання дозволяють шукати та виявляти шаблони у великих обсягах даних і підвищують ефективність систем виявлення шахрайства.

При застосуванні алгоритмів машинного навчання необхідно враховувати такі проблеми, як: дисбаланс класів (дані про транзакції містять набагато більше законних, ніж шахрайські транзакції); дрейф концепції: моделі транзакцій і шахрайства змінюються з часом; вимоги майже до реального часу; категоричні ознаки **(**ідентифікатор клієнта, термінал, тип картки); показники ефективності (стандартні показники для систем класифікації, такі як середня помилка неправильної класифікації або AUC ROC, не дуже підходять через проблему дисбалансу класів і складну структуру витрат на виявлення шахрайства); відсутність загальнодоступних наборів даних.

При розробці системи виявлення шахрайства т.б. бінарного класифікатора необхідно пройти два етапи: навчання системи та прогнозування мітки нових транзакцій (справжні чи шахрайські).

Як відомо, існує чотири підходи: контрольоване навчання, неконтрольоване навчання, ансамблеве навчання та глибоке навчання.

Авторами розглянуті методи: логістична регресія, дерева рішень, випадкові ліси, нейронні мережі/глибоке навчання. Розглядалися питання покращення продуктивності. Продуктивність можна розглядати, як точності виявлення шахрайства, або вимоги до обчислень (пам'ять/час виконання). Оскільки необхідно працювати з великими обсягами даних і в режимі реального часу, тому потрібно розглядати компроміси між точністю та вимогами до обчислень.

На рис.1 показані результати моделювання з параметрами за замовчуванням.

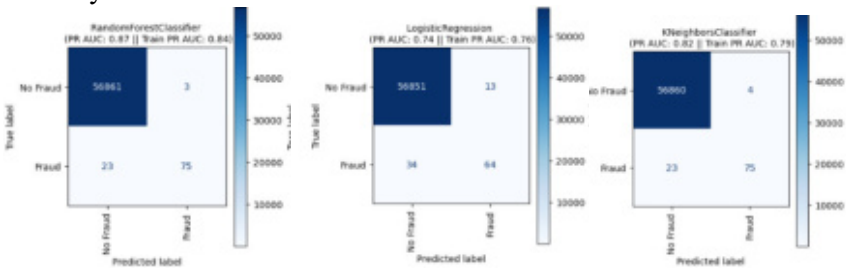


Рис.1.Методи: випадковий ліс, логістична регресія, метод найближчого сусіда.

Показані результати, що отримані за допомогою простих стратегій попередньої обробки та стандартних класифікаторів машинного навчання.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Sixth report on card fraud [Електронний ресурс] – Режим доступу. — URL: http://surl.li/gccpl (дата звернення 04.03.2023)

2. Reproducible Machine Learning for Credit Card Fraud Detection - Practical Handbook– Режим доступу. — URL: http://surl.li/gccqh (дата звернення 04.03.2023)

УДК 004.052.32

Я.В. Мельник
Національний університет оборони України
ім. І.Черняховського, Київ

ЗАСТОСУВАННЯ ТЕОРІЇ ПЕРКОЛЯЦІЇ ТА АНАЛІЗ ІСНУЮЧИХ МЕТОДИК ДЛЯ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ГЕТЕРОГЕННИХ МЕРЕЖ

В останні роки, особливо з початком повномасштабної російської федерації проти України, різко зросли вимоги до надійності існуючих гетерогенних мереж (ГМ), як технологічної основи для забезпечення системи управління. Адже вихід з ладу лише одного елемента існуючої системи управління загрожує втраті системи управління в цілому. Тому побудова надійної ГМ на основі сучасних методик для забезпечення функціонування системи управління є актуальним та важливим завданням.

Оскільки гетерогенні мережі мають більше компонентів, ніж гомогенні мережі, їм потрібні спеціальні методи для забезпечення надійності та безпеки ГМ. Серед основних методик слід виділити наступні:

- метод використання резервування шляху. Цей метод включає створення резервного шляху, який може використовуватися у випадку відмови основного шляху. Резервний шлях може бути створений за допомогою різних методів, таких як використання альтернативних маршрутів або використання дублювання даних.

- метод мультиплексування. Цей метод використовується для розділення ресурсів між різними користувачами та для забезпечення відмовостійкості системи. Методи мультиплексування включають часову, частотну та просторове мультиплексування

- методи резервування пропускної здатності, які передбачають резервування певної кількості пропускної здатності для кожного компонента мережі.

- методи захисту від вторгнень, такі як фільтрація пакетів, віртуальні приватні мережі, фаерволи та інші методи захисту. Фільтрація пакетів дозволяє блокувати певні типи пакетів, що містять шкідливі програми або віруси. Віртуальні приватні мережі дозволяють ізолювати різні частини мережі та забезпечити конфіденційність передачі даних. Файрволи дозволяють

контролювати доступ до ресурсів мережі та перевіряти пакети на наявність шкідливого вмісту.

- метод забезпечення надійності гетерогенних мереж за допомогою технології блокчейн. Це новий метод який дозволяє створювати децентралізовані мережі, де кожен компонент мережі має свій власний ідентифікатор та може перевіряти інформацію, що передається в мережі. Це забезпечує високу надійність та безпеку передачі даних, оскільки будь-яка спроба змінити дані в мережі буде виявлена та заблокована.

В цілому, для забезпечення надійності гетерогенних мереж використовуються різні методики, що включають в себе резервування шляхів, мультиплексування, резервування пропускної здатності, захист від вторгнень та використання технології блокчейн, але кожна методика також має і недоліки (дублювання обладнання, високі витрати на обладнання та інфраструктуру, складність (методики для забезпечення надійності гетерогенних мереж є складними та вимагають великої кількості ресурсів), недостатня масштабованість та інші).

В [1] наводяться рекомендації щодо побудови ГМ на основі порівняльної оцінки їх стійкості. Як результат автори пропонують для оцінки надійності ГМ розглядати передачу інформації у середині мережі як проходження пакетів даних, з одного сегменту ГМ в інший через інфраструктуру провайдерів (мережу Інтернет), за допомогою перколяційних алгоритмів (алгоритмів, побудованих на моделях теорії перколяції). Запропонована методика складається з трьох процедур:

- процедура розкриття структури альтернативних ГМ, одержуваних у результаті вибору того чи іншого оператора зв’язку (провайдера);
- отримання оцінок надійності альтернативних структур ГМ;
- порівняльна оцінка отриманих результатів та вибір структури ГМ.

В рамках процедури розкриття структури мережі запропонований порядок дій для вирішення завдання розкриття структури ГМ за допомогою стандартних інструментальних засобів операційних систем і складання єдиного графа ГМ, який має вузли що не підконтрольні власнику ГМ. Процедура отримання оцінок надійності передбачає комп’ютерне моделювання методом, в якому

передача інформаційних потоків через ГМ розглядається як протікання (просочування) однієї речовини через іншу. Знайдені функціональні залежності стійкості структури мережі до впливу зовнішніх (внутрішніх) факторів (перешкод) порівнюються у процедурі порівняльної оцінки методом інтегральної різниці або на основі експертної оцінки надійності елементів ГМ.

Для цього у методиці, що розроблена, заздалегідь задають параметри елементу ГМ та формують її топологічну схему. В якості параметрів елементу ГМ задають ідентифікатори вузлів мережі, наявність зв'язку між ними, параметри надійності вузла (такі, як тип його устаткування, версія встановленого програмного забезпечення, приналежність вузла державній або приватній установі та ін.).

Забезпечення надійності здійснюється під час проектування або під час роботи ГМ. Під час проектування забезпечення полягає в порівняльному аналізі різних варіантів ГМ будь-яким методом оцінки надійності. Під час роботи надійність забезпечується рівномірним (по можливості) розподілом навантаження на мережу за допомогою протоколів маршрутизації. Територіально розподілені мережі створюються з використанням потужностей (вузлів і каналів) різних провайдерів телекомунікаційних послуг. Таким чином, можна говорити про те, що ГМ не є повністю контрольованою власником системи, а існуючі методи забезпечення надійності недостатньо адаптовані до цих непідконтрольних елементів мережі. Крім того, самі мережі провайдерів є елементами всесвітньої мережі Інтернет. В [2] наведені відповідні методичні рекомендації щодо використання програмного забезпечення та програмних утиліт для визначення топології ГМ, для подальшого знаходження альтернативних варіантів підключення до інших елементів мережі.

Наявність високонадійних, які не належать власнику мережі і отже, невідомих елементів і зв'язків між ними суттєво обмежує застосування методів оцінки надійності систем (рис. 1.). Головна складність полягає в постійних змінах параметрів роботи вузлів системи та їх характеристик. Окремою проблемою є те, що елементи, які досліджуються, є високонадійними в штатних режимах роботи. Це істотно ускладнює збір статистики по відмовах. Розміри елементів ГМ чималі для алгоритмів на графах і,

в той же час, не досить великі для відповідності безмасштабним мережам або іншим моделям випадкових графів. Це призводить до того, що фактично надійність забезпечується надмірним резервуванням ресурсів і алгоритмами маршрутизації.

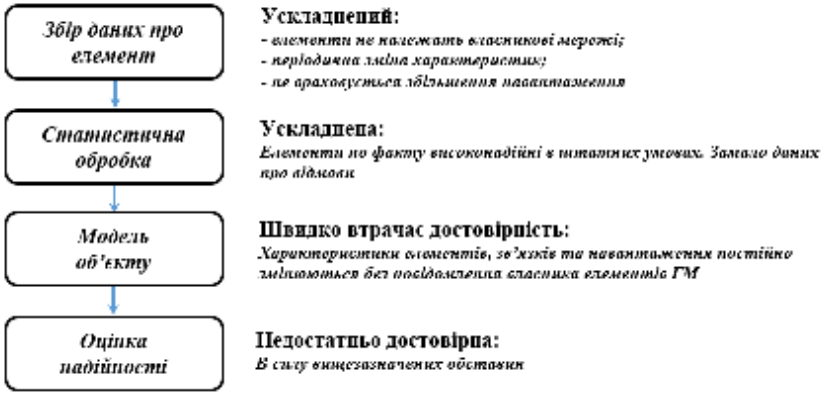


Рис.1. Етапи оцінки надійності систем.

Таким чином використання теорії перколяції дозволяє враховувати вузли що входять до складу локальних сегментів ГМ, які не керовані власниками ГМ і функціонують в умовах впливу перешкод. Теорія перколяції була адаптована до використання в ГМ шляхом визначення меж - вузлів територіально розподілених локальних сегментів ГМ, за допомогою яких здійснюється підключення до ГМ.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Мельник Я.В., Бобильов В.Є., Тимошенко Р.Р. Рекомендації щодо побудови інформаційно-телекомунікаційних мереж на основі порівняльної оцінки їх стійкості. (Modern Information Technologies in the Sphere of Security and Defence) – 2019. № 2(35). – С. 29–34.

2. Мельник Я.В., Бобильов В.Є. Методичні рекомендації щодо використання існуючих програмного забезпечення та програмних утиліт для визначення топології гетерогенних мереж для знаходження альтернативних варіантів підключення (Modern Information Technologies in the Sphere of Security and Defence) – 2019. № 3(36). – С. 19–24.

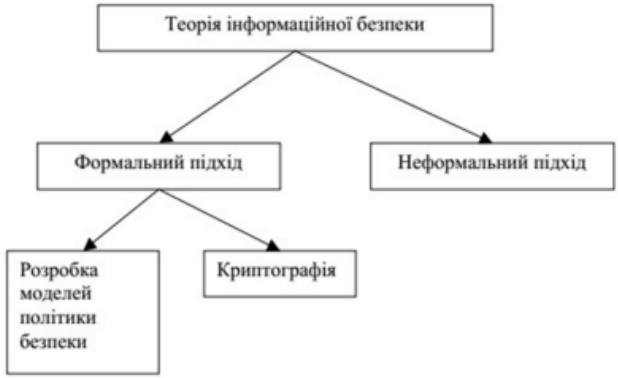
УДК 510.635:004.891(045)

А.В. Мельничук
Національна академія Служби безпеки України, Київ

ТЕОРІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сьогодні інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, суспільство вже не може уявити свій день без гаджетів та Інтернету. Нині високотехнологічна злочинність набуває високих темпів. У зв'язку з цим виникає термінова потреба у створенні не тільки єдиного інформаційного простору, але й адекватного механізму організації інформаційної безпеки. Загалом об'єктами зазіхань можуть бути як технічні засоби (комп'ютери і периферія), так і програмне забезпечення та бази даних, для яких комп'ютер є середовищем. Небезпідставні побоювання викликають вразливості в програмному забезпеченні та в автоматизованих системах. Для зменшення цих ризиків необхідно вжити всіх необхідних заходів для поліпшення кібербезпеки. Аналіз інформаційних ризиків необхідний для визначення можливої шкоди (ризику) за існуючими видами цінної інформації, співвідношення ризику з витратами на забезпечення інформаційної безпеки, оцінки ефективності витрат на забезпечення інформаційної безпеки. Комплексна оцінка захищеності інформаційної системи, оцінка вартості інформації, оцінка ризику, розробка комплексної системи забезпечення інформаційної безпеки – основні завданнями аналізу. Тому метою аналізу інформаційних ризиків є розробка економічно ефективної і обґрунтованої системи забезпечення інформаційної безпеки. Критерії проведення аудиту інформаційної безпеки встановлюються на основі загальноприйнятих міжнародних стандартів (наприклад, міжнародний ISO 17799, німецький BSI і ін.), внутрішніх стандартів аудиторських компаній і вітчизняних відомчих стандартів. Важливий елемент організації інформаційної безпеки – поділ заходів захисту на групи. Основні групи заходів захисту інформації поділяють на активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення), пасивні засоби захисту (наприклад, встановлення екранів несанкціонованому витоку інформації тощо) та комплексні засоби захисту (органічне поєднання названих груп). Визначення і перевірка стану безпеки є важливим шляхом реалізації заходів захисту інформації. Для

успішної розробки хорошої моделі безпеки необхідна наявність чітко визначеної політики безпеки. Визначення умов, яким повинно підкорятися поводження системи, створення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при дотриманні встановлених правил – основна мета створення політики безпеки інформаційної системи. Зв'язок наведених напрямків теорії захисту інформації можна представити у вигляді схеми:



На даний час в Україні сформовано наукові школи з дослідження за різними сферами забезпечення кібербезпеки держави, насамперед, щодо планування і ведення кібероборони та кіберрозвідки, розслідування кіберзлочинів, відбиття кібератак та нейтралізації кіберзагроз; криптографічного та технічного захисту інформації; захисту в кіберпросторі державних інформаційних ресурсів; здійснення захисту та аудиту захищеності інформаційно-комунікаційних і технологічних систем об'єктів критичної інфраструктури держави на вразливість; відновлення сталості і надійності функціонування інформаційно-комунікаційних, технологічних систем після здійснення кібератак.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Захист систем електронних комунікацій: навч. посіб. / В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін. Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

УДК 681.3.06

О.І.Міскевич
Луцький національний технічний університет, Луцьк

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ МЕРЕЖНИХ КОМАНД ТА IP-АДРЕС

Використання мережевих утиліт у будь-якій операційній системі відіграють значну роль. Це питання актуальне, як для глобальних мереж, так і для капсульних, локальних та персональних. Завданням утиліт є діагностика роботи мережі та вузлів, а саме можливість виявити неподадки та налагодити роботу мережі.

