МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

УДК 681.518.54

Тези доповідей

Міжнародної науково-практичної конференції

“Інформаційна безпека та інформаційні технології”
“Information Security and Information Technologies”

24–25 квітня 2019 р.

Харків 2019

УДК 681.518.54

Матеріали Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”: тези доповідей, 24 – 25 квітня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – 68 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор.

СЕКЦІЯ 1
ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 681.3

С.В. Герасимов[1], В.В. Штрибець[2]

gsvnr@ukr.net

[1]*Харківський національний університет Повітряних Сил імені Івана Кожедуба, м. Харків*
[2]*Державний університет інфраструктури та технологій, м. Київ*

РОЗРОБКА МЕТОДУ ДІАГНОСТИЧНОГО КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ ДВИГУНІВ ЗАСОБІВ ВОДНОГО ТРАНСПОРТУ ДЛЯ ЗМЕНШЕННЯ ВИТРАТ НА ПЕРЕВЕЗЕННЯ ВАНТАЖІВ

Останнім часом збільшилась частина вантажоперевезень водним транспортом [1]. Для економії коштів при перевезені вантажів або при перевезені продуктів харчування актуальним є завдання планування (прокладання) оптимального маршруту для зменшення часу руху. Однак, при цьому слід враховувати й технічний стан засобів водного транспорту, який може значно впливати на вартість перевезення. Це забезпечить оптимальні (планові) витрати на перевезення вантажів за допомогою засобів водного транспорту та дозволить зменшити (а може і, взагалі, уникнути), додаткові (непланові) витрати при цьому.

Запропонований метод спрямований на досягнення необхідної достовірності контролю технічного стану [2] двигунів засобів водного транспорту за допомогою спектрального аналізу випадкових сигналів, які виникають при наявності несправностей або порушені алгоритму роботи справних систем.

Методи оптимізації форми амплітудно-частотної характеристики (АЧХ) фільтрів для спектрального аналізу випадкових сигналів отримано для двох критеріїв [2]:

– мінімуму середньоквадратичної похибки апроксимації ідеальної, прямокутної функції спектрального вікна реальної функцією;

– мінімуму впливу бічних пелюсток функції спектрального вікна на похибка вимірювання оцінки спектральної щільності потужності (СЩП).

Використання зазначених критеріїв обумовлено двома можливими постановками задачі оптимізації. У першому випадку (перша задача оптимізації) основною вимогою, що пред'являються до оптимальної АЧХ фільтра, є забезпечення мінімуму середньоквадратичної похибки апроксимації ідеальної АЧХ, але при цьому не накладається ніяких обмежень на поведінку АЧХ як у смузі аналізу, так і поза нею. У другому випадку (друга задача оптимізації) основна увага приділена забезпеченню мінімуму впливу бічних пелюсток функції спектрального вікна на похибка вимірювання оцінки СЩП. Ці дві задачі оптимізації охоплюють найбільш поширені вимоги, що пред'являються до функції спектрального вікна при вирішенні практичних завдань синтезу фільтрів, які використовуються при спектральному аналізі випадкових сигналів.

При розв'язанні першої задачі оптимізації отримана форма спектральної характеристики $\Phi(\omega)$ при заданих значеннях смуги пропускання $\Delta\omega$, часу вимірювання (аналізу) T і змінної $\Omega_i = \omega \pm_{i=1,2} \omega_0 \mp_{i=3,4} \frac{\Delta\omega}{2}$:

$$\Phi(\omega) = \frac{T}{2\Delta\omega}\sum_{i=1}^{4}(-1)^{i-1}\left[\mathrm{si}\left(T\Omega_i\right)+\frac{\pi}{2}\right] = \frac{T}{2\Delta\omega}\times$$

$$\times\sum_{i=1}^{4}(-1)^{i-1}\,\mathrm{si}\,T\Omega_i + \frac{T}{2\Delta\omega}\frac{\pi}{2}\sum_{i=1}^{4}(-1)^{i-1} = \frac{T}{2\Delta\omega}\sum_{i=1}^{4}\mathrm{si}\left(T\Omega_i\right).$$

При розв'язанні другої задачі оптимізації отримана форма спектральної характеристики $\Phi'(\omega)$:

$$\Phi'(\omega) = \frac{T}{2\Delta\omega}\sum_{i=1}^{4}(-1)^{i-1}\,\mathrm{f}\left(T\Omega_i\right),$$

де $\mathrm{f}(x) = \mathrm{Si}(x) - \frac{1-\cos x}{x}$.

Застосування запропонованих оптимальних фільтрів при спектральному аналізі випадкових сигналів діагностування технічного стану двигунів засобів водного транспорту дозволяє своєчасно виявити можливі несправності чи порушення у режимах роботи (відповідно до заздалегідь відомих, справних). Своєчасне виявлення відмов двигунів засобів водного транспорту дозволить уникнути додаткових витрат під час перевезення вантажів, тобто зменшити додаткові (непланові) витрати.

Список літератури

1. С. В. Герасимов, Ю. Є. Шапран, та В. В. Кірвас, "Розробка та дослідження методу розрахунку достовірності вимірювального контролю параметрів радіотехнічних систем морського транспорту", *Системи озброєння і військова техніка*, вип. 4 (52), с. 5 – 10, 2017.

2. С. В. Герасимов, "Постановка проблеми розробки оптимальної методики контролю параметрів технічних систем при експлуатації за станом", *Системи обробки інформації*, вип. 9 (116), с. 7 – 11, 2013.

УДК 004.056.55: 003.26

О. М. Грищук

Ol.Hry@i.ua

Житомирський військовий інститут імені С. П. Корольова, м. Житомир

МАТЕМАТИЧНИЙ ОПИС КРИПТОСИСТЕМИ ФРЕДГОЛЬМА

Проблема кібербезпеки в наш час набуває особливої актуальності [1]. З поміж багатьох підходів до її вирішення особливе місце та роль відводиться криптографії [2]. Поряд з тим, зростання потужності обчислювальних засобів (створення квантових комп'ютерів) та доступність інформаційних технологій до широкого кола користувачів не виключає знаходження ними можливостей для взлому відомих криптоалгоритмів за прийнятний час. Тому задача забезпечення криптостійкості й надалі актуалізується.

Аналіз відомих підходів до забезпечення криптостійкості показав, що більшість з них ґрунтуються на складності вирішення задач факторизації, дискретного логарифмування тощо (для асиметричних криптосистем) або задачах комбінаторної складності (для симетричних криптосистем). Поряд з тим нині існує й ряд інших математичних задач, складність вирішення яких може бути покладена в основу забезпечення криптостійкості алгоритмів шифрування. Таким чином, розроблення нових та адекватних моделей криптографічного захисту для подальшого створення на їх основі відповідних криптоалгоритмів та ефективних засобів безпеки нового покоління, є актуальним науковим та практичним завданням.

Результати вивчення сучасних наукових джерел з питань криптографії показують, що на сьогодні існує ряд математичних задач на основі яких розвинуто чималу кількість нових напрямів у криптографії. Зокрема це когнітивна криптографія, криптографія на основі теорії динамічного хаосу, конструктивна, квантова та постквантова криптографія. Також нині інтенсивно розвивається криптографія на основі алгоритмів ДНК, проксі криптографія, криптографія на основі атрибутів, пакетна та некомутативна криптографія тощо.

Найбільший інтерес з точки зору безпеки на сьогодні становить інтегральна криптографія [3]. Відсутність на сьогодні науково обґрунтованих моделей криптосистем на основі інтегральної криптографії спонукала до формалізації опису однієї з таких систем, яка може бути побудована на основі інтегральних рівнянь Фредгольма першого роду.

Математичний опис криптосистеми Фредгольма матиме наступний вигляд.

Процедура шифрування (пряма задача).

Нехай відправник A повинен відправити незахищеним каналом зв'язку деяке повідомлення $z(s)$ отримувачу B. Повідомлення $z(s)$ є вихідними даними, що підлягатимуть шифруванню A та дешифруванню B відповідно.

Процедура шифрування, яка здійснюється відправником A у відношенні до повідомлення $z(s)$ полягає у вирішенні прямої задачі, яка може бути описана інтегральним рівнянням Фредгольма першого роду

$$\int_a^b K(x,s)\, z(s)\, ds = u(x), \qquad 1)$$

де $K(x,s)$ – секретний ключ (ядро інтегрального рівняння); $z(s)$ – вихідні дані, що підлягають шифруванню/дешифруванню (відкритий текст, вихідні дані); $u(x)$ – зашифровані дані (шифрограма). Таким чином, по відкритому каналу від відправника A до одержувача B передаються зашифровані дані $u(x)$.

Процедура дешифрування (обернена некоректна задача).

Одержувач B отримує від відправника A зашифровані дані $u(x)$. Задача одержувача B полягає у дешифруванні зашифрованих даних $u(x)$ та прочитанні вихідного повідомлення $z(s)$ відправника A. У формалізованому вигляді процедура дешифрування зводиться до вирішення зворотної некоректної задачі (1).

Задача противника E, який має доступ до каналу зв'язку полягає у перехопленні зашифрованих даних $u(x)$ та читанні вихідного повідомлення $z(s)$ у разі злому криптоалгоритму (підбору секретного ключа $K(x,s)$), або їх модифікації.

Таким чином, принципи функціонування криптосистеми зводиться до вирішення прямої (коректної) задачі – процедура шифрування та оберненої (некоректної) задачі – процедура дешифрування, які описуються інтегральним рівнянням Фредгольма першого роду (1).

Список літератури

1. Р. В. Грищук, та Ю. Г. Даник, *Основи кібернетичної безпеки: монографія*, Житомир, Україна: ЖНАЕУ, 2016.

2. R. Hryshchuk, S. Yevseiev, and A. Shmatko *Construction Methodology of Information Security System of Banking Information in Automated Banking Systems : Monograph*, Vienna. Austria: Premier Publishing s.r.o., 2018.

3. Г. К. Броншпак, И. А. Громыко, С. И. Доценко, и Е. Л. Перчик, "Криптография нового поколения: Интегральные уравнения как альтернатива алгебраической методологии", *Прикладная электроника*, №3, с. 337-349, 2014.

УДК 621.317

О.А. Дакі, А.О. Трофименко

olena_daki@ukr.net

Державний університет інфраструктури та технологій, м. Київ

ОБҐРУНТУВАННЯ ПРИНЦИПІВ ПОБУДОВИ АВТОМАТИЧНИХ ПРИЛАДІВ ДЛЯ КОНТРОЛЮ ПАРАМЕТРІВ СИСТЕМ УПРАВЛІННЯ ТА НАВІГАЦІЇ ЗАСОБІВ ВОДНОГО ТРАНСПОРТУ

Системи управління та навігації засобів водного транспорту призначені для забезпечення контролю за значеннями параметрів, які характеризують їх рух. Додержання оптимального маршруту водного транспорту у складних метеорологічних умовах, у ночі майже неможливий без навігаційних приладів, які здатні визначати інформацію про положення засобу водного транспорту на маршруті, напрямок його руху тощо. При додержанні заздалегідь прокладеного маршруту за даними навігаційних приладів (при їх справності та потрібної точності визначення параметрів) забезпечується не тільки економність вантажоперевезень, але й безпека судноплавства [1].

Правильність показань навігаційних приладів залежить від їх технічного стану, який може змінюватися під час експлуатації, особливо в умовах агресивного морського оточення. Тому необхідна апаратура контролю технічного стану навігаційних приладів засобів водного транспорту.

Реалізація існуючого способу визначення характеристик навігаційних приладів засобів водного транспорту ґрунтується на застосуванні генераторів сигналів синусоїдної форми. Однак такі генератори не дозволяють оперативно контролювати технічний стан навігаційних приладів засобів водного транспорту, мають значний час вимірювання параметрів за рахунок послідовного встановлення необхідних частот вимірювального сигналу. Для уникнення такого недоліку пропонується застосування вимірювальних сигналів складної форми [2].

Показано, що апаратура контролю систем навігації та управління засобів водного транспорту за своїм функціональним призначенням складається з апаратури генератора вхідних вимірювальних впливів і апаратури, яка призначена для аналізу параметрів вихідного сигналу об’єкта контролю. Обґрунтована доцільність і можливість побудови такої апаратури на базі цифрової дискретної техніки. Застосування цифрової дискретної апаратури контролю дозволяє реалізувати оптимальні методи контролю, забезпечує високу швидкодію та точність контролю. Застосування такої апаратури дозволяє автоматизувати процес контролю. Принципи побудови та створені на основі цих принципів генератори вимірювальних сигналів дозволяють формувати вхідний сигнал потрібної форми з необхідним ступенем точності.

Експериментальні дослідження та дослідна експлуатація генераторів показали їх хорошу працездатність та надійність. Розглянуті принципи побудови та різні варіанти конструкції, які реалізують оптимальний алгоритм обробки вихідного сигналу об’єкта контролю. При синусоїдній формі вхідного сигналу прилад контролю може бути виконаний на базі аналізатора частотних характеристик. Імітаційна модель одного з варіантів такого приладу підтвердили правильність покладених в його основу принципів і показали високу точність і надійність. Розглянуті варіанти побудови приладу контролю, в яких проводиться обробка вихідного сигналу на основі спрощених алгоритмів, що дозволяють суттєво спростити апаратуру аналізатора при одночасному збереженні достатньо високого захисту від перешкод.

З метою підвищення оперативності контролю може бути використаний комбінований метод, при якому для визначення відхилень невеликої кількості найбільш суттєвих параметрів застосовується оптимальний метод обробки вихідного сигналу, або, який використовує визначення середнього значення вихідного сигналу, а для інтегральної оцінки уходів всіх інших параметрів – метод, заснований на визначенні середньоквадратичного значення вихідного сигналу неузгодження.

Список літератури

1. О. М. Тимощук, А Дакі, та О. М. Коломієць, “Обґрунтування застосування сигналів з нормованим спектром для контролю технічного стану радіонавігаційних приладів засобів водного транспорту”, *Новітні технології*, вип. 2(6), с. 39 – 45, 2018.

2. С. В. Герасимов, О. А. Дакі, та М. Ю. Яковлев, “Синтез полігармонійного вимірювального сигналу з будь-якою кількістю точок перемикання”, *Вимірювальна техніка та метрологія*, №79 (2), с. 73 – 76, 2018.

УДК 004.056.5

К.І. Добринін

kyrylo.dobrynin@gmail.com

Харківський національний університет радіоелектроніки, м. Харків

ПІДХОДИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ ОРГАНІЗАЦІЙ ПРИ ВИКОРИСТАННІ ВНУТРІШНІМИ СТЕЙКХОЛДЕРАМИ МОБІЛЬНИХ ПРИСТРОЇВ

Сучасне функціонування організацій будь яких форм власності практично неможливо без використання співробітниками організацій мобільних пристроїв. Вочевидь, що використання зазначеними співробітниками мобільних пристроїв безпосередньо впливає на рівень інформаційної безпеки. З точки зору організації менеджменту інформаційної безпеки, зазначені особи, які впливають на інформаційну безпеку організації, можуть розглядатися як внутрішні стейкхолдери [1].

Узагальнений аналіз організаційних структур типових підприємств показав, що до категорії внутрішніх стейкхолдерів, які використовують мобільні пристрої, можуть бути віднесені: керівники організацій, особи топ-менеджменту, фахівці IT-відділу, співробітники служби інформаційної безпеки та інші співробітники організації, які безпосередньо або опосередковано опікуються питаннями інформаційної безпеки. Окрім цього, у деяких випадках, у якості внутрішніх стейкхолдерів, слід розглядати і зовнішніх осіб, а саме: акціонерів компаній, зовнішніх аудиторів та технічних експертів, клієнтів та інш.

Вимогами міжнародного стандарту ISO/IEC 27001:2013 [2] встановлюється необхідність не тільки визначення зазначених стейкхолдерів (пункт 4.2 стандарту), але й забезпечення безпеки інформації при використанні ними мобільних пристроїв (пункт А.6.2, А.9.1, А.9.2 та інш.).

Аналіз використання мобільних пристроїв (МП) показав, що на цей час існує кілька сценаріїв використання МП в корпоративному середовищі. Найпопулярнішими підходами до роботи з МП є: BYOD (Bring Your Own Device – принеси свій пристрій), CYOD (Choose Your Own Device – обери свій пристрій) і COPE (Corporate-Owned, Personally Enabled – корпоративні пристрої, налаштуванням і обслуговуванням яких співробітник займається самостійно).

Використання зазначених сценаріїв має на меті вирішення декількох основних питань, а саме: забезпечення мобільності стейкхолдерів та зниження витрат організації на IT-інфраструктуру. Сумісно з цим, використання МП може привести до погіршення стану інформаційної безпеки за рахунок виникнення трьох категорій ризиків: фізичного (втрата, крадіжка, пошкодження МП і т.д); організаційного (низька компетенція стейкхолдерів в функціях МП; зміна поколінь, технологій та програм МП; привілейований доступ до баз даних на МП, нецільове використання співробітником МП та інш.); технічного (витік інформації через шкідливе програмне забезпечення, програми-шпигуни; відстеження поведінки користувача).

З метою мінімізації зазначених ризиків, у доповіді, ретельно проаналізовані типові підходи до побудови та захисту інформації при використанні технологій BYOD, CYOD та COPE. Показано, що використання існуючих підходів [3] до забезпечення захисту інформації не завжди може привести до очікуваного ефекту.

Враховуючи, що, по суті, інформаційна безпека являє собою стан захищеності інтересів стейкхолдерів організації в інформаційній сфері, яка визначається сукупністю збалансованих інтересів особистості, суспільства, держави та бізнесу, у роботі запропоновано сумісно з відомими організаційними та технічними підходами до захисту МП використовувати конкретні типи програмного забезпечення (MDM, MAM, MIM, MxM), використання яких дозволить підвищити рівень інформаційної безпеки та проведено їх аналіз.

Показано, що, найбільш ефективним варіантом є розробка та використання в організаціях, що потребують МП, мобільних пристроїв з апріорі встановленою платформою віртуалізації (по типу гіпервізора) поверх якої встановлюється операційна система стейкхолдера з його базою даних і налаштуваннями, та, так званої, корпоративної операційної системи, управління якою повністю покладається на IT-відділ організації. Це забезпечить розумний компроміс стану інформаційної безпеки та інтересів стейкхолдерів.

Список літератури

1. L. Lankoski, N. Stmith, and L. Van Wassenhove, “Stakeholder Judgments of Value: Advancing Stakeholder”, *Theory through Prospect Theory, INSEAD*. [Online]. Available: http://www.hbs.edu/faculty /conferences/2013-sustainability-andcorporation/Documents/Stakeholder judgments _of_value_0513FV.pdf. Accessed on: March. 19, 2019.

2. “ISO/IEC 27001:2013 Information technology. Security techniques”, *Information security management systems – Requirements*. [Online]. Available: https://www.iso.org/ru/standard/54534.html. Accessed on*:* March. 19, 2019.

3. Практические рекомендации для создания простой и безопасной программы BYOD, CYOD и COPE [Електронний ресурс]. Доступно: https://www.citrix.ru/products/citrix-endpoint-management/byod -best-practices .html. Дата обращения: Март 19, 2019.

УДК 004.056, 655.25

І.М. Дронюк, З.Я. Шпак

ivanna.m.droniuk@lpnu.ua, zshpak@ukr.net

Національний університет "Львівська політехніка", м. Львів

МЕТОД СТВОРЕННЯ ЦИФРОВОГО ПІДПИСУ НА ОСНОВІ УЗАГАЛЬНЕНОГО ПЕРЕТВОРЕННЯ ФУР'Є

Захист даних для суспільства та держави, разом із захистом особистих даних, сьогодні є завданням першочергової важливості. Розроблення нових методів захисту даних тісно пов'язане із завданнями створення умов для безпечної діяльності держави та здійснення заходів для особистої безпеки громадян у державі. В епоху великих даних це завдання набирає ще більшої значущості, оскільки великі обсяги даних є вразливішими. На сьогодні найбільш поширеними для захисту файлів та технічно достатньо простими є методи вбудовування у документи цифрових водяних знаків. Вдалими модифікаціями цих методів є методи вбудовування у файл цифрового підпису, що зараз широко використовується для захисту та ідентифікації електронних документів. Ці методи є одними з найефективніших, якщо критерієм ефективності захисту вважати швидкість створення та розпізнавання цифрових підписів.

У роботі розглядається задача вбудовування цифрового підпису в частотну область одновимірного або двовимірного сигналу. Авторами запропоновано новий метод розв'язання цієї задачі на основі застосування узагальненого перетворення Фур'є.

Застосуємо одновимірне дискретне *Ateb*-перетворення (ДАП). Нехай сигнал заданий у вигляді одномірної дискретної послідовності $S(p)$, де p – біжуче значення сигналу довжиною N. Введемо у розгляд функції $A(m,n,k)$ та $B(m,n,k)$ за формулами:

$$A(m,n,k)=\sum_{p=0}^{N-1}S(p,q)ca^{m}(m,n,-i\frac{2\Pi pk}{N})$$

$$k=1,...,N,$$

$$B(n,m,k)=\sum_{p=1}^{N-1}S(p,q)sa^{n}(n,m,-i\frac{2\Pi pk}{N}),$$

$$k=1,...,N,$$

де p – номери гармонік, $ca(m,n,\omega)$ – функція *Ateb*-косинусу, $sa(m,n,\omega)$ – функція *Ateb*-синусу, $\Pi=\Pi(m,n)$ – напівперіод *Ateb*-функції.

Позначивши $i=\sqrt{-1}$, пряме та обернене ДАП задамо формулами:

$$X(m,n,k)=A(m,n,k)-iB(n,m,k).$$

$$S(m,n,p)=\frac{1}{N}\sum_{k=1}^{N-1}\{A(m,n,k)ca(m,n,-i\frac{2\Pi pk}{N})+$$

$$+B(n,m,k)sa(m,n,-i\frac{2\Pi pk}{N}),\ p=1,...,N.$$

Вхідний сигнал у вигляді вектора $S(p)$ при дії прямого та оберненого ДАП формально трансформується у вектор $B(m,n,p)$. Параметри m та n *Ateb*-функцій можна використати для персоніфікації сигналу. Для фіксованих значень параметрів m, n можна відтворити значення сигналу $S(p)$. Таке представлення дає змогу використовувати запропоновані перетворення для створення прихованих вбудованих повідомлень та персоніфікованого захисту електронних даних. За допомогою прямого ДАП перетворюємо сигнал, а далі застосовуємо наступні два способи вбудовування прихованого цифрового підпису [1].

Перший спосіб: r найбільших значень перетворюємо за формулою для вбудовування прихованого цифрового підпису у вигляді:

$$z^{wp}=z^{p}+\alpha w,$$

де z^{wp} – перетворений сигнал, z^{p} –початковий сигнал, w – приховане повідомлення, α – коефіцієнт для регулювання величини вбудовування.

Другий спосіб: застосовуємо іншу формулу:

$$z^{wp}=z^{p}+e^{\alpha w}.$$

Для перевірки ефективності та стійкості запропонованого методу ідентифікації були проведені експерименти для значень параметрів $m=3$ та $n=1/7$. Реалізовано серію атак зміни розміру вихідного файлу від 10% до 100%. Критерієм присутності прихованого зображення взято кореляцію. Якщо обчислене значення перевищує певне задане порогове значення, то вважаємо, що прихований цифровий підпис присутній, а отже сигнал можна ідентифікувати. Після проведеної атаки у залежності від параметру α 60-100% вдалось розпізнати вбудований цифровий підпис.

Список літератури

1. P. Lipinski, "Odporne cyfrowe znaki wodne w obrazach", *Akademicka oficyna wydawnictwa EXIT*, Warszawa, 2013.

УДК 004.056

В. Б. Дудикевич, Г. В. Микитин, М. В. Мельник, А. І. Ребець

vdudykev@polynet.lviv.ua, cosmos-zirka@ukr.net, melnyk1604@gmail.com, fish914@gmail.com

Національний університет "Львівська політехніка", м. Львів

СЕНСОРНІ МЕРЕЖІ ZIGBEE, WIFI ТА BLUETOOTH В КІБЕРФІЗИЧНИХ ТЕХНОЛОГІЯХ

Актуальність сенсорних мереж в кіберфізичних технологіях. Концепція майбутньої промисловості "Індустрія 4.0" розгортає структуру взаємозв'язку кіберфізичних систем, машинно-машинної взаємодії, промислового Інтернету, Інтернету речей, Інтернету послуг [1]. Сучасні тенденції автоматизації промислових комплексів на основі взаємодії кіберфізичних систем та Інтернет речей, представленої парадигмою "багаторівнева КФС – багаторівнева безпека" розкривають перспективи розвитку безпечних розумних міст. В Україні розпочато проектування та впровадження інформаційних систем "Розумне місто", як цифрових керованих сервісів у сферах освіти і науки, екології довкілля, безпеки міського простору [2]. У цьому зв'язку сенсорні мережі, зокрема такі як. ZigBee, Wi-Fi, Bluetooth слугують комунікаційним середовищем кіберфізичних систем. Розглянемо аспекти сенсорних мереж.

Архітектура стандартів ZigBee, Wi-Fi, Bluetooth [3]. ZigBee – безпровідний стандарт передавання даних з можливістю само-організування та самовідновлення. Особливості функціонування: використання ефективних протоколів; висока сумісність пристроїв; автоматичне відновлення маршрутів.

Wi-Fi – стандарт безпровідного зв'язку передавання даних, який грунтується на сімействі стандартів IEEE 802.11. Особливості функціонування: гарантована сумісність будь-якого обладнання; можливість створення захищеної мережі; використання надійного шифрування.

Bluetooth – технологія економічного безпровідного зв'язку на малих відстанях. Особливості функціонування: підтримка швидкого підключення; можливість використання пристроїв малої потужності; сумісність обладнання різних поколінь. Характеристики ZigBee, Wi-Fi, Bluetooth. ZigBee: частотний діапазон – 868 МГц; 915 МГц; 2,4 ГГц; пропускна здатність – 250 кбит/с; дальність зв'язку – 100 м. Wi-Fi: частотний діапазон – 2,4 ГГц; 5 ГГц; пропускна здатність – 0,4–6,7 Гбіт/с; дальність зв'язку – 100 м. Bluetooth: частотний діапазон – 2,4 ГГц; пропускна здатність – 1 Мбит/с; дальність зв'язку – 100 м.

Безпека ZigBee (IEEE 802.15.4). Розглянемо захист інформації в сенсорній мережі ZigBee на прикладному рівні моделі OSI (ДСТУ ISO/IEC 7498-1,2,3), що виконує такі функції: передача повідомлень, виявлення пристроїв, визначення ролі пристроїв. Для цього рівня характерні загрози: використання безкоштовних ресурсів та програм невідомого походження; недоліки програмного забезпечення (ПЗ); наявність backdoors; обхід стандартних засобів управління безпекою; недостатній контроль засобів захисту; надмірно ускладнений механізм контролю безпеки; збої ПЗ при великих навантаженнях. Технології захисту інформації в ZigBee: контроль на рівні програм, що забезпечує доступ до ресурсів; простий механізм забезпечення безпеки, з метою уникнення складностей у конфігуруванні; реалізація криптографічного та антивірусного захисту даних.

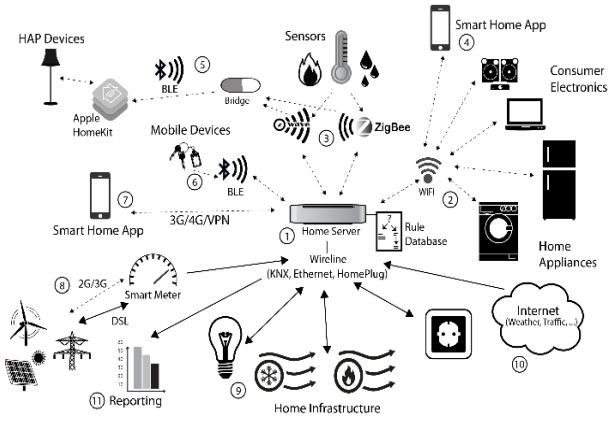


Рис. 1. Сенсорні мережі для розумних об'єктів

На рис. 1: 1 – сегмент домашнього контролера з базою інструкцій; 2 – мережі Wi-Fi; 3 – мережі ZigBee; 4 – локальне ПЗ управління за допомогою мобільних пристроїв; 5 – компоненти розумного будинку; 6 – технологія Bluetooth; 7 – ПЗ для віддаленого керування; 8 – розумна енергетика; 9 – система контролю параметрів будівлі; 10 – інтеграція з Інтернет-сервісами; 11 – система автоматичного генерування звітів про роботу.

Список літератури

1. Industry 4.0. [Електронний ресурс]. Доступно: http://en.wikipedia.org/wiki/Industry_4.0. Дата звернення: Бер. 4, 2019.

2. Kyiv Smart City. Напрямки діяльності. – [Електронний ресурс]. Доступно: http://www.kyivsmartcity.com. Дата звернення: Бер. 4, 2019.

3. А. Ю. Макаренко, А. Ю. Парфенова, та С. Б. Могильний, "Бездротові технології передачі даних", *Вісник Національного технічного університету України "КПІ"*, 181 Серія, Радіотехніка, Радіоапаратуробудування, №41. с. 171–181, 2010.

УДК 621.391

С.П. Євсеєв[1], О. Г. Король[1], А.А. Гаврилова[1], Керім Четінкайя[2]

serhii.yevseiev@hneu.net, korol.olha2016@gmail.com, sharaya1972@gmail.com

[1]*Харківський національний економічний університет імені Семена Кузнеця, м. Харків*
[2]*Університет Карабюк, Турція*

ПОБУДОВА ГІБРИДНОЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ МАК-ЕЛІСА

Криптографічні системи на алгоритмах несиметричної криптографії (RSA, ECC, DSA) вразливі до атак “грубої сили” з використанням повномасштабного квантового комп’ютера. Тому основні дослідження і розробки криптографічних засобів захисту інформації (КЗЗІ) спрямовані на пошуки рішень, що не мали б вразливостей щодо квантових обчислень і були б одночасно стійкими до атак за допомогою звичайних комп’ютерів. Такі алгоритми відносяться до розділу квантово-стійкої криптографії.

Аналіз практичної реалізації алгоритмів шифрування / розшифрування в гібридній крипто-кодовій конструкції (ГККК) Мак-Еліса показує, що досягається зменшення поля до *GF* (2^4) зі збереженням гарантованої стійеості за рахунок використання збиткових кодів та медоів багатоканальної криптографії. Алгоритм формування кодограми (криптограми) що реалізовується за допомогою відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Фіксування кінцевого поля *GF(q)*. Фіксування еліптичної кривої $y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3$ і набір її точок $EC(GF(q)):(P_1, P_2, ..., P_N)$ над *GF(q)*. Фіксування підмножини точок $h(GF(q)): (P_{x1}, P_{x2}, ..., P_{xx}),\ h \subseteq EC(GF(q)),\ /h/=x$ і зберігаємо його в секреті.

2. Фіксування вектору ініціалізації $IV=EC–h_j$, h_j – інформаційні символи рівні нулю, $/h/ = \frac{1}{2}k$, т. то. $I_i = 0,\ \forall I_i \in h$;

3. За введеним інформаційним вектором *I* формування кодового слову *c.* Якщо *(n, k, d)* код над *GF(q)* заданий породжувальною матрицею, то $c=I\cdot G$.

4. Формування випадкового вектору помилки *e* такий, що $w(e)\le t,\ \ t = \lfloor (d-1)/2 \rfloor$. Отримання кодового слову шляхом додавання сформованого вектору до кодового слову: $c^*=c+e$.

5. Формування кодограми, шляхом видалення (укорочення) символів вектора ініціалізації, яка поступає на алгоритм *MV2* [3]: $c_X{}^*=c^*–IV$.

6. Формування прапору $CH_D{}^i\ \left\| f(x)_i \right\|$ і залишку $CFT^i\ \left\| C(x)_i \right\|$ на основі алгоритму *MV2*:

$$C_j^* = C_j - C_{k-h_j},\ E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

Алгоритм розкодування кодограми (криптограми), що реалізовується за допомогою відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Введення кодограми, що підлягає розкодуванню. Осмислення кодограми за алгоритмом *MV2*:

$$E^{-1}_{K_{MV2}} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to C_j.$$

2. Додавання нульових інформаційних символів до отриманої кодограми: $C_j^* = C_j + C_{k-h_j}$;

3. Розкодування отриманого вектору у відповідних пристроях за алгоритмом Берлекемпа-Мессі: $C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$, кодограма – суть кодове слово з помилками еліптичного коду. Вага вектора помилок $w(e) \le t$.

4. Формування інформаційного вектору. Для цього у відповідних пристроях отриманий результат розкодування $M_i \cdot \left(X^u\right)^T$ слід помножити на $\left(X^u\right)^{-1}$:

$$\left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} = M_i.$$

Таким чином використовуючи вектор ініціалізації при формуванні кодограми і універсальний механізм заподіяння збитку на основі алгоритму MV2 забезпечується суттєве зменшення довжини кодового слова який поступає в канал зв’язку, тим самим складність формування криптограми зменшується ≈ в 12 разів і розкодування криптограми ≈ в 20 разів зі збереженням стійкості несиметричної крипто-кодової конструкції.

Список літератури

1. С. П. Євсеєв, “Використання кодів пошкоджень у крипто-кодових системах”, *Інформаційні системи,* № 5 (151), с. 109–121, 2017.

2. С. П. Євсеєв, Г. П. Коц, С. В. Мінухін, О. Г. Король, та А В. Холодкова, “Розробка методу багатофакторної аутентифікації на основі гібридних криптокодових конструкцій на дефектних кодах”, *Східноєвропейський журнал передових технологій*, 5/9(89), с. 19 – 35, 2017.

3. С. .П. Євсеєв, Г. П. Коц, та Є. С. Лєкарєв, “Розробка багатофакторного методу аутентифікації на основі модифікованої криптокодової системи Нідеррайтера-Мак\еліса”, *Східноєвропейський журнал передових технологій*, 6/4(84), с. 1, 2010.

УДК 330.131.7

В.В. Іванієнко

5531viktor@ukr.net

Харківський національний університет ім. С.Кузнеця, м. Харків

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ УМОВАХ ГОСПОДАРЮВАННЯ

У будь-якій галузі базовий принцип інформаційної безпеки полягає в дотриманні балансу інтересів суб'єкта господарювання, громадянина, суспільства і держави. З урахуванням цього будується система інформаційної безпеки підприємства, яка повинна враховувати можливі загрози і методи захисту інформації. До загроз відносять:

1. Неуважність і недбалість співробітників. Завжди є ймовірність того, що хто-небудь відкриє фішингових лист і впровадить вірус з особистого ноутбука на сервер компанії. Або скопіює файл з конфіденційною інформацією на планшет, флешку або КПК для роботи у відрядженні. І жодна компанія не застрахована від пересилання неуважним співробітником важливих файлів не за тією адресою.

2. Використання піратського ПЗ. Неліцензійні програми не дають захисту від шахраїв, зацікавлених в крадіжці інформації за допомогою вірусів. Володар неліцензійного ПЗ не отримує технічної підтримки, своєчасних оновлень, що надаються компаніями-розробниками.

3. DDoS-атаки. Distributed-Denial-of-Service – "розподілена відмова від обслуговування" – це потік помилкових запитів від сотень тисяч географічно розподілених хостів, які блокують обраний ресурс одним з двох шляхів.

Перший шлях – це пряма атака на канал зв'язку. Другий – атака безпосередньо на сервер ресурсу. Зазвичай подібні атаки використовуються в ході конкурентної боротьби, шантажу компаній або для відвернення уваги системних адміністраторів від деяких протиправних дій.

4. Комп'ютерні віруси. Одна з найнебезпечніших на сьогоднішній день загроз інформаційній безпеці. Це можна пояснити появою нових каналів проникнення вірусів. На першому місці як і раніше залишається електронна пошта, але, як показує практика, віруси здатні проникати і через програми обміну повідомленнями, такі як ICQ та інші. Збільшилася і кількість об'єктів для можливих вірусних атак. Якщо раніше атакам піддавалися в основному сервери стандартних веб-служб, то сьогодні віруси здатні впливати і на міжмережеві екрани, комутатори, мобільні пристрої, маршрутизатори. Останнім часом особливо активні стали так звані віруси-шифрувальники.

5. Загрози з боку співвласників бізнесу (легальних користувачів інформації фірми). Такі витоку фахівці називають інсайдерськими.

6. Законодавство. Державні органи наділені правом конфіскувати в ході перевірок обладнання та носії інформації, що завдає збитків компанії [1].

До методів захисту інформації слід віднести:

фізичні засоби захисту інформації (обмеження або повну заборону доступу сторонніх осіб на територію);

базові засоби захисту електронної інформації (численні антивірусні програми, а також системи фільтрації електронної пошти);

використання анти-DDoS (послугу анти-DDoS, пропоновані програмістами);

резервне копіювання даних (особливо актуальною стала послуга віддаленого зберігання різної інформації в "хмарі" дата-центрів);

план аварійного відновлення даних (в ньому обов'язково повинна бути передбачена можливість введення аварійного режиму роботи на період збою, а також всі дії, які повинні бути зроблені після відновлення даних. Сам процес відновлення слід максимально відпрацювати з урахуванням всіх змін системи;

шифрування даних при передачі інформації в електронному форматі (end-to-end protection) [1, 2].

Визначення життєвого циклу інформаційної безпеки підприємства, дослідження основних рівнів інформаційної безпеки підприємства є також важливими аспектами її забезпечення в сучасних умовах їх господарювання.

Список літератури

1. Информационная безопасность предприятия: ключевые угрозы и средства защиты. [Электронный ресурс]. Доступно: https://www.kp.ru/guide/informa-tsionnaja-bezopasnost-predprijatija.html. Дата обращения: Март 15, 2019.

2. Е. К. Грошева, и И. П. Невмержицький, "Информационная безопасность: современные реали", *Международный научный электронный журнал* "*Бизнес-образование в єкономике знаний*", № 3 № 3, с. 35–37, 2017.

УДК 004.621: 683.3

Я.О. Кавуненко, Н.В. Подоляка

yana.kavunenko@nure.ua, nataliia.podoliaka@nure.ua

Харківський національний університет радіоелектроніки, м. Харків

ИССЛЕДОВАНИЕ И ОБОСНОВАНИЕ ВЫБОРА МЕТОДОВ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

За последние два десятилетия биометрические технологии сделали большой шаг вперед. Во многом этому способствовало распространение микропроцессорных технологий. Еще в 80-е годы система контроля доступа, которая использует биометрические характеристики человека, можно было увидеть только в фантастических фильмах.

Сегодня же использования в системах контроля и управления доступом (СКУД) биометрических сканеров практически не усложняет систему безопасности, и ее стоимость для некоторых биометрических методов очень низкая. Более того, около трети ноутбуков выходит сейчас со встроенной системой считывания отпечатка пальцев, а если в ноутбуке есть видеокамера, на него можно установить систему распознавания человека по лицу.

Биометрия (Biometrics) – технология идентификации личности, использующая физиологические параметры субъекта (код ДНК, отпечатки пальцев, радужной оболочке глаза, изображение лица, тембр голоса и т. п.). Биометрические системы можно сравнивать по следующим параметрам [1]:

•FRR (False Rejection Rate) – система не распознает зарегистрированный отпечаток;

•FAR (False Aceptance Rate) – система ошибочно распознает незарегистрированный отпечаток;

•EEF (Equal Error Rate) – вероятность того, что FRR = FAR;

•FER (Failure to Enroll Rate) – вероятность того, что система не сможет зарегистрировать человека;

•ATV (Ability To Verify) – вероятность, с которой система может успешно проверить человека; математически это выражается как (1-FRR)*(1-FAR).

Исходя их того, что пользователем подобных систем является человек, один из самых важных факторов, влияющими на успех применения биометрии - восприятие технологии людьми, которые ее применяют. Статистика использования биометрических методов идентификации сегодня выглядит следующим образом [2]:

•отпечатки пальцев – 59%;

•геометрия лица – 17%;

•радужная оболочка – 7%;

•геометрия руки – 7%;

•рисунок вен – 7%;

•голос – 5%;

•почерк – 1%;

•все остальное – 1%.

Сравнительная характеристика описанных методов приведена в табл. 1.

Таблица 1

Сравнение биометрических систем

Характеристика	Отпечаток пальца	Голос	Радужка	Лицо
Надежность	97-98%	99,2-99,9%	95,4-96%	95,9%
FTE	4%	2%	7%	0,1%
FAR	2,5%	0,75%	6%	0,1%
FRR	0,1%	0,75%	0,001%	2,5%
Цена	100$	400$	500$	1200$

Биометрические технологии аутентификации имеют большие перспективы развития. При использовании систем на основе биометрических методов процедуры доступа становятся быстрее, безопаснее и проще. Но, несмотря на огромное количество преимуществ, биометрические технологии имеют ряд сложностей и проблем. Так, необходимо решать вопрос об использовании устройств биометрической идентификации людьми с некоторыми физическими недостатками, по подготовке профессиональных кадров, уменьшение стоимости устройств и другое.

Список литературы

1. А. А. Гинце, “Новые технологии в СКУД”, *Научно-технический журнал «Системы безопасности»,* № 6, с. 23 – 27, 2005.

2. Н. В. Татарченко, и С. В. Тимошенко, “Биометрическая идентификация в интегрированных системах безопасности”, *Научно-технический журнал “Специальная техника”,* № 12, с. 12 – 17, 2002.

УДК 004.056, 004.75

Н.Ф. Казакова, О.О. Фразе-Фразенко, Ю.В. Щербина

kaz2003@ukr.net, frazenko@gmail.com, shcherbinayura53@gmail.com

Одеська державна академія технічного регулювання і якості, м. Одеса

СПОСОБИ МОДЕЛЮВАННЯ КІБЕРАТАК У СУЧАСНОМУ КІБЕРПРОСТОРІ

Впровадження нових інтелектуальних технологій у сучасні процеси автоматизації документообігу та технологічного управління надають зловмисникам безліч можливих способів подолання засобів захисту. Тому однією із самих актуальних проблем стають кібератаки на інформаційні ресурси. На боротьбу із ними державні та комерційні установи витрачають великі ресурси, як фінансові, так і часові, людські тощо.

Особливістю сучасних технологій роботи з великими даними є відсутність усталеної математичної теорії, що визначає процедури пошуку і оброблення інформації і через це розробники пропонують на ринку програмні продукти, які мають велику кількість уразливостей. Це дозволяє зловмисникам будувати складні алгоритми атак, що можуть досягати своєї мети різними способами, в залежності від ситуації в кіберпросторі. Для реалізації атак у мережному середовищі зазвичай використовуються троянські програми, кінцевою метою яких є впровадження у програмний код атакованої системи додаткових прихованих функцій. Основною проблемою є те, що зазвичай факт втручання може бути виявлений вже після здійснення атаки. Зазвичай, такі несанкціоновані втручання до інформаційної системи не мають чітко визначеної часової закономірності, а їх тривалість є недостатньою для належного реагування. Таким чином, задача полягає у створенні такої стратегії боротьби, яка б дозволяла визначати зловмисні дії вже на перших кроках реалізації кібератак. Однією із умов створення ефективної системи захисту у кібернетичному просторі є володіння інформацією про всі її слабкі місця, а також розуміння формальних моделей організації сучасних атак у середовищі експлуатації інформаційних систем. І самі моделі, і визначення переліку уразливостей ґрунтується на постійному моніторингу можливих джерел загроз, з точки зору їх мотивів та наявності ресурсів для реалізації цих загроз, а також аудиту системи захисту на наявність у ній уразливостей. Відповіді на ці питання дає використання ромбовидної моделі, яка наведена у [1]. Відповідно до [1] зловмисник атакує інформаційний ресурс керуючись своїми мотивами, а не планом вторгнення. Ця модель враховує чотири основних елементи: супротивника і його ресурси, інфраструктуру, здатність до нападу і ціль. Для прогнозування дій порушника найчастіше використовується модель послідовних вторгнень [2]. Порушник крок за кроком виконує спроби подолання системи захисту, намагаючись подолати механізми захисту через уразливості там, де він їх знаходить. Основними елементами моделі послідовних вторгнень є індикатори, під якими розуміється будь-яка інформація, що об'єктивно описує кожний етап вторгнення. Зазвичай, послідовність вторгнення включає сім етапів: розвідку, озброєння, доставку, виконання, створення "чорного входу", установка таємного каналу і зловмисні дії по відношенню до об'єкту атаки. Незважаючи на тип обраної моделі атак, автоматизація процесів протидії нападу на інформаційну систему з боку зовнішнього кібернетичного середовища передбачає створення досить складного програмного коду. Ця робота зазвичай розпочинається із розроблення великої кількості формальних алгоритмів, що потребує використання усталеного математичного апарату. Саме через це, ще на початку розвитку мережного середовища, коли атаки на інформацію були досить простими, для визначення їх архітектури використовували графові моделі [3]. Графи атак являють собою концептуальні діаграми і використовуються для аналізу можливих шляхів реалізації конкретної загрози. Найчастіше – це багаторівневі деревовидні структури, що мають дочірні елементи з одним коренем. У випадку опису сучасної атаки вони мають тисячі вузлів і шляхів подолання механізмів захисту. Тому генерація графів для атак у складних мережах є дуже складною в обчислювальному сенсі.

На основі проведеного аналізу існуючих моделей реалізації мережних атак можна зазначити, що перевага має надаватись таким, які дозволяють, по-перше, оцінити вірогідність нападу з боку можливих джерел загроз, по-друге, визначити стратегію розпізнавання атаки на початку спроби її реалізації порушником безпеки. Модель повинна легко піддаватись формальному опису для подальшого її використання у процедурах автоматизації управління захистом.

Список літератури

1. S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," *DTIC Document, Tech. Rep.*, 2013.

2. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, p. 80, 2011.

3. B. Schneier, "Attack trees," *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21– 29, 1999.

УДК: 005.2::004.04::004.67/656::004.9/338.1

М.Т. Краснюк , О.Д. Кустаровский

krasnyuk@kneu.edu.ua, kust19921987@gmail.com

Київський національний економічний університет імені Вадима Гетьмана, м. Київ

ТОТАЛЬНА ОПТИМІЗАЦІЯ ЛОГІСТИЧНОГО БІЗНЕСУ ЯК ВАЖЛИВИЙ АНТИКРИЗОВИЙ І БЕЗПЕКОВИЙ ІНСТРУМЕНТ

Враховуючи результати аналізу кризового стану вітчизняного логістичного бізнесу [1], важливою та першочерговою задачею в рамках антикризових заходів, є підвищення рентабельності вітчизняних логістичних компаній. Отже, у логістиці, як і в інших галузях, є три основні способи підвищити рентабельність бізнесу:

1) перший – зростання тарифів на послуги. Особливість галузі полягає в тому, що на ринку працює багато дрібних приватних перевізників, які погоджуються на низьку ціну, та й покупці рахують кожну копійку в умовах кризи.

2) другий спосіб – зниження витрат. Звичайно, таке скорочення можна обґрунтовано проводити тільки після всеосяжного аудиту, методику якого викладено в [2]. Проте в умовах високо конкурентного ринка, безпосереднє скорочення видатків без реорганізації бізнес-процесів – може привести до падіння якості логістичних послуг та підвищення всіх типів ризиків логістичної діяльності.

3) третій спосіб підвищення рентабельності – це системна оптимізація бізнесу. При чому, цей прийом антикризового менеджменту має бути націлений на системну та скоординовану оптимізацію всіх функціональних складових на всіх виділених рівнях менеджменту логістичної чи транспортно-експедиційної компанії.

Викладемо результати авторських досліджень щодо компонентного складу та інструментарію задачі оптимізації логістичного бізнесу:

1) оптимізація та автоматизація політики управління запасами (формування та підтримку такої величини складських запасів в розрізі різних складів, який дозволить забезпечити безперебійне постачання асортименту при мінімальних витратах).

2) оптимізація маршрутів та розкладу (оптимізація часу, довжини та вартості маршрутів, аналіз та оптимізація багатомодальних ланцюжків поставки, оптимізація замовлень для одно- або двохетапного крос-докінгу тощо).

3) оптимізація фінансів. Треба окремо відзначити, що перед початком розробки заходів щодо оптимізації фінансів логістичної компанії, обов'язково треба проводити фінансовий аналіз за запропонованою авторами методикою [2]. Оптимізацію фінансової сфери логістичної компанії варто починати з побудови моделі, в якій досягається мінімізація операційних та накладних витрат на: транспортування, зберігання та штрафні санкції. Крім класичного переліку атрибутів для фінансової моделі, що викладені багаторазово у публікаціях, для кожної логістичної компанії в стадії кризи, після аудиту та проведення статистичного аналізу, OLAP та DM – повинні бути актуалізовані вхідні атрибути, що враховують специфіку конкретної компанії, регіональну та загальнодержавну специфіку.

4) оптимізація основних фондів - завантаження і раціональне використання наявних і залучених на умовах аутсорсингу ресурсів;

5) оптимізація кадрів – раціональне використання кадрового складу, відповідність виконуваних функцій рівню підготовки і кваліфікації співробітників;

6) оптимізація та підвищення якості бізнес-процесів (буде розглянута авторами в наступних публікаціях);

7) оптимізація ризиків залежить від багатьох внутрішніх та зовнішніх факторів: починаючи від цінової кон'юнктури і зміни попиту і закінчуючи діяльністю конкурентних організацій і стихійними лихами. Авторами, для вирішення цієї задачі, пропонується сценарне використання в режимі DM інструментарію дерев рішень та нейронних мереж);

8) оптимізація інформаційних ресурсів – вірність, точність, ефективність, своєчасність, результативність та інтерпретованість результатів обробки та аналізу даних. Для вирішення цього етапу оптимізації, авторами нижче викладено результати розробленої комплексної методики ефективного використання технології Data Mining для вітчизняних логістичних компаній.

9) оптимізація та отримання додаткової доданої вартості від накопичених корпоративних даних, нематеріальних активів та знань.

Треба відмітити, що авторами пропонується виконувати 8й та 9й етапи скоординовано, що зумовлено характеристиками та особливостями застосування технологій Big Data та Data Mining.

Список літератури

1. Maxim Krasnyuk, and Oleksandr Kustarovskiy. "The development of the concept and set of practical measures of anti-crisis logistics management in the current Ukraine conditions", *Management theory & practice. Publisher: Warsaw Management University*, # 19 (1), pp. 31-38, 2017.

2. М. Т. Краснюк, та О. Д. Кустаровський, "Дослідження, адаптація методик та удосконалення моделей фінансового аналізу підприємств транспортної галузі в поточних кризових умовах України" *Моделювання та інформ. системи в економіці: Зб. Наук. пр.*, Вип. 93, 2017, с. 175 – 195.

УДК 343.3/.7:004

О. С. Кульчицький, О. А. Ладигіна

Tigger100500@gmail.com, ladyginaoa@ukr.net

Центральноукраїнський національний технічний університет, м. Кропивницький

АНАЛІЗ РОБОТИ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Безпека мережі – це заходи, які приймаються для захисту інформаційної мережі від спроб руйнування, втручання та неправомірних дій по відношенню до даної мережі.

Для забезпечення безпеки інформаційної мережі необхідно захистити дані, програмне забезпечення та обладнання, що використовується.

Усі дані в комп'ютерній системі можуть бути втрачені через розкрадання або несправність, так би мовити, "системних дир". Щоб захистити інформацію треба використовувати апаратні пристрої та засоби.

На даний момент часу є дуже багато способів розкрадання даних. Для отримання інформації не обов'язково підходити до того чи іншого комп'ютера та копіювати файли на флешку, як це робилось раніше. 2019 рік має можливість встановити пристрої, програми в комп'ютер або монітор для виводу шпіонажу на інший монітор чи клавіатуру.

Але не треба відразу "хвататись за голову" та панікувати, адже як вигадали таку загрозу для компаній, людей, так проти неї з'явились методи захисту:

1. Перешкоду можна створити програмними або фізичними засобами.

2. Криптографічні способи – перетворення інформації та її замаскування.

3. Спонукання, або створення умов, які будуть мотивувати користувачів ПК до належної поведінки та завжди дотримується правил поводження з даними.

Усі ці методи захисту будуть реалізуватися за допомогою організаційних та технічних засобів.

Розробка організаційних засобів захисту інформації відноситься до обов'язків служби безпеки:

1. Інструктаж та перевірки усього персоналу компанії.

2. Підписання додаткових угод до трудових договорів з відповідальністю за розголошення таємниць по роботі.

3. Розробка програм, які захищають дані від знищення або копіювання.

Технічні засоби захисту поєднують разом програмну та апаратну частину:

1. Завжди перед будь-якими діями не завадить зробити резервне копіювання даних.

2. З часом з'явилось дуже багато хмарних сервісів для зберігання даних.

3. Встановлення програмного забезпечення, яке захищає базу даних та іншу інформацію від незаконного доступу.

4. Ще можна встановити в офіс камери та сигналізацію разом з охороною аби не пролізли шахраї.

5. Найголовніша міра захисту комп'ютера від людини, яка не за того себе видає – пароль.

Безпечною дією безпеки є аутентифікація. Для неї необхідно знати ім'я користувача та пароль, щоб без перешкод зайти в свій запис.

Спосіб використання лише імені користувача називають аутентифікацією однофакторною. Коли користувач використовує мобільний зв'язок чи кредитну картку, то дана безпека має назву двофакторна аутентифікація. Ще є трьохфакторна аутентифікація, при якій використовується сканування сітківки ока, тобто сканер обличчя чи відбитки пальців. Після проходження даної перевірки, відкривається доступ до користування послуг мережі.

Щоб виявити шкідливі програми, або їх пригнічення, використовується антивірусне програмне забезпечення. Також може використовуватися система запобігання вторгнень. Якщо однією мережею користується декілька комп'ютерів, то зв'язок між ними зашифровується. Дані дії проводяться для дотримування конфіденційності від інших людей.

На підставі вище викладеної інформації можна зробити висновок, що існує декілька видів безпеки захисту роботи комп'ютерних систем та мереж. Кожна з них по-своєму має свої "за" і "проти" для використання в роботі. Тому, користувач або організація вибирає найбільш ефективні способи захисту своєї системи та мережі [3].

Список літератури

1. В. П. Мельников, С. А. Клейменов, и А. М. Петраков, "Информационная безопасность и защита информации", *Академия,* 2011.

2. Способы защиты информации, [Электронный ресурс]. Доступно: https://searchinform.ru. Дата обращения: Апрель 02, 2019.

3. О. С. Кульчицький, "Вимоги протидії кіберзлочинності в умовах громадської локалізації", *Комп'ютерна інженерія і кібербезпека: досягнення та інновації: матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених*, 2018.

УДК 004.056:004.738.5(045)

К.В. Молодецька, Ю.О. Тимонін

kmolodetska@gmail.com, ytimonin45@gmail.com

Житомирський національний агроекологічний університет, м. Житомир

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОГО ВПЛИВУ В СОЦІАЛЬНИХ ІНТЕРНЕТ-СЕРВІСАХ НА ОСНОВІ СИСТЕМНОЇ ДИНАМІКИ

Наразі соціальні інтернет-сервіси (СІС) є платформою, яка використовується для взаємодії користувачів у мережі Інтернет. Одним з найважливіших напрямків дослідження СІС є вивчення їх впливу на процеси державотворення, зокрема прийняття важливих суспільних й політичних рішень тощо. Внаслідок проведення інформаційних операцій в СІС у реальному житті можуть поширюватися прояви соціальної напруженості, маніпуляції суспільної думкою громадян, міжетнічні конфлікти тощо [1]. Особливе місце в дослідженні взаємодії акторів у СІС належить системній динаміці (СД) Дж. Форрестера [2]. При цьому взаємодія акторів у СІС формалізується на основі причинно-наслідкової структури віртуальної спільноти і враховує зворотні зв'язки між окремими акторами. Зворотні зв'язки формуються внаслідок реакції акторів у СІС на деструктивний контент спрямованого змісту і призводять до подальшого поширення цього контенту в інформаційному просторі [1]. Отже, суттєвою перевагою застосування СД для забезпечення інформаційної безпеки держави у СІС є дослідження аспектів поведінки системи в часі з урахуванням зв'язків між акторами віртуальних спільнот. Однак, реалізація принципів СД для забезпечення інформаційної безпеки держави в СІС пов'язана з низкою невизначеностей: 1) велика кількість початкових змінних і елементів; 2) складність процедури детектування схеми взаємодії петель зворотного зв'язку. Отже, дослідження явищ соціальної комунікації в СІС потребує вдосконалення і подальшого розвитку системно-динамічних моделей (СДМ) деструктивного інформаційного впливу в СІС, які дозволять формалізувати та завчасно виявляти процеси поширення контенту спрямованого змісту в СІС й протидіяти загрозам інформаційній безпеці держави.

Запропоновано понятійний базис СДМ інформаційного впливу в СІС, який складається з незалежних і залежних величин. До незалежних величин СДМ належать: 1) фундаментальні змінні інформаційного простору СІС l і часу t; 2) первинні незалежні фазові змінні, які розглядаються як безрозмірні величини: а) кількість публікацій $Y(l,t)$ контенту в СІС, які формують інформаційний вплив; б) інтегральний показник $\Phi(l,t)$ поширення деструктивного контенту $Y(l,t)$ в інформаційному просторі l СІС і часі t. Незалежний понятійний базис СДМ інформаційного впливу в СІС – це мінімальна сукупність змінних $\{Y,\Phi,l,t\}$, яких достатньо для його формалізації. Залежні фазові змінні СДМ та їх зв'язки з незалежними фазовими змінними: а) потік деструктивного контенту в СІС $y(t)=Y'(t)$, $Y(t)=\int y(t)dt$; б) диференціальний показник поширення деструктивного контенту в СІС $\varphi(t)$: $\varphi(t)=\Phi'(t)$, $\Phi(t)=\int\varphi(t)dt$. Залежні величини включають наступні елементи – інтегратор і диференціатор, а робочий понятійний базис опису СДМ у часі представляє собою множину змінних $\{X,x,\Phi,\varphi,t\}$.

Види відношень між змінними: а) кількість публікацій деструктивного контенту в СІС прямо пропорційна показнику руху в інформаційному просторі $Y(t)=b_0\varphi(t)$, де b_0 – коефіцієнт ємності інформаційного простору СІС; б) показник поширення деструктивного контенту в СІС прямо пропорційний його потоку $\varphi(t)=b_1y(t)$, $\Phi(t)=b_1Y(t)$, де b_1 – коефіцієнт рівня критичного мислення акторів віртуальних спільнот у СІС; в) інтегральний показник руху деструктивного контенту в інформаційному просторі СІС прямо пропорційний його потоку $\Phi(t)=b_2y(t)$, де b_2 – коефіцієнт чутливості акторів до контенту деструктивного змісту в СІС.

Отже, відношення між фазовими змінними і операції над ними можуть використовуватися для конструювання СДМ зростання і розсіювання деструктивного контенту в СІС, що в перспективі дозволить ефективно і оперативно протидіяти загрозам інформаційної безпеки держави у СІС.

Список літератури

1. І. Г. Грабар, Р. В. Грищук, та К. В. Молодецька, "Безпекова синергетика: кібернетичний та інформаційний аспекти", *ЖНАЕУ*, 2019.

2. J. W. Forrester, "Lessons from system dynamics modeling", *System Dynamics Review*, *3*(2), pp. 136-149, 1987.

УДК 004.032.2

О.В. Овчаров

prometejso1983@gmail.com

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

ТЕХНОЛОГІЇ ДАТА-ЦЕНТРІВ ТА ОХОРОНА ДОВКІЛЛЯ

Кінець 20-го та початок 21 століття ознаменувались значним розвитком інформаційних технологій. Виникла необхідність збереження, обробки та розповсюдження великих масивів даних. Як наслідок були створені центри зберігання й обробки даних (ЦОД) або дата-центри. Всього у світі понад 3 млн. дата-центрів, площею понад 27 млн. м^2. Абсолютний лідер з їх будівництва – США. В Україні діє понад 30 комерційних та значна кількість державних ЦОДів. Їх збільшення призводить до вилучення значних площ планети для їх будівництва та росту споживання електроенергії. Сьогодні дата-центр великої корпорації споживає стільки ж електроенергії, скільки й невелике місто. При цьому, якщо передові корпорації США, Західної Європи та Японії постійно вживають належних заходів з енергозбереження та охорони довкілля від впливу дата-центрів, то в Україні цьому питанню приділяється дуже й дуже мало уваги [1].

Негативний вплив ЦОДа на стан довкілля обумовлюється шумовою, електромагнітною та тепловою складовими. В ЦОДах шум зазвичай випромінюється від: жорстких дисків серверів та їх масивів, двигунів приводу цих дисків, груп вентиляторів та серверних стояків; систем вентиляції та кондиціювання приміщень; систем централізованого та індивідуального опалення; систем аварійного електрозабезпечення. Це обладнання створює у головних приміщеннях дата-центру рівні шуму в 70-85 дБ. Такий шум викликає перевтому, зниження уваги, підвищену нервову збудженість, розлад нервової системи та тиннітус (дзвін у вухах).

Джерелами електромагнітного випромінювання в дата-центрі є: серверне обладнання, комутатори, маршрутизатори, системи зберігання даних, системи резервного копіювання та відновлення даних, системи передачі даних, системи електроживлення, вентиляції, кондиціювання, освітлення та інші. Вони випромінюють електромагнітні хвилі переважно в діапазоні промислових частот (у тому числі 50 Гц). Внаслідок негативного впливу цих хвиль у працівників ЦОДів та населення, що мешкає поблизу, виникають порушення роботи шлунку, печінки, селезінки, спостерігається розлад сну, головний біль, серцеві болі, пітливість та слабкість.

Дата-центри споживають близько 10% усієї виробленої у світі електроенергії. 50% експлуатаційних витрат ЦОД становить вартість спожитої ними електроенергії. 50% енергоспоживання ЦОДу припадає на IT-устаткування, 40% – на систему охолодження і 10% – на систему безперебійного електропостачання. 90% всієї вхідної потужності дата-центри перетворюють на тепло. Джерелами теплового випромінювання в ЦОДах являються: серверні стояки; системи живлення; системи вентиляції, кондиціювання, освітлення, тощо. Надлишкове тепло призводить до інтенсифікації процесів випаровування та кліматичних змін. Накопичення тепла в приземному прошарку атмосфери вже збільшило кількість реалізованих повеней, туманів, буревіїв, засух, пожеж. А відтак значне тепло викликає в людини захворювання серцево-судинної системи, дихальних шляхів, лімфатичної та кровотворної систем, тощо [2].

Отже для зменшення негативного впливу дата-центрів на довкілля необхідно:

1. Зменшити шум і вібрацію в технологіях. Провести протишумову обробку приміщень з використанням амортизуючих пристроїв. Між ЦОД і житловою зоною впровадити звукопоглинаючі екрани.

2. Зменшити електромагнітні випромінювання за рахунок: використання обладнання з оптимальними потужностями; екранування джерел випромінювання; дотримання відстаней до житла; розміщення випромінювачів за стінами; заземлення металевих дахів та перешкод.

Для утилізації тепла дата-центрів пропонується: обладнувати ЦОДи вітрогенераторами і сонячними мініелектростанціями; за рахунок рекуперації тепла впровадити обігрів суміжних приміщень взимку; за рахунок надлишків тепла серверних приміщень нагрівати воду для душових влітку; використовувати спеціальний тепловий насос для нагріву взимку води в радіаторах та повітря в припливній вентиляції; застосовувати для генерації електроенергії мікротурбіни на природному газі (генерують струм та тепло); впровадити термоелектричні генератори; перетворювати тепло процесорів серверів в електрику в піроелектричних пристроях; охолоджувати серверні стояки за допомогою холодильників-чилерів [3].

Список літератури

1. Дата-центр. [Електронний ресурс]. Доступно: https://uk.wikipedia.org. Дата звернення: Квіт. 15, 2019.

2. Дата-центр в цифрах і фактах. [Електронний ресурс]. Доступно: www.compress.ru. Дата звернення: Квіт. 15, 2019.

3. Теплота – Харків. [Електронний ресурс]. Доступно: www.teplota.kh.ua. Дата звернення: Квіт. 15, 2019.