Мережні команди є ефективні у порівнянні з графічними інтерфейсами. Розглянемо основні команди та їх використання на практиці у нашій роботі:

- ipconfig – команда для діагностичної інформації в ОС Windows про мережний інтерфейс (мережної плати, мережного адаптера) вузла. Використовується для визначення неправильних IP-адрес, масок підмереж та адрес широкомовної розсилки. В ОС UNIX – Ifconfig;

- ping – команда для перевірки зв'язку з віддаленим вузлом та статистики про втрати пакетів та про час їх доставки.

- tracert – стандартна утиліта, що дозволяє відстежити шлях IP-пакетів та відображається інформація про всі проміжні маршрути, через які запити проходять шляхом до потрібного ресурсу, фіксується час кожної частки маршруту у мілісекундах.

За допомогою цих команд було вирішено наступнні завдання -

- знайдено IP-адреси;

- досліджено маршрути до 3х комп'ютерів, розташованих в різних кінцях світу (Бельгія, Шрі-Ланка та Монголія) за допомогою команди tracert;

- оцінено довжину пройденого шляху.

IP – це віртуальна адреса. Кожен, хто бачить IP-адресу, може дізнатись місцезнаходження, а саме - місто, штат, поштовий індекс і країну, але не особисту інформацію. Щоб захистити себе від кіберзлочинців можна приховати або змінити IP-адресу. Таку можливість дає підключення до сервера NordVPN. Ваш трафік буде зашифровано, використовуючи алгоритми шифрування нового покоління. Це стає безпечним та приватним переглядом контенту, і

жодна організація не зможе відстежити вас. Пошук IP-адрес є законним, загальнодоступним та безкоштовним.

У роботі було знайдено IP-адреси трьох потрібних нам країн та використовуючи команду tracert визначено маршрути прямування даних та проблемні ділянки.

Проведені дослідження показали ефективність використання мережних команд та утиліт для відстеження та трасування.

На рис.1 наведено звіт по роботі.

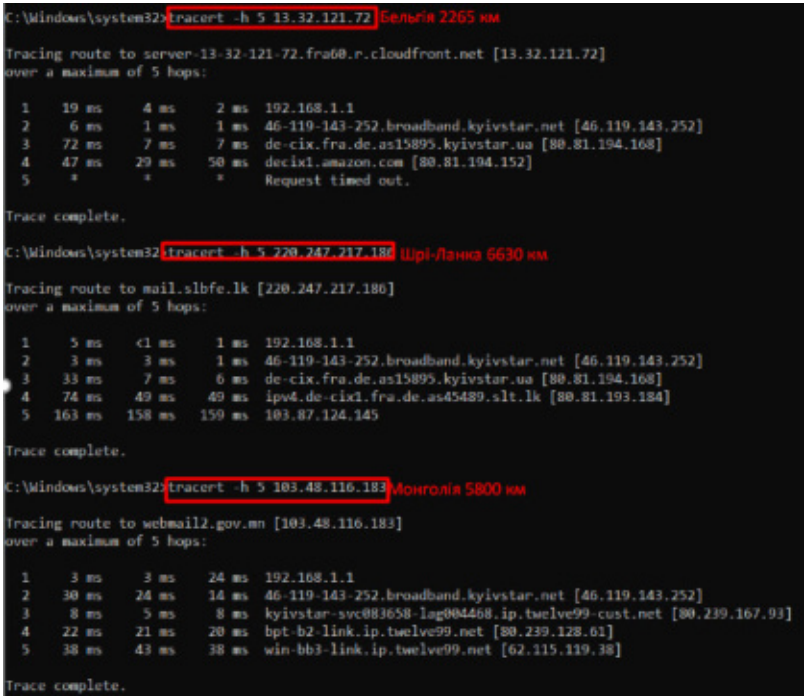


Рис.1. Використання команд tracert

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Information security. Textbook / Yu. Ya. Bobalo, I.V. Gorbaty, M.D. Kiselychnyk, A.P. Bondarev, S.S. Voitusik, A. Ya. Gorpenyuk, O.A. Nemkova, I.M. Zhuravel , B.M. Berezyuk, E.I .Yakovenko, V.I. Otenko, I.Y. Tyshyk. Lviv: Lviv Polytechnic Publishing House, 2019. – 580 p.

УДК 004.056.5

Т.В. Німченко, к.т.н.,
Т.В. Мелешко,
Л.І. Моржова
Національний авіаційний університет, Київ

СИСТЕМИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

На сьогодні інформація є найціннішим ресурсом. Тому перед організаціями та підприємствами гостро постає завдання збереження інформації, у тому числі відомостей, що становлять комерційну або державну таємницю [1].

Ефективність бізнесу в багатьох випадках залежить від збереження конфіденційності, цілісності та доступності інформації. В даний час однією з найбільш актуальних загроз у сфері інформаційної безпеки є витік конфіденційних даних від несанкціонованих дій користувачів [2]

Як показують опубліковані дані опитування Deloitte провідних світових фінансових компаній, 49% респондентів зафіксували внутрішні інциденти (пов'язані з IT-безпекою). У 31% випадків інсайдери занесли віруси зсередини корпоративної мережі, а з інсайдерськими шахрайством зіткнулися 28% респондентів. 18% організацій стали жертвами витоку приватної інформації клієнтів, а 10% виявили, що інсайдери скомпрометували корпоративну мережу [2-3].

Широке застосування для захисту інформаційних ресурсів знайшли системи DLP. Системи DLP це технології, що дозволяють запобігти витоку конфіденційної інформації. У перебігу останніх декількох років використовувалася велика термінологія: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) та ін. Але остаточним і найбільш точним терміном прийнято вважати Data Leak Prevention (DLP, запропонований агентством Forrester в 2005 р.).

В рамках створення таких систем вирішуються завдання: запобігання витоків конфіденційної інформації по основних каналах передачі даних; витікаючий веб-трафік (HTTP, FTP, P2P та ін.); вихідна електронна пошта, внутрішня електронна пошта; системи миттєвого обміну повідомленнями, мережевий та

локальний друк; контроль доступу до пристроїв і портів введення-виведення до яких відносяться: дисководи, CD-ROM, USB - пристрої, інфрачервоні, принтерні (LPT) і модемні (COM) порти.

Для запобігання витоку інформації системи DLP мають вбудовані механізми ступеню конфіденційності перехопленого документа: шляхом аналізу вмісту документа або шляхом аналізу спеціальних маркерів (грифів). Вони наділені можливостями аналізу за словником, лінгвістичного аналізу, аналізу транслітерації.

У DLP-системах зазвичай використовуються три методи ідентифікації: імовірнісний, детерміністський та комбінований.

Системи, засновані на першому методі, основним чином використовують лінгвістичний аналіз контенту та «цифрові відбитки» даних. Такі системи прості в реалізації, але недостатньо ефективні і характеризуються високим рівнем помилкових спрацювань. Системи, що використовують детермінований підхід (мітки файлів), дуже надійні, але їм невистачає гнучкості.

Комбінований підхід поєднує обидва методи з аудитом середовища зберігання та обробки даних, що дає можливість досягти оптимального вирішення проблеми захисту конфіденційності інформації [4].

Звісно, гарантувати абсолютний захист від наслідків діяльності працівників не може жодна DLP-система, однак вона дозволить значно мінімізувати ризики та наслідки людських помилок. Отже, використання систем DLP є одним з ефективних варіантів захисту конфіденційної інформації.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.ohttps://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

2.ohttps://ua.ikmj.com/isms-access-control/

3.ohttp://integritysys.com.ua/security/dlp/

4. О.В. Богуславський, Д.А. Кирилюк. DLP системи як засіб виявлення інсайдера. Міжнародна науково-практична конференція Інформаційні технології та взаємодії. – 2018. – С. 249.

УДК 004.2 (076)

Д.Ю. Омельчук,
Н.А. Христинець, к.т.н.

Луцький національний технічний університет, Луцьк

ПЕРЕВАГИ МІКРОАРХІТЕКТУРИ RISC У СУЧАСНИХ ПРОЦЕСОРАХ APPLE M1

Функціонування сучасних настільних комп'ютерів різних виробників довгий час було окреслене архітектурою систем команд CISC. Проте, останні три роки компанія Apple почала випускати комп'ютери на базі власного процесора M1.

Вперше ці процесори були представлені у листопаді 2020 року, показавши що навіть процесори на незвичній мікроархітектурі для десктопних ПК архітектури RISC [1] можуть добитися схожої або й кращої одно процесорної продуктивності ніж у багатьох сучасних процесорів Intel та AMD. Зокрема, процесор M1 є одним з найбільш енергоефективних процесорів на ринку й досі, враховуючи що Apple M2 отримав покращення у продуктивності, але не енергоефективності і навіть поступається в цьому параметрі своєму попереднику.

Щоб добитися такої продуктивності у власному десктопному процесорі, Apple знадобився весь досвід, який вони набули за час створення процесорів серії A, кожен з яких був побудований на мікроархітектурі RISC [2]. За цей час вони виділили багато переваг цієї мікроархітектури і працювали над тим, щоб ці переваги були ще більш виразними.

Через фіксовану довжину інструкцій, завантаження великої кількості інструкцій і виконання паралельних операцій з ними це стало доволі простою задачею. Цей етап становлення мікроархітектури названий компанією «позачерговим виконанням». Суть його полягає в наступному. CISC інструкції отримують доступ до пам'яті перед завершенням операції, тому паралельне виконання стає важчою задачею, ніж у обмежених у довжині RISC інструкціях.

Наприклад, для виконання операції множення, CISC-процесор потребує однієї комплексної інструкції, щоб отримати доступ до двох комірок пам'яті. Для цієї ж операції потрібно 4 інструкції RISC, з яких дві – завантаження чисел і по одній для виконання

операції множення і збереження результату. Щоб скористатися цією перевагою, Apple M1 має великий буфер пере-упорядкування, який зберігає інструкції для подальшого аналізу на можливість виконання паралельно.

Це означає, що M1 має перевагу у більшій кількості паралельних операцій через коротші інструкції і збереження їх в буфері пере-упорядкування. M1 включає в себе набагато більшу кількість декодерів інструкцій, ніж процесори на мікроархітектурі x86 через те, що це набагато простіша задача, якщо працювати з інструкціями фіксованої довжини. Більша кількість декодувальників дозволяють інструкціям ділитись на мікрооперації для паралельного виконання. Це ще один приклад простішої реалізації паралельних обчислень у цьому процесорі.

Intel та AMD також використовують буфер переупорядкування у своїх процесорах, але він має набагато менший об'єм пам'яті, ніж процесор Apple [3].

Отже, M1 є так званим проривом серед процесорів мікроархітектури RISC та водночас доказом того, що, не зважаючи на довжину інструкцій, можливо створити швидкий та енергоефективний процесор.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Архітектура комп'ютерів. Частина 1 : лабораторний практикум / Л. В. Крупельницький, А. В. Снігур, С. В. Богомолов. – Вінниця : ВНТУ, 2020. – 104 с.

2. Frumusanu A. Apple Announces The Apple Silicon M1: Ditching x86 - What to Expect, Based on A14 [Електронний ресурс] / Andrei Frumusanu // Anandtech. – 2020. – Режим доступу до ресурсу: https://www.anandtech.com/show/16226/apple-silicon-m1-a14-deep-dive

3. Truly A. M1 Mac: How RISC Makes Apple Silicon Faster Than Intel [Електронний ресурс] / Alan Truly // Screen Rant. – 2020. – Режим доступу до ресурсу: https://screenrant.com/apple-silicon-m1-mac-risc-faster-than-intel

УДК 004.45

В.В. Пась,
Н.А. Христинець, к.т.н.
Луцький національний технічний університет, Луцьк

МОЖЛИВОСТІ ВИКОРИСТАННЯ СИСТЕМНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СТВОРЕННЯ ІНТЕРАКТИВНИХ ВІЗУАЛІЗАЦІЙ ДАНИХ У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Термін «візуалізація даних» стає все більш важливим елементом вищої освіти. Університети, викладачі та студенти звертаються до програмного забезпечення для візуалізації даних та для спілкування через низку програмних засобів. Крім того, візуалізація даних полегшує аудиторії чітке розуміння даних, а користувач може передавати інформацію ефективніше.

Основна мета дослідження полягає у тому, щоб створити візуальне представлення шаблонів, тенденцій і контурів, які можна залучити, зрозуміти та поділитися з аудиторією [1]. Багато з цих візуалізацій є інтерактивними, що дозволяє користувачам здійснювати власні налаштування та бачити їх роботу у реальному часі. Коли збирається та аналізується все більше даних, використання програмного забезпечення візуалізації даних допомагає покращити аналітичні результати, щоб розрізнити численні змінні, повідомити концепції, передбачити тенденції минулого, теперішнього та навіть майбутнього.

Програмне забезпечення для візуалізації даних дозволяє користувачеві виявляти нові закономірності у величезній кількості багатоваріантних даних. Наявність можливості досліджувати величезні обсяги даних (великі дані) і обмінюватися ними на настільному комп'ютері чи мобільному пристрої у зручній програмі є ключем до розуміння. Суть полягає в тому, щоб максимізувати збереження релевантної інформації аудиторією, забезпечуючи не тільки пасивне, але більш активне середовище навчання [2].

Користувач повинен знати контекст і розуміти, що саме він намагається візуалізувати та передати з кожного набору даних. Крім того, інструмент буде корисним, лише якщо гарантувати якість цих даних. Майбутнє бізнес-аналітики – це

візуалізація даних. Кількість нових стартапів із візуалізації даних зростає експоненціально, і більшість із них починають сьогодні лідирувати на ринку програмного забезпечення. Це зростання дозволяє встановити конкурентоспроможні ціни та створити додаткові функції та вдосконалення програмного забезпечення для візуалізації даних. Із зростанням сумісності веб-програм HTML5 і Javascript веб-сайти, які відображають інтерактивні діаграми даних і карти, набувають усе більшої популярності [3]. Візуалізація може перетворити складні проблеми на прості, зробити шаблони очевидними.

У процесі навчання, візуалізацію даних для студентів можна використовувати для опису явищ (подій, процесів, концепцій), де студенти представляють колекцію інформації (чисел, формул, слів), де зображення даних можна візуалізувати та обробити, щоб отримати глибше розуміння суті понять.

Динамічні та інтерактивні візуалізації можна вбудовувати в онлайн-матеріали навчальних курсів, чого не можна легко досягти при використанні традиційних підручників. Отже, візуалізація робить користувачів більш продуктивними.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Data Visualization Software | Academic Technologies. Academic Technologies | University of Miami Information Technology. URL: https://academictechnologies.it.miami.edu/explore-technologies/technology-summaries/data-visualization-software/index.html (date of access: 30.03.2023).

2. Brush K., Burns E. What is data visualization and why is it important?. Business Analytics. URL: https://www.techtarget.com/searchbusinessanalytics/definition/data-visualization (date of access: 30.03.2023).

3. Boxiang L. Analysis and Visualization of Spatial Transcriptomic Data / L. Boxiang, L. Yanjun, Z. Liang. // Sec. Computational Genomics. – 27. – С. 54–62.

УДК 004.056

О.С.Потенко

Інститут проблем моделювання в енергетиці ім. Є.Пухова, Київ

РОЗРОБКА МЕТОДИКИ ВИБОРУ СКЛАДУ ПРОФІЛЮ ПРОТИДІЇ ЗАГРОЗАМ НА ОСНОВІ АНАЛІЗУ ВІРОГІДНОСТІ ЇХ РЕАЛІЗАЦІЇ

Проблема інформаційної безпеки в інформаційно-телекомунікаційних системах (ІТС), та побудови комплексних систем захисту інформації (КСЗІ) останнім часом привертає все більш серйозну увагу з боку фахівців, особливо, якщо таку систему використано на об’єктах критичної інфраструктури. Комплексна система захисту інформації – це сукупність організаційних та інженерно-технічних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

Необхідність створення КСЗІ в ІТС регламентується законодавством України. Оцінити наявність послуг безпеки в комп'ютерній системі дозволяють функціональні критерії, а критерії гарантій дозволяють оцінити коректність реалізації послуг. Щоб задовольняти певним вимогам захищеності інформації, яка обробляється в ІТС, комплекс засобів захисту (КЗЗ) обчислювальної системи повинен відповідати профілю захищеності, що являє собою перелік мінімально необхідних рівнів послуг.

З метою перевірки, аналізу та оцінки КСЗІ ІТС щодо їх відповідності вимогам нормативних документів з технічного захисту інформації та можливості їх використання для забезпечення технічного захисту інформації (далі - ТЗІ) проводиться державна експертиза у сфері технічного захисту інформації.

Однією із наукових задач яка вирішується для забезпечення процедури проведення державної експертизі у сфері технічного захисту інформації це вибір методу побудові складу профілю протидії загрозам на основі аналізу вірогідності їх реалізації

Для вирішення задачі проектування профілів, адаптивних загрозам за підкласами АС, пропонується використовувати метод динамічного програмування. Використовуючи класичний підхід [1], можна розробити прикладний алгоритм (методику) оцінки профілів, адаптивних загроз за підкласами автоматизованих систем

АС-1, АС-2, АС-3, на кроки, на кожному із яких склад профілю буде покращено. Для цього необхідно провести дослідження реалізації вимог НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99 та визначити прикладний фізичний зміст, що дозволить розробити методику обчислення параметрів цільової функції під час оптимізації.

Крок 1: Введення початкових значень

Крок 2: Розрахунок цільової функції апроксимованого виду для n об'єктів

Крок 3: Знайти максимальне значення математичного очікування втрат на перших n об'єктах АС

Крок 4: Порівняти значення математичного очікування втрат із початковим. Якщо воно більше, то перейти к пункту 6. Якщо ні, то – до кроку 5.

Крок 5: Прийняти N=N+1 та перейти до кроку 2.

Крок 6: Знайти розподіл атакуючих потенційних загроз по n об'єктах захисту.

Розроблено програмне забезпечення для реалізації методики обчислення параметрів цільової функції під час оптимізації, яке за рахунок використання методу динамічного програмування надає можливість реалізувати принцип оптимальності Р. Беллмана: з якого б етапу ми не почали визначати новий склад профілю для протидії загрозам в залежності від наявності ресурсів захисту щодо апаратного та програмного забезпечення (модернізація, удосконалення, переоснащення, нова політика безпеки тощо), то всі подальші етапи будуть більш оптимальними.

Тестування програмного забезпечення дозволило отримати аналітичні залежності для різних профілів протидії загрозам, що дозволяє оптимізувати процедуру вибору профілю в залежності від вимог до інформації яка обробляється.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Richard E. Bellman. Dynamic Programming. - Princeton University Press, 2010. – 392 p.

УДК 004.451.44

O.V. Rusanova, Ph.D,
O.V. Korochkin, Ph.D,
V.V. Fomin
NTUU "Igor Sikorsy Kyiv Polytechnic Institute", Kyiv

PROBLEM OF AGGREGATION BIG DATA SETS OPTIMIZATION

Nowadays, there is a tendency to digitalization all business processes around us - online supermarkets, smartphone documentation, marriage, childbirth, vehicle registration, banking sector etc. Today state and educational institutions work in online format. There are a lot of smartphone or web application that support digitalization. The main problem of such software is the query processing optimization in databases that include a huge information amount because there are stored tables with millions of rows.

This paper is devoted to the method of preliminary calculations of big data sets, its analysis and comparison with the usual "direct" approach. Firstly, we consider and analyse the methods of processing tables creation and their metrics determination which are used for formulas displaying of aggregated data. Our proposed approach is an improved version of "Materialized view", characterized by dynamism, high scalability and ease of setup.

The following components of the preliminary data calculation approach are analyzed:

- Data aggregation methods;
- Formula metrics;
- The essence of the preliminary calculations tables;
- Raw data source entities.

The optimization is an important component of any software and a much-needed component of applications that store large data amounts. Therefore we propose an approach to storing and using aggregate data based on the authors experience in real projects. The advantages and disadvantages of this approach are considered.

We present the process of preliminary data calculations, which consists of three following stages:

- Export of data sets for aggregation;
- Execution of the data aggregation process in accordance with the established metrics;

- Storing calculations for later using.

There are also discussed ways to unify all these stages and the possibility of moving to a dynamic approach. This will allow you to scale this functionality with minimal effort, with obtaining the desired result.

The approach proposed in this work was implemented and experimentally studied in real software projects. We present examples of statistical results "before" and "after" using this approach in experiments.

Milliseconds are selected as the unit of measurement. Therefore, the result of the experiments during 12 months before the introduction of work optimization with aggregated data was 56,180 milliseconds, which is an incredibly big number for the user to wait a response from the server. After applying the described approach, we`ve got the result 2170 milliseconds. Therefore, it can be argued that the results prove the effectiveness of the proposed approaches. The results of the described approach were used in the development of a universal software application for business management, which allows you to minimize the time and cost of developing projects for new clients due to the unification of the created functionality. To implement the system, the microservice architecture of the application was chosen, consisting of eight main microservices: Identity Service, Booking Service, Activity Analyzer, Email Processor, SMS Processor, Survey Processor, Reporting Service and Storehouse Service. Database were developed according to proposed approach.

REFERENCES

1. D. Tow. SQL Tuning: Generating Optimal Execution Plan. First edition // Performanse of SQL queries – 2003. Vol.4. – P.112-116.

2. M. Winand. SQL Performance // Clustering data to improve performance – 2012. Vol.5 . – P.135-140.

3. B. Scalzo. Database Benchmarking and Stress testing // Recognize and avoid common mistakes in benchmarking database performance – 2018. Vol.5. – P.171-185.

4. M. O'Brien. SQL Performance Tuning // Indexes, including B-trees and bitmaps – 2012. Vol.5. – P.459-460.

УДК 004.621 (043.2)

А.С. Савченко, д.т.н.,
О.В. Толстікова, к.т.н.,
Л.П. Клобукова
Національний авіаційний університет, Київ

СПЕКТРАЛЬНА ЕФЕКТИВНІСТЬ СИГНАЛІВ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

В останні роки безпроводові мережі (БПМ) передачі даних стали одним із головних напрямків розвитку мережної індустрії. Безпроводові локальні мережі можна розглядати як розширення безпроводової мережі з безпроводовим зв'язком "останньої милі" для підключення великої кількості мобільних терміналів. Перевагою безпроводових локальних мереж є порівняльна простота реалізації: не потрібні кабелі, топологія БПМ може динамічно змінюватися разом із підключенням, переміщенням і відключенням мобільних користувачів без особливих втрат часу.

Успіх безпроводових мереж значною мірою залежить від розробки мережних продуктів для множинного доступу до безпроводового середовища та відповідних стандартів. Одним із таких стандартів є протокол IEEE 802.11, що стосується специфікацій на рівнях *MAC* і *PHY* для безпроводових мереж.

Надзвичайно актуальним є впровадження сучасних безпроводових технологій у промисловому та сільськогосподарському виробництві. При впровадженні безпроводових технологій у цих галузях слід враховувати специфіку побудови таких систем та особливі вимоги, визначені стандартами, а саме:

- традиційні мережі виробничого призначення підтримують три рівні моделі *ISO-OSI*: фізичний, передачі даних (канальний) та прикладний. При цьому для таких мереж немає єдиного стандарту: різні мережі працюють за своїми протоколами верхнього рівня;
- пред'являються спеціальні вимоги до надійності передачі на фізичному і канальному рівнях моделі *OSI*;
- при введенні нового комплексу послуг (голос, відео, дані) пріоритет з якості обслуговування (*QoS*), як правило, віддається даним.

При виборі безпроводової, в тому числі, сенсорної технології для мереж виробничого застосування необхідно також враховувати:

- інтенсивність обміну даними на польовому рівні;
- можливість використання автономних джерел електроживлення різної ємності;
- топологію побудови радіомережі. Необхідно забезпечити надмірність зв'язків, також можливість самоорганізації мережі. Це підвищить надійність радіомережі, а також спростить введення в дію кінцевих об'єктів (безпроводових датчиків та виконавчих механізмів).

Ідея відмови від проводів є дуже привабливою. Можуть бути вирішені проблеми, пов'язані з заміною частини проведення вже впроваджених промислових мереж. Мережні вузли та кабелі можуть повільно руйнуватися, особливо в агресивних хімічних середовищах. Відновлення проводової мережної інфраструктури вельми трудомістке і потребує великих фінансових витрат.

Перераховані чинники технічного та економічного характеру, безумовно, важливі, але звернемо увагу, що основні стандарти безпроводових мереж, перш за все, стосуються специфікацій фізичного рівня та у деякій мірі підрівнів *MAC* і *PHY* рівня передачі даних (канального рівня). Тому при розробці та проектуванні БПМ основна увага приділяється вдосконаленню теоретичних методів синтезу та аналізу радіосигналів як матеріальних носіїв інформації, що переноситься у вільному середовищі. У статті, що пропонується до розгляду, зроблена спроба торкнутися найбільш актуальних, на наш погляд, проблем, які неминуче виникають у безпроводових мережах: спектральної ефективності сигналів, завадозахищеності та електромагнітної сумісності.

Практично в усіх роботах, присвячених дослідженню сигналів безпроводових мереж обміну даними, енергетична та спектральна ефективність сигналу протиставляються одне одному. При цьому у рекомендаціях Міжнародної спілки електрозв’язку [1] чітко вказується, що порівнювати коефіцієнт використання спектру, ефективність використання спектру та відносну спектральну ефективність для різних радіосистем просто марно. Крім того, відмічається, що, хоча спектральна ефективність являється важливим чинником, оскільки від неї залежить кількість

радіослужб, які можуть працювати водночас, вона не може бути єдиним чинником, який підлягає розгляду. Треба враховувати також вартість, доступність та сумісність обладнання, надійність та інші техніко-експлуатаційні характеристики.