УДК 004.056

Л.Д. Плиска, В.А. Лахно

luba.pliska@gmail.com, valss21@ukr.net,

Національний університет біоресурсів і природокористування України, м. Київ

РОЗВИТОК МЕТОДІВ І МОДЕЛЕЙ ДЛЯ ОЦІНЮВАННЯ СТРАТЕГІЙ ІНВЕСТУВАННЯ В СИСТЕМИ КІБЕРБЕЗПЕКИ

Сьогодні інформація є найціннішим активом для будь-якої організації, а основою всіх бізнес-процесів є інформаційні технології. Основною умовою конкурентоспроможності та розвитку для організації служить грамотно вибудуваний захист інформації. Слабка захищеність даних може спричинити появу серйозних проблем для бізнесу, які можуть привести до його повної зупинки.

Сучасні кібератаки посприяли розвитку досліджень, які пов'язані з інтелектуалізацією обчислень в області підтримки прийняття рішень захисту інформації та кібербезпеки для різних інформаційних систем і технологій. У той же час, розробляються нові методи та моделі для підтримки прийняття рішень щодо вибору стратегії фінансування.

Аналіз математичних моделей стратегій інвестування для систем кібербезпеки (КБ) показав, що основні засоби та сили застосовуються до питань визначення розміру інвестицій для захисту інформаційних систем (рис. 1). Крім того, наявні моделі рідко враховують, як правопорушник змінює тактику своїх кібератак, реагуючи на додаткові інвестиції для інформаційної безпеки. Існують труднощі в отриманні даних для моделей, таких як числова оцінка завданих збитків, ймовірності появи загроз і вразливості.

У процесі досліджень, нами був виконаний аналіз наявних моделей для оцінювання ефективності інвестування в системи захисту інформації та кібербезпеки різних об’єктів інформатизації. Показано, що більшість досліджень в даній області акцентовано лише на економічній постановці завдання пошуку оптимальних стратегій вкладення фінансових коштів в системи захисту і не враховують тенденції, що стосуються впровадження інформаційних технологій в процедури контролю та прийняття рішень для інвестиційних проектів.

Показано, що недоліком більшості розглянутих моделей, є відсутність конкретних рекомендацій щодо формування стратегій фінансових інвестицій в системи захисту і кібербезпеки. Обґрунтовано необхідність розробки нових моделей систем підтримки прийняття рішень (СППР), які дозволять знайти оптимальні стратегії фінансових інвестицій в захист інформації та кібербезпека підприємств.

З’ясували, що СППР в завданнях інвестування в КБ можуть бути побудовані на основі застосування математичних моделей теорії ігор, які дозволяють знаходити оптимальні стратегії інвестування [1, 2].

	Математичні моделі стратегій інвестування для інформаційної безпеки					
Критерії порівняння	Модель Гордона-Лоеба	Модель Вухен Шима	Модель Архипова	Модель Левченко - Прус	Модель Задіраки	Модель Аметова - Малюкова
Розрахунок оптимального рішення в динамічному режимі						
Облік уразливості об'єктів						
Оптимізація розподілу ресурсів						
Облік засобів захисту						
Облік засобів нападу						
Різниця позитивних і негативних ефектів						
Облік вартості кожного засобу захисту						

- не враховує

- враховує

Рис. 1. Порівняльна характеристика математичних моделей стратегій інвестування для систем кібербезпеки

Список літератури

1. V. Lakhno, V. Malyukov, and N. Gerasymchuk, “Development of the decision making support system to control a procedure of financial investment”, *Eastern-European Journal of Enterprise Technologies*, Vol. 6, №3, pp. 24-41, 2017.

2. V. A. Lakhno, “Development of a support system for managing the cybersecurity”, *Radio Electronics, Computer Science, Control*, Vol. (2), pp. 109–116, 2017.

УДК 621.317

В.В. Пустоваров

pustovarov78volodymyr@gmail.com

Харківське представництво генерального замовника – ДКА України, м. Харків

ОБҐРУНТУВАННЯ ПРОПОЗИЦІЙ ЩОДО ЗАСТОСУВАННЯ СУЧАСНИХ СУПУТНИКОВИХ ТЕХНОЛОГІЙ ДЛЯ ТОПОГЕОДЕЗИЧНОГО ЗАБЕЗПЕЧЕННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Центральне місце в управлінні польотами БПЛА займає планування, яке є обов'язковим, невід'ємним елементом цього процесу. Планування польоту конкретного апарату починається на етапі проектування при визначенні льотних характеристик і параметрів бортових систем. У процесі наступної реалізації життєвого циклу БПЛА видозмінюється й план польоту, набуваючи того вигляду, який використовується на стадії управління польотом [1].

Інформаційне забезпечення управління польотом включає багато складових. Не зменшуючи значення інших видів інформаційного забезпечення, слід визнати, що одне з центральних місць в завданні управління польотами відводиться топогеодезичному забезпеченню. Взагалі кажучи, термін “забезпечення” умовний і недостатньо повно відбиває істоту вирішуваних завдань отримання й використання сукупності топогеодезичних даних, необхідних для планування, підготовки до запуску, пуску й польоту БПЛА або їх угрупування.

Існуючи види інформаційного забезпечення управління польотом БПЛА значною мірою впливають через фундаментальні властивості динамічних систем, такі як керованість і оперативність коригування даних, на структуру автоматизованої системи управління БПЛА у цілому.

Система управління польотом БПЛА у сукупності з його бортовими комплексами, агрегатами, механізмами і елементами конструкції, об'єктами управління, що являються, утворює контур управління польотом [2].

Топогеодезична прив’язка БПЛА складається з визначення прямокутних координат точок маршруту, їх абсолютних висот, географічної широти та зближення меридіанів, визначення дирекційних кутів (азимутів), перерахунок прямокутних координат точок маршруту у зоні польоту та визначення поправки до дирекційного кута на перехід в суміжну зону. На практиці топогеодезична прив’язка БПЛА виконується за даними навігаційних систем завчасно при підготовці маршруту [2].

Розроблено методологічний підхід до оцінки можливостей використання сучасних супутникових технологій для топогеодезичного забезпечення БПЛА. Визначені технічні вимоги до апаратури комплексної навігаційної системи бортового обладнання БПЛА. Сформульована основні вимоги до технічних характеристик навігаційних систем БПЛА.

Сформульовані наступні пропозиції щодо практичного застосування сучасних супутникових технологій для топогеодезичного забезпечення польотів БПЛА.

1. Для розв’язання задач топогеодезичного забезпечення можливо впровадження сучасних супутникових технологій для визначення прямокутних координат і висот позиції запуску, розробки комплексних одометричних навігаційних систем з коригуванням від засобів супутникової навігації, а також їх використання для точного визначення дирекційних кутів (азимутів) орієнтирних (вихідних) напрямків як існуючих, так і перспективних БПЛА.

2. Для оцінки можливостей використання сучасних супутникових технологій для топогеодезичного забезпечення БПЛА пропонується використовувати методику, яка заснована на визначенні відносного зниження коефіцієнту ефективності виконання задач польоту за рахунок помилок топогеодезичної підготовки.

3. Обґрунтовано доцільність використання комплексованої (інерціальна система разом з GPS) системи топоприв’язки для забезпечення точності навігаційних вимірювань.

4. Комплексована система, що пропонується, повинна забезпечувати необхідну точність підготовки навігаційних даних для забезпечення функціонування як існуючих, так і перспективних БПЛА у різних варіантах застосування.

Список літератури

1. А. В. Костров, и А. М. Шатило, “Модельно-экспериментальные методы определения аэромеханических характеристик летательных аппаратов на баллистических трасса”, *Москва: МО СССР*, 1982.

2. С. В. Герасимов, А. М. Гричанюк, та О. О. Журавльов, “Дослідження високоточних систем навігації літальних апаратів за наземними орієнтирами” *Зб. наук. пр. Харківського національного університету Повітряних Сил*, Вип. 5(54), 2017, с. 48 – 53.

УДК 004.67

А. М. Соболєв, Д.В. Ланде

artem1sobolev@gmail.com

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", м. Київ

ПОШУК КРИТИЧНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ В ЗАСОБАХ МАСОВОЇ ІНФОРМАЦІЇ

Засоби масової інформації стали невід'ємною частиною сучасного суспільства. Останні десятиліття відзначилися активним розвитком засобів масової інформації (ЗМІ), які через застосування різноманітних технологій істотно впливають на формування та трансформацію суспільної свідомості. Саме ЗМІ здійснюють своєрідний інформаційний фон, на основі якого людина формує певний світогляд щодо способу і стилю життя, моделей поведінки та отримує необхідну інформацію яка відбується у світі. Основним інструментом ефективного інформаційного впливу є ЗМІ мережі Інтернет, так як вони мають широке охоплення аудиторії, високу швидкість поширення інформації, можливість інтеграції в одному повідомленні контенту різного типу (текст, відео, фото, аудіо та ін.).

Необхідність перевірки джерел ЗМІ для запобігання злочинних намірів розповсюдження неправдивої інформації та маніпуляцією суспільною думкою є ключовим аспектом даної роботи. Охоплення та узагальнення великих динамічних інформаційних потоків, які безперервно генеруються в засобах масової інформації, вимагає якісно нових підходів. Саме тому останнім часом використовують системи моніторингу ресурсів, які тісно пов'язані з контент-аналізом. Але даний підхід є не зовсім ефективний з боку масової атаки інших інформаційних джерел і потребує доопрацювання.

Для дослідження інформаційних джерел вибрано відомий сервіс моніторингу новин InfoStream, який дозволяє отримати інформацію про всі періодичні видання глобальної мережі Інтернет поточного та архівного періоду. Початковими значеннями пошуку вибрано щоденні видання, які публікуються у вітчизняному просторі. За результатами дослідження інформаційних джерел виявлена закономірність процесу опублікувань новин. Визначено, що існують джерела, які підтримуються для інформаційних атак у сфері ЗМІ в необхідний період часу. Зазвичай, такі інформаційні джерела перебувають у режимі спокою, тобто кожного дня як і звичайні джерела публікують певну не велику кількість новин. Для простоти такі джерела також можуть використовувати новини вже опубліковані на інших сайтах.

У визначений час такі джерела починають масово робити інформаційне вливання фейкових новин, що викликає великий ажіотаж на інших сервісах, які поступово починають також розповсюджувати дану інформацією на своїх ресурсах. Такий процес набуває великих масштабів, так як відомі джерела новин використовують інформацію з інших менш відомих сайтів і тим саме несуть неправдиву інформацію своїм користувачам.

Рис. 1. Типовий приклад інформаційного вливання фейкових новин інформаційним джерелом

На рис. 1 візуально відображено періодичність опублікування інформаційним джерелом новин на своєму ресурсі за період двох місяців. Було виявлено, що 22 квітня даним ресурсом опубліковано 190 публікацій за середнім розподілом в день близько 27 публікацій, що в 7 разів більше середньої норми. Після більш детального вивчення даного ресурсу визначено що він належить до типу ресурсів, які періодично вкидують фейкові новини для маніпуляцією суспільною думкою.

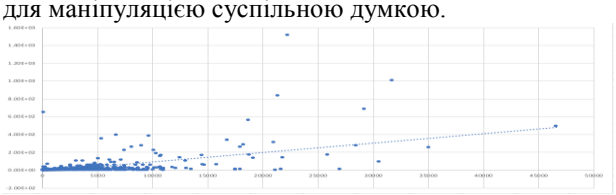


Рис. 2. Графік дослідження інформаційних ресурсів

На рис. 2 зображено графік розподілу середньо квадратичного відхилення публікацій інформаційних ресурсів відносно загальної кількості опублікованих новин. Вищезазначений графік дозволяє візуально визначити інформаційні джерела, що потребують особливої уваги під час отримання інформаційних публікацій з даних ресурсів, так як вони можуть зловживати інформацією відносно читачів.

В ході роботи, визначено особливість, яка дозволяє виявити джерела ЗМІ, що використовуються як інструмент інформаційного навіювання для маніпуляції в глобальній мережі. Розроблено модель розпізнання інформаційних джерел ЗМІ в мережі Інтернет та виявити ознаки не надійності інформаційного ресурсу і у разі його активізації для інформаційної атаки використовуватись як інструмент для прийняття рішень по протидії.

УДК 004.4, 004.6, 004.9

С.О. Скирда

stanislav.skyrda@nure.ua

Харківський національний університет радіоелектроніки, м. Харків

АНАЛІЗ ВРАЗЛИВОСТЕЙ WINDOWS-ПОДІБНИХ СЕРВЕРНИХ ОПЕРАЦІЙНИХ СИСТЕМ ТА ЗАГАЛЬНЕ ОПИСАННЯ МЕХАНІЗМІВ ЇХ ЗАХИСТУ

На теперішній час Windows-подібні серверні операційні системи є найпоширенішими у світі. Цей беззаперечний факт підтверджується величезним різноманнітям програмного забеспечення для таких систем, але, в одночас, це означає, що такі серверні системи є більш наражуваними на різну небезпеку, бо, кожна організація, що має такий сервер, має в своєму розпорядженні широкі локальні мережі з підключеними до неї персональними комп'ютерами, і тому безпека на серверному рівні є однією з найважливіших для такої мережі.

Сервери є централізованим місцем зберігання важливої інформації і файлів організації, а також підтримують критичні мережеві служби на зразок пошуку в каталогах і аутентифікації, тому вони так і приваблюють зловмисників.

У цих тезах ми проаналізуємо вразливості саме в Windows-подібних серверних системах через їх більший обсяг можливостей для продуктивної роботи працівників. Розглянемо механізми ефективного захисту і запобігання зовнішніх загроз. Визначимо вимоги до серверної системи і наведемо загальні рекомендації щодо забеспечення безпеки. На основі аналізу вимог до функціональності сервера були визначені компоненти, які є найбільш необхідними для роботи інформаційної системи. До них можна віднести службу каталогів ADDS, DNS, DHCP, службу віддалених робочих столів RDS та файловий сервер. Незважаючи на досить невеликий перелік необхідних компонентів, кожен з них має достатню кількість «лазівок» для зловмисника, які можуть спричинити наступні загрози. Неправильне проектування служби каталогів та складна стратегія управління можуть стати причиною компрометації системи, перевищення повноважень користувачами, які в свою чергу можуть бути використані для впровадження шкідливого програмного забезпечення. Система доменних імен без додатків лише прив'язує IP-адресу до символьного імені домена, і не призначена для виконання будь-яких функцій захисту. Це може бути використано зловмисником для створення атаки відмови в обслуговуванні та для впровадження шкідливих програм в сердце системи. Без додаткових налаштувань, протокол DHCP не контролює пристрої, які можуть отримувати IP-адрес у мережі. Ігнорування даного факту може призвести до несанкціонованого доступу до системи та до відмови в обслуговуванні.

Однією з найприємніших можливостей серверних систем є можливість підключення до системи з будь-якої машини, яку надає служба віддалених робочих столів RDS. Разом з перевагами використання даної служби, при неправильному налаштуванні, може існувати ймовірність компрометації конкретного користувача чи системи загалом. Зберігання всіх файлів в одній системі є надзвичайно зручним для контролю над ними, але є величезним ризиком для втрати всієї інформації у разі несанкціонованого доступу чи цілеспрямованої атаки. З метою мінімізації загрози, пропонується розглянути деякі методи захисту інформації за ролями і службами. Щодо служби каталогів, пропонується створення групової політики для кожного користувача, так само необхідно налаштування паролів для кожного користувачі і всановлення прив'язки кожного користувача до його робочого місця. Для системи доменних імен пропонується відключення автооновлення DNS-AD, а також використання Domain Name System Security Extensions. Для забезпечення безпеки служби віддаленого робочого столу необхідно застосувати ліцензування віддалених робочих столів, так само необхідно заборонити користувачам багато-сеансовий вхід в мережу і скласти список людей які можуть користуватися службою віддалених робочих столів. Також потрібно не забувати про примусове включення протоколу NTLMv2, який допоможе забезпечити додатковий рівень аутентифікації користувачів у мережі.

Для файлового сервера, пропонується провести аудит доступу до файлів і забезпечення налаштування прав доступу користувачів, та необхідно скористатися системою EFS, яка допоможе шифрувати файлі в системі, або застосувати файлову систему ReFS. У деяких випадках, звичайних механізмів захисту мало. В такому разі, використовуються зовнішнє програмне забезпечення, наприклад BitLocker. Це приклад програми, що шифрує вміст дисків і забеспечує один із кроків до захисту файлів організації.

Таким чином, можна зробити висновок, що при конфігурації сервера необхідно проводити ретельний і максимально повний аналіз майбутньої інформаційної системи. До того ж, їх як фізичного, так і логічного рівня, з точки зору працездатності та безпеки, що дозволить уникнути організації незапланованих інформаційних і матеріальних втрат.

УДК 004.056.55

О. С. Циганенко[1], С. П. Євсеєв[1], Б. П. Томашевський[2]

oleksii.tsyhanenko@hneu.net, serhii.yevseiev@hneu.net, bogdan_tomashevsky@tntu.edu.ua

[1]*Харківський національний економічний університет імені Семена Кузнеця, м. Харків*
[2]*Тернопільський національний технічний університет ім. І. Пулюя, м. Тернопіль*

ГІБРИДНА КРИПТО-КОДОВА КОНСТРУКЦІЯ НІДЕРРАЙТЕРА НА ЗБИТКОВИХ КОДАХ

Вступ людства до ери високих технологій стимулює подальше розширення можливостей обчислювальних систем. Стрімке зростання і розширення функціональних можливостей корпоративних систем і соціальних мереж, дозволяє будувати інтегровані соціально-інформаційні мережі для вирішення різноманітного спектра завдань. Подальший розвиток технології передачі даних Ethernet формує глобальну ідеологію побудови телекомунікаційних мереж [1].

Використання модифікованої крипто-кодової конструкції (МККК) Нідеррайтера з додатковими векторами ініціалізації (з множиною неприпустимих позиційних векторів вектора помилок і множиною позицій укорочення вектора помилки) вимагає збільшення швидкодії криптоперетворень системи в цілому. Для цього пропонується використовувати збиткові коди. Збиткові коди дозволяють збільшити швидкість кодових перетворень за рахунок зменшення потужності поля при нанесенні збитку відкритого тексту і зменшити обсяг переданих даних за рахунок нанесення шкоди шифртексту. Такий підхід дозволяє будувати гібридні крипто-кодові конструкції на основі синтезу модифікованих криптокодових конструкцій Нідеррайтера на модифікованих (укорочених або подовжених) кодах на еліптичних кривих з процедурами нанесення збитку. Суттєвою відмінністю від класичних гібридних (комплексних) криптосистем є використання несиметричної криптосистеми для забезпечення безпеки даних з швидкими процедурами криптоперетворень (формування та розкодування кодограми). Використання механізму нанесення збитку MV2 в крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах в Інтернет-технологіях та мобільних мережах, забезпечення практичної реалізації на сучасних платформах та необхідної криптостійкості в умовах постквантової криптографії [2].

Розглянемо формальний опис гібридної математичної моделі несиметричної крипто-кодової конструкція Нідеррайтера на збиткових кодах.

На основі рівноважного кодування формується закритий текст $C_j \in C$ за введеним відкритим текстом $M_i \in M$ і заданим ключем H_X^{ECu}, $u \in \{1,2,...,s\}$. Це здійснюється шляхом формування синдромної (в термінах завадостійкого кодування) послідовності S_{X_j}, що відповідає рівноважній послідовності $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$:

$S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \times \left(H_X^{ECu}\right)^T$, причому вага Гемінга (кількість ненульових елементів) вектора e не перевищує виправної здатності використовуваного алгебраїчного блокового (n,k,d) коду:

$$\forall i : 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Потужність множин M та C визначається допустимим спектром ваг $w(M_i)$, тобто в загальному випадку (для всіх допустимих значень $w(M_i)$) маємо:

$m = \sum_{i=0}^{t} (q-1)^i \times C_n^i$, де C_n^i – біноміальний коефіцієнт, $C_n^i = \frac{n!}{i! \cdot (n-1)!}$.

Сформований закритий текст $C_j \in C$ однозначно відповідає вектору $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Відкритий ключ формується шляхом множення перевірочної матриці алгеброгеометричного коду на матриці маскування:

$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u$, $u \in \{1,2,...,s\}$,

де H^{EC} – перевірочна $n \times (n-k)$ матриця алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$.

В канал зв'язку поступає синдромна послідовність: $S^*_{r-h_e} = (e_n - h_e) \times H_X^{EC^T}$.

Список літератури

1. Ethernet и промышленные сети [Электронный ресурс]. Доступно: https://www.osp.ru/lan/2013/09/13037411/. Дата обращения: Март 23, 2019.

2. S. Yevseiev, O. Tsyhanenko, A. Gavrilova, V. Guzhva, O. Milov, V. Moskalenko, and et. al, "Development of Niederreiter hybrid crypto-code structure on flawed codes", *Eastern-European Journal of Enterprise Technologies*, 1 (9 (97)), pp. 27–38, 2019.

УДК 004.056

Н.В. Шостак, А.А. Астраханцев

natalia.shostak@nure.ua, andrii.astrakhantsev@nure.ua

Харківський національний університет радіоелектроніки, м. Харків

ДОСЛІДЖЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ВБУДОВУВАННЯ ДАНИХ В ВІДЕОФАЙЛИ ДО АТАК

На сьогоднішній день ЦВЗ використовується як засіб захисту документів з фотографіями – паспортів, водійських посвідчень, кредитних карток з фотографіями. Об'єкти мультимедіа в цьому випадку будуть являти собою контейнери (носії) даних.

В ході дослідження були реалізовані декілька стеганографічних алгоритмів вбудовування інформації в відеофайли:

- метод вбудовування ЦВЗ на основі заміни НЗБ;
- метод вбудовування ЦВЗ на основі алгоритму Коха-Жао;
- метод вбудовування ЦВЗ на основі ДВП.

Також були проаналізовані відкриті джерела щодо методів вбудовування ЦВЗ в відео, що мають схожі властивості з реалізованими методами [3]. Для порівняльного аналізу з реалізованими методами були вибрані два алгоритми:

- автентифікація відео на основі вмісту за допомогою ДВП;
- ефективне вбудовування ЦВЗ в відео з використанням ДВП.

Стійкість реалізованих методів до певних атак можна покращити використанням завадостійких кодів. Для підвищення стійкості реалізованих методів було запропоновано використовувати завадостійкі коди Хемінга (7,4) та коди Ріда-Соломона.

В роботі розглядалися лише атаки, що направленні на порушення цілісності ЦВЗ. Атаки, що направлені на порушення цілісності ЦВЗ, можна поділити на 2 групи: геометричні атаки і атаки обробки сигналів. Геометричні атаки модифікують кадри зображень завдяки різним геометричним перетворенням. Серед геометричних атак були реалізовані:

- афінні перетворення;
- локальні спотворення.

При використанні атак обробки сигналів відеофайли розглядаються як сигнали. Тому атаки направленні на спотворення сигналу, а не кадрів. Серед атак обробки сигналів були реалізовані наступні:

- накладення шуму на відеофайл;
- перекодування відеофайлу;
- стиснення відеофайлу.

Для аналізу стійкості методу вбудовування ЦВЗ у відеофайл до певних видів атак необхідно провести порівняльний аналіз оригінального ЦВЗ з вилученим ЦВЗ з відеофайлу, що піддався атакам.

Результати проведення атак при використання завадостійких кодів представлений на рис. 1.

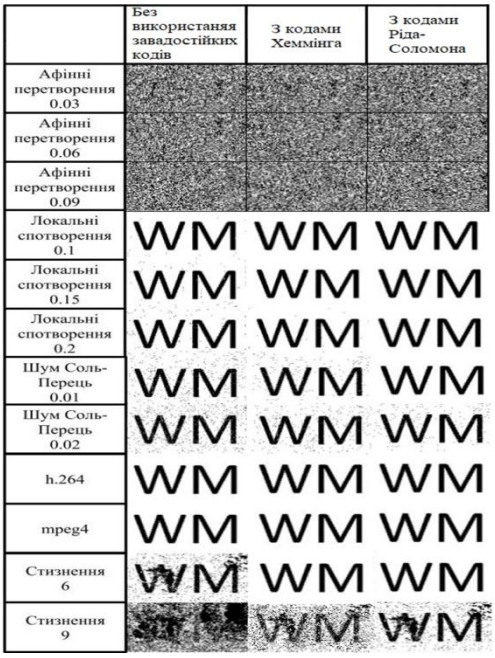


Рис. 1. Результати вилучення цифрових водяних знаків після проведення атак при застосуванні завадостійких кодів

Проаналізувавши результати можна зробити висновок, що використання завадостійких кодів значно підвищує стійкість алгоритмів до проаналізованих атак. До того ж застосування завадостійких кодів Ріда-Соломона, через кращі самокоригувальні властивості, значно підвищує стійкість алгоритмів вбудовування цифрових водяних знаків у відеофайли.

Список літератури

1.Г. Ф. Конахович, и А. Ю Пузыренко, “Компьютерная стеганография. Теория и практика”, *МК-Пресс*, 2006.

2.Н. В. Шостак, А. А. Астраханцев, та С. В. Романько, “Дослідження стійкості алгоритмів захисту авторських прав на відеопродукцію”, *Системи обробки інформації*, №2, с. 138–143, 2017.

СЕКЦІЯ 2
ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.04:519.72

А.А. Борисенко, О.В. Бережная, А.И. Новгородцев, В.В. Сердюк, М.Н. Яковлев

5352008@ukr.net, o.berezhna@ekt.sumdu.edu.ua, a.novhorodtsev@ekt.sumdu.edu.ua, viktman2012@gmail.com

Сумский государственный университет, г. Сумы

ОЦЕНКА ПОМЕХОУСТОЙЧИВОСТИ СИСТЕМ ПЕРЕДАЧИ ДАННЫХ НА ОСНОВЕ КОДОВ С ПОСТОЯННЫМ ВЕСОМ

Одной из актуальных задач при построении адаптивных систем передачи данных (СПД) является эффективное помехоустойчивое кодирование при передаче данных по нестационарным каналам связи с изменяющимся уровнем степени его асимметричности. В существующих методиках обобщенной оценки помехоустойчивости СПД [1] предполагается, что в случае искажения кодовой комбинации в процессе передачи она может быть обнаружена или не обнаружена. Вероятность необнаруживаемых ошибочных переходов при этом определяется выражением:

$$V = \sum_{i-1}^{M} P_i \sum_{j=1, j\neq i}^{M} P_{ij}^{н} ,$$

где $P_{ij}^{н}$ – вероятность необнаруживаемого ошибочного перехода i-й комбинации, появляющейся с вероятностью P_i, в j-ю разрешенную из M возможных.

Достоинством этого способа оценки является его универсальность. Однако, применение его в работе адаптивной СПД затруднительно из-за значительной вычислительной сложности при оценке помехоустойчивости СПД. Поэтому при построении адаптивных СПД целесообразно, во-первых, применение более простых алгоритмов помехоустойчивого кодирования по сравнению с такими распространенными кодами как циклические, а во-вторых – наличие для таких кодов аналитических выражений для оценки вероятности необнаруживаемых переходов. Исследования показали, в качестве примера таких кодов могут служить равновесные коды [2]. Их достоинством является простота алгоритмов помехоустойчивого кодирования и соответственно простота кодирующих и декодирующих устройств. Равновесные коды характеризуются длиной кодовых комбинаций n и постоянным числом единиц в кодовых комбинациях $к$. Вероятность необнаруживаемых ошибочных переходов для равновесных кодов длины n с k единицами определяется выражением:

$$V = \sum_{r=1}^{k} C_k^r C_{n-k}^r P_{01}^r P_{10}^r P_{11}^{k-r} P_{00}^{n-k-r} .$$

Искаженная равновесная кодовая комбинация с необнаруживаемыми ошибками является тоже равновесной. Такое необнаруживаемое искажение сопровождается переходом r единиц в нули с одновременным переходом такого же количества нулей в единицы. В ходе исследований проведен сравнительный анализ помехоустойчивости циклических и равновесных кодов (рис. 1), в том числе и для асимметричных каналов связи, степень асимметрии которых удобно оценивать коэффициентом $\beta=p_{01}/p_{10}$, когда вероятности искажений нулей p_{01} и единиц p_{10} могут значительно отличаться.

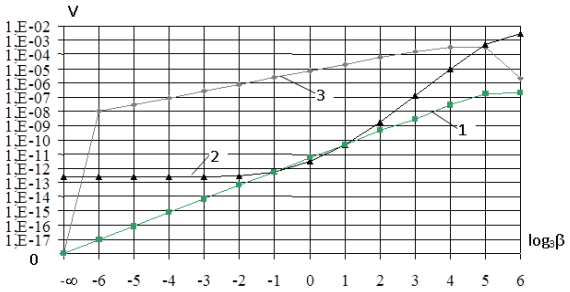


Рис. 1. Диаграммы зависимостей $V(\log_3\beta)$ $p_{10} = 10^{-3}$
1– равновесный код (n=8, k=4); 2– циклический код (8,3); 3– равновесный код (n=8, k=1)

Диаграммы показывают, что применение равновесных кодов для маломощных алфавитов предпочтительнее, по сравнению с циклическими, при достаточно большой степени асимметрии канала связи. Для равновесных кодов разработано аналитическое выражение для оценки их помехоустойчивости в зависимости от параметров искажений в асимметричном канале связи и от параметров равновесного кода. Этот подход и применение равновесных кодов позволили уменьшить вычислительную сложность оценки помехоустойчивости СПД и упростить сложность кодирующих и декодирующих устройств при построении адаптивных систем передачи данных.

Список литературы

1. А. А. Борисенко, и Е. Л. Онанченко, “Оценка помехоустойчивости неразделимых кодов”, *Вісник Сумського державного університету*, №2, с. 64-68, 1994.

2. А. А. Борисенко, О. В. Бережная, и И. А. Кулик, “Оценка помехоустойчивости системы передачи данныхна основе равновесных кодов”, *Вісник Сумського державного університету*. №1, с. 79-82, 1999.

УДК 519.6

A.E. Goloskokov, I.V. Liutenko

goloskokov@ukr.net, liv@kpi.kharkov.ua

National Technical University "Kharkiv Polytechnic Institute", Kharkiv

THE DECISION-MAKING PROBLEM IN CONDITIONS OF FUZZY INITIAL INFORMATION

The problem of decision making or the problem of choosing alternatives is one of the most common classes of tasks that not only the researcher faces. The authors formulated the decision making problem as follows. There are many solutions (alternatives), the implementation of each of which leads to the onset of some consequences (outcomes). Analysis and evaluation of outcomes by a set of performance indicators (criteria) uniquely characterizes alternatives.

It is necessary, having studied the preferences of the decision maker (DM), to construct a model for choosing an alternative that is the best in a certain concrete sense. The system of preferences of decision makers will be understood as the totality of its ideas (about the criteria for achieving the goal, advantages and disadvantages of the compared alternatives), allowing to make a targeted choice of elements from a variety of alternatives. Decision makers' preferences are identified, structured and formalized in the course of a special study aimed at building a model. The decision maker is often forced to act in the face of uncertainty, that is, the decision maker has less information than is necessary for the expedient organization of his actions in the decision-making process. The use of fuzzy verbal concepts used by the decision maker allows to introduce into consideration qualitative descriptions and take into account the uncertainty of the decision-making task, to achieve a complete description of all factors relevant to this task and not amenable to an exact quantitative description. The processing of fuzzy information in decision-making tasks is ensured by applying a linguistic approach. Applying the expected utility as a criterion for the selection of alternatives in the conditions of stochastic uncertainty, the analysis of the solution boils down to obtaining initial data of two types: 1) information about the preferences of the decision maker, which is then formalized as a utility function; 2) information about stochastic uncertainty, which is then formalized as a probability distribution.

Under the usefulness authors understand the degree of suitability of the alternative to the goal facing the decision maker. If the utility value is considered on the interval [0; 1], then the information about the preferences of the decision maker, formalized as a utility function, is given in the form of statements [1]:

<Outcome with criterial evaluation of G has utility υ>.

Obtaining information about stochastic uncertainty for specifying a probability distribution when objective data are not available happens as follows. It is assumed that the source of this information is the decision maker with his experience and knowledge of the decision-making environment. The continuous probability distribution is specified as a distribution function or corresponding density. To effectively solve the problem of choosing the optimal alternative in the conditions of fuzzy initial information, the authors suggest solving the following problems. 1. Checking the external consistency of the fuzzy source information formalization. 2. Checking the consistency of the fuzzy source information formalization about the probabilities of the alternatives outcomes appearance.

The paper presents a procedure for checking the external consistency of formalization of the initial data on the utility function based on the use of informational granules. External consistency assessment of the fuzzy source information formalization about the utility function is reduced to a comparison of the obtained membership functions of fuzzy values of the expected utility. The properties of vagueness and stochasticity of the initial information make it necessary to check its consistency. Namely, the verification of the conformity of the formal data of the task with the representations of the decision maker. At the same time, one can single out the consistency, completeness and redundancy check.

Consider the process of checking the consistency of the fuzzy source information formalization about the probabilities of the alternatives outcomes appearance in a decision-making task. At the same time, the authors distinguish two subtasks: checking internal consistency and checking external consistency. The procedure for checking internal consistency is considered. Introduced a criterion of internal consistency of the original data in probability. The external consistency of the formalization of non-clear initial data on the probabilities of occurrence of outcomes - alternatives was checked. External consistency means the correspondence of the conclusions obtained on the basis of informational granules to the representations of the decision maker. The considered procedure for checking the consistency of the fuzzy source information formalization about the probabilities of the alternatives outcomes appearance reveals the need to correct the formalization of the source data and thereby increase their consistency in the decision-making task.

References

1. А. Е. Голоскоков, "Задача выбора оптимальной альтернативы в условиях нечеткой исходной информации", *Вестник Харьковского государственного политехнического университета.* № 121, с. 99-103, 2000.

УДК 004.657

А.С. Гавриленко, А.Г. Савенко

savenko@bsuir.by

Институт информационных технологий Белорусского государственного университета информатики и радиоэлектроники, г. Минск, Республика Беларусь

РАСПРЕДЕЛЕНИЕ НАГРУЗКИ ПРИ ПОСТРОЕНИИ ОТЧЁТОВ И ЗАПРОСОВ С БОЛЬШИМ ОБЪЁМОМ ДАННЫХ

При увеличении запросов в небольших и средних по объёмам обрабатываемой информации приложениях или сайтах, возникает вопрос о расширении тех или иных возможностей для ускорения отображаемых или загружаемых данных.

Рассмотрим проект, имеющий мобильное, web- и desktop-приложения. Все они подключаются к определенному API для осуществления взаимодействие по схеме клиент-сервер. В какой-то момент единственный воркер (процесс который выполняется в фоновом режиме) работающий на сервере начинает отключаться, вследствие чего, возникает ошибка. Данные события характеризуются тем, что API не хватает мощностей проекта, и даже после очередной перезагрузки воркера, работоспособность инструмента не будет восстановлена. Решением, в данном случае, может являться распределение нагрузки между нодами (сервер, или несколько серверов) расположенных на компьютерах, которые перенаправляют всю нагрузку от одного сервера на другие, тем самым упрощая и ускоряя работу единственного сервера.

Предлагается следующая схема перераспределения нагрузки. Для API, которое изначально выполняло функции получения информации, её обработке и выдаче, оставляется только первая. Получая какой-либо запрос (GET, POST, PUT, DELETE), API отдает параметры запроса в очередь RabbitMQ (брокер сообщений). Rabbit должен состоять из следующих частей: exchange (коммутатор), подписчиков, сообщений, имеющих хэш, записываемый в Redis (быстрая база данных по типу ключ-значение), который выступает в роли ключа и параметров запроса, выступающих в роли значения. К данным параметрам добавляется также статус, в котором находится текущий процесс, (request, process, succeed). В сообщениях также передается routing_key – ключ назначения. В данном случае ключ служит для перенаправления на нужный контроллер, в котором метод осуществляет логику. Запустив очередной воркер, осуществляется подписка на коммутатор, который выполняет распределение нагрузки между подписчиками следующим образом: если подписчик занят в текущий момент, коммутатор передаст сообщение тому, кто свободен или будет ждать того, кто быстрее всего освободится. Таким образом, подписчики выполняют все действия, которые ранее выполняло единственное API. Используя любую страницу, запрос, действие или функцию проекта, осуществляется распределение на воркер с наименьшей нагрузкой. Воркер, который выполнил определенный алгоритм действий, передает ответ в конкретную очередь, предназначенную для выполнения алгоритмов, и которая указана в сообщении. Параллельно всем действиям происходит подписка на очередь ответа (reply-to), в которую передается ответ алгоритма, заданного в воркере. И в случае какого-либо результата – передается ответ клиенту.

Проанализируем данную схему на предмет быстродействия. Данные для обработки, будут поступать под разнообразные задачи. Может наступить момент, когда воркеры загружены большими длительными задачами и мешают выполнению мелких задач. Для того чтобы это не происходило, необходимо разграничить воркеры. Для разграничения воркеров, нужно выявить мелкие задачи и задачи с большими объемами данных, тем самым разделив воркеры на несколько групп (в том числе группу воркеров обрабатывающих отчеты). Этими действиями можно добиться максимального ускорения системы, т.к. воркеры, будут разграничены, а мелкие задачи, не буду ждать воркеров, обрабатывающих большие данные. Однако, если ограничиться равным количеством воркеров, это не повысит, т.к. некоторые воркеры будут простаивать впустую. Для исключения такой ситуации, нужно распределить количество воркеров: для мелких задач необходимо выделить небольшое количество воркеров (т.к. задачи быстро выполняются), а для более сложных задач следует выделить большее количество воркеров (т.к. они обрабатываются долго). Если для схемы будет использоваться только один клиент, а результат при множественных одинаковых запросах обрабатывается каждый раз, то использование серверных мощностей будет не совсем рационально. Чтобы не загружать сервера на которых работают воркеры можно использовать сервер Redis, как средство для хранения кэша обработанных результатов. Поиск текущего хэша в Redis производится быстрее, чем очередная обработка такого же результата с последующей его обработкой на воркерах. Для осуществления кэширования, требуется результат выполнения воркера отправить в Redis, где результат будет значением, а хэш, который был сгенерирован ранее, будет ключ

УДК 621.37/.39

І. Г. Гусарова, О. М. Соловйов

iryna.husarova@nure.ua, oleksii.soloviov@nure.ua

Харківський національний університет радіоелектроніки, м. Харків

РЕЗУЛЬТАТИ ЧИСЕЛЬНОГО МОДЕЛЮВАННЯ НЕСТАЦІОНАРНИХ РЕЖИМІВ З ВИКОРИСТАННЯМ МЕТОДУ БРОЙДЕНА

Існує велика кількість чисельних методів, для розв'язання широкого спектру проблем. Більшість з цих методів з'явилися у 20 столітті з появою ЕОМ. Зараз можливості ЕОМ збільшились в мільйони разів, і багато людей за допомогою комп'ютера можуть проводити експерименти, результати яких будуть застосовані у реальних видах діяльності. Одним з таких видів діяльності є транспортування газу. Транспортування газу не новий вид діяльності, і вже є робочі методи для цієї галузі, але все ще є можливості для покращення існуючих методів.

Важливим елементом системи транспортування газу є як ця система може обробляти нештатні ситуації. Режим течії газу в цих ситуаціях є нестаціонарним та неізотермічним. Рівняння математичної моделі такого режиму доцільно вирішувати за допомогою метода скінченних різниць з неявною рівномірною скінчено-різницевою сіткою [1]. В процесі розв'язання з'являється система нелінійних рівнянь. Цю систему зазвичай вирішують за допомогою методу Ньютона, тому що він має квадратичну збіжність, при цьому він буде збігатися оскільки початкове приближення, яке необхідно для методу, береться близьким до розв'язку. У методі Ньютона в даному випадку є один недолік: на кожному кроці необхідно перераховувати матрицю Якобі. Метод Зейделя, модифікований метод Ньютона, метод Бройдена в процесі розв'язання системи використовують апроксимацію матриці Якобі. Це може покращити швидкодію програми, яка обчислює параметри газового потоку.

За математичну модель нестаціонарного неізотермічного режиму течії газу (НН РТГ) по ділянці трубопроводу (ДТ) беремо квазілінійну систему диференційних рівнянь у частинних похідних, які випливають із загальних рівнянь Нав'є-Стокса газової динаміки для одновимірного випадку [1]. Ця система має вид:

$$\frac{\partial \phi}{\partial t} + B(x,t,\phi)\frac{\partial \phi}{\partial x} = \Phi(x,t,\phi), \quad (1)$$

де B, Φ – матриці, елементами яких задані неперервно диференційовані в деякій області зміни своїх аргументів функції змінних x,t,W,P,T; $W(x,t),P(x,t),T(x,t)$ – витрата газу, тиск газу, температура газу; $\phi = \left(W(x,t),P(x,t),T(x,t)\right)$ – деякий неперервно диференційований в деякій області, розв'язок рівняння (1).

Для розв'язку системи (1) з відомими граничними та початковими умовами використаємо метод скінченних різниць з рівномірною скінчено-різницевою сіткою. Для цього ділимо відрізок $[0,L]$ на n відрізків, де L – довжина ДТ. В систему (1) підставляємо апроксимацію похідних, та отримуємо систему нелінійних алгебраїчних рівнянь.

Для розв'язку системи нелінійних рівнянь використовуємо метод Бройдена. На S-й ітерації отримуємо лінійну систему рівнянь, яка в загальному вигляді має вид:

$$\left[\frac{\partial \psi^k}{\partial \phi^k}\right]_{\phi^{k,0}} \delta\phi^{k,1} = \psi^{k,0} \text{ при } s=0,$$

$$A^{k,s}\delta\phi^{k,s+1} = \psi^{k,s} \text{ при } s=1,2\ldots,$$

де $A^{k,s}$ – апроксимація матриці Якобі, яка на кожному кроці перераховується по формулі:

$$A^{k,s+1} = A^{k,s} + \frac{(\psi^{k,s+1} - \psi^{k,s} + A^{k,s}\delta\phi^{k,s+1})\delta\phi^{k,s+1}}{\left\|\delta\phi^{k,s+1}\right\|^2}.$$

Після розв'язку лінійної системи ми отримуємо параметри газового потоку на даному часовому шарі.

Для початку роботи алгоритму необхідні дані з попереднього часового шару та граничні умови.

Цей алгоритм був реалізований у математичному пакеті Mathematica 11.3, проведено ряд чисельних експериментів, пов'язаних з підключення та відключення великого споживача.

В результаті чисельного моделювання НН РТГ з використанням методу Бройдена на етапі розв'язку системи нелінійних рівнянь був показаний задовільний результат.

Список літератури

1. И. Г. Гусарова, и Д. В. Мелиневский, "Численное моделирование режимов течения газа методом конечных разностей", *Системи Обробки Інформації: збірник наукових праць.* №4(141), с.23-27, 2016.

УДК 004.94

Г.М. Дрєєва, О.А. Смірнов

gannadreeva@gmail.com, dr.smirnovoa@gmail.com

Центральноукраїнський національний технічний університет, м. Кропивницький

ГЕНЕРУВАННЯ ФРАКТАЛЬНОГО ТРАФІКУ ЗА ДОПОМОГОЮ МОДЕЛІ ГЕНЕРАТОРА НА ГРАФІ

Багато комп'ютерних систем представлені математичними моделями у вигляді систем масового обслуговування. Також актуальним це є при розробки систем забезпечення обміну інформацією в комп'ютерних та телекомунікаційних мережах. Доведено, що трафік в комп'ютерних мережах на певних масштабах є фракталоподібним і при цьому класичні закони розрахунку параметрів системи масового обслуговування дають хибні результати. Найбільш надійними засобами розрахунку параметрів системи масового обслуговування з фрактальним трафіком на сьогодні є результати імітаційного моделювання, бо переважна більшість фрактальних джерел трафіку не піддаються аналітичному розв'язанню. Тому для проведення чисельних експериментів з імітуванням необхідно мати генератори фракталоподібного трафіку. Вже традиційно для отримання фракталоподібного трафіку на сьогоднішній день використовують випадкові числа, які генеруються за законами розподілу з "важким хвостом".

Розподіли з "важким хвостом" мають повільно спадаючий характер розподілу густини ймовірності, що призводить до нескінченного значення дисперсії розподілу, коли математичне сподівання має конкретне значення; іноді використовуються моделі в яких математичне сподівання теж прямує до нескінченності. На жаль, математичні абстракції та узагальнення, які полегшують математичні перетворення або взагалі роблять їх можливими, мають межі практичного використання. Яскравим прикладом зловживання нескінченно малими величинами при використанні інтегрально-диференціального обчислення можна знайти в фізиці матеріалів: застосування інтегралу для рахування енергії напруження матеріалу тріщин призводить до виникнення нескінченності в напруженості матеріалу в точці росту тріщини. Фізично таке не є можливим, причиною цього є порушення закону Юнга при значних деформаціях та дискретна природа речовин – речовина складається з дискретних часток і інтегральне числення є по факту наближенням до реальності і використовується лише з причин математичного спрощення моделі фізичних процесів.

Відповідно до трафіку в комп'ютерній мережі, вузол зв'язку не може отримати нескінченно великий запит на обслуговування з причини обмеження швидкості передачі по лініям зв'язку. Обмеження генерованого запиту в процесах імітаційного моделювання систем масового обслуговування проводиться штучно, але це порушує теоретичні властивості фрактальності трафіку, тому результати моделювання не можуть вважатися надійними. За зазначеними проблемами з використанням розподілів з "важким хвостом" в роботі пропонується використовувати генератор фрактального трафіку на основі графу скінченного автомату.

Нехай проводиться вивчення поведінки маршрутизатору в телекомунікаційній комп'ютерній мережі, з наступними параметрами:

– має N рівнозначних каналів з підключеними клієнтами;

– має можливість перенаправити M пакетів за одиницю часу;

– містить загальний внутрішній буфер-чергу на K пакетів.

Тоді клієнти, які під'єднані до ліній входу/виходу, є генераторами фрактального трафіку та споживачами цього трафіку. Кожен клієнт генерує фракталоподібний трафік, але й зміна адреси посилання повинна змінюватися фрактально. Для забезпечення роботи описаної схеми потрібно мати генератор фракталоподібного трафіку з можливістю регулювання інтенсивності запитів та їх фрактальної розмірності.

Таким чином, у даній роботі, для формулювання методу генерування фрактального трафіку за допомогою моделі генератора на графі, вирішені наступні завдання:

– Показано актуальність задачі створення генераторів фрактальних бінарних послідовностей без використання нескінченних розподілів.

– Запропоновано використати генератор фрактальної бінарної послідовності на основі скінченного автомату.

– Показано можливість попереднього визначення фрактальної розмірності генерованого трафіку при інтенсивності τ=0.5.

– Проведено аналітичні оцінки показника Херста генерованої бінарної послідовності при інтенсивності трафіку τ=0.5.

– Показано варіативність фрактальної розмірності бінарної послідовності й при інших інтенсивностях τ.

– Виведено аналітичні вирази для отримання параметрів генератора з заданою густиною вихідних бітів з керуванням їх фрактальної розмірності.

Роботу потрібно продовжити покращенням аналітичних оцінок та їх узагальнення на довільну інтенсивність генерованого трафіку.

УДК 621.391

В.Г. Иванов

vladimir-ivanov50@ukr.net

Национальный юридический университет имени Ярослава Мудрого, г. Харьков

СЖАТИЕ ИЗОБРАЖЕНИЙ НА ОСНОВЕ АВТОМАТИЧЕСКОЙ И НЕЧЕТКОЙ КЛАССИФИКАЦИИ ФРАГМЕНТОВ

Метод автоматической классификации базируется на алгоритме k- средних. Для сжатия изображений алгоритм *k*-средних используется следующим образом. Изображение разбивается на одинаковые, например, квадратные элементы с размером стороны *m* пикселей. Яркости пикселей каждого элемента составляют m^2-мерный вектор. К совокупности всех элементов применяется алгоритм *k*-средних, что приводит к разбиению изображения на *k*, как правило, несвязных областей $S_1,...,S_k$, каждая из которых состоит из почти одинаковых элементов. Для кодирования изображения нужно составить карту регионов, определяющую размещение областей, и для каждой области S_j указать ее представителя, в качестве которого используется ее центр [1].

В более совершенном варианте алгоритма сжатия к каждому квадратному элементу изображения пред классификацией применяется декоррелирующее преобразование – дискретное косинусное преобразование Фурье или преобразование Хаара. Далее в качестве пространства признаков используется то или иное число коэффициентов, полученных при одном из этих преобразований. Нечеткой классификацией множества *X* *p*-мерных векторов по *k* классам $S = (S_1,...,S_k)$ понимается сопоставление каждому элементу *x* из *X* набора *k* неотрицательных чисел $(\alpha_1(x),\alpha_2(x),...,\alpha_k(x))$, в сумме составляющих 1. Эти числа называются коэффициентами принадлежности классу и могут трактоваться как вероятности того, что данный элемент принадлежит тому или иному классу. Задача нечеткой классификации состоит в нахождении минимума суммы взвешенных дисперсий нечетких множеств *S*, то есть функционала

$$Q(S) = \sum_{l=1}^{k} \sum_{x \in X} \alpha_l^2(x) \|x - e_i\|^2 ,$$

где $(e_1,...,e_k)$ – набор центров нечетких множеств, а символ $\|v\|$ означает, как и выше, длину вектора v из X.

Алгоритм С-средних, позволяющий решить эту задачу, состоит в следующем.

Параметром классификации является число классов *k*. Из множества *X* произвольно выбирается *k* векторов $e_1,...,e_k$, которые рассматриваются как центры классов в первом приближении. После чего строится нечеткое разбиение множества *X* на классы, порождаемое этими центрами. То есть для каждого вектора *x* вычисляются коэффициенты принадлежности:

$$\alpha_j(x) = \left[\sum_{i=1}^{k} \left(\frac{\|x - e_j\|^2}{\|x - e_i\|^2} \right) \right]^{-1}, \; j = 1,2,...,k .$$

Заметим, что коэффициент $\alpha_j(x)$ принадлежности вектора *x* классу S_j тем больше, чем ближе центр e_j этого класса к этому вектору.

После этого для каждого построенного класса находятся центры второго приближения как средневзвешенные средние:

$$e_j = \sum_{x \in X} \frac{\alpha_j^2(x)}{\sum_{x \in X} \alpha_j^2(x)} x .$$

Далее процедура полностью повторяется, но уже с новыми центрами классов. Описанные итерации заканчиваются, когда центры классов перестают изменяться. Переход от нечеткой классификации к обычному разбиению на классы осуществляется следующим образом: каждый элемент приписывается тому классу, коэффициент принадлежности к которому для этого элемента является наибольшим. Метод сжатия изображений на основе автоматической и нечеткой классификации фрагментов различной размерности позволил существенно, в несколько раз, уменьшить объем данных для изображений, сильно насыщенных деталями, например, оттисков печатей, по сравнению с результатами, полученными методами на основе косинус- и вейвлет-преобразований.

Список литературы

1. В. Г. Иванов, Ю. В. Ломоносов, и М. Г. Любарский, “Сжатие изображений на основе автоматической и нечеткой классификации фрагментов”, *Проблемы управления и информатики*, № 1, с. 52 – 63, 2009.

УДК 004.4

І. А. Карпов, О. М. Верес, Н. Е. Кунанець

shad1ksen@gmail.com nek.lviv@gmail.com

Національний університет «Львівська політехніка», м. Львів

СИСТЕМА ПІДТРИМАННЯ ПРИЙНЯТТЯ РІШЕНЬ ДІЯЛЬНОСТІ КОМПАНІЙ У СФЕРІ ОБСЛУГОВУВАННЯ

В умовах жорсткої конкуренції сучасний ринок характеризується змінами стосунків між клієнтами та постачальниками. Постачальники не тільки вступають у жорстоку конкуренцію за кожного клієнта, але і докладають все більше зусиль, щоб задовольняти вимоги клієнтів. Для завоювання чи утримання сегменту ринку, діяльність постачальника має бути високоефективною. В таких умовах проблема збуту стає дуже важливою. Це приводить до того, що за клієнтами починаються буквально полювати, переконуючи за допомогою реклами в доцільності придбання товару саме цієї фірми.

Дослідження поведінки клієнта і врахування результатів при створенні товарів і способів їх просування на ринок – це необхідна умова виживання в умовах жорсткої конкуренції. Дослідження потенційних клієнтів дозволяє виявляти звички і бажання. Для досягнення успіху компанії повинна підлаштовуватися під побажання клієнта. Глобалізація ринку і всепроникаючі інформаційні мережі відкрили для багатьох людей і організацій можливість обрання найпривабливіших товарів та послуг, а сучасні технології дозволяють запропонувати товари, послуги створені на їх індивідуальне замовлення. Дана робота присвячена аналізу функціональності інтелектуальної системи, яка забезпечує ефективну комунікацію з клієнтами у сфері обслуговування.

Практично у всіх компаніях є функціональні підрозділи, які забезпечують бізнес-процеси, орієнтовані на залучення клієнтів, – маркетингу та продаж [1]. Саме вони традиційно формують основу комерційного успіху в рамках компанії. основі якої інші підрозділи компанії будують свою політику

Такий підході фактично призводить до того, що закінчення терміну дії угоди з клієнтом, клієнт стає не “цікавим” для компанії, і саме це засвідчують дослідження. Комунікаційні стосунки з. клієнтом розриваються чи ослаблюються, якщо фірма не сповідує стратегію утримання. Для реалізації такої стратегії необхідно створення окремого підрозділу, на який покладається функція побудови ефективної комунікації з клієнтами. Завдяки створенню такого відділу компанії можуть формувати цілісну організаційну структуру, орієнтовану на клієнта [2].

Отже, аналізуючи функції відділу комунікації з клієнтом, можна зробити висновок, що досягнення поставлених задач щодо управління взаємовідносинами з клієнтами неможливе без злагодженої робити усіх підрозділів. В такій ситуації формується корпоративна стратегія роботи з клієнтами, на основі якої інші підрозділи компанії будують свою політику. Таким чином, робота різних підрозділів набуває клієнтоцентриського забарвлення і стає фокусом корпоративних інвестицій.

Таким чином, клієнтоцентриська стратегія забезпечує цільові налаштування роботи організації для задоволення потреб клієнтів.

Інтелектуальна система підтримки комунікаційних процесів з клієнтом складається, як правило, з модулів автоматизації [2]: Продажів, Маркетингу, Обслуговування клієнтів. А основою інтелектуальної системи є застосунки, на які покладаються наступні функції: Ведення календаря подій і планування роботи, Управління контактами, Аналіз запитів клієнтів, Моніторинг потенційних продажів, Потокова організація продажів, Надання інформації про ціни, Надання інформації про стан справ у представництвах, Формування звітів. Діаграма активності відображена на рис. 1.

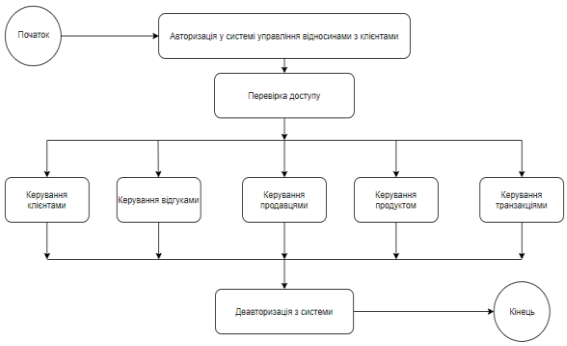


Рис. 1. Діаграма активності

Підводячи підсумок, слід зазначити, що в сучасному світі успіх компанії залежить від налагодження ефективних взаємовідносин з клієнтами. Зміни у зовнішньому середовищі потребують перегляду основ управління та перерозподілу обов’язків всередині організації. Отож, кожен виробник, мусить прагнути до побудови довготермінових комунікацій з клієнтами.

Список літератури

1. Луис Бун, и Дэвид Куртц, “Современный маркетинг”, *ЮНИТИ-ДАНА*, 2012.

2. Патрик Молино, “Технологии CRM: Экспресс-курс”, *Фаир-Прессь*, 2004.

УДК 519.816.009.12

В.М. Косарєв

ut5ex@ukr.net

Університет імені Альфреда Нобеля, м. Дніпро

ЗАСТОСУВАННЯ МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ ПРОТИДІЇ КОНКУРЕНТІВ

В останні десятиліття розгорнулася наукова дискусія між прихильниками раціональної поведінки при підготовці і прийнятті рішень і прихильниками обліку нераціонального поведінки осіб, які приймають рішення, через їх «асиметричної реакції на можливі втрати і придбання» [1, 2].

Опоненти дискусії, Вернон Сміт і Даніель Канеман, займали протилежні позиції. Однак комітет з Нобелівських премій в 2002 р. прийняв об'єктивне рішення: вони разом отримали Нобелівську премію [2].

Як відомо, корисність і ризик прийнятих рішень у вигляді виграшу і втрат залежать від переваг особи, що приймає рішення [1-4]. Теорія прийняття рішень і практика підтверджують необхідність і раціонального, і евристичного начала. Неминучі при цьому три етапи: етап підготовки рішення; етап власне прийняття вольового рішення; етап прогнозування наслідків прийнятого рішення.

Перший етап реалізують за допомогою моделі функції корисності і ризику. Вона повинна адекватно відображати зв'язки рівнів придбань і втрат з можливостями їх появи в умовах протидії конкурентів.

На другому етапі діє особа, яка, як правило, "симетрично реагує на можливі втрати і придбання", віддаючи переваги зменшенню ризиків ціною відмови від можливих придбань.

Третій етап, як правило, доцільно присвячувати експериментально розрахунковому прогнозування наслідків рішення шляхом обробки обмеженою сукупності вихідних даних, одержуваних, наприклад, в ході ділової гри, де роль конкуруючої сторони виконують свої ж особи.

Метою дослідження є розвиток теорії доцільної, компромісної поведінки, заснований на взаємопов'язаному застосуванні цих трьох етапів.

На першому, найбільш трудомістким етапі, в якості основи моделі функції корисності і ризику, яка описує здобутки та втрати на шляху до досягнення мети операції, мабуть, доцільно вибрати, наприклад, криву розвитку логістичного типу і для виграшів, і для втрат.

Другий етап є наближеним. Він носить суто особистісний характер. Відображає переваги особи, що приймає рішення. Витрати часу на реалізацію цього етапу менше, ніж на реалізацію першого етапу в середньому приблизно в сім разів. Таке припущення ґрунтується на загальноприйнятій рекомендації, відомої з досвіду підготовки та прийняття рішень: "сім разів відміряй – один раз відріж!".

Третій етап – не менше трудомісткий, ніж перший. Він націлений на прогнозування наслідків прийнятого рішення в умовах невизначеності випадкового і антагоністичного типу. Іншими словами, наслідки рішення залежать від сукупної безлічі непередбачених випадковостей і реакцій конкурентів.

Тому основу вихідних даних для прогнозування можуть скласти раніше спостерігаємо результати рішення, прийнятого в аналогічних умовах.

Більш надійними є експериментально отримані вихідні дані про результати впливу протидіючих чинників на досяжні придбання і очікувані втрати.

Нарешті, менш витратну основу для вирішення завдання придбання даних для прогнозування можуть скласти результати спеціально організованої ділової гри. Роль протиборчої сторони повинні виконувати спеціально призначені, підготовлені менеджери з багатим особистим досвідом.

У всякій ситуації необхідний об'єктивний прогноз розвитку процесу досягнення мети операції. Цю мету необхідно висловити, перш за все, кількісної характеристикою. Доцільною характеристикою є ймовірність досягнення встановленого виграшу і величини втрат під дією детермінованих і випадкових факторів.

Об'єктивний прогноз можливий за умови, що основний механізм, який породжує зміни тренду процесу, є постійно діючим і практично не змінюється його інтенсивність впливу.

Отже, пропонована модель для ухвалення рішень в умовах протидії конкурентів ґрунтується: на поетапної побудові функції корисності і ризику; на обліку асиметричного відносини особи, яка приймає рішення до втрат і придбань; на статистичному прогнозуванні параметрів функції корисності і ризику.

Список літератури

1. D. Kahneman, and A. Tversky, "Prospect theory: An analysis of decisions under risk", *Econometrica*, Vol. 47, № 2, pp. 263-291, 1979.

2. Ф. Борисов, "Дэниел Канеман – стратег принятия решений", *Информационно-аналитическая газета* , № 5 (148), с. 9, 2011.

3. "Теория прогнозирования и принятия решений", *Москва: Высшая школа*, 1977.

4. П. Фишберн "Теория полезности для принятия решений", *Москва: Наука*, 1978.

УДК 004.832.28

І. О. Кріслата, Н. Е. Кунанець

irynakrislata@gmail.com, nek.lviv@gmail.com

Національний університет "Львівська політехніка", м. Львів

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ З УПРАВЛІННЯ ТРАНСПОРТНИМИ ПОТОКАМИ ВЕЛИКОГО МІСТА

Сучасні тенденції розвитку великого міста генерують потребу формування пріоритетів, до яких належить створення технологічної інфраструктури міського транспорту та систем управління, спрямованих на задоволення постійно зростаючого попиту населення, а також зниження перевантажень.

Стійкість транспортних систем у великих містах і мегаполісах визначається стабільністю їх підсистем, а також стійкістю відносин між ними. Ця стабільність забезпечується, в значній мірі, якістю управління. Для управління великими інфраструктурами, зокрема транспортними, створюються спеціальні інструменти, такі як системи підтримки прийняття рішень. Їх призначення полягає у забезпеченні стратегічного управління, а також вирішенні локальних тактичних завдань. Раціональне управління дозволяє не тільки поліпшити економічні показники, але й вирішувати соціальні завдання щодо покращення транспортного обслуговування населення та зменшення негативного впливу транспортного комплексу на довкілля. В.В. Семенов [1] подає розгорнуте обґрунтування необхідності застосування методів математичного моделювання для ефективної побудови транспортних потоків. Він наголошує, що при вирішенні даної проблеми не можливо опиратися на статистичні дані чи експертні оцінки в силу непередбачуваності поведінки кожного водія з приводу вибору маршруту, манери водіння, а також впливу випадкових факторів (ДТП, погоди), зростання чи зменшення потоків у вихідні чи святкові дні. Автор зауважує, що засобами математичного моделювання можна вирішувати актуальні задачі в масштабі міської агломерації: прогнозування змін у роботі транспортної системи при додаванні нових елементів, реорганізацію транспортної інфраструктури міста при будівництві нового житлового району, перерозподілу потоків пасажирів і транспорту в разі тимчасового закриття чи ліквідації одного із елементів транспортної системи, вивчення ризиків при долученні автоматизованої системи управління дорожнім рухом; а також вирішувати задачі локального масштабу: прогнозування ефекту від перепланування перехрестя чи групи перехресть, розширення проїжджої частини вулиці, оптимізації світлофорного регулювання тощо; необхідність перепланування роботи дорожньої мережі, пасажирського і вантажного транспорту.

Дайгенг Н. [2] запропонував нові методи для формалізації транспортного потоку шляхом подання математичними моделями. Автор детально зупиняється на характеристиці транспортних потоків, аналізує можливості використання інтелектуальних транспортних систем (ITC технологій) і моніторингу руху.

В світовій практиці інтелектуальні транспортні системи вважаються сервісною системою, призначеною для обслуговування користувачів-водіїв, пішоходів та велосипедистів, пасажирів громадського транспорту, перевізників, операторів транспорту, а також споживачів послуг з експлуатації транспортної інфраструктури, працівників аварійних служб.

При розробленні ITC методологічно грунтуються на системному підході, формуючи її як цілісну систему, у якій взаємодіють окремі модулі. Формується відкрита архітектура системи, протоколи обміну інформацією, форма транспортних документів, стандартизуються процеси комунікації, обираються параметри технічних засобів, підходи до проведення контролю та процедур управління тощо.

Запропонована ITC передбачає наявність багатовимірної інтелектуальної моделі даних для ефективного управління трафіком, збору, зберігання інформації про функціонування дорожньої мережі та формалізації параметрів. Оперативна інформація, яка надходить в центр управління в реальному масштабі часу з різних джерел, опрацьовується і сприяє коректному моделюванню реальних подій та оперативному корегуванню дорожньої ситуації.

Економічний ефект застосування ITC визначається зменшенням транспортних витрат шляхом оптимізації маршрутів та підвищення ефективності автопарку. Екологічний ефект, який може бути досягнутий шляхом раціонального перерозподілу транспортних потоків на мережах автомобільної дороги міста, полягає в зменшенні негативного впливу на навколишнє середовище. Соціальний ефект сприятиме зменшенгю ризику захворювання через якість повітря у місті. Отже, запропонована ITC покликана не лише підвищити якість життя мешканців міста, але й поліпшити його екологічний стан.