Твердження, що довжина сигналу та ширина його спектру пов'язані зворотно пропорційною залежністю, випливає безпосередньо з властивостей перетворення Фур'є. Воно є уповні очевидним. Менш очевидними є самі поняття довжини та ширини спектру сигналу. В інженерній практиці застосовуються різні визначення, вибір яких залежить, перш за все, від швидкості убування спектральної щільності [5]. Загальноприйняте визначення енергетичного критерію базується на ширині смуги частот, у якій міститься певна доля повної енергії сигналу, та оцінці протяжності залишків спектру поза даною смугою. Нарешті, основоположне значення має розподіл енергії сигналу по часу та частоті.

При підсумовуванні ряду Фур'є, яким описується *OFDM*-сигнал, не треба забувати, що ряд Фур'є неперервної функції, строго кажучи, не зобов'язаний збігатися. Значить, функцію *OFDM*-сигналу неможливо отримати безпосереднім підсумовуванням ряду Фур'є. Однак цю проблему можна розв'язати методом Фейєра підсумовування середніх арифметичних [2]. Використовуючи метод Фейєра, можна, по-перше, знайти частинні суми довільної сигнальної функції, а по-друге (і це значно важливіше), аргументовано провести порівняльний аналіз різних сигнальних функцій по критеріям спектральної та енергетичної ефективності.

Розглянемо деяку 2π-періодичну неперервну функцію $f_p(t)$, яка може бути єдиним образом розкладена у ряд Фур'є:

$$f_p(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cos nt + b_n \sin nt \right). \qquad (1)$$

Нехай існує послідовність частинних сум $\Sigma_k \ \left(k = 1,2,\ldots,K,\ K < \infty\right)$ ряду Фур'є функції $f_p(t)$:

$$\Sigma_k(t) = \frac{a_0}{2} + \sum_{m=1}^{k} \left(a_m \cos mt + b_m \sin mt \right).$$

Розрахуємо середньоарифметичне частинних сум Σ_k:

$$\mathbf{\Sigma}_K(x) = \frac{\Sigma_0(x) + \Sigma_1(x) + \ldots + \Sigma_{K-1}(x)}{K}. \qquad (2)$$

Вирази виду (2) для довільного K називають сумами Фейєра функції $f_p(t)$. Згідно з теоремою Фейєра суми Фейєра 2π-періодичної неперервної функції $f_p(t)$ збігаються до $f_p(t)$ рівномірно на всій числовій вісі.

Теорему Фейєра можна розглядати як посилення теореми Вейєрштраса про апроксимацію неперервних функцій тригонометричними поліномами. Теоремою Вейєрштраса встановлюється лише факт того, що будь-яка неперервна функція є рівномірний ліміт деякої послідовності тригонометричних поліномів, а теорема Фейєра визначає уповні конкретну послідовність, яка має цю властивість – послідовність сум Фейєра (2).

Згідно з теоремою Фейєра у точці неперервності t_0 функції $f_p(t)$ її ряд Фур'є, який підсумовується по Фейєру, рівномірно збігається до $f_p(t_0)$. Якщо ж у точці t_g існує розрив першого роду, то ряд Фур'є збігається до $f_p(t_g) = \frac{f_p(t_g + \varepsilon) + f_p(t_g - \varepsilon)}{2}$, де ε – мала околиця точки t_g.

Оскільки при цьому рівномірна збіжність ряду Фур'є вже не гарантується, результат Фейєра був посилений Лебегом, який показав, що для будь-якої функції, що підсумовується, її ряд Фур'є збігається до $f_p(t)$ майже усюди.

Тут треба відмітити, що число розривів *OFDM*-сигналу як 2π-періодичної функції $f_p(t)$ завжди є скінченим, тому звісна "множина міри нуль", із-за якої й виникає додаток "майже всюди", в інженерній практиці не зустрічається.

Що ж стосується практичного використання результатів теореми Фейєра, представимо частинну суму Σ_k у вигляді інтегралу:

$$\Sigma_k(t) = \frac{1}{2\pi k} \int_{-\pi}^{\pi} \left(\frac{\sin k\frac{\tau}{2}}{\sin\frac{\tau}{2}} \right)^2 f(t+\tau)\, d\tau, \qquad (3)$$

який називається інтегралом Фейєра. Ядро цього інтегралу:

$$\Phi_k(t) = \frac{1}{2\pi k} \left(\frac{\sin k\frac{\tau}{2}}{\sin\frac{\tau}{2}} \right)^2,$$

(4)

відповідно, називається ядром Фейєра.

З урахуванням (4) вираз (3) запишемо у наступному вигляді:

$$\Sigma_k(t) = \frac{1}{2\pi k} \int_{-\pi}^{\pi} \left(\frac{\sin k\frac{\tau}{2}}{\sin\frac{\tau}{2}} \right)^2 f(t+\tau)\, d\tau, \qquad (5)$$

що, по суті, представляє собою інтеграл згортки досліджуваної функції з ядром.

Наведені результати використані для дослідження *OFDM*-сигналу. У роботі [3] розраховані функції розкладання *OFDM*-сигналу з п'ятьма піднесучими в ряд Фур'є, який обмежений п'ятьма членами. Умова ортогональності не дотримується: бічні пелюстки парціальних спектрів перетинаються у точках, де їх значення є довільними та не дорівнюють нулю.

Для отримання порівняльних результатів підсумовування за методом середньоарифметичних досліджено ядро Фейєра. За формулою (4) розрахований графік ядра Фейєра для випадку $k = 1$. Графік зображений на рис. 1. Можна бачити, що отримана функція у деякій мірі нагадує графік гаусівського або косинус квадратного імпульсу. Параметри реального ядра Фейєра узгоджуються з параметрами вибраного *OFDM*-сигналу. Графік відповідного ядра зображений на рис. 2.

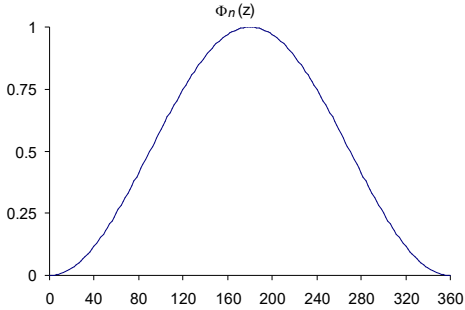


Рис. 1. Графік ядра Фейєра; $k = 1$

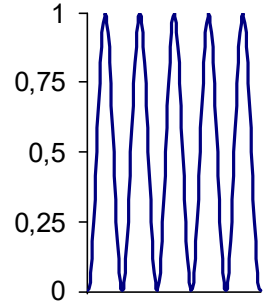


Рис. 2. Графік ядра Фейєра; $k = 5$

З використанням виразу (5) було знов розраховано графіки розкладання *OFDM*-сигналу з п'ятьма неортогональними піднесучими (рис. 3) та графік сумарного сигналу зі згладжуванням по Фейєру (рис. 4). З рис. 3 та рис. 4 видно, що при використанні згладжуючого ядра Фейєра рівень бічних пелюсток піднесучих значно знижується Відповідно, відновлений сумарний сигнал набуває в околиці плоскої частини імпульсу форми, більш близької до прямокутної. Фронт та зріз імпульсу втрачають коливальний характер, стають монотонними, при цьому, що уповні логічно, сумарний сигнал на низькому рівні бічних пелюсток розширяється.

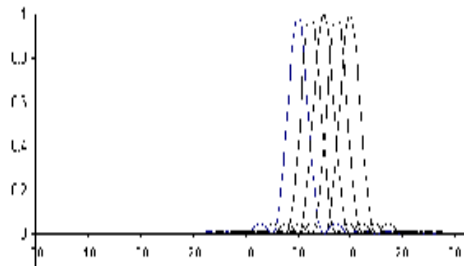


Рис. 3. Графіки п'яти піднесучих *OFDM*-сигналу зі згладжуючим ядром Фейєра

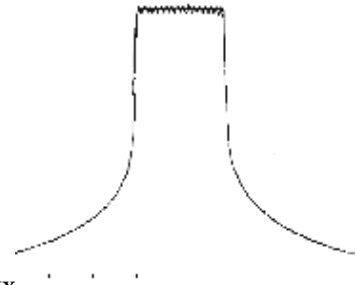


Рис. 4. Графік сумарного сигналу зі згладжуючим ядром Фейєра

Таким чином, спектральна ефективність сигналу в цілому покращується. За критерієм оптимального частотно-часового розподілу енергії сигналу суперечностей між енергетичною та спектральною ефективністю не спостерігається.

ВИСНОВКИ

Успіх безпроводових мереж супроводжується новими викликами, у першу чергу, об’єктивною обмеженістю частотного ресурсу. У зв’язку з цим виникає проблема забезпечення максимально доступної спектральної ефективності сигналів, які переносять інформацію у каналах обміну. Показано, що при розкладанні довільного сигналу у ряд Фур'є відновлення сигналу можна достатньо успішно забезпечити шляхом застосування методу Фейєра підсумовування середніх арифметичних частинних сум ряду.

У роботі [3] доведено, що ядро Фейєра може служити інструментом згладжування форми сигналу. Відповідно, забезпечується потрібна спектральна ефективність сигналу, і, як наслідок, найбільш повне використання частотного ресурсу (який завжди обмежений, особливо у безпроводових мережах). Більш того, завдяки використанню згладжуючих ядер Фейєра у певній мірі усуваються суперечності між енергетичною та спектральною ефективністю сигналів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Recommendation ITU-R SM.1046-3 (09/2017). Definition of spectrum use and efficiency of a radio system SM Series Spectrum management. Geneva, ITU, 2017. – 55 p.

2. Kohlenbach U. Quantitative results on Fejer monotone sequences // Ulrich Kohlenbach, Laurentiu Leustean, Adriana Nicolae - Communications in Contemporary Mathematics, 2018. - 39 p. Електронний ресурс. Режим доступу: DOI: 10.1142/S0219199717500158

3. А.С. Савченко, О.В. Толстікова, Л.П. Клобукова. Критерії вибору спектрально-ефективних сигналів у безпроводових інформаційних мережах. Наукоємні технології. – К.: НАУ, 2022. – Вип. №4 (56). – С. 268-273.

УДК 004.032.26-048.34(043.2)

М.А. Сіренко
Національний авіаційний університет, Київ

ПОКООРДИНАТНИЙ СПУСК ДЛЯ НАЛАШТУВАННЯ ПАРАМЕТРІВ НЕЙРОКОМП'ЮТЕРНИХ СИСТЕМ РОЗПІЗНАВАННЯ ОБРАЗІВ

Сучасні інформаційні технології важко уявити без використання нейрокомп'ютерних систем, проте ефективність їх роботи, значно залежить від правильного налаштування параметрів нейронної мережі [1]. У зв'язку з цим, дослідження безградієнтних методів оптимізації, зокрема поєднання алгоритму покоординатного спуску та елементів методу золотого перетину для налаштування параметрів нейрокомп'ютерних систем розпізнавання образів є на сьогодні важливим напрямком дослідження, що може покращити ефективність їх використання у системах з обмеженими ресурсами.

Для обґрунтування наукових результатів проведеного дослідження було використано метод моделювання, який включав розробку програмної моделі для перевірки адекватності функціонування створеного алгоритму.

Автором запропонований прототип моделі нейромережі для розпізнавання образів, в основі якої використаний покоординатний спуск та метод золотого перетину для вирішення задачі одновимірної оптимізації.

Концепція покоординатного спуску полягає в послідовній оптимізації функції багатьох змінних, шляхом оптимізації одного напрямку в конкретний момент часу. Метод покоординатного спуску для мінімізації $F : R^d \rightarrow R$ задається ітерацією [2]:

$$\omega_{k+1} \leftarrow \omega_k - \alpha_k \nabla_{ik} F(\omega_k) e_{ik}, \text{де } \nabla_{ik} F(\omega_k) \coloneqq \frac{\partial F}{\partial \omega^{ik}}(\omega_k).$$

ω^{ik} представляє i_k-й елемент вектора параметрів, а e_{ik} представляє i_k-й вектор координат для деякого $i_k \in \{1, \ldots, d\}$.

Ідея методу золотого перетину полягає в діленні відрізка за пропорціями так званого золотого перетину (значення якого приблизно дорівнює 1,618) та порівнянні значень функції в кінцевих точках отриманих інтервалів.

Реалізація моделі здійснена завдяки мові програмування *Python* та типових модулів: *numpy*, *random, time* та *matplotlib.*

Характеристика розроблюваної моделі: багатошаровий перцептрон, нейронні мережі прямого поширення, навчання з вчителем, неоднорідна структура мережі.

Для нейронів прихованого шару використана активаційна функція типу *ReLU*, для нейронів вихідного шару – типу *Softmax*.

Гіперпараметри моделі підбирались методом тестування та задовільних результатів, з точки зору точності та швидкості навчання, вдалось досягнути при наступних значеннях: к-сть прихованих шарів - 16, швидкість навчання - 0.05 с, кількість епох - 1000, розмір зміщення - 10. Для перевірки адекватності моделі використані тестові та валідаційні дані, при яких точність навчання наближається до 100%.

Для систем розпізнавання образів з обмеженими інформаційно-обчислювальними ресурсами, доцільно застосовувати методи налаштування параметрів, заснованих на безградієнтних методах оптимізації. В проведеному дослідженні пропонується модифікація алгоритму покоординатного спуску, який продемонстрував задовільні результати під час навчання моделі нейронної мережі для розпізнавання образів.

На рис. 1 наведений процес збіжності навченої моделі.

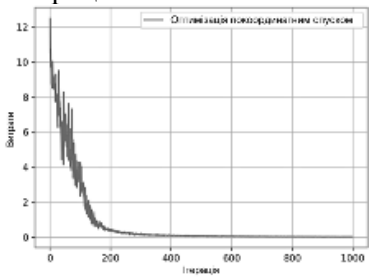


Рис.1. Ілюстрація процесу збіжності

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Y. LeCun, Y. Bengio, and G. Hinton. Deep learning. Nature, 521, 436–444, 2015.

2. L. Bottou, F. E. Curtis, and J. Nocedal. Optimization methods for large-scale machine learning. arXiv:1606.04838v3, 2018.

3. G. Taylor, R. Burmeister, Z. Xu, B. Singh, A. Patel, and T. Goldstein. Training neural networks without gradients: A scalable admm approach. arXiv:1605.02026v1, 2016.

УДК 510.635:004.891(045)

А.І. Слюсар
Національна академі Служби безпеки України, Київ

ЕФЕКТИВНІСТЬ СУЧАСНИХ МЕТОДІВ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ

З розвитком інформаційних технологій та глобальної інфраструктури Інтернету важливість безпеки мережі стає все більш важливою. Тестування на проникнення є одним із ключових інструментів для захисту комп'ютерних систем і мереж. У цій статті розглядаються сучасні методології тестування на проникнення на основі аналізу авторитетних джерел і практичних застосувань. Особливу увагу приділено технічним аспектам і деталям реалізації цих методів.

Автоматичні сканери вразливостей, такі як Nessus, OpenVAS і Nexpose, можуть швидко виявляти вразливості в системах і мережах [1,2]. Вони забезпечують огляд великої кількості систем за короткий проміжок часу, але можуть забезпечити обмежений аналіз і вимагати ручного втручання експерта для виявлення складніших уразливостей.

Автоматизовані засоби атаки на паролі, такі як John the Ripper, Hashcat і Hydra, можуть виявляти слабкі паролі та відновлювати хешовані паролі [3]. Ці інструменти ефективні для виявлення слабких паролів, але можуть бути менш успішними для взлому надійних паролів і безпечних систем.

Проведення симульованої атаки «Red Team» дозволяє імітувати реальну атаку, що допомагає виявити слабкі місця в системі та оцінити ефективність заходів безпеки [4]. Цей підхід передбачає багатосторонню атаку, включаючи соціальну інженерію, фізичне проникнення та використання вразливостей мережі.

Підхід «Білої команди» передбачає реалізацію заходів активного захисту, спрямованих на підвищення рівня безпеки системи та запобігання можливим атакам [5]. Ці методи включають моніторинг мережі, оцінку ризиків і реагування на інциденти кібербезпеки.

Такі метричні системи, як CVSS, DREAD і метод оцінки ризику OWASP, дозволяють оцінити ефективність тестування на проникнення та розробити стратегії підвищення безпеки [6]. Ці

системи враховують усі аспекти вразливості та допомагають приймати обґрунтовані рішення щодо розподілу ресурсів для підвищення безпеки мережі.

Для підвищення ефективності тестування на проникнення необхідна інтеграція автоматизованих методів і сучасних методів [7]. Це передбачає планування та виконання всебічного тестування, аналіз результатів і внесення змін до систем безпеки для підвищення їх ефективності.

Для забезпечення ефективності тестування на проникнення основна увага приділяється навчанню персоналу та розвитку культури кібербезпеки. Це передбачає проведення навчальних семінарів, регулярне оновлення знань експертів та підвищення обізнаності користувачів щодо кіберзагроз.

Сучасні методи тестування на проникнення в контексті кібербезпеки включають як автоматизовані інструменти, так і комплексні підходи до оцінки та підвищення рівня захисту систем. Інтеграція автоматизованих методів з сучасними підходами дозволяє підвищити ефективність тестування на проникнення та розвивати культуру кібербезпеки. Підготовка персоналу та залучення співробітників до процесу забезпечення кібербезпеки є важливими аспектами успішного застосування методів тестування на проникнення.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Tenable. Nessus. – 2021 https://www.tenable.com/products/nessus

2. Greenbone Networks – 2021 – OpenVAS. https://www.openvas.org

3.Steube, J. Hashcat – 2021 – https://hashcat.net/hashcat/

4.Red Team Journal. What is a Red Team? – 2021 – https://redteamjournal.com

5.National Initiative for Cybersecurity Education (NICE) – 2021 – White Team Roles and Responsibilities. https://www.briskinfosec.com/blogs/blogsdetail/Red-vs-Blue-vs-Purple-vs-Orange-vs-Yellow-vs-Green-vs-White-Cybersecurity-Team

6.CVSS, DREAD, and OWASP Risk Rating Methodology – 2021 – https://owasp.org/www-community/Application_Threat_Modeling

7.McMillan, R. Integrating Automated and Manual Penetration Testing. – 2021 – https://www.darkreading.com/vulnerabilities-threats/integrating-automated-and-manual-penetration-testing/a/d-id/1334610

УДК 004.7

А.Л. Столяр
Національний авіаційний університет, Київ

ПРОБЛЕМИ ВИЯВЛЕННЯ АНОМАЛІЙ В КОМП'ЮТЕРНИХ МЕРЕЖАХ У РЕЖИМІ РЕАЛЬНОГО ЧАСУ

Аномалії – це несподівані або незвичайні події, які відбуваються в мережі, а виявлення аномалій – це процес ідентифікації цих подій. У комп'ютерних мережах аномалії можуть бути спричинені різними факторами, такими як апаратні та програмні збої або кібератаки. Виявлення аномалій у режимі реального часу передбачає процес, який ефективно й точно визначає аномалії шляхом одночасного збору й обробки даних із високою обчислювальною ефективністю. Однак виявлення аномалій у реальному часі пов'язане з низкою проблем, які необхідно подолати. Далі розглядаються деякі з ключових проблем, пов'язаних із виявленням аномалій у комп'ютерних мережах.

Виявлення аномалій у реальному часі може бути складним через високу швидкість отримання даних і великий обсяг даних, які необхідно обробити. Обсяги даних можуть варіюватися від гігабайт до терабайт і більше, залежно від розміру і складності мережі. Додатково, мережа може обробляти від тисяч до мільйонів точок даних в секунду. Одним із рішень цієї проблеми є використання розподілених обчислень. Дані можуть оброблятися на декількох серверах, здатних впоратися з великими обсягами і швидкістю даних. Розподілені обчислювальні системи, такі як Hadoop і Spark, використовуються для обробки даних в реальному часі. Іншим рішенням є використання вибірок і фільтрації для зменшення обсягу даних, які необхідно проаналізувати.

Системи виявлення аномалій у реальному часі повинні обробляти різні типи даних, такі як мережевий трафік, системні журнали, метрики додатків і події безпеки. Оскільки кожен тип даних має власну структуру, формат і характеристики, може бути важко співвідносити та аналізувати різні джерела даних. Щоб подолати цю проблему, одним із рішень є використання методів нормалізації даних, щоб забезпечити узгодженість форматів даних. Ще один підхід – конструювання ознак, який представляє собою процес ідентифікації та вибору вагомих атрибутів даних. Це може

допомогти зменшити вплив різноманітності даних і спрямувати увагу системи на найважливіші характеристики.

Якість даних є ще однією проблемою при виявленні аномалій у реальному часі. Дані можуть бути неповними, зашумленими або містити помилки. Проблеми з якістю даних можуть бути спричинені кількома факторами, такими як помилки датчиків, перевантаження мережі або помилки при передачі даних. Система виявлення аномалій у реальному часі повинна вміти виявляти і фільтрувати такі дані. Система також повинна вміти обробляти неповні або відсутні дані та обчислювати або інтерполювати відсутні значення для проведення точного аналізу. Цього можна досягти, використовуючи фільтрування та нормалізацію – це дві процедури попередньої обробки, які можуть допомогти усунути шум і непотрібні дані з вхідного потоку.

Системи виявлення аномалій у реальному часі повинні досягати високої точності виявлення аномалій, мінімізуючи кількість хибнопозитивних і хибнонегативних результатів. Хибнопозитивні спрацьовування виникають, коли нормальна поведінка класифікується як аномальна, тоді як хибнонегативні результати виникають, коли аномальна поведінка класифікується як нормальна. Одним із способів вирішення цієї проблеми є використання машинного навчання. А саме, навчання алгоритму на великих наборах даних для підвищення його точності. Іншим рішенням є використання ансамблевого навчання. Це об'єднання декількох алгоритмів для підвищення їхньої точності.

Системи виявлення аномалій у реальному часі повинні адаптуватися до змін у поведінці мережі та виявляти нові типи аномалій. Мережі є динамічними і можуть змінюватися з часом під впливом різних факторів. Системи виявлення аномалій в реальному часі повинні мати можливість адаптуватися до цих змін і виявляти нові типи аномалій без необхідності конфігурації або ручного втручання. Система виявлення аномалій в реальному часі також повинна вміти вчитися на попередніх аномаліях і вдосконалювати моделі та алгоритми виявлення з часом. Одним із способів подолання цієї проблеми є використання онлайн-навчання. Це дозволить оновлювати алгоритм в режимі реального часу на основі нових даних. Іншим рішенням є використання динамічних порогів.

Це дозволяє коригувати поріг для виявлення аномалій на основі поточних даних.

Системи виявлення аномалій в реальному часі вимагають великих обчислювальних ресурсів для обробки великих обсягів даних в режимі реального часу і виявлення аномалій. Система виявлення аномалій в реальному часі повинна мати можливість горизонтального і вертикального масштабування, щоб бути здатною обробляти зростаючі обсяги даних і трафіку. Крім того, системи виявлення аномалій в реальному часі повинні оптимізувати алгоритми і структури даних для зменшення обчислювальних витрат і досягнення високої продуктивності. Одним з рішень для вирішення цієї проблеми є використання хмарних обчислень. Для обробки даних використовуються віддалені сервери, що дозволяє зменшити навантаження на локальну мережу. Іншим рішенням є використання апаратного прискорення. Для цього використовується спеціалізоване обладнання, таке як графічні процесори для більш ефективної обробки даних.

Усі ці заходи разом забезпечують ефективний моніторинг як зовнішніх, так і внутрішніх ризиків, одночасно підвищуючи загальний рівень продуктивності

У цьому дослідженні було проаналізовано ключові проблеми, які виникають при виявленні аномалій в реальному часі та запропоновано рекомендації, які дозволять перебороти ці проблеми та покращити ефективність роботи систем виявлення аномалій, які працюють у реальному часі.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Limthong K. Real-Time Computer Network Anomaly Detection Using Machine Learning Techniques. Journal of Advances in Computer Networks. – 2013. – P. 1-5.

2. Chuadhry M.A., Gauthama R.M.R., Aditya M. Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems. Proceedings of the 6th ACM on Cyber-Physical System Security Workshop. – Association for Computing Machinery, New York, USA, 2020.– P. 23-29.

3. Hadoop vs. Spark: What's the Difference? URL: https://www.ibm.com/cloud/blog/hadoop-vs-spark (дата звернення: 27.03.2023).

UDC 004.738

I.V. Teleshko, Ph.D.**,**
O.K. Bobrov
National Aviation University, Kyiv

STATIC ADDRESSING FOR MOBILE DEVICES IN A CORPORATE NETWORKS

Mobile communications system refers generally to any telecommunications system which enables wireless communication when users are moving within the service area of the system. Often the mobile communications network is an access network providing a user with wireless access to external networks, hosts, or services offered by specific service providers.

One of the main targets in the development of mobile communications networks is to provide the user with IP (Internet Protocol) service, i.e. access to the Internet through a corporate communication network. It is desired that the IP will be implemented as an overlay of the mobile network while maintaining backwards compatibility with present systems, assuming minimal modifications in the present standards. However, a problem is that the basic IP concept does not support the mobility of the user: IP addresses are assigned (allocated) to network interfaces in dependence on their physical location.

In order to enhance mobility in the Internet, a Mobile IP protocol for version 4 has been introduced by the Internet Engineering Task Force (IETF) in the standard RFC2002. Mobile IP enables the routing of IP datagrams to mobile hosts, independently of their point of attachment in the subnetwork. Mobile Node MN (also called Mobile Host MH) refers to a Cost that changes its point of attachment from one network or subnetwork to another.

A mobile node may change its location without changing its IP address; it may continue to communicate with other Internet nodes at any location using its (constant) IP address. In the mobile IP concept, a datagram is encapsulated and routed to a known decapsulation agent, which decapsulates the datagram and then correctly delivers it to its ultimate destination. Each mobile node is connected to a home agent over a unique tunnel, identified by a tunnel identifler which is unique to a given Foreign Agent/Home Agent pair. In the mobile IP, the mobile

host is identified with respect to its home IP network. Thus, the Mobile IP solves the mobility management problem of the basic IP by adapting to the inflexibility of the IP address, but IP the mobile host is still identified with respect to its home IP network[1].

From the one hand the prior art mobile IP schemes are not very suitable for a mobile communication system 'which does not employ IP as a network protocol. The TETRA network, which tunnels IP traffic through a non-IP protocol, is an example of such a system. The TETRA system is a digital mobile communication system developed primarily for professional and governmental users, such as the police, military forces, oil plants, etc.[2].On the other hand, using the Mobile Host service from cellular providers is very expensive.

The authors suggest the use of tunnel protocols to obtain static addresses of mobile devices in the corporate network. In this case, the source of IP addresses is a VPN server that assigns addresses from its own address pool. If the address allocated in the pool is made static, the mobile device will have the same internal address regardless of the it location. Additional binding of the internal address to the specified external address on the corporate router allows you to also fix the external address of the specified device. In this case, we also get a static external address. In general, this allows you to preserve all access rights and permissions of the specified device to the information resources of the corporate network, regardless of the location of the device.

The possibility of using two tunnel protocols, namely PPTP and L2TP, is considered. From the point of view of security, preference should be given to the L2TP protocol, but this approach may face problems of interaction with some public cellular providers. Because of this, the PPTP protocol should be considered more universal. Using the PPPoE protocol may be of some interest, despite the fact that it is now considered obsolete. But this question goes beyond the scope of this work.

REFERENCES

1. Igor Iartym, Jari Maki. (2004). Ip address allocation in a mobile communications system. U.S. Patent No. 6,771,735. Washington, DC: U.S. Patent and Trademark Office.