Список літератури

1. В. В. Семенов, *Математическое модели-рование динамики транспортных потоков мегаполиса*, Институт прикладной математики им. М.В. Келдыша, 2004.

2. Ni Daiheng, *Traffic Flow Theory: Characteristics, Experimental Methods, and Numerical Techniques*, Butterworth-Heinemann, 2015.

УДК 004.627

И.А. Кулик, Е.М. Скордина, М.С. Шевченко

i.kulyk@ekt.sumdu.edu.ua, e.skordina@ekt.sumdu.edu.ua, marishev1993@gmail.com

Сумский государственный университет, г. Сумы

МОДИФИЦИРОВАННЫЕ СПОСОБЫ ПОДСЧЕТА ДВОИЧНЫХ ЕДИНИЦ

Вычисление числа двоичных единиц в исходных последовательностях является одной из самых значимых операций для методов защиты и сжатия данных, включая методы двоичного биномиального сжатия [1].

Тривиальный способ подсчета единиц заключается в последовательном просмотре каждого разряда a_i исходной двоичной последовательности $A_j = a_1 a_2 ... a_i ... a_n$, и если $a_i = 1$, то переменной единиц задавать соответствующее приращение. Значительный недостаток такого способа – необходимость тратить большое время (равное n тактов) для подсчета k единиц в наихудшем случае.

Предлагается более быстрый метод вычисления единиц, в основе которого лежит алгоритм, использующий вычислительную процедуру вида $S \leftarrow S \wedge (S-1)$, где S – двоичный набор [2]. Метод такого подсчета единиц будем называть арифметическим. Конечная цель предлагаемых усовершенствований − увеличить скорость подсчета числа единиц в двоичных последовательностях.

Способы применения арифметического метода зависят от метода защиты или сжатия информации. В случае использования методов преобразования двоичных данных, для которых необходимо точное знание k, предлагается в модели процесса подсчета единиц выполнять наряду с набором операций $A \leftarrow A \wedge (A-1)$ и процедуру вида $\overline{A} \leftarrow \overline{A} \wedge (\overline{A}-1)$. Данное изменение позволит как минимум в два раза уменьшить среднее время вычисления количества единиц. Для методов защиты и сжатия двоичной информации, условия работы которых зависят от граничных значений k, предлагается помимо $\overline{A} \leftarrow \overline{A} \wedge (\overline{A}-1)$ ввести еще и ограничивающую переменную L, которая будет равна границам α или $n-\alpha$. При превышении переменной числа единиц (нулей) значения L дальнейший подсчет единиц прерывается в виду того, что далее нет необходимости знать точное значение k. Такое усовершенствование также, как и предыдущее, позволяет в существенной степени сократить время вычисления k двоичных единиц.

Тогда модель процесса вычисления точного числа единиц для двоичной последовательности выглядит следующим образом.

Этап 1. Производится инверсия A_j: $\overline{A}_j = \overline{a}_1 \overline{a}_2 ... \overline{a}_i ... \overline{a}_n$, получая тем самым возможность оперировать не только с A_j, но и ее инверсной формой $\overline{A}_j$.

Этап 2. Если $A_j = 00...0$, то процесс подсчета двоичных единиц завершается, а переменная k содержит искомое значение.

Этап 3. Если $\overline{A}_j = 00...0$, то следует выполнить $k = n - k$. Далее процесс подсчета двоичных единиц также завершается, а переменная k будет содержать искомое значение. В противном случае необходимо перейти к следующему этапу.

Этап 4. Выполняются операции над A_j, $\overline{A}_j$:

$$A_j \leftarrow A_j \wedge (A_j - 1), \quad \overline{A}_j \leftarrow \overline{A}_j \wedge (\overline{A}_j - 1)$$

с дальнейшим приращением на единицу переменной $k = k + 1$. После этого осуществляется переход к этапу 2 для контроля равенства нулю A_j и $\overline{A}_j$.

Для методов преобразования двоичной информации, когда точное значение k необходимо только до граничных значений α или $n-\alpha$ приведенная выше модель при изменении этапа 4 дополняется этапом 5, позволяющим завершить подсчет при превышении граничного значения α.

Этап 5. Если выполняется $k \le L$, где $L = \alpha$, то осуществляется переход к этапу 2. В противном случае процесс подсчета завершается и k присваивается шаблонное значение $k = L + 1$.

Список литературы

1. И. А. Кулик, А. А. Борисенко, и О. Аджири, "Модели сжатия и восстановления данных на основе двоичных биномиальных чисел", *Збірник доповідей V Міжнародної наук.-практ. конф. "Методи та засоби кодування, захисту й ущільнення інформації"*, 2016, с. 101-105.

2. Э. Рейнгольд, Ю. Нивергельт, и Н. Део, "Комбинаторные алгоритмы. Теория и практика", *Мир,* 1980.

УДК 004.5/004.7

Н. Е. Кунанець, В. В. Пасічник, А. В. Ржеуський, Ю. В. Дубас, О. О. Кунанець

nek.lviv@gmail.com, vpasichnyk@gmail.com, antonii.v.rzheuskyi@lpnu.ua

Національний університет «Львівська політехніка» м. Львів

РОЗРОБЛЕННЯ КОМП'ЮТЕРНОЇ ПРОГРАМИ "STAT TRACKER"

Вступ. Сьогодні у процесах розроблення програмних засобів широко застосовують новітні технологічні вирішення та складні математичні моделі. Також розвиток програми-трекера вимагає досконалого знання області дослідження, щоб отримати бажані результати, однак це може виявитися недостатнім для створення успішної програми-трекера. **Стан дослідження проблеми.** Програмний продукт Tracker може використовуватись у різних сферах діяльності людини. Так, під час дослідження нами було встановлено, що інтерактивна комп'ютерна програма Tracker, використовується для аналізу процесу гальмування автомобіля [1]. Відеоаналіз за допомогою програмного забезпечення Tracker здійснюється в навчальній лабораторії фізики [2].

Мета. Метою даної роботи є аналіз основних принципів та засобів розроблення такого класу програмних продуктів як комп'ютерні програми-трекери, для їх використання у мережі Інтернет.

Постановка проблеми. Важливою проблемою розроблення програмних продуктів є зростання складності алгоритмів та моделей їх функціонування. Також однією із проблем сучасних комп'ютерних програм типу "tracker" є несприйняття потреби їх створення як окремого програмного продукту. Більшість ігор володіють вбудованими трекерами для збереження статистики та її аналізу. Звісно, це не враховано при розробці Колекційно-карткової гри (ККІ), де узагалі відсутні вбудовані трекери. Невід'ємною проблемою будь-якої популярної ККІ, є відсутність будь-яких можливостей записування зіграних матчів чи ведення по них статистики [1]. Проект є орієнтованим на інноваційність у програмному аспекті, маркетинговій галузі та вирізняється інформаційною моделлю.

Виклад основного матеріалу. Отримана у ході дослідження інформація показала високу конкуренту спроможність на IT ринку, відповідність загальним вимогам та критеріям оцінювання, вимогам якості. Запропонований програмний продукт відповідає вимогам якості , зокрема таким як: уніфікація; мобільність; масштабованість; взаємодія з користувачем. Вимоги якості FURPS+ дають високу оцінку проекту як такому, що забезпечує накопичення та аналіз статистичних даних.

Розроблений проект є інтелектуальною системою, що поєднує в одному додатку введення даних, здійснення їх перевірки та аналіз статистичних результатів. Додаток функціонує як інтелектуальна система, у якій можливе обрання версії для використання – тестової версії або ж платної підписки.

Проте лише при використанні версії, що передбачає платну підписку, можливе використання інтелектуальної системи у повному обсязі без функціональних обмежень, що притаманні тестовій версії. Основна платформа інтелектуальної системи поділяється на три основні елементи: модуль введення користувачем даних про свою фракцію та фракцію суперника, а також його нікнейм; модуль отримання даних з таблиці рейтингів; модуль опрацювання даних та вирахування прогнозованого результату при перемозі чи програші.

Висновки. Підтримка ігрових програмних продуктів допоміжним програмним забезпеченням є важливим завданням сучасного IT ринку. Запропонована інтелектуальна система належить до класу саме таких програмних продуктів і вирізняється від аналогів.

Список літератури

1. Peter Hockicko, Beáta Trpišová, et Ján Ondruš, "Correcting Students' Misconceptions about Automobile Braking Distances and Video Analysis Using Interactive Program Tracker", *Journal of Science Education and Technologyю,* vol. 23, iss. 6, , pp 763–776, 2014.

2. Arandi Ginane Bezerra Jr, Leonardo Presoto de Oliveira, Jorge Alberto Lenz, and Nestor Saavedra, "Videoanálise com o software livre Tracker no laboratório didático de Física: movimento parabólico e segunda lei de Newton", *Caderno Brasileiro de Ensino de Física*, v. 29, n. 1, pp. 469-490, 2012.

УДК 004.41

Ю.Е. Парфьонов

Yurii.Parfonov@m.hneu.edu.ua

Харківський національний економічний університет ім. С. Кузнеця, м. Харків

ПІДСИСТЕМА УПРАВЛІННЯ ДАНИМИ КОРИСТУВАЧІВ ВЕБ-ЗАСТОСУНКУ НА БАЗІ ФРЕЙМВОРКУ DJANGO

У 2018 році автором зареєстровано авторське право на програмний продукт “Knowledge Assessment System” (KnAS), призначений для комп'ютерного оцінювання рівня навчальних досягнень студентів [1].

Однак, йому притаманні певні недоліки, для подолання яких, розроблено веб-застосунок на базі серверного веб-фреймворку Django, який будемо називати KnAS Online. Цей застосунок має є два типи «звичайних» користувачів: студент і викладач. Для реалізації вимог до нього створено своя власна модель користувача CustomUser та моделі профілів користувачів зазначених типів.

Для забезпечення можливості управління даними користувачів KnAS Online з використанням сайту адміністратора Django, по-перше, доцільно при створенні нового користувача і подальших операціях з ним мати можливість роботи з його профілем. По-друге, профіль поточного користувача повинен вибиратися динамічна під час виконання.

Перше завдання вирішується шляхом використання так званих «inlines», тобто однієї або декількох залежних моделей всередині батьківської. Для цього необхідно визначити клас CustomUserAdmin, що представляє модель CustomUser в застосунку адміністратора Django.

Однак, найпростіша реалізація цього класу не дозволяє використовувати форми профілів користувачів динамічна. В літературі по фреймворку Django інформація про шляхи вирішення даної проблеми практично відсутня, за винятком [2], де згадується, що необхідно перевизначити функцію-генератор get_formsets_with_inlines класу UserAdmin. В результаті аналізу можливих варіантів реалізації даної функції, в клас CustomUserAdmin був доданий код, завдяки якому форма профілю щойно створеного користувача, відповідна його типу, з’являється тільки на сторінці редагування:

```
# перевизначена функція-генератор (псевдокод)
def get_formsets_with_inlines():
   if custom_user created:
      for inline in inline_instances():
         if custom_user_type  equals TEACHER and
                  inline is instance of TeacherInline:
            custom_user_is_staff = True
            yield (custom_user, inline)
   elif custom_user_type equals STUDENT and
                  inline is instance of StudentInline:
            yield (custom_user, inline)
```

Тепер на сторінці додавання нового користувача KnAS Online на сайті адміністратора Django будуть відображатися тільки поля для введення логіна, пароля і підтвердження пароля. Але, кожен користувач застосунку також повинен мати прізвище, ім’я та по батькові. Крім того, для вибору форми профілю користувача, яка згодом буде відображатися на сторінці редагування, при створенні нового користувача необхідно забезпечити можливість введення його типу. Для цього необхідно перевизначити поле add_fieldsets в класі CustomUserAdmin наступним чином:

```
add_fieldsets = UserAdmin.add_fieldsets + (
      (None, {'fields': ('user_type',)}),
      ('Personal info', {'fields': ('last_name', 'first_name',
'middle_name')}),)
```

Щоб на сторінці редагування користувача відображалися тільки його логін і форма для редагування профілю, необхідно також перевизначити поле fieldsets в класі CustomUserAdmin:

```
 fieldsets = (
      (None, {'fields': ('username',)}),
      ('Personal info', {'fields': ('last_name', 'first_name',
'middle_name')}),)
```

Таким чином, в роботі розглянуті питання реалізації підсистеми управління даними користувачів веб-застосунку для комп'ютерного тестування рівня навчальних досягнень студентів, розробленого на базі фреймворку Django. Створена модель даних користувача, що розширює стандартну модель AbstractUser, а також моделі профілів користувачів.

Використання розробленої підсистеми управління даними користувачів із застосунком адміністратора Django, дозволяє динамічна вибирати профіль користувача в залежності від його типу.

Список літератури

1. Ю. Е. Парфьонов, “Комп’ютерна програма “Knowledge Assessment System”, *Свідоцтво про реєстрацію авторського права на твір № 77613*, Март 14, 2018.

2. The Django admin site. [Online]. Available: http://docs.djangoproject.com/en/2.1/ref/contrib/admin. Accessed on: March 1, 2019.

УДК 621.397

В.І. Солодка

valyaonas@gmail.com

Одеська національна академія зв'язку ім. О.С. Попова, м. Одеса

СІТКОВІ 3D-ОБ'ЄКТИ ЇХ ОЦІНКА ТА ЯКІСТЬ ПРИ РІЗНИХ ШВИДКІСТЯХ ЦИФРОВОГО ПОТОКУ

У сучасному світі однією з актуальних задач об'ємного телебачення є удосконалення сіткових методів створення передавання і візуалізації тривимірного зображення [1].

Для опису складних об'ємних реальних об'єктів сітками необхідно рухатися в напрямку зменшення обчислювальних потужностей, так як в класичному вигляді кожна вершина об'єкта піддається математичному перетворенню, що збільшує на порядок обчислювальні витрати. Для зменшення обчислювальної складності сіткові моделі пропонується перехід в спектральну область, шляхом розбиття об'єкта на субполосні області з подальшою фільтрацією за допомогою Wavelet-перетворень.

Для збільшення швидкості обробки реальних об'єктів в даній роботі використовуються Wavelet-перетворення: Daubechies 4, Wavelet Coiflets 2, Symlets 4, Discrete Meyer, Biorthogonal 2.4, Biorthogonal 4.4 [2].

При дослідженні проектування сіткового 3D об'єкту в двовимірні координати було виявлено, що частина вершин накладається одна на одну, ми їх видаляємо децимацией, а також проводимо клиппинг – видаляючи невидимі вершини і відрізки.

Проведено дослідження передачі вершин, що залишилися в двовимірному полі, при черезстрочной і відрядковій телевізійних розгорток. З метою зменшення потоку даних доцільно перед перетворенням тривимірного сіткового зображення в двовимірне проводити спектральне Wavelet-перетворення.

При видаленні незначимих значень Wavelet-коефіцієнтів можливо досягти стискування в 5 разів, при цьому якість зображення, представлена відношенням сигнал / шум, досягає значення 35 дБ – оцінка показника прийнятної візуальної якості для комфортного перегляду [3].

При подальшому видаленні Wavelet-коефіцієнтів в двовимірному просторі починають спостерігатися відхилення координат вершин об'єкту від початкових і з'являються спотворення типу "брижі". Отже, нижче 35 дБ не доцільно стискати сіткові тривимірні об'єкти.Для підтримки переконливого рівня реалізму 3D сіткових об'єктів багато застосувань вимагають високій деталізації складних моделей. Такі моделі вимагають широкої смуги частот і великих витрат для передачі.

Для вирішення цих проблем були запропоновані багато алгоритмів стискування 3D сіток. В якості одного з відомих методів кодування тривимірної сітки (3D МК) були введені в стандарти MPEG – 4 і MPEG – 7. 3D МК забезпечує представлення і стискування вершин 3D сіткових об'єктів, а також забезпечує такі додаткові функції, як висока міра стискування, рендерінг, і стійкість до помилок. Стискування вершин сіткових об'єктів в сцені розроблені в ISO/IEC 14496-2, ISO/IEC 14496-11 і ISO/IEC 14496-16.

Для Wavelet- перетворень в літературі перевагу віддають Daubechies і Symlets, але, як видно, для кодування сіткових об'єктів можна використати усі існуючі перетворення.

Також більше увагу необхідно приділяти кількості рівнів квантування. Розрядність вектору Z – координати є найбільш не критичною координатою до кута повороту, оскільки визначає глибину об'єкту. Як сказано в цій роботі аналізу спектральних коефіцієнтів розкладання досліджуваних об'єктів, сплески по осях X і Y більше виражені, ніж по осі Z, тому крок дискретизації по осі Z можна вибирати більше, що дозволяє заощадити час обробки координат об'єкту в середовищі Matlab.

Відомо, що роздільна здатність людської зорової системи найменш чутлива, до глибини, таким чином, вісь Z можна піддавати більшому кроку квантування і дискретизації.

Ієрархічні спектральні перетворення по вибраних порогах дозволяють підвищити точність відновлення координат сіткових об'єктів, забезпечуючи різну детальність тривимірних сіткових об'єктів в телевізійних відтворюючих пристроях.

Список літератури

1. В. И. Солодка, "Спектральные свойства сеточных моделей видеоизображений", *68 науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова*, 2013, с. 18 – 19.

2. С. А. Лавров, "Разработка устойчивых методов реконструкции изображений с применением Wavelet-преобразования", дис. канд. физ.-мат. наук, фак-т інформ., Снежинск, 2011.

3. В. Е. Джакония, А. А. Гоголь, и Я. В. Друзин, "Телевидения", *стереотип. Горячая линия – Телеком*, 2007.

УДК 004.41

Т.В. Смірнова, О.М. Дрєєв, Є.К. Солових

sm.tetyana@gmail.com, drey_sanya@gmail.com

Центральноукраїнський національний технічний університет, м. Кропивницький

ХМАРНИЙ СЕРВІС ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ОПТИМІЗАЦІЇ ТЕХНОЛОГІЧНОГО ПРОЦЕСУ ВІДНОВЛЕННЯ ТА ЗМІЦНЕННЯ ПОВЕРХОНЬ ЗІ СТАЛІ

Сучасні лінії відновлення поверхонь деталей працюють в умовах гнучкої зміни параметрів проведення технологічних операцій. Тобто у таких умовах, коли самі технологічні процеси відновлення та зміцнювання поверхонь, у свою чергу можуть змінюватися іншими технологіями відновлення в залежності від видів пошкодження матеріалів та від вимог щодо умов експлуатації кінцевого продукту. В той час, як активно розроблюються інформаційні системи підтримки прийняття рішень для забезпечення оптимізації окремих технологічних процесів, систем для вирішення задачі побудови оптимізованого ланцюга технологічних процесів, з вибором більш оптимального процесу серед альтернативних за задачею, не вистачає. Крім того, з розвитком комп'ютерних технологій, зростає актуальність використання хмарних технологій в реалізації інформаційних систем. На основі зазначених актуальних проблем в інформаційному забезпеченні експертних систем оптимізації ланцюга технологічних процесів, сформульовано наступну мету, яка розв'язується в роботі: реалізувати хмарну рекомендаційну систему як сервіс (SaaS) з отримання поверхонь сталі із заданими характеристиками на основі комбінації декількох технологічних процесів.

Досягнення поставленої мети вимагає розв'язання низки задач, однак для їх формулювання та визначеності в застосовуваних хмарних інформаційних технологіях, потрібно визначити види та область застосування експертних та рекомендаційних систем для забезпечення оптимізації ланцюга технологічних процесів. Подальші задачі проблематики побудови інформаційних технологій оптимізації комбінованих технологічних процесів відновлення та зміцнювання поверхонь деталей будуть поставлені по розв'язанню поточної задачі реалізації хмарної рекомендаційної системи як сервіс з отримання поверхонь валів зі сталі СТ45 із заданими характеристиками на основі комбінації декількох технологічних процесів.

В процесі побудови експертних систем оптимізації технологічного процесу потрібно пройти наступні етапи: 1. Визначення вхідних-вихідних даних. 2. Складання словника атрибутів, які притаманні обраній технологічній операції. 3. Виявлення об'єктів та понять. 4. Виявлення зв'язків між вхідними керованими та не керованими параметрами технологічної операції. 5.Визначення цілей оптимізації. 6. Визначення стратегій визначення параметрів технологічної операції для досягнення поставлених оптимізаційних задач.

Наведемо ілюстрацію інформаційної моделі технологічного процесу на основі відновлення поверхні електродуговим покриттям. Модель дозволяє отримати інформацію для розрахунку характеристик які отримуються в результаті обробки. При побудові математичної моделі технологічного процесу зазвичай обмежуються представленням об'єкту дослідження у вигляді "чорного ящика". В результаті виникає потреба у функціональному пов'язуванні вхідних даних та визначених некерованих величин до параметрів, які вимагаються від технологічного процесу.

Схема передбачає наявність ітераційного пошуку методом поступового покращення результату з початкового припустимого режиму роботи системи. Для більш надійного результату, при наявності значної нелінійності, такий процес можна проводити з кількох початкових точок.

В роботі запропоновано інформаційну технологію оптимізації технологічного процесу відновлення та зміцнювання поверхонь валів зі сталі як хмарний сервіс. Для цього були вирішені наступні завдання:

– розглянутий абстрактний технологічний процес, його властивості та методи переходу до конкретного технологічного процесу;

– розглянута інформаційна модель технологічного процесу та методи її отримання;

– розглянуті абстрактні експертні системи, їх складові;

– проведено огляд відомих експертних систем оптимізації технологічних процесів, приведення їх до абстрактного вигляду:

– запропонована формалізація підмножини абстрактних експертних систем оптимізації технологічних процесів:

– запропонована формалізація рекомендаційних систем для забезпечення оптимізації ланцюга технологічних процесів, як надбудову експертної системи над експертними системами окремих технологічних процесів.

Таким чином у сукупності запропонована інформаційна технологія у вигляді хмарної системи вирішення задачі побудови оптимізованого ланцюга технологічних процесів відновлення та зміцнювання поверхонь валів, з вибором більш оптимального процесу серед альтернативних, за задачею.

УДК 004.042

І. О. Ушакова

varavina_ira@mail.ru

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

ВИМОГИ ДО СЕРВІСІВ ДОСТАВКИ PUSH-СПОВІЩЕНЬ КОРИСТУВАЧАМ

Стрімкий розвиток сучасних інформаційних технологій дозволяє бізнесу впроваджувати такі системи і сервіси, які вже стали стандартом в розповсюдженні інформації. Прикладом такого важливого механізму є сервіс повідомлення користувачів. [1–3]. У зв'язку з постійним поширенням доступу до Інтернету зростає і інформаційний потік, в якому з кожним днем все складніше фільтрувати і убирати непотрібну інформацію. Для вирішення проблеми надлишкового потоку інформації були створені технології для оповіщення користувачів тільки про саму важливу інформацію. Серед цих технологій найпоширеніші:

RSS-канали,

Email-розсилки,

месенджер-розсилки,

Push-сповіщення.

RSS-канали – простий спосіб залишатися в курсі новин обраних веб-сайтів, наприклад таких як блоги і online журнали. Якщо сайт має RSS-канал, підписавшись на нього, стане можливим отримання повідомлень про останні новини.

Email-розсилка повинна використовуватися при передачі основної інформації, яка не залежить від часу. Електронну пошту використовують для того, що б користувачі повернулися в певний момент часу до інформації. До такої інформації відносять завершення реєстрації, підтвердження, коди посилань, замовлення, квитанції тощо. Все, що пов'язано з обліковим записом і змінами в сервісі, також має передаватися електронною поштою.

Месенджер-розсилки – порівняно новий але все більш популярний канал комунікації. Однак його використання обмежене необхідністю дотримання політикам розробників месенджерів і залежність від функціонування самого месенджера.

Push-сповіщення відправляють в центр повідомлень або рядок стану смартфона користувача і є стандартним способом зв'язку для додатків на смартфонах. Це вважається менш нав'язливим сервісом, ніж SMS, тому що push-сповіщення може бути доставлено на екрани користувачів без переривання їх поточної активності.

Однак при відправленні push-повідомлень слід враховувати важлтвість контенту для користувача, а також проміжки часу між повідомленнями, щоб не бути надто надто нав'язливим, і користувач не скасував підписку на такі повідомлення. Push-сповіщення повинне використовуватися, коли в додатку відбувається значна подія або активність, яка вимагає від користувача виконання дії, або це інформація, чутлива до часу і яка принесе користь їм. Приклади включають повідомлення від інших користувачів, нагадування для певних завдань, новий контент в додатку і спеціальні пропозиції.

Розроблення сервісу Push-сповіщень та управління ним на сьогоднішній день для більшості сайтів є необхідністю, бо цей сервіс виступає як засіб залучення нових клієнтів та утримання існуючих. Push-сповіщення повинно включати певні складові (рис. 1).

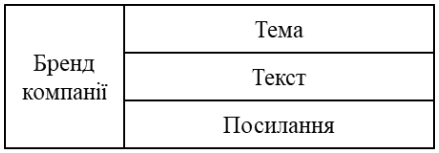


Рис.1. Складові Push-сповіщення

До сервісу Push-сповіщень пред'являються наступні вимоги:

оперативність надання сповіщення;

зміст і вигляд повідомлення повинен бути персоналізованим, цікавими та інтересними;

можливість персонального налаштування повідомлень користувачем;

супроводження повіломлень звуком;

використання lending page для посилань в повідомленнях;

максимум конкретної інформації в повідомленні;

збирання статистики;

створення inbox для зберігання повідомлень для користувачів, які відмовилася від підписки.

Список літератури

1. Анатомия новых push-уведомлений Google Chrome и преимущества для сайтов. [Электронный ресурс]. Доступно: https://vc.ru/flood/8661-push-chrome. Дата обращения: Март 17, 2019.

2. Ю. Ю. Гавриленко, Д. Ф. Саада, Е. А. Ильюшин, и Д. Е. Намиот, "Разработка прогрессивного web-приложения для системы управления push-уведомлениями", *International Journal of Open Information Technologies*, Том 6, №.9, с.42–49, 2018.

3. Introduction to Push Notifications, Google Developers. [Online]. Available: https://developers.google.com/web/ilt/pwa/introduction-to-push-notifications. Accessed on: March 1, 2019.

.

УДК 004.75

Б. П. Худоба, Н. Е. Кунанець, А. В. Катренко

bohdan.khudoba@gmail.com, nek.lviv@gmail.com

Національний університет «Львівська політехніка», м. Львів

СИСТЕМА ПІДТРИМАННЯ ПРИЙНЯТТЯ РІШЕНЬ ПРИ ФОРМУВАННІ НАВИЧОК НАУКОВОЇ РОБОТИ

Формування навичок проведення наукових досліджень – це один з ключових пунктів у розвитку майбутнього науковця, оскільки прищеплює вміння проведення наукових пошуків, експериментів тощо.

Наукова діяльність – це найвища форма інтелектуальної діяльності людини. Компетентності щодо проведення наукової роботи виробляються у результаті здобуття навичок ефективно засвоювати знання і використовувати їх на практиці. Інноваційні засоби та методи навчання допомагають підвищити ефективність навчального процесу та проведенню наукових розвідок. Зменшення кількості випускників закладів вищої освіти, що пов'язують свою долю із науковими дослідженнями може спричинити гострий дефіцит кадрів вищої кваліфікації.

На допомогу молодим науковцям, для розвитку теоретичних та здобуття практичних навичок у мережі Інтернет присутня велика кількість ресурсів. Але достовірність інформації та фаховий рівень таких ресурсів викликає певні застереження.

Для віртуального проведення експериментів при дослідженні хімічних чи фізичних процесів часто використовують он-лайн тренажери, що дозволяють симулювати роботу у лабораторії. Професійні віртуальні тренажери допомагають проводити досліди, яких вони не мають можливості провести у своєму навчальному закладі чи науково-дослідному інституті. Але все ж вони мають обмежені можливості та забезпечують можливості проведення всіх необхідних дослідів та експериментів. Молоді науковці беруть участь в наукових конференціях, семінарах та хакатонах. Але важливо розуміти, що такі заходи допомагають сформувати у них вміння представити науковій спільноті результати своїх напрацювань, а такий досвід набувається тривалими напрацюваннями.

Один з можливих варіантів розвитку та формування навичок виконання науково-дослідної роботи є геймифікація. Геймифікація – це особливий підхід до процесу гри, який не пов'язаний безпосередньо з грою, з її базовими принципами. Тобто, щоб досягти певного рівня освоєння компетентностей використовують різні рівні гри. У процесі проходження рівнів здобуваються знання та формуються навички [1]. Зокрема, такий підхід використовують не лише для навчання, а й для підвищення продуктивності праці працівників різних галузей.

Комп'ютерні та мобільні ігри набрали великої популярності. Відомо, що середній вік «геймера» – 30 років, серед них 47% складають представники жіночої статі. Середньостатичний «геймер» освоює одразу декілька ігор і проводить значну частину вільного часу у грі. Для удосконалення освітніх процесів в останні роки використовується імітаційне навчання, основою якого є імітаційно-ігрове моделювання, що відбуваються в реальній інтелектуальній системі [2].

Запропоновано створити систему, у якій молоді науковці чи студенти зможуть вдосконалювати свої знання та освоювати навички проведення наукових досліджень. За основу взято систему ejudje, яка створена для проведення олімпіад зі спортивного програмування, але внесено певні зміни. Для кожного користувача генерується індивідуальне завдання, побудоване у формі гри, для знаходження алгоритму найоптимальнішого чи найрозумнішого його вирішення.

Для побудови таких алгоритмів користувачу потрібно буде застосовувати здобуті під час навчання знання та вдосконалювати свої навички в області теорії алгоритмів та структур даних. На перших етапах користувачу надаються простіші завдання, а з часом їх рівень ускладнюється, що забезпечує можливість користувачу позмагатися з партнерами у вирішенні різних задач.

У процесі таких змагань користувачами освоюються нові алгоритми та структури даних, а з часом і удосконалюються та створюються власні алгоритми чи застосувати існуючі у новому поданні.

За результатами таких змагань аналізуються математичні моделі та обґрунтовується доцільність їх використання у власних наукових розвідках.

Отже, назріла нагальна потреба у створенні системи підтримки прийняття рішень, яка б сприяла формуванню та розвитку навичок проведення наукових досліджень.

Список літератури

1. Karl Kapp, Ed.D. "The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education", 2012.

2. О. В. Шестопалюк,"Інноваційні моделі навчання в діяльності вищих навчальних закладів, *Теорія і практика управління соціальними системами,* №3, с. 118–124, 2013.

УДК 004.75

В. В. Шатських, Н. Е. Кунанець, В. В. Литвин

victorshats@gmail.com, nek.lviv@gmail.com

Національний університет "Львівська політехніка", м. Львів

ОБҐРУНТУВАННЯ РОЗРОБКИ СИСТЕМИ ПІДТРИМАННЯ ПРИЙНЯТТЯ РІШЕНЬ НАДАННЯ РЕЛЕВАНТНИХ РЕКОМЕНДАЦІЙ ФІЛЬМІВ З ВРАХУВАННЯМ ОСОБИСТИХ ПОТРЕБ КОРИСТУВАЧА

Рекомендаційні системи (РС) є ефективними інструментами надання пропозицій щодо раціонального використання об'єктів, які представляють інтерес для конкретного користувача. Пропозиції стосуються різних процесів прийняття рішень, зокрема щодо доцільності придбання певних речей, прослуховування музики або перегляду фільму чи телесеріалу.

Рекомендаційні системи використовуються на популярних інтернет-сайтах, таких як YouTube, Netflix, Last.fm, Spotify, Facebook, Tripadvisor, LinkedIn та IMDb. Значна частина медіа-компаній зараз розробляють і розгортають РС як частину послуг, які вони надають своїм абонентам. Наприклад, Netflix, онлайн-провайдер потокових мультимедійних даних, які надаються за запитом користувача, присудив премію у мільйон доларів команді, якій вперше вдалося значно покращити продуктивність системи рекомендацій [1].

Існує низка причин, які спонукають постачальників послуг до використання цієї технології:

- Збільшення кількості проданих товарів.
- Продаж більш різноманітних предметів.
- Підвищення задоволеності користувачів.
- Збільшення кількості користувачів.
- Краще розуміння потреб користувач.