2. ETSI-European Telecommunications Standards Institute. 2004. TETRA.

УДК 510.635:004.891(045)

Н.А. Товстуха
Національна академія Служби безпеки України, Київ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ: ЗА ТА ПРОТИ

Штучний інтелект (ШІ) з кожним днем стає актуальним в інформаційній безпеці. На сьогодні близько 50% підприємств вже використовують комбінацію ШІ та інструментів машинного навчання, а понад 90% організацій планують запровадити такі інструменти в майбутньому. І це не дивно, адже такі системи можна використовувати починаючи від перевірки на вразливість і закінчуючи захистом даних, а в поєднанні з досвідченим, у сфері кібербезпеки, фахівцем, стає надзвичайно ефективним.

Так чому ж ШІ викликав до себе такий інтерес з боку фахівців з кібербезпеки? Бо система має ряд переваг, таких як:

1. Виявлення загроз. Найбільша проблема, з якою постійно зустрічаються фахівці з кібербезпеки – величезний обсяг даних, в якому звичайні системи забезпечення не можуть виявити значну кількість нових вірусів. Штучний інтелект, здатен швидко аналізувати шаблони в базах даних, щоб виявити аномальну поведінку чи ідентифікувати загрози.

2. Автоматизація. ШІ розгортають для того, щоб автоматизувати та оптимізувати аспекти кібербезпеки. Тобто, це дозволяє фахівцям зосередити увагу на розслідуванні та ліквідуванні складних загроз, тоді як ШІ виконує монотонні базові завдання.

3. Самонавчання. Одна з переваг технології ШІ є здатність вчитися та вдосконалюватися. Маючи дані минулих атак, алгоритми машинного навчання ідентифікують закономірність, а потім розробляють нові та покращені методи виявлення. Тому хакерам буде важче перехитрити ШІ.

4. Виявлення внутрішніх загроз. Ці загрози ще більш небезпечні, тому що їх складно виявити, оскільки залучені особи мають законний доступ до даної мережі. Але системи на базі штучного інтелекту можуть аналізувати поведінку користувачів і таким чином визначати характерні риси, що вказують на внутрішню загрозу.

5. Передбачення загроз. Аналізуючи великі обсяги даних, ШІ

може передбачити загрози, її масштаб, а також як і де найімовірніше буде взлом. Цю інформацію потім можна використовувати для розробки ефективних методів стратегії кібербезпеки.

6. Рішення безпеки кінцевих точок, що базуються на штучному інтелекті, використовують алгоритми машинного навчання для виявлення небезпечної поведінки та раніше невідомих загроз. Цей підхід ефективніший, ніж традиційні методи, оскільки дозволяє ідентифікувати небезпеку, яка за іншими обставинами була б непоміченою.

Але не дивлячись на ряд переваг, система має суттєві недоліки:

1. Нездатність працювати автономно. Оскільки вони ще не в стані повністю замінити людські рішення, залишаються задачі, які вимагають втручання людини.

2. Проблема з приватністю. Аналіз великого обсягу даних може призвести до того, що як приватні, так і суспільна інформація буде аналізована ШІ, що зможе призвести до втрати конфіденційності інформації.

3. Відсутність контролю. Найбільш поширеною проблемою є побоювання з приводу того, що ШІ може вийти з під людського контролю через унікальний непередбачуваний характер, до якого не можливо застосувати правові рамки

4. Етнічні проблеми. На цей час ШІ не має морального кодексу, отже рішення, які приймаються замість людини, не обов'язково будуть такими ж, якби такі рішення приймала людина.

Отже, ШІ – це дуже перспективний інструмент у сфері кібербезпеки, який потребує подальшого вдосконалення, та контролю зі сторони людей.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. *Artificial Intelligence in Cybersecurity, Nadine Wirkuttis and Hadas Klein, p. 103-119*
2. *https://cybersecurityforme.com/artificial-intelligence-for-cybersecurity/*
3. *https://www.cybertalk.org/2023/03/27/how-artificial-intelligence-is-revolutionizing-cyber-security/*

УДК 004.82.519.81;519.86

Ю.П. Чаплінський, к.т.н.,
О.В. Субботіна
Інститут кібернетики ім. В.Глушкова НАН України, Київ

БАГАТОМОДЕЛЬНЕ УПРАВЛІННЯ ДАНИМИ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Сучасний погляд на прийняття рішень визначає перехід від вузькодисциплінарного прийняття рішень до взаємодіючої множини предметних областей, що об'єднує різні аспекти розгляду: представлення, зміст, інтерпретацію та використання, постійною зміною середовища прийняття рішень, постійного накопичення нових знань, використання активних знань. При цьому необхідно враховувати, що прийняття рішень відбувається в умовах інформаційної та реалізаційної неоднорідності, розподіленості та автономності інформаційних ресурсів системи.

Сьогодні для розв'язання проблеми «різноманітності» даних пропонується використовувати багатомодельне управління даними. Існує два концепції багатомодельної системи управління даними: багатоваріантне зберігання (polyglot persistence) [1] та мультимодельне зберігання (multi-model) [2].

Polyglot persistence (багатоваріантне зберігання) базується на принципі, що у межах однієї системи доводиться зберігати даних і розв'язувати різні задачі за допомоги різних засобів управління даними, кожний з яких підтримує свою модель даних. Використання Polyglot persistence в рамках прийняття рішень має наступні переваги: хороша масштабованість застосування, ефективне управління різнорідними даними, більш швидкий час відгуку і як наслідок більш висока продуктивність. Але це вимагає розробку проміжного програмного забезпечення для інтеграції всіх баз даних, що веде до складності та підвищення вартості експлуатаційних витрат. Прикладом такої системи є проект BigDAWG (Big Data Working Group) в Массачусетському технологічному інституті, який базується за використанні трьох різних інтегрованих систем управління даними: PostgreSQL, SciDB та Accumulo.

Інша концепція Multi-model (мультимодельне зберігання) полягає в створенні єдиної бази даних для керування різними моделями даних із повністю інтегрованою серверною частиною для

задоволення системних вимог щодо продуктивності, масштабованості та відмовостійкості. Multi-model спрямована на об'єднання різних логічних моделей даних в єдиний інтегрований засіб, який використовує уніфіковану мову запитів і надає єдиний API, який використовується у всіх моделях даних. Прикладом реалізації такого підходу є СУБД Oracle Database 19c, яка підтримує декілька моделей — реляційну та нереляційну — у складі єдиної платформи. Порівняно з polyglot persistence, підхід до баз даних, що базується на кількох моделях, може зменшити витрати на інтеграцію, міграцію, розробку та обслуговування на кількох платформах.

В Інституті кібернетики імені В.М. Глушкова НАН України при виконанні проектів, що пов’язані з реалізацією процедур підтримки прийняття рішень на основі системної оптимізації, вибрано концепцію багатоваріантного зберігання (Polyglot persistence). В якості засобу для реалізації роботи з реляційною моделлю даних використовується MS SQL Server 2019. Для структурованих даних використовується мова програмування SQL. Для представлення знань у вигляді відповідної множини онтологій, що створені в Protégé та представляють собою графову базу даних, використовується RDF, а мовою запитів до даних в графовій базі даних використовується мова SPARQL. Для побудови правил виведення використовується мова SWRL.

Багатомодельна концепція дає змогу підтримати зміну джерел даних (наприклад, бази даних) у відповідь на зміну певних предметних областей, що є характерною для системної оптимізації та вимагає розгляду незалежною від програми.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Fowler Martin NoSQL DISTILLED. A Brief Guide to the Emerging World of Polyglot Persistence / Martin Fowler, Pramod J. Sadalage. Addison-Wesley Professional, 2013. - 192 p.

2. Liu Zhen Hua Multi-Model Database Management Systems - a Look Forward / Zhen Hua Liu, Jiaheng Lu, Dieter Gawlick, Heli Helskyaho // Heterogeneous Data Management, Polystores, and Analytics for Healthcare 2019. – p. 16-29.

УДК 510.635:004.891(045)

І.І. Чернега
Національна академія Служби безпеки України, Київ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ДЕРЖАВНОЇ ІНФОРМАЦІЇ

Криптографічний захист державної інформації є важливим. Існують багато методів, таких як симетричне та асиметричне шифрування, хешування та цифровий підпис. Вони можуть використовуватися окремо або в комбінації. Криптографічний захист допомагає забезпечити безпеку та конфіденційність даних в електронному вигляді. Відповідні методи шифрування та протоколи обміну ключами запобігають несанкціонованому доступу та забезпечують цілісність даних.

Криптографічний захист інформації може комбінуватися з фізичним захистом для забезпечення безпеки та конфіденційності даних у державних установах. У асиметричному шифруванні використовується два ключі - публічний та приватний. Публічний ключ використовується для зашифрування даних, а приватний - для їх розшифрування.

Хеш-функції використовуються для створення унікального "відбитка" даних, який може бути використаний для перевірки їх цілісності. Криптографічний захист інформації є важливим для захисту даних в електронному вигляді. Комбінація криптографічного захисту та фізичного захисту пристроїв та мереж може допомогти забезпечити безпеку та конфіденційність даних. Наприклад, шифрування даних за допомогою AES з використанням ключа довжиною 256 бітів є дуже надійним методом захисту.

Цифрові підписи, такі як RSA та DSA, можуть використовуватися для підтвердження автентичності та цілісності документів. Асиметричне шифрування використовує два ключі - публічний та приватний, і використовується для безпеки передачі даних в мережі Інтернет. Для симетричного шифрування використовуються AES, DES та 3DES. Хешування застосовується для захисту від несанкціонованого доступу та вторгнень, включає в собі захист паролів та перевірку цілісності даних.

Цифровий підпис - це криптографічний механізм, що дозволяє забезпечити автентифікацію та цілісність даних, Криптографічний підпис дозволяє зберігати конфіденційність, цілісність та доступність даних у державних органах. Крім того, цифровий

підпис може бути використаний для підтвердження автентичності документів та повідомлень. Державні органи можуть використовувати алгоритми, такі як RSA та DSA, для створення цифрових підписів.

Протоколи обміну ключами - це методи забезпечення безпеки при обміні даними між сторонами за допомогою обміну криптографічними ключами. Основні протоколи цього типу включають: Діффі-Геллмана, RSA та ECDH. Вони використовуються в інтернет-безпеці, банківських транзакціях та інших сферах. Наприклад, TLS використовує протокол Діффі-Геллмана. Ці протоколи допомагають захистити конфіденційну інформацію та запобігти злому системи через перехоплення ключів під час їх передачі.

Основні методи захисту - симетричне та асиметричне шифрування, хешування, криптографічний цифровий підпис та протоколи обміну ключами. Для криптографічного захисту використовуються різні технології, такі як блочне шифрування, RSA, ECC, AES, SHA, MD5 та інші.Криптографічний захист повинен використовуватись разом з іншими методами захисту та дотримуватись стандартів та рекомендацій, надійності та безпеки системи. Наприклад, важливо забезпечити фізичну безпеку пристроїв, які зберігають чутливу інформацію, а також регулярно оновлювати криптографічні ключі та протоколи, щоб запобігти їх компрометації. Потрібно дотримуватись стандартів та рекомендацій щодо криптографічного захисту, оскільки неправильне застосування може привести до порушення безпеки даних.

Загалом, криптографічні методи та технології є невід'ємною частиною захисту інформації у державних органах та дозволяють зберігати конфіденційність, цілісність та доступність данихКрім того, важливо дотримуватись стандартів та рекомендацій щодо криптографічного захисту, оскільки неправильне застосування може привести до порушення безпеки даних.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Stallings, W. (2017). Криптографія та мережева безпека: принципи та практика.

2. Paar, C., & Pelzl, J. (2010). Розумна криптографія: підручник для студентів та фахівців.

УДК 004.738 (043.2)

І.П. Швець
Національний авіаційний університет, Київ

УПРАВЛІННЯ ЖИВУЧІСТЮ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗА УМОВ НЕВИЗНАЧЕНОСТІ ВПЛИВУ ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ

Основний принцип роботи нових мереж (так званих Future Networks) – множинний доступ з часовим розділенням каналів. Якщо раніше в традиційних телекомунікаційних мережах циркулював виключно мовний трафік, а телеграфні та телетайпні повідомлення передавалися по окремим лініям зв'язку, то в сучасних телекомунікаційних мережах циркулює змішаний трафік: Triple Play (мова – відео – дані) або Quadruple Play (мова – відео – дані – мобільні абоненти).

У зв’язку із тенденцією інтенсивного застосування обчислювальної техніки та автоматизованих систем обробки інформації, особливої актуальності набуває проблема забезпечення її безпеки для ефективного передавання інформації по телекомунікаційним мережам нових поколінь. Задача оцінювання живучості інформаційно-комунікаційних систем та мереж, зокрема, телекомунікаційних мереж нових поколінь є актуальною. Більш того, нагальність цієї задачі з плином часу тільки зростатиме.

Дестабілізуючі фактори здійснюють шкідливий вплив на стійкість та живучість мережі як складної технічної системи. Найбільш інформативним підходом до кількісного оцінювання впливу дестабілізуючих факторів на характеристики телекомунікаційної мережі є статистичний підхід з аналізом ключових показників ефективності (KPIs). Цей метод широко використовується для статистичного аналізу та прогнозування параметрів та стану технічних, економічних та соціальних систем [1].

Розглянемо систему управління живучістю безпроводової телекомунікаційної мережі як невід'ємної частини мереж майбутнього покоління (*Future Networks*). Специфікою сучасних безпроводових телекомунікаційних мереж, на відміну від проводових (кабельних та оптоволоконних) є наявність зовнішніх електромагнітних завад як ненавмисного, так і навмисного характеру. Завади будь-якого характеру можна віднести до

зовнішніх дестабілізуючих факторів.

Врахування взаємного впливу дестабілізуючих факторів є нетривіальною задачею. Найбільш доступним та придатним для практичного застосування є статистичний підхід [2], зокрема, кореляційно-регресійний аналіз. Основне призначення лінійної множинної регресії полягає в аналізі зв'язку між кількома незалежними змінними (званими також регресорами) і залежної змінної. Для отримання результатів об'єднуючого характеру доцільно застосовувати узагальнені лінійні моделі [3]. Призначення як традиційних лінійних, так і узагальнених лінійних моделей полягає в вираженні взаємозв'язку між змінною, що спостерігається, Y, та рядом коваріатів (також званих змінними предіктора), X. Обидві моделі розглядають спостереження y_i як такі, що є реалізаціями випадкової величини Y. Узагальнені лінійні моделі складаються з широкого спектру моделей, які включають лінійні моделі як частинний випадок. Припущення стосовно узагальненої лінійної моделі є наступними.

1. Імовірнісний розподіл повністю визначається середнім значенням та дисперсією.

2. Дисперсія змінної Y є функцією середнього значення.

Щоб підкреслити відмінність другої властивості, дисперсію D_{Yi} виражають як $D_{Yi} = \frac{\phi V(\mu_i)}{\omega_i}$, де $\mu_i = E[Y_i]$ – середнє значення залежної *i*-ї залежної змінної; V (x), так звана дисперсійна функція, є заданою функцією; параметр φ масштабує дисперсію; ω_i - константа, яка визначає вагу або надійність *i*-му спостереженню.

Враховуючи, що уведені узагальнення моделі формально можна розглядати як множники масштабування, розглянемо задачу множинної лінійної регресії за тими же показниками, що й у звичайному випадку..

Технічні показники функціонування мережі, як правило, представляються таблицями статистичних даних:

$$\begin{pmatrix} y(1) & y(2) & \cdots & y(i) & \cdots & y(N) \\ x_1(1) & x_1(2) & \cdots & x_1(i) & \cdots & x_1(N) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_j(1) & x_j(2) & \cdots & x_j(i) & \cdots & x_j(N) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_k(1) & x_k(2) & \cdots & x_k(i) & \cdots & x_k(N) \end{pmatrix}.$$

У загальному випадку, процедура побудови множинної регресії полягає в оцінюванні параметрів лінійного рівняння. Функціональна залежність результату від факторів впливу представляється рівнянням регресії:

$$\mathbf{E}\left[\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_m \end{pmatrix}\right] = \begin{pmatrix} E[y_1] \\ E[y_2] \\ E[y_3] \\ \vdots \\ E[y_m] \end{pmatrix} = \begin{pmatrix} 1 & x_{11} & x_{12} & \dots & x_{1n} \\ 1 & x_{21} & x_{22} & \dots & x_{2n} \\ 1 & x_{31} & x_{32} & \dots & x_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix} \cdot \begin{pmatrix} \theta_0 \\ \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{pmatrix},$$

або те ж саме в компактному вигляді: $E[\vec{y}] = \mathbf{X}\vec{\theta}$.

В якості основних характеристик статистичного зв'язку зазвичай використовують матриці коефіцієнтів множинної кореляції і системи рівнянь множинної лінійної або поліноміальної регресії [4].

Розглянемо процес прогнозу параметрів мережі як завдання передбачення *k*-ї змінної Y_k, $k = \overline{1, N}$ по *M* змінним X_m, *m=1,2,…,M; m≠k*. У загальному випадку *M≠N*. При *m=1* маємо рівняння лінійної або поліноміальної регресії незалежної змінної X_m на залежну змінну Y_k, при *m*>1маємо систему рівнянь множинної регресії змінних $X_1,X_2,\dots,X_m$ на Y_k. (Мається на увазі функціональна, а не статистична залежність.) У розглянутій задачі незалежні змінні $X_1,X_2,\dots,X_m$ – це випадкові величини, які не обов'язково є статистично незалежними.

Змінну Y_k апроксимуємо функцією регресії $\psi(\cdot)$ що містить оцінки *KPIs* й невідомі коефіцієнти. Рівняння моделі лінійної регресії незалежних змінних $X_1,X_2,\dots,X_m$ на залежну змінну Y_k запишемо в наступному вигляді:

$$Y_k = a_{0k} + a_{1k}X_1 + \ldots + a_{mk}X_m + \varepsilon, \qquad (1)$$

де ε – помилка апроксимації.

Нехай $X_{1j} = X_1^j$. Тоді можна записати рівняння поліноміальної регресії у вигляді

$$Y_k = a_{0k} + a_{1k}X_1 + a_{2k}X_1^2 \ldots + a_{mk}X_1^m + \varepsilon. \qquad (2)$$

Параметри моделі регресії оцінюються за вибіркою обсягу, взятої з деякою генеральної сукупності. Теоретично генеральна сукупність має нескінченний об'єм або є весь набір даних, який існує в принципі.

Вибірка формується таким чином. За результатами тесту функціонування мережі фіксуємо першу вибірку незалежних змінних $X_{11}, X_{12}, \ldots, X_{1m}$ і розраховуємо залежну змінну Y_1. Потім фіксуємо другу вибірку незалежних змінних $X_{21}, X_{22}, \ldots, X_{2m}$ і розраховуємо залежну змінну. Продовжуємо процедуру до отримання N змінних. Отримуємо вибірку з спостережень:

$$\{Y_1 : X_{11}, X_{12}, \ldots, X_{1m}\}, \{Y_2 : X_{21}, X_{22}, \ldots, X_{2m}\}, \ldots, \{Y_N : X_{N1}, X_{N2}, \ldots, X_{Nm}\}.$$

Система рівнянь множинної лінійної регресії набуває вигляду:

$$\left.\begin{array}{l} Y_1 = a_{01} + a_{11}X_{11} + \ldots + a_{m1}X_{1m} + \varepsilon_1 \\ Y_2 = a_{02} + a_{12}X_{21} + \ldots + a_{m2}X_{2m} + \varepsilon_2 \\ \ldots \\ Y_k = a_{0k} + a_{1k}X_{k1} + \ldots + a_{mk}X_{km} + \varepsilon_k \\ \ldots \\ Y_N = a_{0N} + a_{1N}X_{N1} + \ldots + a_{mN}X_{Nm} + \varepsilon_N \end{array}\right\}, \qquad (3)$$

де $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$, $k = \overline{1, N}$ – невідомі коефіцієнти;

$\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \ldots, \varepsilon_N\}$ – випадкові помилки, які логічно вважати нормальними однаково розподіленими з параметрами $\{0, \sigma_\varepsilon^2\}$.

Для отримання оцінок за методом найменших квадратів необхідно мінімізувати суму S_k квадратів відхилень в кожній точці. Найкраще наближення відповідає мінімальній величині виразу

$$S_k = \sum_{k=1}^{N} \left(Y_k - a_{0k} - a_{1k}X_{k1} - \ldots - a_{mk}X_{km}\right)^2 \cdot \qquad (4)$$

Величина S_k є мірою помилки, пов'язаної з прив'язкою наявних даних до обраної моделі регресії. Мінімум S_k досягається диференціюванням останнього виразу за коефіцієнтами $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$, $k = \overline{1, N}$ прирівнюванням відповідних похідних нулю

і розв'язанням системи рівнянь відносно $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$,.
Отримуємо систему рівнянь для оцінки частинних коефіцієнтів регресії:

$$\left.\begin{array}{l} \overline{Y}_1 = \overline{\alpha}_{01} + \overline{\alpha}_{11} X_{11} + \ldots + \overline{\alpha}_{m1} X_{1m} \\ \overline{Y}_2 = \overline{\alpha}_{02} + \overline{\alpha}_{12} X_{21} + \ldots + \overline{\alpha}_{m2} X_{2m} \\ \quad \ldots \\ \overline{Y}_k = \overline{\alpha}_{0k} + \overline{\alpha}_{1k} X_{k1} + \ldots + \overline{\alpha}_{mk} X_{km} \\ \quad \ldots \\ \overline{Y}_N = \overline{\alpha}_{0N} + \overline{\alpha}_{1N} X_{N1} + \ldots + \overline{\alpha}_{mN} X_{Nm} \end{array}\right\}. \qquad (5)$$

Тут $\overline{\alpha}_{0k}, \overline{\alpha}_{1k}, \ldots \overline{\alpha}_{,mk}$ – оцінки для $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$.

Оцінки є незміщеними і ефективними, тобто мають мінімальну дисперсію для вибірки $X_1, X_2, \ldots, X_m$ серед всіх лінійних оцінок для прогнозування змінних Y_k, $k = \overline{1, N}$.

Регресійні коефіцієнти представляють вклади кожної незалежної змінної в прогнозування залежної змінної. Для відбору остаточного рівняння регресії зазвичай використовують два протилежних критерії.

1. Щоб зробити рівняння корисним для передбачення, спостерігач повинен прагнути включити в модель по можливості більше незалежних змінних з тим, щоб можна було більш надійно визначити прогнозовані величини.

2. Через витрати, пов'язані з отриманням інформації при великій її кількості і подальшою перевіркою, необхідно прагнути, щоб рівняння включало якнайменше незалежних змінних.

Введемо поняття відсутніх значень. Представимо систему рівнянь моделі множинної лінійної регресії (3) в матричної формі:

$$\mathbf{Y} = \overline{\mathbf{X}}\mathbf{B} + \mathbf{E}, \qquad (6)$$

де $\overline{\mathbf{X}} = \begin{pmatrix} 1 & X_{11} & \cdots & X_{1m} \\ 1 & X_{21} & \cdots & X_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & X_{N1} & \cdots & X_{Nm} \end{pmatrix}$ – так звана матриця плану.

Для регресійній моделі, по суті, це матриця незалежних змінних, доповнена першим стовпцем вагових коефіцієнтів поточних спостережень; $\mathbf{B}^T = \{\beta_0, \beta_1, \ldots, \beta_m\}$ – вектор параметрів рівняння

регресії; $\mathbf{E}^{\mathrm{T}}=\{\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_k,\ldots,\varepsilon_N\}$ – вектор помилок оцінювання, що має багатовимірний гаусівський розподіл з нульовим вектором математичних сподівань і матрицею дисперсій виду $\sigma^2\mathbf{I}$; $\mathbf{I}$ – одинична матриця; T – символ транспонування.

Тоді рівняння (4) можна представити в матричному вигляді як

$$S=\left(\mathbf{Y}-\overline{\mathbf{X}}\mathbf{B}\right)^{\mathrm{T}}\left(\mathbf{Y}-\overline{\mathbf{X}}\mathbf{B}\right) \tag{7}$$

Вектор оцінок за методом найменших квадратів є рішення системи нормальних рівнянь

$$\left(\mathbf{X}^{\mathrm{T}}\overline{\mathbf{X}}\right)\mathbf{B}=\mathbf{XY}, \tag{8}$$

розв'язок якої має вигляд

$$\mathbf{B}=\left(\mathbf{X}^{\mathrm{T}}\overline{\mathbf{X}}\right)^{-1}\left(\mathbf{XY}\right)\cdot \tag{9}$$

З урахуванням того, що матриця дисперсій вектора помилок оцінювання описується виразом $\sigma^2\mathbf{I}$, кореляційна матриця вектора $\mathbf{B}$ дорівнює $\mathbf{R}_{\mathrm{B}}=\sigma^2\left(\mathbf{X}^{\mathrm{T}}\overline{\mathbf{X}}\right)^{-1}$.

Відзначимо також, що при збільшенні кореляції між різними ключовими показниками ефективності матриця $\mathbf{X}^{\mathrm{T}}\overline{\mathbf{X}}$ буде мати діагонально-домінантну структуру, тобто діагональні елементи будуть превалювати над сумами елементів за відповідними рядками. При цьому процедури пошуку рішення рівнянь (6) і (7) спрощуються.

чевидно, в даному випадку простіше замість оптимальної оцінки як вихідної величини, яка визначається матричних рівнянням, шукати оптимальну оцінку як рішення двоїстого йому різницевого рівняння. Коефіцієнти різницевого рівняння визначаються статистикою спостережень і завад і в загальному випадку є змінними величинами, залежними від часу. Перевагою такого підходу є те, що якщо навіть не вдається отримати аналітичний розв'язок різницевого рівняння, то завжди можна отримати його чисельне рішення на обчислювальній машині. Більш того, рішення можна отримувати в реальному масштабі часу з урахуванням знову одержуваної інформації про зміни параметрів спостережень і перешкод.

Слідуючи [4], побудуємо ітераційний алгоритм розв'язання рівняння (6) у вигляді

$$\mathbf{FB}\left[\overline{\mathbf{X}}(\mathrm{k})-\overline{\mathbf{X}}(\mathrm{k}-1)\right]=\mathbf{G}\left[\mathbf{Y}-\mathbf{E}-\overline{\mathbf{X}}(\mathrm{k})\mathbf{B}\right], \tag{10}$$

де **F** та **G** – матричні множники, визначники яких не дорівнюють нулю, або ненульові скалярні множники.

Ці множники вибираються таким чином, щоб забезпечити максимальну швидкість збіжності без втрати стійкості алгоритму (10). Для оптимального вибору значень **F** та **G** можна застосувати до рівняння (10) операцію *z*-перетворення

$$\mathbf{FB}\left[\overline{\mathbf{X}}(z)\left(1-z^{-1}\right)\right]=\mathbf{G}\left[\mathbf{Y}-\mathbf{E}-\overline{\mathbf{X}}(z)\mathbf{B}\right], \qquad (11)$$

і обчислити корені характеристичного рівняння, які повинні бути по модулю менше одиниці. Тоді загальний розв'язок рівняння (11) при необмеженому зростанні числа ітерацій $k\to\infty$ асимптотично сходиться до точного рішення рівняння (6). Швидкість збіжності залежить від величини максимального по модулю кореня характеристичного рівняння. Задаючись величиною модуля відносної помилки рішення, можна оцінити потрібне число ітерацій як локальну або нелокальну характеристику ефективності пошуку рішення.

Конкретизуючи чисельні значення результату y_i, i=1,2,…,N проаналізуємо ключові показники ефективності інформаційно-комунікаційних мереж.