Перший чинник, який слід врахувати при розробці РС, є область застосування, оскільки вона має значний вплив на алгоритмічний підхід, який необхідно використовувати. Сформовані ресурси, які надають таксономію РС і класифікують наявні РС за конкретними доменами застосунків [1]. Аналіз доменів дозволяє визначити їх загальні класи для найбільш поширених систем застосування:

- Розваги – рекомендації фільмів, музики, ігор та IPTV.
- Контент – персоналізовані газети, рекомендації щодо документів, рекомендації веб-сторінок, програм для електронного навчання та фільтри електронної пошти.
- Електронна комерція – рекомендації продуктів для покупців, таких як книги, мобільні телефони, ПК та ін.
- Послуги – рекомендації туристичних послуг, рекомендації експертів для консультацій, рекомендації будинків для оренди або надання послуг із знайомств.
- Соціальні – рекомендації людей для спілкування у соціальних мережах та контенту соціальних медіа, таких як твіти, канали Facebook, оновлення LinkedIn та інші.

Формування рейтингів є найпопулярнішою формою подання даних про транзакції. Ці рейтинги можуть зберігатися у базах даних РС явно або неявно. З використанням явного набору оцінок користувачу пропонується думка експертів про предмет у рейтинговій шкалі. Інша форма оцінки надається користувачу у формі тегів, асоційованих з іншими елементами, які система представляє. Наприклад, у MovieLens (https://movielens.org/) теги РС містять інформацію, як його користувачі сприймають фільм, наприклад: "затягнутий" або "драйвовий".

Застосування систем рекомендацій достатньо поширене для простих і недорогих продуктів, таких як фільми, музика, новини та книги. Хоча існують системи, що керують більш складними типами елементів, наприклад, фінансовими інвестиціями або подорожами [2].

При створенні РС потребують детального дослідження алгоритми формування пропозицій щодо об'єктів певної предметної області та інтерфейси користувачів, що сприяє створенню узгоджених послідовностей рекомендацій. Зокрема, слід моделювати вплив на користувача декількох контекстних умов, таких як спосіб, у який могли б бути надані рекомендації, та форма їх подання.

Таким чином, рекомендаційні системи сучасний засіб інформаційного обслуговування користувачів у швидкоплинному потоці інформації та пропозицій.

Список літератури

1. M. Jones, "Recommender systems, Part 1. Introduction to approaches and algorithms. Learn about the concepts that underlie web recommendation engines". [Online]. Available: https://www.ibm.com/ developer works/opensource/library/os-recommender1. Accessed on: March 12, 2019.

2. P. Melville, R. Mooney, and R. Nagarajan, "Content-Boosted Collaborative Filtering for Improved Recommendations*", National Conference on Artificial Intelligence: "AAAI-2002"*, pp. 187 – 192, 2001.

СЕКЦІЯ 3
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

УДК 621.39

Алиев Тимур Чингиз оглы[1], Гасанов Узеир Ильхам оглы[2]

imct_asoiu@mail.ru, uzagasanov@gmail.com

[1]*Azerbaijan State Oil and Industry University , Baku, Azerbaijan*
[2] *"Caspian Pipe Coatings" LLC., Baku, Azerbaijan*

ПРИМЕНЕНИЕ АТМОСФЕРНОЙ ОПТИЧЕСКОЙ СВЯЗИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Атмосферная оптическая связь (АОС) использует для передачи данных модулированную коллимированную световую энергию, обычно в форме инфракрасного (ИК) лазера. Это дает АОС много привлекательных качеств, таких как очень высокая пропускная способность, высокий уровень безопасности благодаря низкой вероятности обнаружения (НВО) и низкой вероятности перехвата (НВП), а также сигнала, который не подвержен радиочастотным (РЧ) помехам или регулированию.

Военная связь требует широкополосных возможностей на самом высоком уровне безопасности в невероятно плотной рабочей среде. Пропускная способность и качество безопасности АОС делают её подходящей технологией для военных коммуникаций. Тем не менее, строгое требование прямой видимости и затухание линии в плохих атмосферных условиях ограничивают его применение.

Несколько компаний и групп разрабатывают и внедряют коммуникационные решения АОС по всему миру в ответ на потребность в широкополосной связи без радиочастотных помех по относительно низкой цене. Последние достижения в гибридных системах АОС-РЧ позволили повысить производительность в любых атмосферных условиях. В данной работе изучается текущее состояние систем связи АОС и анализируется её пригодность в качестве решения для военной связи.

Производительность линии АОС напрямую связана с атмосферными условиями, в которых он работает. Частицы в воздухе, турбулентность и нерегулярная плотность воздуха влияют на работу линии АОС. По этой причине трудно точно определить, как АОС будет работать в заданной среде с течением времени, пока он действительно не будет протестирован в этой среде в течение соответствующего периода времени. Это также верно для радиочастотной связи, но влияние атмосферных воздействий на АОС намного выше, чем на РЧ. Это очень актуально, если рассматривать АОС как коммуникационное решение, где высокая доступность при любых погодных условиях является приоритетом.

Внедрение гибридного двухрежимного решения АОС-РЧ или АОС-миллиметрового диапазона может смягчить ухудшение связи в неблагоприятной атмосфере. Тем не менее, при этом нарушается защита канала от вероятности обнаружения и перехвата. Кроме того, существует несколько возможных применений АОС, в которых неблагоприятные атмосферные условия, скорее всего, не встретятся. К ним относятся космические применения, воздушные связи на большой высоте и беспилотные летательные аппараты, которые способны работать только в умеренных метеорологических условиях из-за ограничений датчика ISR и / или самолета.

Полученные данные указывают на необходимость дальнейших исследований, разработок и улучшения производительности линии связи до того, как будет осуществлена большая часть коммуникаций АОС.

Список литературы

1. А. Л. Дмитриев, *Оптические системы передачи информации*. СПбГУИТМО, 2007.

2. S. Bloom, "The Physics of Free-Space Optics," AirFiber, Inc., White Paper (802-0006-000), May 2002.

3. H. Willebrand and B. S. Ghuman, *Free Space Optics: Enabling Optical Connectivity in Today's Networks*. Indianapolis, IN: Sams Publishing, 2002.

4. B. Lundy, *Telegraph, Telephone, & Wireless: How Telecom Changed the World. Charleston*, SC: BookSurge , pp. 27–30, 2008.

УДК 681.396

Г.В. Альошин[1], О.В. Коломійцев[2], В.В. Посохов[3]

Dr.aloshin@mail.ru, Alexus_k@ukr.net, Posohovv@ukr.net

[1]*Українська державна академія залізничного транспорту, Харків*
[2]*Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків*
[3]*Національна академія національної гвардії України, Харків*

ОСНОВИ ТЕОРІЇ ОПТИМІЗАЦІЇ РАДІОЕЛЕКТРОННИХ ВИМІРЮВАЧІВ

Бурхливий розвиток ракетно-космічної науки та техніки, зв'язку та інформаційних технологій привів до того, що існуючих методів радіовимірювань стало вже недостатньо. Крім потреби в показниках точності вимірювань з'явилася потреба в урахуванні широкого апріорного діапазону часу вимірювань для процесів, що швидко змінюються, надійності у стикуванні шкал, відношенні сигналу до шуму, а також у використанні вартості.

Сучасні методи вимірювань, які існують в метрології виконують функцію порівняння параметра, що вимірюється з відповідним еталоном (з його часткою). Для радіоелектронних вимірювань це – самий точний нуль-метод, а також різницевий метод, функціональний метод – прямопоказувальні пристрої, метод заміщення, ноніусний метод та ін. Але цих методів вже недостатньо для радіоелектронних вимірювань, де потрібні: точність оцінки; точність апріорних даних; швидкість, або час вимірювань; довірча ймовірність зістиковки шкал; відношення потужностей сигналу до шуму; вартість для оптимізації систем; метод синтезу систем із загальних позицій і тощо [1 – 5]. Ці проблеми (оптимізації вимірювальних систем) пропонується вирішувати завдяки використання узагальнюючого виразу для отримання кривих обміну якостей за Гуткіним Л.С. [1]. Отже, для задач оптимізації вимірювальних систем та отримання кривих обміну, цільову функцію для них можна знайти для всіх типів вимірювачів. Задачі оптимізації будуть сформовані, якщо знайти обмеження за вартістю, піковою потужністю і тощо. Таким чином, формулювання узагальненого показника якості вимірювальних систем з єдиних позицій є актуальною науковою задачею.

В результаті розв'язання задач оптимізації радіоелектронних засобів Гуткін Л.С. [1] виявив таку особливість їх оптимального рішення, що якщо поступово змінювати показники обмеження і вирішувати задачу за головним показником, то можливо отримати взаємозалежність між оптимальними показниками – кривою обміну. Тобто це буде цілий клас задач оптимізації, що вирішуються.

Результати оптимізації ряду задач [3–6] методом сепарабельного програмування дозволили отримати рішення в аналітичному вигляді, які одразу ж можна назвати кривими обміну.

Виявлено, що для задач оптимізації вимірювальних систем і для отримання кривих обміну цільову функцію для них можливо знайти для всіх типів вимірювачів. Задачі оптимізації можуть бути сформовані, якщо знайти обмеження за вартістю, піковою потужністю і тощо.

Якщо метою і головною проблемою наукових розробок є оптимізація вимірювальних систем, то вона звичайно вирішується на етапі отримання кривих обміну цільової функції. Отже, необхідно сформулювати узагальнений показник якості вимірювальних систем з єдиних позицій.

За результатами проведених наукових досліджень запропоновано метод формування узагальненого показника якості вимірювальних систем. Показано, що узагальнений показник якості справедливий для всіх типів дискримінаторних вимірювачів. При цьому, узагальнений показник якості справедливий як для вимірювачів і каналів будь-якого типу, так і для різних параметрів, що вимірюються. Узагальнений показник якості вимірювальних систем також легко доповнюється зв'язками з іншими показниками.

Список літератури

1. Л. С. Гуткин, *Оптимизация радиоэлект-ронных устройств по совокупности показателей качества*, Москва, 1974.

2. Ф. М. Вудворд, *Теория вероятности и теория информации с применением в радиолокации*, Москва, 1968.

3. Г. В. Алешин, Ю. А. Богданов, *Эффектив-ность сложных радиотехнических систем*, Киев, 2008.

4. Г. В. Алешин, *Оцінка якості інформаційно-вимірювальних систем*, Харків, 2009.

5. Г. В. Алешин, *Ефективність інформаційно-вимірювальних радіотехнічних систем*, Харків, 2005.

UDK: 656.256

[1]Lala Rustam Bakirova, [2]Aladdin Rashid Bayramov

lala_bekirova@mail.ru, bayramov-aladdin@mail.ru

[1]Azerbaijan State Oil and Industry University , Baku, Azerbaijan
[2] "Azerbaijan railways" CJSC., Baku, Azerbaijan

RAILS CONDITION CONTROL SYSTEM FOR ENSURING TRAFFIC SAFETY OF TRAINS

Structural model of complex control management system, enabling the solution of the problem of the rails integrity, which is one of the factors directly affecting the traffic safety of trains, has been developed. Additional sensors and measurement-control method used in the system enable both to detect the presence of trains on the base of axle meter method and make accurate, operative decisions in the safe management.

The signaling system is of great importance in ensuring the traffic safety of trains in railway transport. Information about the location of trains, maintaining a safe brake path between them, speed limits on stations and transition roads, reducing intervals between trains, increasing train releasing capacity of transition roads, detecting rails break, and at the same time emergency braking are carried out by various methods and means. One of these methods is an axle meter method, so that the meter is mounted on rails along the railroad and actually detects the presence of the wheels [1].

In sources [2] and [3] concerning the rail cycle, the information is given on controlling the integrity of the rails, the rail lines condition within the controlled part of the road while detecting rails break, the gap in the rail line part of the road and good condition of rails, occupation of rail line part of the road by the train, or the control on the electric integrity breakdown. At this time, the transmitter controlling the condition of railways is called rail cycle and a railway line is taken as its main element.

In the axle meter method, based on mounting in block area boundaries, the working principle, computing wheel pairs when the wheel pair enter the block area and leave that area from another point, LC oscillator is used in order to detect the wheel pair when wheel pairs pass in the variable magnetic field arise around the cap. However, because of the lack of control over the integrity of the rails, which are important issues for the traffic safety in the sources dedicated to the application of the abovementioned method, it can be considered as the biggest shortage of that system [4].

The integrity of the rails is of great importance in terms of traffic safety of trains. From this point of view, as the rails break is not taken into account and the information on the situation is not available, it is possible to cause certain problems in controlling the movement of trains in the axle meter method.

The issue, which is being solved, is the development of a complex control-management system, realizing on the base of additional sensors and measurement-control method to eliminate the above-mentioned problem.

In order to solve the problem, the moving train is considered an active object and, in addition to the active and passive sensors installed in the rail cycle, additional sensors are considred to be mounted to expand the truthfulness of the obtained information and reliability of the made decisions.

An active object (train) enables to install additional sensors to its autonomous board computing system (measuring circuit, control system), which make it possible to detect the problem and take into account the obtained information while controlling the object itself and other objects along the traffic line.

Hence, various options of structural and algorithmic models of system implementation modifications are proposed to control the integrity of the rails which is the major shortage of the axle meter system.

References

1. Blake A. Kozol, David F. Thurston, "Axle Counters vs. Track Circuits – Safety in Track Vacancy Detection and Broken Rail Detection "conference_proceedings", arema.org, pp. 1–8, 2010

2. Jodi Scalise, "How Track Circuits detect and protect trains", railwaysignalling.eu, pp. 1-5 , 2014

3. Gerhard Grundnig, Cristian Pucher, "Track circuits versus wheel detection and axle counting for urban and suburban rail transportation systems". White paper, www.frauscher.com pp. 9-12, 2013

4. Martin Rosenberger, "The future challenges of wheel detection and axle counting", Part 1, Volume 9, irse.org, pp. 2–10, 2011

UDK:681.325.5.181.4:528.8

Lala Rustam Bakirova, Elvira Maharat Bunyatova

lala_bekirova@mail.ru, jenifer671.3@mail.ru

Azerbaijan State Oil and Industry University , Baku, Azerbaijan

INCREASING THE DETERMINATION ACCURACY OF THE SURFACE COLOR BY CALORIMETRIC METHOD

Abstract: The problem of increasing the accuracy and reliability of the colour measurment results has been studied in order to control the surface quality. A structural and algorithmic model has been proposed to increase the color measurment accuracy by colorimetric system. The proposed information-measuring and control system allows to arrange the subranges in which the measurement is carried out and accordingly the number of channels in order to increase the measurment accuracy.

Keywords: colorimeter, spectrometer, color measurement, surface texture, measuring range, measurement accuracy, reliability.

Introduction: Quality indices of materials can be determined according to various contact-based (on the base of samples) methods and means. As this type of index, along with the human eye, being rough measurement source, colorimeter and spectrometer-based measurements are used to determine the surface color of materials.

As the human eye can not accurately determine the color, this method is almost never used.

As long-term durable work causes eye fatigue, and the color comparison is inaccurate by mass analysis, i.e accurateness is less, colorimetric method is less commonly used. Spectrophotometers are more commonly used to measure the luminous flux intensity, determine the surface color, and increase its accuracy.

Spectrophotometers allow for more complex color measurements and obtain more color-connective data. Colorimeters are used to measure three colors (green, red, blue), however, they measure the color less accurately.

The colorimetric method applied to control the surface colour is used which relatively differs from the simplicity of the system (for being based on the measurement results that are added to only three wavelengths) [2]. However, in this system as such external factors like environment, etc. and the nature of the material influence the accuracy and reliability of the measurement results, the use of the method makes it possible to carry out these measurements on the base of additional measures and approaches.

The solution of the stated problem by the spectrometric method allows to obtain more accurate data in accordance with the colour of the research object in small xsubranges [3]. Arranging the measurement and control by the spectrometric method requires more complex structure and algorithmic solution.

At this time, not all of the obtained information is informative, and excessive (surplus) data load does not allow making operative decisions on the state of the object according to the planned research.

The problem to be solved is to increase the reliability of colour control system data of the object and operativeness of decisions by a simpler and adaptive (intelligent) structure and algorithmic model.

It is suggested to manage optical receiver block in the object color control system in accordance with the conditions by calorimetric method for solving the proposed problem. At this time, the problem of changing the location and number of subranges to be measured at the next step is solved on the base of operative processing and analysis of the obtained information to approach the required accuracy.

The algorithm carrying out measurement error determination principle ($F(x)=f(\Delta l, n)$) was developed depending on the number of measurements to be taken on each channel on the base of the obtained data. As a result of the initial processing, additional measurement arrangement are carried out accordingly in sub ranges the measurement error of which is obtained greatly.

In this case, the arrangement and change of the measurements in other subranges are carried out according to the relevant operational reports. Flexible algorithm allows for the proper solution of existing problems.

Flexible algorithm and structural model have been developed as a intelligent material with the use of liquid crystal-based blocks having a multifunctional characteristic and being able to change their constructions in the optical receiver block in order to achieve the solution of the stated problem.

Optical-electronic block-based structural model created on the base of intelligent materials enables to increase the measurement accuracy of the colour being the quality index of the surface being studied on the base of the proposed algorithm.

References

1. Features of selection of the device for color measurement, [Online]. Available: https://tecsa.com.ua/ osobennosti-podbora-pribora. Accessed on: March 1, 2019.

2. Visual method for determining color. [Online]. Available: https://chem21.info/info/1757696. Accessed on: March 1, 2019.

3. Tim Mouw, “Colorimeter or spectrophotometer”, [Online]. Available: https://www.xritephoto.ru/ colorimeter-spectrop. Accessed on: March 1, 2019.

УДК 331.5

Н.О. Бринза, А.А. Гаврилова

brynz@ukr.net, sharaya1972@gmail.com

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

ДОСЛІДЖЕННЯ БАГАТОФАКТОРНОЇ МОДЕЛІ ОЦІНКИ ПОКАЗНИКІВ РОЗВИТКУ ІТ-ГАЛУЗІ ЗА РЕГІОНАМИ УКРАЇНИ

На етапі апробації моделі, що сформована для оцінки комплексного показника стану ІТ-галузі за регіонами України [1], необхідно з'ясувати силу зв'язку між обраними факторами та комплексним показником, значність впливу факторів на комплексний показник, а також оцінити адекватність моделі.

Сила зв'язку та вплив факторів на результат було досліджено за допомогою кореляційно-регресійного аналізу, який дозволяє провести дослідження щодо: виміру тісноти зв'язку між змінними і оцінити чинники, які надають найбільший вплив на результативну ознаку; вибору форми зв'язку і типу моделі для визначення розрахункових значень залежної змінної. Тому методи кореляційного і регресійного аналізу використовуються в комплексі. Найбільш розробленою в теорії і широко застосованою на практиці є парна кореляція, коли досліджуються співвідношення результативної ознаки і однієї факторної ознаки [2].

Коефіцієнти парної кореляції між "Внутрішній стан ІТ-ринку" та комплексним показником стану ІТ-галузі регіону становить 0,74, "Інвестиційна привабливість" та комплексним показником стану ІТ-галузі регіону становить 0,478, "Заробітна плата" та комплексним показником стану ІТ-галузі регіону становить 0,75. У першому та третьому випадках оцінка значень коефіцієнтів кореляції за шкалою Чеддока сильна та пряма, а у другому – помірна та пряма.

Також необхідно оцінити тісноту лінійного кореляційного зв'язку між результатом і всіма факторами. Коефіцієнт множинної кореляції $R = 1$, отже зв'язок між ознакою Y та факторами X_i сильний.

Рівняння множинної регресії наступне:

$$Y = 0{,}000301 + 0{,}3331X_1 + 0{,}3321X_2 + \\ + 0{,}3345X_3.$$

Економічна інтерпретація параметрів моделі така: збільшення X_1 на 1 од.вим. призводить до збільшення Y в середньому на 0,333 од.вим.; збільшення X_2 на 1 од.вим. призводить до збільшення Y в середньому на 0,332 од.вим.; збільшення X_3 на 1 од.вим. призводить до збільшення Y в середньому на 0,335 од.вим.

При проведенні перевірки значимості рівняння і його коефіцієнтів, об'єктивна оцінка представлена скоригованим коефіцієнтом детермінації, який дорівнює 1. І це підтверджує той факт, що дане рівняння регресії пояснює поведінку Y.

Також необхідно перевірити побудовану модель на адекватність реальному процесу шляхом порівняння даних, розрахованих за моделлю і визначених експериментально.

Для перевірки адекватності моделей обраний критерій Фішера [3]:

$$F_e = \frac{S_{ad}^2}{S_e^2},$$

що є відношенням двох дисперсій – відтворюваності (S_e^2) та адекватності (S_{ad}^2) [3].

Теоретична залежність покладається адекватною дослідній, якщо отримане експериментальне значення критерію Фішера (F_e) менше табличного ($F_{табл}$), обраного за кількістю ступенів свободи чисельника і знаменника, а також довірчої ймовірності α [4]:

$$F_e < F_{табл}.$$

В даному випадку табличне значення при ступенях свободи $k_1 = 3$ та $k_2 = n - m - 1 = 17 - 3 - 1 = 13$, $F_{табл}(3;13) = 3{,}41$, а експериментальне $F_e = 1{,}50762 \cdot 10^{-5}$.

Експериментальне значення критерію Фішера не перевищує табличного значення. Тому розроблену модель можна вважати адекватною і покласти в основу подальших досліджень.

Список літератури

1. Н. А. Брынза, та А. А. Гаврилова, "Многофакторная оценка показателей развития IT-отрасли в регионах Украины", *Збірник наукових праць "Системи обробки інформації"*, № 2(56), 2018, с. 159 – 169.

2. Л. Т. Гиляровская, *Экономический анализ*, Москва, 2011.

3. Т. Я. Таванюк, А. П. Николаенко, А. В. Романченко, и Т. А. Шумакова, "Оценка адекватности математических моделей характеристик электрогидравлических следящих приводов", *Вісник східноукраїнського національного університету імені Володимира Даля*, № 7(237), с. 89–94, 2017.

УДК 338.22:005.922.1:33

Є.В. Воронюк

Sm1581@gmail.com

Харківський Національний Університет ім.. Семена Кузнеця, м. Харків

ОРГАНІЗАЦІЙНІ РІВНІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

Економічна безпека підприємницької діяльності уявляє собою широке і багатогранне поняття. На думку Л. Гнилицької гносеологічне коріння категорії "економічна безпека" проявляється через розгляд взаємозв'язку між розвитком і безпекою, що має складний діалектичний характер. Категорія розвитку імпліцитно містить у собі категорію безпеки, без якої не може існувати. Тому розвиток та безпека – це дві сторони загального процесу життя суспільства, а отже, і існування підприємства, що функціонує в цьому суспільстві [1, с.41]. Підприємство, як форма реалізації підприємницької діяльності існує в економічному середовищі країни, тому організація механізму забезпечення його економічної безпеки проходить на макро, мезо та мікрорівні. Рівні організації наведені на рис.1.

Рис. 1. Рівні організації економічної безпеки підприємницької діяльності

Відповідно до рис. 1, структурні рівні організаційного забезпечення економічної безпеки підприємницької діяльності формуються та залежать один від одного.

Так, макрорівень або загальнодержавний рівень постає структуроутворюючим рівнем в організаційному забезпечені, тому що на цьому рівні створюються і впроваджуються основні вимоги, правила, норми за якими функціонує підприємництво. На цьому рівні формуються такі зовнішні загрози і ризики для економічної безпеки підприємництва як курс валют, податкова та соціальна політика.

На мезорівні організовуються такі елементи забезпечення економічної безпеки, які мають загальнодержавний характер, але їх впровадження та функціонування обмежується рамками регіону, галузі, підприємства. Прикладом такого елемента слугує профспілка, організація якої проходить безпосередньо на підприємстві, але у взаємозв'язку з профспілками та законодавством на галузевому, регіональному, загальнодержавному та міжнародному рівнях. Крім того на мезорівні, організація економічної безпеки підприємницької діяльності доповнюється локальними законодавчими актами, та регіональними програмами, втілення яких сприяє розвитку підприємницької діяльності в окремих областях держави.

На мікрорівні організовується безпосередньо система економічної безпеки на підприємстві. Її створення проходить відповідно до стандартів, норм і правил встановлених на попередніх двох рівнях. Таким чином створення якісного організаційного забезпечення економічної безпеки на макрорівні неможливо без існування функціонального і працездатного забезпечення на макрорівні.

Список літератури

1. Л. Гнилицька, *Основи економічної безпеки підприємства*, Бухгалтерський облік і аудит, № 7, с. 41–48, 2013.

2. Л. Я. Малюта, "Інституційні детермінанти організаційного забезпечення економічної безпеки підприємств в контексті їх інноваційно-технологічного розвитку", дис. докт. ек. наук, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, 2018.

УДК 681.518.2

А.А. Засядько

sagitta@bigmir.net

Черкаський навчально-науковий інститут ДВНЗ «Університет банківської справи», м. Черкаси

СИМВОЛІЧНІ МОДЕЛІ ФІЗИЧНИХ ПРОЦЕСІВ, ЩО ОПИСУЮТЬСЯ ІНТЕГРАЛЬНИМ РІВНЯННЯМ ФРЕДГОЛЬМА ПЕРШОГО РОДУ

Процес вимірювання сигналу вимірювальними перетворювачами і первинними датчиками описується математичною моделлю у вигляді інтегрального рівняння Фредгольма першого роду (ІРФПР). Розв'язати задачу відновлення сигналу для такого рівняння – означає знайти сигнал, спотворений вимірювальною апаратурою з відомою апаратною функцією. Крім задачі відновлення сигналів ІРФПР описується також широке коло інших обернених задач: задача відновлення зображень, задача редукції реального приладу до ідеального, задача розподілу електричного потенціалу всередині напівпровідника та ін. [1, 2].

Актуальність теми полягає в тому, що дана задача є некоректною, а вимірювання експериментальних даних дає похибки, що викликають нестійкість розв'язку. Це в свою чергу вимагає застосування прийомів, які отримують розв'язок, стійкий до похибок.

В роботі [1] розроблена диференціально-тейлорівська модель (ДТ-модель) задачі відновлення у спектроскопії, що дозволяє представити за допомогою диференціальних тейлорівських перетворень (ДТ-перетворень) з прийнятною точністю складну обернену задачу простішою моделлю, вираженою системою лінійних алгебраїчних рівнянь невеликої розмірності. Застосуємо цей підхід для моделювання задач математичної фізики, які можна звести до ІРФПР.

При математичному моделюванні фізичних об'єктів і процесів, які описуються диференціальними й інтегральними рівняннями, ДТ-перетворення дозволяють замінити операції інтегрування й диференціювання еквівалентними алгебраїчними операціями як у числовому так і в аналітичному вигляді. Математична модель системи у вигляді диференціальних або інтегральних рівнянь може бути перетворена в так звану спектральну або символічну модель. Спектральна модель звичайно уявляє собою систему кінцевих рівнянь, з якої знаходяться невідомі дискрети диференціального спектра. Правила знаходження диференціальних спектрів детально описано в роботі [3].

В роботі застосовані ДТ-перетворення для розв'язання ряду задач, які доцільно представляти в ІРФПР, та продемонстровані переваги використання ДТ-перетворень на трьох різних моделях.

Була знайдена невідома функція розподілу електричного потенціалу всередині напівпровідника. Отримана символічна ДТ-модель ІРФПР з невідомою функціональною залежністю в верхній межі інтегрування прийнятно апроксимує початкову фізичну модель.

За допомогою ДТ-перетворень також отримана стійка до похибок експериментальних даних модель на основі ІРФПР, придатна для дослідження теплофізичних характеристик деталей вузлів транспортних засобів, зокрема дослідження теплового стану двигунів; перегріву гальмівних колодок та опорів, букс, підшипникових вузлів тощо. В цьому випадку рівняння теплопровідності є диференціальним рівнянням в частинних похідних параболічного типу.

Наступна задача, що розглядалася в даній роботі, описує високотемпературний режим з унесенням маси розплавленої речовини. На основі оберненої коефіцієнтної задачі теплопровідності, що описує динаміку прогріву твердого тіла при руйнуванні поверхні, наприклад, процес руйнування захисного шару аерокосмічного транспорту [2], також розроблена стійка до похибок в початкових даних символічна модель на основі ДТ-перетворень для визначення теплофізичних характеристик матеріалів, зокрема коефіцієнта температуропровідності.

Розглянутий в роботі підхід пропонується використовувати і в інших задачах, коли фізичні процеси доцільно розглядати в інтегральній формі. Використання ДТ-перетворень дозволяє звести розв'язування складної задачі до простішої, тим самим зменшивши обчислювальну складність.

Список літератури

1. А. А. Засядько, "Дифференциально-тейлоровская модель задачи восстановления в спектроскопи", *Электронное моделирование*, Т. 24, № 6, с. 97–105, 2002.

2. Г. А. Фролов, и В. Л. Баранов, "Динамика прогрева твердого тела при тепловом разрушении поверхности", *Инженерно-физический журнал*, Т. 80, № 6, с. 30–43, 2007.

3. Г. Е. Пухов, *Дифференциальные спектры и модели*, Наук.думка, 1990.

УДК 316.77-022.326.5:338.48

Г.Г. Зубрицька

halyna.zubrytska@student.uj.edu.pl

Ягеллонський університет у Кракові, м. Краків (Польща)

КРИЗОВІ КОМУНІКАЦІЇ В СВІТОВІЙ ТУРИСТИЧНІЙ ІНДУСТРІЇ

В останні роки туризм є одним з найбільш важливих секторів світової економіки. За оцінками Всесвітньої ради з туризму та подорожей (WTTC) ще в 2017 році внесок туризму у світовий ВВП становив понад 10% від його загального обсягу. При цьому туристична індустрія забезпечує кожне десяте робоче місце в світі. В даний час понад 1,3 мільярда людей щорічно перетинають кордони своїх країн для бізнесу або відпочинку. Мільярди подорожують у середині своїх країн [1].

Стрімке зростання інформаційних технологій суттєво підвищило мобільність та кругозір багатьох туристів. У той же час зростання політичних ризиків, геополітична нестабільність та природні катаклізми обумовлюють необхідність забезпечення відповідних гарантій безпеки споживачів і мінімізацію ризиків у сфері туризму.

Також як і будь-який інший ринок, туристичний та його учасники не застраховані від кризових ситуацій. Вони можуть виникнути до, в процесі або після безпосереднього надання туристичних послуг та мати різні причини [2]:

- політичні (дестабілізація політичної обстановки, масові акції протесту, страйки);
- військові (раптова агресія, розв'язання бойових дій, тероризм);
- економічні (кризи внутрішнього і зовнішнього характеру, інфляція, різкі коливання обмінних курсів);
- технічні (техногенні аварії, аварії та збої функціонування об’єктів інфраструктури або розміщення);
- природні (катаклізми, стихійні лиха, епідемії небезпечних захворювань).

У загальному випадку кризова ситуація - це переломний момент, який може привести як до негативних, так і до позитивних наслідків. Процес прийняття рішень в умовах кризи, як правило, жорстко обмежений часом і обсягом інформації, яку має організація, що приймає рішення.

Враховуючі важливість даної проблеми ще в 2012 році Всесвітньою туристичною організацією (UNWTO) було представлено практичне керівництво щодо ефективного вирішення кризових проблем в туризмі за допомогою комунікацій [3].

В даний час комунікації відіграють важливу роль в діяльності будь-якої організації. Досить часто успішно реалізована комунікаційна складова роботи компанії забезпечує її лідерські позиції на ринку. Роль комунікацій особливо зростає під час кризових ситуацій, так як виникає особлива необхідність підтримки інформаційного потоку, витриманого в вигідному для організації світлі. У той же час такий підхід повинен виключати помилкову інформацію, спотворення фактів або інші нелегальні способи маніпуляції свідомістю суспільства. Однак висвітлення подій з позицій організації – це невід'ємний елемент стратегії захисту і відновлення репутації компанії під час кризової ситуації. При цьому, наслідки будь-якої кризової ситуації безпосередньо залежать від своєчасності правильних оцінки обстановки та прийнятих рішень на кожному з етапів.