Ключовими параметрами є затримка передачі, пропускна здатність, втрати пакетів і рівень безпеки. Ці параметри мають найбільший вплив на результуючу якість сервісу. В роботі [1] відзначається, що число *KPIs*, які обирають для аналізу, має бути мінімальним, причому у всіх випадках недоцільно брати більше 20 таких показників. Ці міркування враховані при завданні набору *KPIs*.

У якості параметрів задачі, що оптимізуються, обрано такі:

– затримка передачі τ;

– пропускна спроможність C_p;

– втрати пакетів при передачі даних L_p;

– рівень безпеки та захисту даних при передачі по мережі D_{sp};

– якість *Web*-сервісу;

– якість передачі аудіо (звукові файли, звичайна й *IP*-телефонія);

– швидкість і надійність обміну файлами по протоколу *FTP*;

– швидкість і надійність роботи електронної пошти (*E-mail*);

– якість передачі відео.

Розглянуто гіпотетичну мережу *WLAN IEEE* 802.11*n*, дані для розрахунку параметрів якої взяті з роботи [1]. Для розрахунків

використовувалася програма множинного кореляційного аналізу, наведена в [4] і модифікована для даної задачі.

У табл. 1 наведені частинні коефіцієнти кореляції параметрів, що оптимізуються. За цими коефіцієнтами кореляції в подальшому з використанням рівнянь (1)–(3) можна розраховувати частинні коефіцієнти регресії.

Таблиця 1

Коефіцієнти взаємної кореляції параметрів, що оптимізуються

Параметр	τ	C_p	L_p	$\mathbf{D_{sp}}$	**Web**	Аудіо	*FTP*	*E-mail*	Відео
τ	1,0	0,98	0,69	0,89	0,75	0,85	0,27	0,17	0,87
C_p	0,98	1,0	0,68	0,86	0,76	0,64	0,75	0,22	0,89
L_p	0,69	0,68	1,0	0,69	0,36	0,50	0,63	0,34	0,84
D_{sp}	0,89	0,86	0,69	1,0	0,77	0,56	0,61	0,78	0,82
Web	0,75	0,76	0,36	0,77	1,0	0,30	0,57	0,30	0,53
Аудіо	0,85	0,64	0,50	0,56	0,30	1,0	0,44	0,36	0,67
FTP	0,27	0,75	0,63	0,61	0,57	0,44	1,0	0,16	0,79
E-mail	0,17	0,22	0,34	0,78	0,30	0,36	0,16	1,0	0,30
Відео	0,87	0,89	0,84	0,82	0,53	0,67	0,79	0,30	1,0

Між основними ключовими параметрами виявляється сильна кореляція. Це пояснюється тим, що вони дають значний вплив на вимоги до живучості. Виняток становить електронна пошта, оскільки, на відміну від потокового аудіо, відео, Web-сервісу і передачі файлів по протоколу FTP, для неї не критичні ні смуга пропускання каналу, ні затримка доставки. Однак необхідно відзначити, що параметр D_{sp} – рівень безпеки та захисту даних є критичним практично для всіх представлених параметрів, оскільки навіть для таких видів еластичного трафіку, як електронна пошта, захист даних є невід'ємною вимогою забезпечення якості сервісу *QoS*.

Результати кореляційного аналізу служать також ключовим індикатором моніторингу та регулювання потокових даних і *Web*-сервісу. Це необхідно для забезпечення безпечної передачі

інформації по мережі, прогнозування і запобігання перевантажень контрольованого мережного сегмента. Таким чином, поточний моніторинг і управління рівнем живучості мережі, які є невід'ємною частиною завдання загального управління якістю сервісу, можна успішно здійснювати статистичними методами, зокрема, методом кореляційно-регресійного аналізу.

Крім того, необхідно відзначити, що повністю скомпільована програма розрахунків займає в пам'яті обчислювального пристрою від 80 до 500 кілобайт в залежності від масштабу мережі і обсягу оброблюваної вибірки. Оскільки в даний час практично будь-який мережний вузол, по суті, являє собою спеціалізований обчислювач або навіть багатопроцесорну систему, завдання апаратурної реалізації запропонованого методу може вирішуватися порівняно просто.

Основний недолік будь-якого з методів оцінювання $\bar{\mathbf{X}}$ та $\boldsymbol{\Sigma}$ (або, що еквівалентно, матриці кореляцій **R**), коли відсутні деякі значення, пов'язаний з тим, що їх статистичні властивості за рідкісним винятком невідомі. Крім того, застосування таких методів часто призводить до зміщених оцінок. Компроміс між цими критеріями може бути досягнутий за рахунок вибору "найкращого" рівняння, що включає оптимальну кількість незалежних змінних. В роботі для пошуку "найкращого" рівняння регресії застосований крокový метод (покрокова регресія).

З огляду на все це елементи вибірки та/або змінні з відсутніми значеннями повинні бути видалені так, щоб забезпечити баланс між рештою числа змінних і числом елементів, що залишилися, тобто, максимізувати число комплектних елементів вибірки.

Отже, якщо елемент містить багато пропусків, його потрібно видалити. З іншого боку, слід видалити змінну, якщо її значення невідомо для більшості елементів. Після цього можна звичайним чином використовувати метод найменших квадратів або процедури багатовимірного статистичного аналізу

Одним з рішень є покрокова регресія (пряма), коли незалежні змінні одна за одною включаються в підмножину згідно попередньо заданому критерію. У той же час деяка змінна може бути замінена іншою змінною, яка не входить в набір, або видалена з нього. Сукупність критеріїв, що визначають, які змінні включати, замінювати і видаляти, називається покроковою процедурою.

За допомогою покрокової процедури виходить упорядкований список предикторів. Наприклад, якщо p=5, такий список може мати вигляд X_2,X_5,X_1,X_4 і X_3. Для визначення «найкращої» підмножини з цього списку вибираються $m \leq p$ перших змінних так, щоб

a) вони, можливо, краще передбачали Y і $\overline{\mathbf{X}}$,

b) їх число t було якомога менше.

Іншими словами, економний набір складається зі змінних впорядкованого списку, які мають найбільш високу здатність до прогнозування. У прикладі, наведеному вище, такий набір міг би складатися тільки з змінних X_2 і X_3, якби регресія по ним була майже такою ж «якісною», як і регресія з X_2,X_5,X_1,X_4 та X_3.

Процедура визначення числа t називається правилом зупинки. Методика безперервної діагностики мережі, тобто аналізу впливу дестабілізуючих факторів на загальну ефективність функціонування мережі полягає в розбитті процесу на наступні взаємопов'язані етапи:

1. Проводиться діагностика на фізичному рівні для виключення помилок і правильної інтерпретації результатів подальшого тестування.

2. Проводиться діагностик термінальних вузлів мережі шляхом стресового тестування мережі в двох режимах:

– режим калібрування з навантаженням тільки на мережу для виявлення помилок апаратної і програмної реалізації;

– режим з навантаженням тільки на мережу для виявлення проблем взаємодії станцій, вузьких місць на сервері і в каналах зв'язку.

3. На наступному етапі проводиться діагностика каналів зв'язку і серверів з використанням аналізаторів протоколів і аналізаторів серверів. Спільна обробка і аналіз отриманих в процесі тестування швидкісних характеристик, трендів характеристик мережного трафіку і лічильників серверів також здійснюється статистичними методами. Така методика дозволяє встановити причини неправильного функціонування того чи іншого каналу зв'язку (або сервера) та дати кількісні оцінки впливу внутрішніх та зовнішніх дестабілізуючих факторів на ключові показники ефективності мереж.

За результатами теоретичного аналізу та обчислювального експерименту встановлено, що між основними ключовими

параметрами впливу дестабілізуючих факторів на якість сервісу інформаційно-комунікаційної мережі виявляється сильна кореляція. Однак параметр D_{sp} – рівень безпеки та захисту даних є критичним практично для всіх представлених параметрів, оскільки навіть для таких видів еластичного трафіку, як електронна пошта, захист даних є невід'ємною вимогою забезпечення якості сервісу *QoS*. Завдяки використанню імовірнісного підходу отримані статистичні характеристики стійкості мережі до впливу дестабілізуючих факторів: вектор математичних сподівань та матрицю кореляції. При стаціонарності (або хоча б локальній стаціонарності на інтервалі спостереження) вхідних сигналів, шумів та завад можна отримати асимптотичні оцінки та зробити прогноз живучості з задовільною точністю. Однак при наявності суттєвої нестаціонарності отримані оцінки можуть ставати не спроможними. Відповідно, інтервал, на якому точність прогнозу може лишатися у припустимих межах, ставатиме занадто малим для практичних застосувань. Цей недолік випливає з іманентних властивостей нестаціонарних процесів, обумовлених відсутністю позитивного визначення нестаціонарності. Обмеження, притаманні звичайним методам множинної кореляції та регресії, долаються при застосуванні послідовного (покрокового) кореляційно-регресійного аналізу. При уточненні моделі нестаціонарності водночас зменшуватиметься й обчислювальна складність. Зокрема, при застосуванні моделі процесу зі стаціонарним математичним сподіванням та з нестаціонарною дисперсією квадратичного зростання обчислювальна складність буде асимптотично знижуватися до поліноміальної.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Kreher R. (2006). UMTS Performance Measurement: A Practical Guide to KPIs for the UTRAN Environment. – John Wiley & Sons Ltd, The Atrium, of Computational Statistics: Concepts and Methods (2nd Ed.), Springer- Southern Gate, Chichester, 227 pp.

2. Gentle J. E., Härdle W. K., Mori Y. (Eds.) (2012). Handbook Verlag Berlin Heidelberg, 2012. – 1192 pp.

3. Deb A. Control systems analysis and identification / CRC Press, 2018. – 364 p.

4. Afifi A. (1979) Statistical Analysis, Second Edition: A Computer Oriented Approach 2nd Edition /A. A. Afifi, S. P. Azen. - Academic Press; 2 ed. – 442 pp.

УДК 510.635:004.891(045)

І.О. Шиян
Національна академія Служби безпеки України, Київ

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ КОНТРОЛЮ ЗА ДОПОМОГОЮ IP-КАМЕР У БОРОТЬБІ ПРОТИ АГРЕСОРА

У 2022 році практично неможливо обійтися без камер відеоспостереження, особливо набрали популярності IP-камери [1]. Вони призначені для запобігання крадіжкам майна в магазинах, будинках, бізнес-закладах. Але іноді камери служать помічником для стеження або крадіжки. Саме тому важливо дослідити вразливості IP-камер, до яких належать всі проблеми, пов'язані з реалізацією функціональності IP-камер. Головна з них полягає в тому, що вартість апаратної частини камер значно менша, ніж витрати на розробку прошивки. Результатом прагнення компаній заощадити стають найдивніші рішення, наприклад:

1. не оновлювані прошивки або прошивки без автоматичного оновлення;
2. можливість отримати доступ до веб-інтерфейсу камери шляхом багаторазових спроб ввести неправильний пароль або натискання кнопки «Скасувати»;
3. відкритий доступ до всіх камер із сайту виробника;
4. заводський сервісний обліковий запис зі стандартним паролем або без нього, що не відключається (таку вразливість використовувала в 2016 році хакерська група Lizard Squad для створення DDoS-ботнета з потужністю атак до 400 ГБ/с з камер відеоспостереження);
5. можливість несанкціонованої зміни налаштувань навіть при включеній авторизації та забороні анонімного доступу;
6. відсутність шифрування відеопотоку та/або передача облікових даних у відкритому вигляді;
7. використання вразливого веб-сервера GoAhead;
8. тиражування вразливих прошивок (поширене серед китайських виробників пристроїв);
9. вразливості пристроїв для зберігання відео - наприклад, зовсім недавно була опублікована інформація про проникнення на мережні накопичувачі Synology і Lenovo Iomega шкідливих файлів, що видаляють або шифрують і вимагають викуп [2].

CVE - (Common Vulnerabilities and Exposures) - база даних загальновідомих уразливостей інформаційної безпеки. Кожній вразливості надається ідентифікаційний номер виду CVE-рік-номер, опис та ряд загальнодоступних посилань з описом [3].

Навіть якщо виробники камер виправлять усі помилки та випустять ідеальні з точки зору безпеки камери, це не врятує ситуацію, оскільки нікуди не подінуться рукотворні вразливості [4], причина яких у людях, які обслуговують обладнання, наприклад, використання паролів за замовчуванням, якщо є можливість змінити їх; відключення шифрування або VPN, якщо камера дозволяє його використовувати (заради справедливості скажемо, що далеко не всі камери мають достатню продуктивність для такого режиму роботи, перетворюючи цей спосіб захисту на чисту воду декларацію); відключення автоматичного оновлення прошивки камери; забудькуватість або недбалість адміністратора, що не оновлює прошивку пристрою, який не вміє робити це автоматично.

За допомогою зламаних IP-камер відеоспостереження на території країни-агресора або окупованих територіях особливо цінуються камери з виходом на дорогу та підозрілі будівлі. Завдяки цим даним можна стежити за рухом окупантів і коригувати артилерію на техніку і бази навіть не доїхавши до території України. Дані зі зламаних камер передаються в Службу безпеки України для того, щоб зібрати повну картину на окупованих територіях.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Що таке IP-камера: основні відмінності від аналогових та цифрових камер відеоспостереження, URL: https://smartel.ua/articles/chto-takoe-ip-kamera-osnovnye-otlichiya-ot-analogovykh-i-tsifrovykh-kamer-videonablyudeniya/

2. Вразливість безпеки у стандартній реалізації Dahua Open Network Video Interface Forum. URL: https://www.onvif.org/

3. Курс Cisco Networking Academy: IT Essentials.

4. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні інформаційні: Мережі, технології, безпека, економіка, регулювання. – Видання друге (доповнене). – / За загальною ред. Довгого С.О. – К.: «Азимут-Україна». – 2013. – 608 с.

Наукове видання

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ
XIV МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖНІ ТЕХНОЛОГІЇ»

(CSNT-2023)

13–14 квітня 2023 року

Тези доповідей надруковані в авторській редакції однією із двох робочих мов конференції: українською, англійською.