У дослідженнях, присвячених кризовим комунікаціям можливо виділити наступні теорії та напрямки [4]:

- ситуаційна теорія W. Timothy Coombs [5];
- теорія атрибутивних процесів A. Schwarz [6];
- теорія відновлення іміджу W. L. Benoit [7];
- теорія інтегрованого моделювання криз Y. Jin, A. Pang, G. T. Cameron [8].

Значний вплив на попит у сфері туристичних послуг здійснюють зміни у суспільній психології споживання. Результати досліджень свідчать, що в більшості випадків в кризових ситуаціях люди формують думку та приймають рішення на основі своїх почуттів та інтерпретації власних емоцій щодо проблеми, що їх викликала [10]. Співвідношення емоцій людей та зацікавлених груп до типу кризової ситуації та рівня участі суспільства надано на рис. 1.

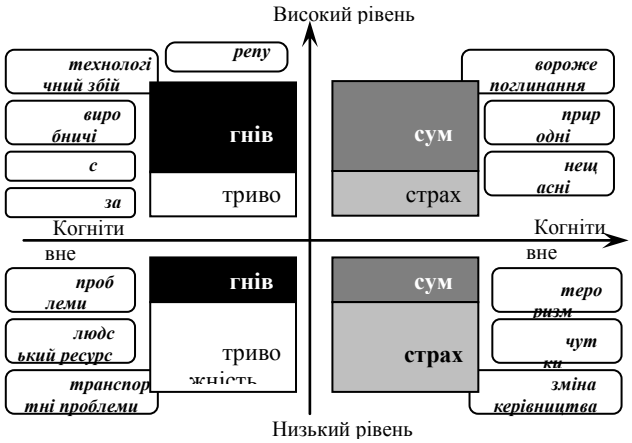


Рис. 1. Співвідношення емоцій з типом кризової ситуації [9]

Проходження організацією кризових ситуацій дозволяє їй придбати комунікаційні навички, найбільш важливими з яких є [9]:

- аналіз кризової ситуації, виявлення справжніх і потенційних загроз з метою запобігання

повторного виникнення кризи;

- чесність і відкритість повідомлень, що містять інформацію про реальний стан справ, причини виникнення кризи та можливі негативні наслідки, діяльність компанії з протидії кризі та нейтралізації негативних наслідків;

- висока ступінь відповідальності компанії по відношенню до зацікавлених груп в рамках врегулювання ситуації з найменшими втратами;

- постійна комунікація з зацікавленими групами протягом всієї кризи, з більш інтенсивним і оперативним інформаційним потоком;

- виступи керівництва компанії, що розкривають її потенціал і наявність всіх необхідних ресурсів для успішного подолання кризи.

Прикладом успішного використання кризових комунікацій в туристичній індустрії є дії уряду Ісландії, що пов'язані з виверженням вулкана Ейяф'ядлайєкюдль в 2010 році. За оцінками фахівців, виверження вулкана могло привести до скорочення туристичного потоку на 20% [11]. Виходячи з цього, уряд країни та зацікавлені сторони в сфері туризму розробили тримісячний проект. Основною метою проекту була демонстрація безпеки та привабливості туризму в Ісландії за винятком регіону, якого торкнулося виверження вулкану.

На першому етапі були задіяні інструменти SMM-комунікації. У соціальних мережах був організований конкурс на найкраще відео «Ісландія надихає». У режимі "онлайн" проводились відеотрансляції з найпопулярніших туристичних місць Ісландії.

На другому етапі лунав заклик до ісландців бути максимально відкритими для туристів і "впустити їх в своє життя". Ця ініціатива була підтримана Президентом країни, який в своєму відеозверненні запрошував всіх бажаючих відвідати його резиденцію і спробувати традиційні ісландські млинці, приготовані його дружиною. Приклад Президента підтримала вся Ісландія. Це обумовило максимальне наближення масової антикризової комунікації до міжособистісної та дозволило забезпечити постійне зростання туристичного потоку Ісландії у наступні роки (рис. 2).

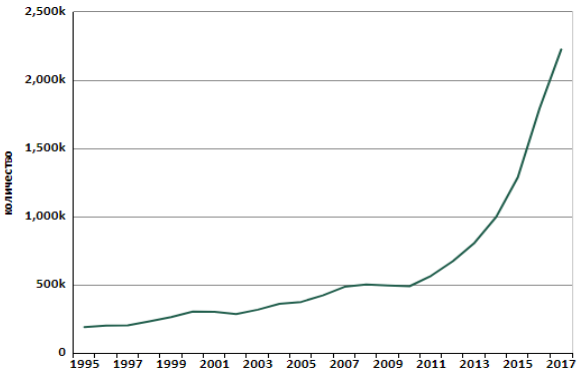


Рис. 2. Кількість туристів, які прибули до Ісландії [12]

Необхідно відзначити, що при відносно невеликих затратах у розмірі 1,25 млн. фунтів стерлінгів, антикризова програма «Натхненний Ісландією» забезпечила повернення інвестицій у співвідношенні 61:1, що принесло додаткові 71 млн. фунтів стерлінгів в економіку Ісландії [11].

Таким чином, найбільш дієвими способами комунікаційної боротьби з кризовою ситуацією є безперервний моніторинг інформації, постійне і оперативне інформування про реальний стан справ, звернення до аудиторії перших посадових осіб, онлайн взаємодія з підтриманням зворотного зв'язку. Компанії, які строго дотримуються принципу прямої залежності змінних "масштаб кризи" / "ступінь відповідальності" і "ступінь активності при здійсненні кризових комунікацій" долають кризу в максимально швидкі терміни при мінімальних матеріальних витратах і репутаційних втратах. Виникаючі при цьому міжкультурні зв'язки й особисті дружні стосунки є важливим фактором забезпечення міжнародної безпеки, сприяють створенню атмосфери довіри і взаєморозуміння між народами різних країн.

Список літератури

1. World Tourism Organization UNWTO. Why tourism? [Online]. Available at: http://www2.unwto.org/content/why-tourism. Accessed Feb. 16, 2019.

2. P. Patsek, "Military and non-military aspects of security of Poland", *Science and Technology of the Air Force of Ukraine*, No. 4(33), pp. 107-118. doi: 10.30748/nitps. 2018.33.14.

3. World Tourism Organization. Toolbox for Crisis Communications in Tourism – Checklists and Best Practices. [Online]. Available at: https://www.e-unwto.org/ doi/book/10.18111/9789284414161. Accessed on: Feb. 16, 2019.

4. A. Schwarz, M. Seeger, and C. Auer, *The Handbook of International Crisis Communication Research*, Wiley-Blackwell, 2016.

5. W. T. Coombs, "*Crisis and crisis management. Encyclopedia of public relations*", SAGE Publications, pp. 217–220, doi: 10.4135/9781452276236.n115, 2013.

6. A. Schwarz, "Stakeholder Attributions in Crises: The Effects of Covariation Information and Attribution Inferences on Organizational Reputation", *International Journal of Strategic Communication*, No. 6(2), pp. 174–195. doi: 10.1080/1553118x.2011.596869, 2012.

7. W. Benoit, *Accounts, excuses, and apologies. Albany*, State University of New York Press, 1995.

8. Y. Jin, A. Pang, and G. T. Cameron, "The role of emotions in crisis responses: Inaugural test of the integrated crisis mapping (ICM) model", *Corporate Communications: An International Journal*, № 15(4), pp. 428–452, doi: 10.1108/13563281011085529, 2010.

9. G. Lippitt, *Organization renewal*, Englewood Cliffs: Prentice-Hall, 1982.

10. B. F. Liu, L. Austin, and Y. Jin, "How publics respond to crisis communication strategies: The interplay of information form and source", *Public Relations Review*, No. 37(4), pp. 345–353. doi: 10.1016/j.pubrev.2011.08.004, 2011.

11. K. Hauksson, "*Case Study: Inspired by Iceland Best Marketing*". [Online]. Available: http://www.best-marketing.eu/case-study-inspired-by-iceland/. Accessed on: Feb. 17, 2019.

12. KNOEMA, "*Iceland – International tourism*" [Online]. Available: https://knoema.ru/atlas. Accessed on: Feb. 17, 2019.

УДК 004.85, 004.89

І. В. Ізонін, Р. О. Ткаченко

ivanizonin@gmail.com, roman.tkachenko@gmail.com

Національний університет «Львівська політехніка», м. Львів

ПОБУДОВА КОМІТЕТУ НЕЙРОПОДІБНИХ СТРУКТУР МПГП З ПОЛІНОМІАЛЬНИМ РОЗШИРЕННЯМ ВХОДІВ ДЛЯ ЗАДАЧ ВЕЛИКИХ ДАНИХ

Точність розв'язання задач апроксимації нелінійних залежностей являється однією із важливих задач сьогодення. В еру Великих даних задача ще більше ускладнюється за рахунок таких факторів як наявність величезних обсягів даних для опрацювання та багатопараметричними залежностями кожного вхідного вектора. Існуючі методи машинного навчання не завжди забезпечують можливість їх використання для отримання достатньо точних результатів розв'язання цієї задачі

У роботі розглядається задача множинної регресії для випадку опрацювання великих наборів даних. Завдання полягає у прогнозуванні залежної змінної на основі набору незалежних шляхом побудови дерева регресії. Авторами запропоновано новий метод розв'язання цієї задачі на основі застосування комітету лінійних неітеративних нейроподібних структур Моделі Послідовних Геометричних Перетворень (МПГП). Його особливістю є те, що для процедур поділу на кластери та прогнозування на кожному кроці методу додатково використовується розширення входів на основі полінома Колмогорова-Габора.

В основі запропонованого підходу лежить побудова бінарного дерева рішень для поділу вибірки даних на частини (кластери). Такий поділ відбувається шляхом порівняння спрогнозованих значень залежної змінної y_i^{pred} до її середнього значення $y_i^{average}$ у кластері на попередньому кроці $(i-1)$. З ростом кроків поділу число кластерів подвоюється. Кожен з них використовує свою нейроподібну структуру МПГП з попереднім опрацюванням вхідних даних на основі поліному Колмогорова-Габора. Основним призначенням нейроподібних структур комітету є формування коефіцієнтів полінома для кожного окремого кластера даних. Такий підхід надає можливість представити результат в компактному вигляді полінома Колмогорова-Габора. На рис. 1 подано структурну схему поділу вибірки до утворення двох кластерів. Проте у випадку опрацювання даних великих обсягів такий поділ можна продовжувати.

Моделювання роботи запропонованого методу відбувалося на задачі прогнозування медичних страхових виплат. Матриця навчальних даних містила 1070 векторів, а розмірність матриці тестових даних становила 268 векторів.

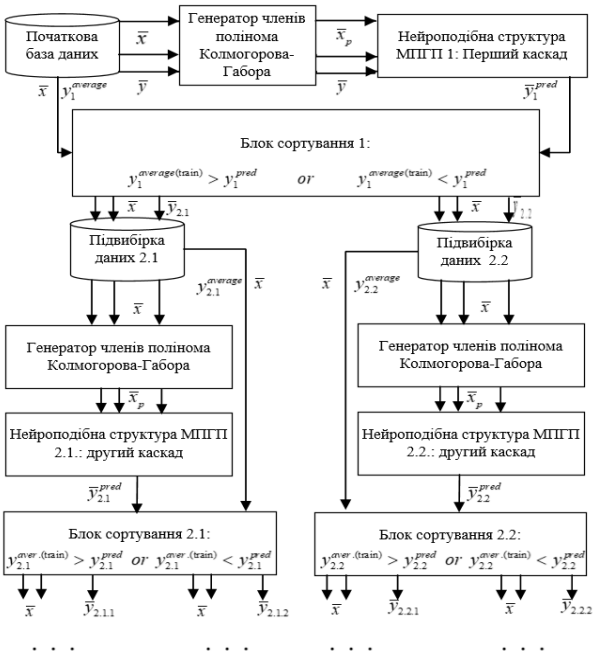


Рис. 1. Структурна схема розробленого методу

Порівняння результатів розробленого методу з існуючими на основі MAPE наведено на рис. 2

Рис. 2. MAPE для усіх досліджуваних методів

Як видно з рис. 2, розроблений метод забезпечує найвищу точність прогнозування.

Список літератури

1. R. Tkachenko, I. Izonin, N. Kryvinska, V. Chopyak, N. Lotoshynska, and D. Danylyuk, "Piecewise-linear Approach for Medical Insurance Costs Prediction using SGTM Neural-Like Structure", *CEUR-WS: Proceedings of the 1st International Workshop Informatics & Data-Driven Medicine (IDDM 2018)*, Lviv, Ukraine, pp. 170 – 179, 2018.

УДК 659.44

К.В. Ковальчук

kristina983@ukr.net

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПОЗИЦІОНУВАННЯ БРЕНДУ

Назва торгівельної марки завжди формує сприйняття продукції споживачем. Назва продукту обов'язково повинна залучити увагу та запам'ятуватися покупцю та створити ряд позитивних вражень та асоціацій для покупця. Найважливіша частина створення бренду це- неймінг – це одна з головних сторін позиціонування бренду.

В основі процесу будь-якої діяльності лежить технологія. Категорія "технологія" являє собою систему знань про способи і засоби здійснення процесу будь-якої сфери діяльності. Технологія брендинга – це сукупність знань про способи і засоби управління процесом формування та розвитку бренду.

Дослідження, проведене компанією Комкоп-Вектор по споживанню товарів різних груп, з'ясувало, що купують тільки одну марку 23–39% покупців, а одну або дві марки – 48–65%. На основі методики IBIS (Investing in Brands in Store) компанія Research international провела кластерний аналіз відносин до брендам і ступеня лояльності до них споживачів Дані показують, що за два роки кількість активних споживачів, які купують певну марку товарів, зросла в 2,4 рази (з 13,4 до 31,5%), а число покупців, що орієнтуються на марку в числі інших факторів, за цей же період збільшилася в 1,7 рази (з 25,4 до 43,3%). [1]

Зараз на ринку з'являється безліч брендів та торгових марок, формується велика кількість назв, комбінацій та слів. Насамперед для кожного покупця важливо, що чим простіше назва тим швидше вона запам'ятовується. Часто можна помітити, що назвою відомого бренду є ім'я та фамілія засновника бренду. Важливу роль відіграє асоціація з якою пов'язана назва компанії чи бренду. Це можуть бути тварини, квіти, історичні або літературні персонажі і т. д. Для назви бренду можна використовувати різноманітні комбінації слів, однак за зіставленням комбінації декількох слів не завжди можна получити бажану назву тому потрібно до цього процесу відноситися обережно аби не зробити помилок. Назва завжди запам'ятовується краще коли є рима, ритм або повторювання слів словосполучення має бути легковимовляємим [1].

Важливий аспект для формування брендингу це відносини в залежності від характеру зв'язків і відносин бренду з споживачами, що представляє собою сукупність емоційних, раціональних і поведінкових відносин. як правило, є лояльні відносини, які визначаються ступенем задоволення потреб покупця при використанні товару торгової марки (бренду). Ступінь задоволення потреб покупця залежить від іміджу бренду, очікувань, сприйняття інформації про якість товару і ціни.

Процес позиціонування бренду складається з наступних етапів: аналіз товару і ринку, вивчення конкурентів, сегментування, порівняльний аналіз і формування позиції бренду. На першому етапі необхідно визначити призначення товару, тобто до якої товарної групи він відноситься, для якого виду споживання призначений, яку користь або вигоду несе споживачеві, а також виявити, як сприймає споживач повідомлення про товар і що він очікує від бренду. Другий етап – вивчення всіх конкурентних брендів в різних товарних групах (суміжних, що діють, групах товарів-замінників і товарів-прототипів). Зіставлення позицій конкурентних брендів дозволяє визначити, яким чином споживачі відрізняють і об'єднують продукцію в одну товарну групу. Ця інформація дозволяє виявити незаповнені ніші серед марочних позицій. Після цього необхідно розділити по можливості споживачів торгової марки на однорідні групи – сегменти.

Для ефективного формування брендингу необхідно побудувати систему відносин, в залежності від характеру зв'язків і відносин бренду з споживачами, що представляє собою сукупність емоційних, раціональних і поведінкових відносин.

При формуванні інформаційного забезпечення процесу позиціонування бренду необхідно дотримуватися наступних вимог;

простоти – інформація про бренд повинна бути простою, зрозумілою, короткою;

актуальності – повідомлення про бренд має відповідати потребам, бажанням і намірам споживачів;

відмінності – в змісті бренду повинні бути чітко відображені основні відмінні ознаки даного товару від аналогічних;

сталості – необхідно протягом тривалого часу не зраджувати позиції бренду, щоб у споживача виробилися стійкі позитивні емоції (сприйняття) щодо вигод і переваг, які пропонує цей бренд [1].

Список літератури

1. Вестник Харьковской торгово-промышленной палаты, № 1, с. 40–44, 2017.

УДК 621.391

В.В. Ковширко

kyreevav@gmail.com

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ГРАФІЧНОГО КОНТЕНТУ ДЛЯ ІНФОРМАЦІЙНОГО ВПЛИВУ НА АКТОРІВ СОЦІАЛЬНИХ МЕРЕЖ

В сучасних умовах кількість користувачів мережі Інтернет постійно зростає, внаслідок чого соціальні мережі (СМ) перетворилися на один з найпопулярніших засобів масової комунікації. СМ – це програмний сервіс, платформа для взаємодії акторів (користувачів) в групі чи групах. Завданням такого сервісу є забезпечення акторів усіма можливими інструментами для спілкування один з одним – відео, чати, зображення, музика, блоги, форуми тощо [1]. В умовах зростання своєї популярності СМ трансформувалися в своєрідний плацдарм інформаційної війни. З їх використанням створюються передумови для невдоволеності акторів соціальним становищем, появи конфліктів на різному підґрунті, маніпулювання суспільною думкою тощо. Також СМ стали дієвим інструментом інформаційного впливу і прихованого управління процесами прийняття рішень громадянами у реальному житті. Такий інформаційний влив здійснюється з використанням контенту СМ. Тому дослідження особливостей використання такого контенту для здійснення інформаційного впливу на громадян при використанні ними СМ є актуальним.

Аналіз досліджень і публікацій показав, що термін контент (англ. content – зміст, вміст) є комбінованим і характеризує будь-яку інформацію. У СМ контент – це інформація, яка публікується у інформаційному просторі сервісу, будь-яке інформаційно значуще наповнення інформаційного ресурсу. Найпоширенішими є такі типи контенту: текстовий, графічний, аудіо- та мультимедійний.

Встановлено, що виявленню загроз інформаційній безпеці акторів у СМ присвячена значна кількість публікацій, однак проблема виявлення інформаційного впливу на акторів у графічному контенті опрацьоване недостатньо. Відомо, що найбільш дієвим є інформаційний вплив, який ґрунтується на використанні не тільки текстового, але і графічного контенту СМ. При цьому він може містити деструктивний інформаційний вплив на акторів у явному або прихованому вигляді.

Відомо, що значний вплив на свідомість людини несуть графічні та аудіо- та мультимедійний файли. Будь який візуальний контент несвідомо впливає на людину, та в залежності від характеру зображення формує негативне чи позитивне бачення ситуації.

Відповідно до інформаційних загроз, які можуть проявлятися за допомогою візуального контенту дослідники виділяють наступні :

створення атмосфери бездуховності та аморальності, негативного відношення до культурної спадщини;

маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни з метою створення політичної напруженості та хаосу;

дестабілізація політичних відносин між партіями, об'єднаннями і рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємознищення;

зниження рівня інформаційного забезпечення органів влади та управління, інспірація помилкових управлінських рішень;

дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;

провокування соціальних, політичних, національних та релігійних зіткнень;

ініціювання страйків, масових заворушень та інших акцій економічного протесту;

утруднення прийняття органами управління важливих рішень;

підрив міжнародного авторитету держави, його співробітництва з іншими країнами;

нанесення шкоди життєво важливим інтересам держави в політичній, економічній, оборонній та інших.

Для попередження і виявлення інформаційних впливів необхідно досліджувати контент, який актори розміщують та поширюють в СМ. Для цього можливо використовувати методику контент-аналізу. Яка складається з трьох наступних етапів:

аналіз текстового контенту

аналіз графічного контенту

аналіз загального візуального сприйняття.

Список літератури

1. Aleman, Ana M. Martinez; Wartman, Katherine Lynk, “Online social networking on campus: understanding what matters in student culture”, New York and London : Routledge, 1st edition, 2009].

УДК 004.056, 004.75

Т.В. Козуля, М.М. Козуля

mariya.kozulya7@gmail.com

Національний технічний університет «Харківський політехнічний інститут», м. Харків

РОЗВ'ЯЗАННЯ СИСТЕМНИХ ЗАДАЧ ЗА СЦЕНАРНО-ЦІЛЬОВИМ ПІДХОДОМ НА ОСНОВІ РОЗРОБКИ ЗНАННЯ-ОРІЄНТОВАНИХ СИСТЕМ

Інформаційна організація об'єкта системного аналізу виходить за межі класифікаційного поняття складності (великі системи тощо), стає доцільним відображати його як комплексне утворення і корпоративну систему з кооперативними зв'язками, які становлять основу її самоорганізації з досягнення стабільності і рівноважного розвитку (синергетика) [1].

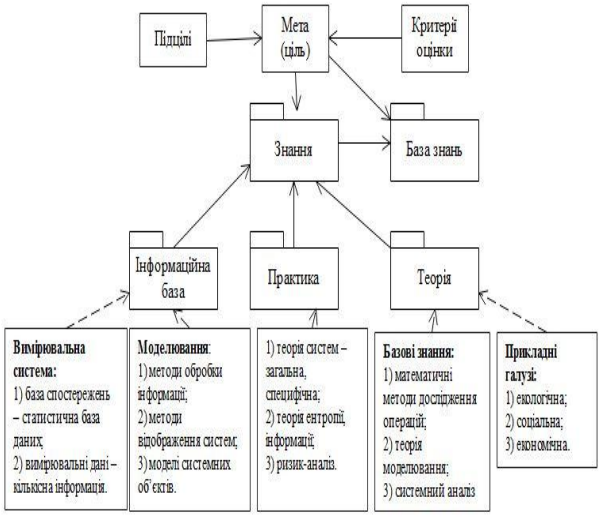
У складному об'єкті дослідження запропоновано виділяти цільовий комплекс «(система $\xleftrightarrow{\text{процес}}$ зовнішнє середовище) $\xrightarrow{\text{стан}}$ система $\xrightarrow{\text{процес}}$ зміни системи – процес – ((стан системи)′ – зовнішнє середовище)», в якому як елементи розглядають системи, їх зовнішнє середовище, що утворює внутрішній простір об'єкта, де самоорганізуються зв'язки і таким чином формується структура об'єкта, взаємодіючого з навколишнім середовищем. Кооперативна дія внутрішніх і зовнішніх процесів стабілізує складну систему, що і відповідає уявленням синергетики про явища [1].

При аналізі складних об'єктів використовуються знання з врахуванням, що кожна аналізована система об'єкта є високоорганізованою, тобто має розвинену й складну структуру, менш організованою з простою структурою, зовсім хаотичною, коли її елементи розподілені випадково й, у середньому, однорідним чином. Для аналізу необоротних процесів використовують фундаментальні положення теорії утворення структур і звертаються до фрактальної геометрії для отримання зв'язку базових понять *хаос* і *структура*, *різні ентропії* з *кількісної оцінки систем різної природи*.

Головне завдання при синергетичному аналізі складних систем полягає у виявленні головних факторів на кожному етапі послідовного і незворотного переходу від одного стану систем до іншого з реалізацією певного рівня внутрішньої організації і ступеню зв'язаності структурних елементів при перевазі певного типу зв'язку між ними. Для ідентифікації передкризових станів запроваджується комплексний сигнальний підхід на основі сучасних методів синергетики, мультифрактального та вейвлет аналізу, ентропійних методів, графологічних моделей тощо.

Інформаційне навантаження за таким системним аналізом передбачає базу знань з 2-х аспектів – конкретні галузеві знання економічних, соціальних і екологічних наук; теоретико-практичні знання процесів і динаміки розвитку систем. Кожна система знань надає інформаційне забезпечення про обсяги даних у певній галузі, що є основою розв'язання саме її задач і в той же час є складовою у вирішенні проблемних задач системних утворень, що розвиваються [2].

У базі знань предметних областей мають місце відомості, дані про розробки різноманітних моделей, аналіз і синтез яких виконується у відповідності до розв'язання конкретних задач, які розглядалися авторами на прикладі завдань екологічної безпеки (рис. 1).



– інформаційна підтримка подолання невизначеності

Рис. 1. Сценарно-цільовий підхід розробки знання-орієнтованих систем

Таким чином, взаємоузгодженість різнопланових визначень і оцінок у межах комплексного дослідження складних об'єктів, зазначених як системні утворення, досягається завдяки усвідомленню знань-інформаційних даних (експериментально-дослідної інформації) відповідно до опису поводження складних систем у термінах ентропія, антиентропія, узагальнена негентропія й ентропійний баланс.

Список літератури

1. М. М. Козуля, "Комплексна інформаційно-системна оцінка рівня екологічної безпеки складних об'єктів", дис. канд. наук., Сум. держ. ун-т, Суми, 2017.

2. T. V. Kozulia, and M. M. Kozulia, "Integrated information system assessment of complex objects safety level", *Вісник НТУ «ХПІ». Серія: Системний аналіз, управління та інформаційні технології,* №55(1276), с. 39 – 45, 2017.

УДК 004.94

А.М. Копп, Д.Л. Орловський

kopp93@gmail.com, ordm@kpi.kharkov.ua

Національний технічний університет «Харківський політехнічний інститут», м. Харків

ЦИКЛ ПЕРЕТВОРЕННЯ ЗНАНЬ ЯК СКЛАДОВА ЧАСТИНА КОНЦЕПЦІЇ BPM

Управління бізнес-процесами – BPM (Business Process Management) – одна з найбільш поширених та популярних на сьогоднішній день управлінських концепцій. Згідно з BPM, бізнес-процесом (БП) є структурована послідовність дій, яка перетворює один або декілька типів ресурсів на продукт або послугу, що має цінність для певних споживачів. В основі BPM полягає набір методів та інструментів побудови, аналізу, вдосконалення, та автоматизації БП підприємства.

Основним інструментом концепції управління бізнес-процесами є моделювання БП, на меті якого є забезпечення [1]:

1) кращого розуміння бізнес-процесів;

2) документування бізнес-процесів (наприклад, з метою використання моделей бізнес-процесів для інструктажу співробітників);

3) аналізу бізнес-процесів (наприклад, з метою виявлення потенційних помилок на основі аналізу побудованих моделей бізнес-процесів);

4) вдосконалення бізнес-процесів, описаних за допомогою побудованих моделей бізнес-процесів.

Моделювання бізнес-процесів розглядається в якості ключового компонента управління знаннями (KM, Knowledge Management), за допомогою якого виконується перетворення неформалізованих знань про діяльність підприємства на формалізовані, що прискорює розповсюдження та сприяє повторному використанню знань, представлених за допомогою моделей БП [2]. Повторне використання моделей БП дозволяє зменшити витрати на моделювання БП "з нуля", завдяки використанню існуючих моделей.

Зазвичай в ролі централізованого сховища для накопичення та колективного використання моделей БП для їх повторного використання застосовується спеціалізована база даних – репозиторій моделей бізнес-процесів. Використання репозиторію моделей БП надає усім зацікавленим сторонам (stakeholders) можливість вилучати моделі для кращого розуміння діяльності підприємства, оновлювати, аналізувати та повторно використовувати збережені моделі БП [3].

Модель життєвого циклу організаційних знань SECI включає наступні етапи [2]:

1) соціалізація (socialization) – обмін неявними знаннями між співробітниками;

2) екстерналізація (externalization) – перехід від неявних знань до явних, шляхом їх документування;

3) комбінація (combination) – створення нових знань шляхом використання інших знань;

4) інтерналізація (internalization) – перехід від явних знань до неявних шляхом їх засвоєння.

Таким чином, життєвий цикл моделей бізнес-процесів в рамках концепції BPM, можна розглядати з точки зору перетворення знань про бізнес-процеси підприємства відповідно до моделі SECI (рис. 1).

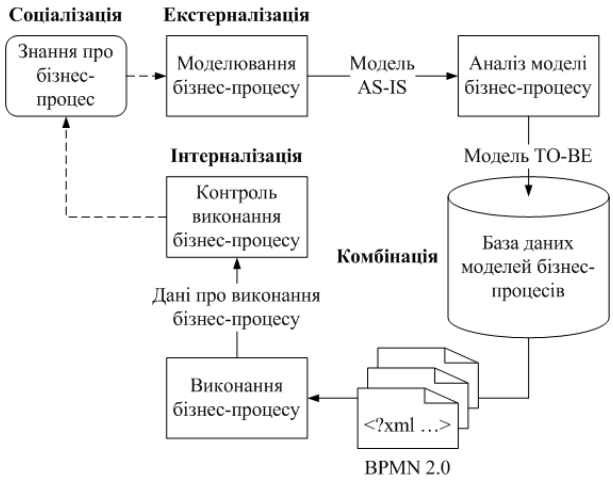


Рис. 1. Життєвий цикл моделей БП

Носіями знань про діяльність підприємства є його співробітники, документація, а також системи класу BPM або ERP (Enterprise Resource Planning). На основі знань про поточний стан БП створюється модель "as-is", виконується її аналіз та формується модель "to-be", позбавлена можливих недоліків.

Найпоширеніша на сьогоднішній день нотація моделювання БП BPMN (Business Process Model and Notation) використовується разом з системами BPM для автоматизації виконання БП. Окрім графічних моделей БП, дана нотація дозволяє використовувати XML-подібний формат BPMN 2.0 з метою обміну визначеннями БП між різними інструментами BPM.

Отримання нових знань про БП здійснюється на основі використання засобів BPI (Business Process Intelligence) та зокрема Process Mining.

Список літератури

1. W. M. P. Van Der Aalst, *Business process management: a comprehensive survey*, ISRN Software Engineering, 2013.

2. B. Kalpic, and P. Bernus, "Business process modeling through the knowledge management perspective", *Journal of Knowledge Management*, vol. 10, no. 3, pp. 40–56, 2006.

3. M. Elias, *Design of business process model repositories: requirements, semantic annotation model and relationship meta-model*, Department of Computer and Systems Sciences, Stockholm University, 2015.

УДК 005.94:004.9

Н.В. Куліш, Р.П Шкребень

Otenkoip@gmail.com

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

КОНЦЕПТУАЛІЗАЦІЯ ОРГАНІЗАЦІЙНО-ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ФОРМУВАННЯ СИСТЕМИ ЗНАНЬ ПІДПРИЄМСТВА

В основу організаційно-інформаційної підтримка формування стратегічних знань покладений принцип формалізації і кодифікування, відповідно до якого знання співпрацівників узагальнюються і фіксуються на електронних і паперових носіях для того, щоб решта зацікавлених співпрацівників могла скористатися цими знаннями надалі. Відповідно основними принципами організаційно-інформаційного забезпечення управління знаннями виступають[1]:

створення надійної і повної підтримки процесів ухвалення рішень за рахунок: формування баз знань, правил, експертних систем для вирішення певних завдань; організацію збереження і публікації призначеної для користувача інформації і формалізованих знань; організації доступу до створюваних баз знань зацікавлених співпрацівників підприємства, так само як і до формалізованих знань, що вже зберігаються в базі даних підприємства; забезпечення технологіями пошуку і систематизації формалізованих знань, що зберігаються в організаційній базі знань;

відкритість для зовнішніх знань через створення можливостей кінцевим користувачам взаємодіяти з численними джерелами зовнішніх знань і інформації: від інформаційних ресурсних баз до навчання та консалтингу.

Комплексним вирішенням проблеми кодифікування знання є створення корпоративної інформаційної системи, бази, що зв'язує воєдино дані й інформаційні потоки комп'ютерних систем компанії [2]. Використання такої системи дозволяє не лише знизити операційні витрати на виконання рутинних процедур, але й вирішить проблеми координації діяльності співпрацівників і підрозділів, забезпечення їх необхідною інформацією і контролю виконавської дисципліни. При цьому керівництво отримує своєчасний доступ до достовірних даних про хід виробничого процесу і має засоби для оперативного ухвалення та реалізацію своїх рішень.

З позиції персоналізації, формування стратегічних знань пов'язано з необхідністю організації взаємодії персоналу, тому організаційно-інформаційне забезпечення повинне задовольняти таким вимогам [3]: ключовими елементами є комунікаційні технології та засоби, що забезпечують спільну роботу співпрацівників: мережеві технології, технології спільного ухвалення рішень і технології, що підтримують неформальне спілкування і обмін думками; підтримка процесів ухвалення рішення повинна базуватися на доступі до співпрацівників-носіїв знань. Реалізація даного принципу полягає у формуванні внутрішньо організаційних каталогів експертів з різних питань і організації доступу співпрацівників, зацікавлених в отриманні консультацій від експертів; інформаційно-технологічні засоби повинні забезпечувати можливість обміну неформальними знаннями з елементами зовнішнього середовища.

Виділення завдань та етапів кодифікування стратегічних знань ґрунтується на наступних положеннях: кожний етап повинен мати самостійне значення в загальному процесі управління й формалізований, тобто на кожному етапі повинні бути отримані якісні і кількісні показники, аналіз яких дасть можливість формувати конкретні рекомендації з удосконалення управління знаннями підприємства; етапи повинні бути взаємозалежні, тобто основні характеристики (параметри), що одержуються на кожному з них, повинні бути вихідними передумовами для реалізації завдань управління на наступних етапах організаційно-інформаційного забезпечення управління знаннями; загальним спрямуванням методичного підходу повинне бути зменшення невизначеності процесу управління знаннями підприємства, тобто перехід від загальних, агрегованих категорій до визначення конкретних характеристик цього процесу.

Список літератури

1. О. В. Денисюк, та Я. М. Стоказ, “Методичний підхід до формування та розвитку стратегічних знань підприємства”, *Проблеми економіки*, № 2 (36), с. 191–198, 2018.

2. І. П. Отенко, та О.С. Преображенська, “Розвиток компетенцій на основі стратегічних знань”, ВД “ІНЖЕК”, 2012.

3. О. С. Преображенська, та Я. М. Стоказ, “Механізми захисту стратегічних знань підприємства”, *Материалы XV Всеукраинская научно-практическая конференция «Проблемы устойчивости функционирования субъектов рыночной экономики Украины», Симферополь: ИТ «АРИАЛ»*, 2013, с. 88–91.

УДК 004.738.5:339.138

К. І. Куценко

ekaterina.markina994@gmail.com

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В МАРКЕТИНГОВІЙ ДІЯЛЬНОСТІ ПРОМИСЛОВИХ ПІДПРИЄМСТВ

На теперішній час актуальним постає питання проблеми адаптації і функціонування соціально-економічних структур в ринкових відносинах. Суттєвий вплив на виробничі відносини суб`єктів господарської діяльності надає саме маркетингова діяльність та дослідження. У сучасному стані трансформацій економіки для ведення ефективної господарської діяльності необхідно застосовувати нові методи та принципи інформаційних технологій та їх використання, які адаптовані під сучасний стан економіки та враховують фактори зовнішнього та внутрішнього середовища. Цьому сприяв світовий розвиток віртуального простору.

Щоб сучасному промисловому підприємству (далі – підприємство) забезпечити стійкий розвиток, високу конкурентоспроможність, слід розглядати маркетингову діяльність, як одну з найважливіших складових підприємницької діяльності. Саме вона забезпечить довгострокові та продуктивні відносини із споживачем, який виступає основним елементом у системі маркетингу.

Отже, зростає важливість інформаційних технологій під час ведення маркетингової діяльності.

Сучасні інформаційні технології розвиваються дуже швидко та прогресивно, за допомогою яких прискорився процес ведення маркетингових досліджень. Тобто інформація та інформаційні технології відіграють важливу роль для ведення діяльності підприємств у цілому.

На сьогодні основними функціями інформаційних технологій слід вважати:

- пошук інформації;
- збір інформації;
- аналіз інформації;
- вироблення нової інформації;
- структурування і зберігання інформації;

Інформація на даний час постає одним із найважливіших ресурсів суспільства, без якого не можливе успішне управління функціонуванням жодного із суб'єктів господарської діяльності. За підрахунками фахівців її обсяг зростає удвічі кожних 2–3 роки [1].

Інформаційні технології стали важливою складовою ефективного управління в умовах нагромадження обсягів зовнішніх та внутрішніх інформаційних потоків. Свідченням цього є те, що було включено до розрахунку індексу економіки знань – комплексного показника, який характеризує стан розвитку економіки, основаної на знаннях, групи показників, які описують стан розвитку інформаційної і комунікаційної інфраструктури [2].

Ефективність та успішність ведення маркетингової діяльності залежить від того, як підприємства використовують свій інформаційний потенціал, як основу забезпечення інформацією для проведення маркетингових досліджень та прогнозування. Один із широковідомих інструментів інформаційних технологій це – Інтернет. Завдяки цьому інструменту реалізуються основні функції інформаційних технологій. Значна частина маркетингової діяльності підприємств спирається саме на використання такого інструменту. Інтернет, як інформаційна технологія в маркетинговій діяльності підприємств, виконує такі дві функції:

- внутрішня;
- зовнішня.

До внутрішніх функцій такого інструменту можна віднести:

- збір, обробка, аналіз інформації;
- систематизація та накопичення інформації;
- створення локальної мережі для корпоративного користування.

До зовнішніх функцій слід віднести:

- розміщення реклами у соціальних мережах;
- розміщення реклами у віртуальному просторі;
- зв'язок із споживачем;
- вивчення ринку та конкурентів.

Саме інформаційні технології сприятимуть сталому розвитку та ефективному веденню маркетингової.

Отже, господарська діяльність підприємств залежить від багатьох факторів зовнішнього та внутрішнього середовища, які швидко змінюються та впливають, як на діяльність підприємства так і на обсяги інформації. Вони збільшуються, а це означає що її треба постійно оновлювати та обробляти. Це неперервний зв'язок. Саме інформаційні технології допоможуть покращити та удосконалити цей процес підприємству.

Список літератури

1. А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, и И. И. Холод, *Технологии анализа данных: DataMining, VisualMining, OLAP*, БХВ-Петербург, 2007.

2. Индекс экономики знаний – информация об исследовании. [Электронний ресурс]. Доступно: http://gtmarket.ru/ratings/knowledge-economy-index/knowledge-economy-index-info. Дата обращения: Март 19, 2019.

УДК 004.652.4+004.827

Н.І. Мельникова[1], В.А. Мельников[2]

melnykovanatalia@gmail.com,v.melnikov2013@gmail.com

[1] *Національний Університет «Львівська політехніка», м. Львів*
[2] *Львівський Національний Медичний Університет ім. Д. Галицького, м. Львів*

ПЕРСОНАЛІЗОВАНИЙ ПІДХІД ЩОДО ОБРОБКИ ТА АНАЛІЗУ МЕДИЧНИХ ДАНИХ ПАЦІЄНТІВ

Стрімке зростання обсягу зібраних даних, відсутність альтернативних методів їх ефективного аналізу, потреба у значних людських ресурсах для підтримки процесу аналізу даних. Це зумовлює необхідність появи нових методів та засобів опрацювання, консолідації персоналізованих даних для процесу збору гетерогенних даних великих обсягів а також підтримки прийняття лікарських рішень

Специфіка опрацювання медичних даних великих обсягів визначає потребу у розробці нових методів аналізу, консолідації, прогнозування для підтримки лікарських рішень під час діагностування, лікування та реабілітації хворих. Процес налізу медичних даних характеризується рядом визначених проблем, які виникають під час розв'язання такого класу задач, а саме [1]: нечіткість представлених даних; класифікація даних; консолідація даних; визначення загального стану хворого; визначення персоналізованих рішень щодо лікування; оцінка ступеня надійності результуючих висновків; оцінка появи ризиків; прогнозування станів хворого під впливом застосованої терапії.

Як наслідок виникають проблеми при обробці даних, а саме: відсутність методів аналізу, придатних до застосування через їх різнотипність (для медицини – це часово-залежні дані загального стану хворого, і слабоструктуровані дані лабораторних досліджень, тощо), потреба у значних людських ресурсах для підтримки процесу аналізу даних, висока обчислювальна складність наявних алгоритмів аналізу та стрімке зростання обсягу зібраних даних. Це в свою чергу призводить до постійного зростання часу, що витрачається на аналіз даних навіть при регулярному оновленні комп'ютерних засобів, а також – необхідність роботи із розподіленими базами даних, можливості яких більшість існуючих методів аналізу даних не використовують ефективно [2].

Таким чином, виникає задача розроблення ефективного уніфікованого методу аналізу та консолідації персоналізованих даних, що дозволить його застосовування не лише для медицини але і для інших предметних областей. Персоналізовані дані *PD* – це множина даних, елементами якої є підмножини часо-незалежних даних *(A)* та часово-залежних даних (*S)* досліджуваного об'єкта, що характеризують загальних його стан:

$$\mathrm{PD} = \{\{\mathrm{A}\},\{\mathrm{S}\}\} \qquad (1)$$

Відповідно до визначених множин даних для забезпечення персоналізації рішень пропонується концептуальна модель персоналізації рішень щодо визначення лікування, рис.1.

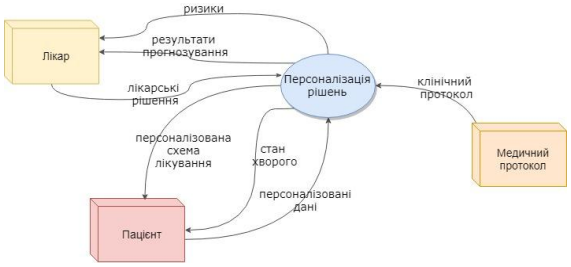


Рис. 1. Концептуальна модель персоналізації рішень щодо визначення лікування

Процес опрацювання та аналізу персоналізованих даних для пошуку лікарських рішень представимо у вигляді пари:

$$\mathrm{APD} = \{\mathrm{GS}, \mathrm{PD} \bigcup \mathrm{D}\}, \qquad (2)$$

де GS – множина станів пацієнта; PD – множина персоналізованих даних; *D* – множина персоналізованих рішень.

Проаналізовано методи опрацювання персоналізованих медичних даних: метод уніфікації персоналізованих схем лікування, мережа Байєса, метод асоціативних правил, метод логічного виведення, що сформувало бачення щодо ефективності їхнього застосування для такого типу задач. Як результат отримали, що у методі уніфікації персоналізованих схем лікування збільшення критеріїв відбору (параметрів пацієнта) обернено пропорційно впливає на перелік запропонованих терапевтичних схем. Це дозволяє підвищити швидкодію пошуку, за рахунок збалансованості дерева пошуку та опрацювання лише персоналізованих даних, що надходять у вхідному наборі даних.

Список літератури

1. N. Melnykova, and O Markiv, "Semantic approach to personalization of medical data", *Computer Sciences and Information Technologies – Proceedings of the 11th International Scientific and Technical Conference*, pp. 59 – 61, 2016.

2. N. Melnykova, and U. Marikutsa, "Specifics personalized approach in the analysis of medical information", *ECONTECHMOD: An International Quarterly Journal on Economics of Technology and Modeling Processes*, Vol. 5, No 2, pp. 113 – 120, 2016.

УДК 336.71:005.922.1:33

О.Ю. Мішин, С.В. Мішина

oleksandr.mishyn@hneu.net, svitlana.mishyna@hneu.net

Харківський національний економічний університет ім. С. Кузнеця, м. Харків

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ

В управлінні економічною безпекою банківських установ пріоритетне значення має формування інформаційно-аналітичного забезпечення, оскільки воно є інформаційною основою для прийняття рішень в системі банківської безпеки.

Теоретичні засади інформаційно-аналітичного забезпечення економічної безпеки банку (ІАЗЕББ) знайшли відображення у праці [1].

Метою даного дослідження є уточнення організаційних засад ІАЗЕББ.

Як на думку авторів, ІАЗЕББ – це вид інформаційно-аналітичного забезпечення, що полягає в зборі, обробці, зберіганні і наданні необхідної інформації щодо стану економічної безпеки банку відповідним користувачам. Мета формування ІАЗЕББ полягає у своєчасному виявленні і попередженні загроз економічній безпеці банку.

Керівництво ІАЗЕББ має здійснювати начальник служби безпеки. ІАЗЕББ повинна формувати служба безпеки на основі власної інформації та інформації інших структурних спецпідрозділів: кредитного відділу, відділу валютних операцій, розрахунково-касового обслуговування, охорони та ін.

Основним змістом управління ІАЗЕББ є збір і аналіз даних щодо вірогідних загроз та засобів протидії їх негативному впливу з метою прийняття рішень щодо всебічного забезпечення економічної безпеки банку. ІАЗЕББ має забезпечувати потреби керівництва та служби безпеки в інформації щодо загроз економічній безпеці банку.

Організація ІАЗЕББ – це комплекс організаційних і практичних заходів, щодо розробки змісту, способів дій, термінів і послідовності виконання силами й засобами служби банківської безпеки інформаційно-аналітичних завдань. В числі елементів організації ІАЗЕББ, як на нашу думку, слід виділити такі: постановка мети, завдань ІАЗЕББ; планування ІАЗЕББ; визначення виконавців інформаційно-аналітичної роботи; визначення методів, способів, інструментів формування та забезпечення функціонування ІАЗЕББ; формування бази даних; формування системи аналітичних показників; контроль за виконанням поставлених завдань.

Інформаційно-аналітична робота банку із забезпечення економічної безпеки – це комплекс заходів, які проводяться відділом безпеки банку з метою збору та обробки інформації про загрози і стан безпеки та розробки відповідних інформаційно-аналітичних документів для керівництва банку.

Етапи функціонування інформаційно-аналітичного забезпечення економічної безпеки банку повторюються циклічно і включають: збір та пошук інформації; облік, попереднє вивчення, інформаційно-аналітичну обробку, формулювання висновків; підготовку інформаційно-аналітичних документів.

ІАЗЕББ має будуватися на таких принципах: 1) достовірність інформації. Інформація повинна відображувати реальні процеси та показники, що мають місце в банку; 2) вичерпність інформації. Інформація корисна тільки в тому випадку, коли вона є повною, а не частковою, оскільки це може призвести до викривлення результатів інформаційно-аналітичної роботи; 3) зіставність інформації. Інформація з різних джерел щодо одного й того ж процесу чи явища має бути ідентичною; 4) оперативність отримання інформації. Інформація має цінність тільки якщо є актуальною; 5) ефективність інформації. Інформаційно-аналітична обробка інформації має бути доцільною, тобто ефект від такої обробки має перевищувати витрати на її здійснення; 6) зручність інформації. Інформація повинна бути представлені в зручному для користування вигляді; 7) доцільність інформації. Інформація має бути корисною, тобто необхідною для здійснення аналітичних розрахунків. Не повинно відбуватися перевантаження системи ІАЗЕББ побічною інформацією, що не має відношення до економічної безпеки чи загроз їй.

ІАЗЕББ формується з використанням автоматизованої банківської системи. Вона включає такі підсистеми: операційний день банку; управління кредитними ресурсами банку; управління валютними операціями; управління депозитами; управління цінними паперами; управління касою; внутрішньобанківський облік; управління розрахунками з використанням пластикових карток; звітність банку; аналіз діяльності банку.

Кожна з цих підсистем є джерелом інформації, що використовується при формуванні ІАЗЕББ. У Банк даних щодо загроз економічній безпеці банку має автоматично потрапляти інформація з підсистем автоматизованої банківської системи.

Таким чином, науковим результатом даного дослідження є уточнення теоретико-методичних засад формування ІАЗЕББ.

Список літератури

1. М. І. Зубок, та С. М. Яременко, *Безпека банківської діяльності*, КНЕУ, 2012.

УДК 004.9

В.В. Москаленко, Н.Г. Фонта, О.В. Афанас'єв

valentinamosk17@gmail.com, natalia.fonta@dataart.com, grothentor@gmail.com

Національний технічний університет «Харківський політехнічний інститут», м. Харків

ВИКОРИСТАННЯ СЕРВІС-ОРІЄНТОВАНОЇ АРХІТЕКТУРИ ДЛЯ СИСТЕМИ РІВНЯ ENTERPRISE PERFORMANCE MANAGEMENT

Різноманіття задач стратегічного менеджменту обумовлює безліч інформаційних систем для їх розв'язання [1]. Такі широко відомі програмні продукти, як SAP SEM, SAS Strategy Management, Oracle Hyperion EPM та ін, найбільш повно охоплюють процеси стратегічного управління. На теперішній час є актуальною задача управління ефективністю сучасного підприємства, яке є складною техніко-економічною системою. Ця задача повинна вирішуватися на всіх рівнях управління: стратегічному, тактичному та оперативному. Тому все це потребує великої кількості різнорідної інформації, розв'язку складних задач, які в більшості є слабоформалізованими. Тому пропонуються на ринку IT системи нового покоління, побудованих на принципах управління ефективністю підприємства (Enterprise Performance Management – EPM). За їх допомогою вирішуються питання узгодженого бізнес-планування, координації зусиль різних підрозділів і співробітників, пов'язуючи стратегічні пріоритети підприємства з поточною діяльністю. Крім того, з використанням цієї системи забезпечується моніторинг роботи підприємства на основі безлічі критеріїв, що дозволяє керівникам приймати рішення, спираючись на результати аналізу великого обсягу структурованої бізнес-інформації.

На підставі аналізу систем класу EPM, що існують на ринку IT, можна зробити такий основний висновок: програмні продукти, що реалізують всі компоненти для стратегічного управління, або є досить громіздкими, з великою вартістю та вимагають підтримку своїх платформ, без яких робота не можлива, або мають обмежену функціональність, якщо це невеликі програми. Впровадження таких програмних продуктів може привести до їх неокупності, збитковості або до низької ефективності їх експлуатації. Що є проблемою для багатьох підприємств. Тому пропонується будувати системи класу EPM на інших принципах.

Одним з найбільш поширених архітектурних шаблонів модульного програмування на даний момент є сервіс-орієнтована архітектура (Service-oriented architecture, SOA). SOA – це така архітектура програмного забезпечення, в якій компоненти або "сервіси", маючи узгоджені спільні інтерфейси, використовують єдині правила (контракти) для визначення того, як викликати сервіси і як вони будуть взаємодіяти один з одним [2]. Оскільки EPM як система стратегічного управління буде впроваджуватися на підприємстві, яке вже має безліч працюючих корпоративних систем (ERP, CPM і т.д.), тому її сервіс-орієнтована архітектура надає можливість для реалізації слабо-пов'язаної інтеграції систем різного рівня. Також, розбивання системи на сервіси дозволить легко розширювати і замінювати функціональність без впливу на всю інформаційну екосистему компанії. Концептуальна модель EPM системи з використанням SOA охоплює основні сервіси, кожен з яких призначений для розв'язку класів задач стратегічного управління(рис.1).

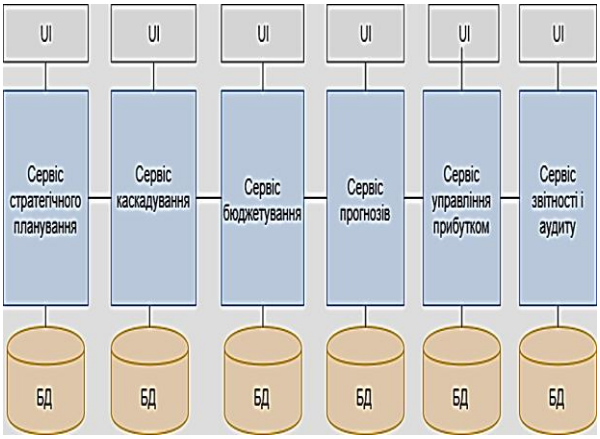


Рис. 1. Концептуальна модель ІС стратегічного управління з використанням SOA

Однак такі недоліки, як висока складність системи, необхідність додаткового мережевого рівня для обміну даними; висока складність підтримки системи, необхідність додаткових програм для моніторингу даних; неможливість забезпечення узгодженості, доступності та стійкості одночасно всіх складових, висока ймовірність дублювання даних в сервісах, обмежує застосування SOA для систем управління ефективністю.

Список літератури

1. О. М. Балахонова, "Обзор информационных систем для решения задач стратегического менеджмента", *Науково-практичний рецензуємий журнал "Статистика и Экономика"*, № 5, с.154-158, 2015.

2. Р. Г. Клапчук, та В. С. Харченко, "Монолітні веб-сервіси та мікросервіси: порівняння та вибір", *Науково-технічний журнал "Радіоелектронні і комп'ютерні системи"*, № 1, с. 51–56, 2017.

УДК 658:005.922.1:3

П.В. Отенко

Otenkoip@gmail.com

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

КОНЦЕПТУАЛЬНІ ПОЛОЖЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ РОЗВИТКУ ПІДПРИЄМСТВА

Концептуальні положення формування економічної безпеки розвитку повинні спиратися на принципи, які відповідають специфіки управління, дії економічної безпеки на підприємстві та мають стратегічну направленість стосовно зазначених цілей розвитку[1]. З огляду на принцип керованості економічною безпекою, для вирішення завдання її інтеграції в систему управління функціонуванням та розвитком підприємства теоретичною базою її дослідження та управління виступає системний підхід, що обумовлює необхідність узгодження функцій системи стратегічного управління розвитком з функціями управління економічною безпекою: оцінювально-аналітична, що представлена аналізом та оцінкою, діагностикою, моніторингом; планово-прогнозна, що забезпечує розробку планів та програм; організаційна, яку визначають інтеграція, узгодження, координація, підтримка, реалізація, контроль; мотиваційна орієнтує персонал на розвиток та навчання, забезпечує його готовність до реалізації інноваційних змін [2].

Стратегічна направленість дії системи економічної безпеки представлена принципами [3]: інноваційної активності – коли інноваційні зміни носять проактивний характер, ініціюються підприємством та дозволяють уникнути погіршення становища, призупинення розвитку, сприяють не тільки збереженню, а й подальшому підвищенню його темпів. В таких випадках акцент робиться на стратегічний потенціал певних напрямків діяльності. Залежно від характеристик цього потенціалу від деяких напрямків варто було б відмовитись, інші необхідно розвивати, оскільки вони мають перспективні можливості на певних ринках. Стратегічне бачення та ефективне використання цих можливостей повинне відповісти на запитання про стійкість реалізації процесів розвитку; стійкості конкурентної позиції підприємства на ринку, що забезпечується активним пошуком найкращої моделі стратегічних дій, вибором доцільних шляхів досягнення стратегічних цілей. Даний принцип пов'язаний з необхідністю відповідати реальним зовнішнім і внутрішнім умовам діяльності, постійно враховувати появу нових погроз і можливостей, безупинно відслідковувати зміну ситуації на ринку, а також забезпечувати надійну підтримку таких процесів через забезпеченість ресурсами, стійкість фінансово-економічного стану, стратегічну компетентність управлінського персоналу – його знання, досвід, навички. З таких позицій системі управління розвитком необхідно мати комплекс можливих стратегій, методів, моделей та організовувати чіткий зворотній зв'язок з ринком для отримання інформації щодо змін; організаційної адаптивності забезпечується використанням нових форм співробітництва, між організаційної взаємодії, надійністю партнерів. Система пріоритетних інтересів підприємства повинна бути узгоджена з інтересами взаємодіючих з ним суб'єктів зовнішнього середовища та обрані такі організаційні форми та засоби гармонізації або узгодження цих інтересів, щоб результати взаємодії з цими суб'єктами забезпечили досягнення цілей, залучення та створення нових стратегічних знань; корпоративної соціальної відповідальності та екологічності підприємства через узгодження інтересів та досягнення консенсусу в прийнятті стратегічних рішень. Відповідно сучасної концепції корпоративної соціальної відповідальності такий принцип представляє добровільну діяльність компаній приватного та державного секторів, спрямованою на дотримання високих стандартів операційної та виробничої діяльності, соціальних стандартів та якість роботи з персоналом, мінімізацію шкідливого впливу на навколишнє середовище, з метою вирівнювання існуючих економічних і соціальних диспропорцій, створення довірливих взаємовідносин між бізнесом, суспільством та державою; функціональної ефективності – досягається за рахунок формування та ефективного використання техніко-технологічного та організаційного потенціалу; модернізації та переозброєння, впровадження нової техніки, що забезпечить скорочення та мінімізацію витрат на виробництво.

Список літератури

1. Г. В. Козаченко, В. П. Пономарьов, та О. М. Ляшенко, *Економічна безпека підприємства: сутність та механізм забезпечення*, Лібра, 2003.

2. О. М. Ляшенко, *Концептуалізація управління економічною безпекою підприємства*, Вид-во СНУ ім. В. Даля, 2011.

3. І. П. Отенко, Д. В. Комарков, та Р. П. Шкребень, "Організація фінансово-економічної безпеки бізнес-процесів інноваційного розвитку підприємства", *Бізнес-Інформ*, №10, с. 23-26, 2017.

УДК 004.9

І.М. Порохня[1], В.А. Лахно[1]

closirr@gmail.com, valss21@ukr.net

[1]*Національний університет біоресурсів і природокористування України, м. Київ, Україна*

МЕТОДИ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ КЛАСТЕРНОГО АНАЛІЗУ НАДЗВИЧАЙНИХ СИТУАЦІЙ В СМАРТ-СІТІ

Забезпечення техногенної безпеки ву смарт-сіті на сьогоднішньому етапі полягає у районуванні територій за ступенями ризику, здійснення заходів з попередження аварій і техногенних катастроф, підготовці сил для ліквідації наслідків, державний контроль питань техногенної безпеки, соціальний захист постраждалого населення.

Вирішення проблем безпеки вимагає великих зусиль, пов'язаних не тільки зі встановленням нормативів, проведенням заходів для попередження екстремальних ситуацій, а в першу чергу направлених на моделювання кластерного аналізу, для попередження виникнення та техногенних катастроф.

Характеристики оцінювання результатів моделювання кластерного аналізу надзвичайних ситуацій як складного процесу визначаються як властивостями його складових, так і характером взаємодії між ними. Слід врахувати такі особливості процесу оцінювання:

- його стан описується потужним вектором динамічних змінних;
- виявляє якісні зміни поведінки його складових;
- включає нелінійні взаємодії основних його складових і обернені зв'язки між ними, які також містять нелінійності.

Серед основних задач, що є актуальними в процесі оцінювання результатів кластеризації надзвичайних ситуацій в смарт-сіті, є розробка його моделі шляхом відтворення зв'язків і відношень між основними його складовими [2].

Для дослідження процесу оцінювання результатів кластерного аналізу надзвичайних ситуацій в смарт-сіті з використанням фізичного моделювання, як одного з найбільш поширених на

практиці підходів, в якості фізичної моделі може виступати:

- процес фізичної природи, що описується аналогічним математичним апаратом;
- процес аналогічної фізичної природи, але в другій області параметрів (масштабна модель).

Оскільки підбір процесу фізичної природи аналогічного процесу оцінювання результатів кластерного аналізу і відповідного математичного апарату, є складним, можна зробити висновок про недоцільність застосування даного виду моделювання для розв'язання поставленої задачі [1].

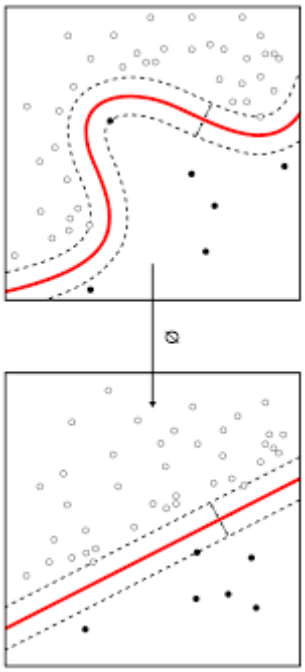


Рис. 1. Принцип роботи алгоритму алгоритму k-means

Іншим підходом, також достатньо популярним в практиці дослідження, є математичне моделювання, яке дозволяє оцінювати результати кластерного аналізу надзвичайних ситуаційв смарт-сіті, враховуючи його якісні та кількісні характеристики, що є доцільним для проведення оцінювання результатів функціонування програмних засобів, що базуються на відповідних алгоритмах.

Отже, оцінювання результатів кластерізації за допомогою засобів, що базуються на класичному та модифікованому алгоритмах k-means для аналізу надзвичайних ситуацій в смарт-сіті, доцільно проводити за допомогою математичного моделювання.

Список літератури

1. А. А. Барсегян, М. С. Куприянов, В. В. Степаненко, и І. І. Холод, *Методы и модели анализа данных: OLAP и Data Mining*, Издатель: БХВ-Петербург, 2004.

2. С. А. Айвазян, В. М. Бухштабер, и И. С. Енюков, *Прикладная статистика: Классификация и снижение размерности*, Финансы и статистика, 1989.

УДК 004.056, 004.75

Н.О. Пунченко[1], О.В. Цира[2]

iioonn24@rambler.ru, aleksandra.tsyra@gmail.com

[1]*Одеська державна академія технічного регулювання та якості, м. Одеса*
[2]*Одеська національна академія зв'язку ім. О.С. Попова, м. Одеса*

СТРАТЕГІЯ РІШЕНЬ НАДАННЯ ПРОФЕСІЙНОЇ МЕДИЧНОЇ ДОПОМОГИ В РАЙОНАХ ТЕХНОГЕННИХ КАТАСТРОФ НА БАЗІ ВИСОКИХ ТЕХНОЛОГІЙ

Госпітальні суда оснащені хірургічним відділенням з операційними залами, реанімаційним, терапевтичним і прийомним відділеннями, відділенням інтенсивної терапії, рентгенівським кабінетом, діагностичним центром, обладнанням ультразвукового дослідження, аптекою, поліклінікою та медичним складом. Крім госпітальних судів для зон стихійних лих, у багатьох країнах вдаються до допомоги плавучих поліклінік для жителів віддалених населених пунктів.

Парк високих технологій є найбільш перспективною стратегією розвитку економічного потенціалу будь-якої країни та потребує можливостей розвитку таких нових наукоємних напрямків, які тісно взаємодіють з IT-сферою [1]. Ефективність роботи систем безпосередньо залежить від інтеграції різноманітних медичних ресурсів в глобальні системи.

Для полегшення впровадження в медицину сучасних інформаційних технологій: використовуючи програмне забезпечення. На сучасному етапі серед розробників медичних стандартів, виділяють двох лідерів: стандарти, які претендують на роль широкого міжнародного використання – HL7 CEN/TC 251

Сучасне високотехнологічне обладнання в операційних блоках на госпітальних судах вимагає спеціального підходу для його конфігурації і структуризації робочого процесу персоналу.

Підвищення ефективності медичних інформаційних систем в сучасних умовах неможливе без використовування в задачах перетворення неперервних сигналів аналого–цифрового перетворювача (АЦП).

Незважаючи на ряд вже вирішених питань, при застосуванні швидкодійних АЦП високочастотних сигналів з покращеними параметрами існує ще багато проблем, які стримують широке використання АЦП в комп'ютерних системах, які входять до складу медичних інформаційних систем. А саме: обмежений динамічний діапазон у смузі високих частот вхідних сигналів (від 10 МГц і вище), недостатньо розроблені принципи побудови швидкодійних АЦП, що спричиняє обмеження ефективної розрядності перетворювачів [2]. Динамічні властивості цих засобів визначаються повними динамічними характеристиками: передатною функцією, амплітудно-частотною характеристикою, фазочастотною характеристикою, імпульсною або перехідною характеристикою. Повні динамічні характеристики аналогових засобів однозначно зв'язують між собою співвідношення:

- перехідна функція

$$h(t) = \int_0^t g(\tau) d\tau; \qquad (1)$$

- імпульсна перехідна характеристика

$$g(t) = \frac{dh(t)}{dt}; \qquad (2)$$

- комплексний коефіцієнт передачі

$$K(j\omega) = \int_0^\infty g(t) \cdot e^{-j\omega t} dt. \qquad (3)$$

В результаті перехідних процесів в колах АЦП у кожному циклі перетворення виникає похибка сигналу.

На динамічні властивості та роздільну здатність АЦП впливає також внутрішній шум, підключений до його входу.

Середнє квадратичне значення шуму для заданої смуги частот дозволяє оцінити повний розмах гауссового шуму і його вплив на похибку перетворення.

При проведені аналізу динамічних характеристик і параметрів АЦП показано, що для ефективного аналізу якості АЦП широкосмугових сигналів потрібно визначати повні характеристики, які є основою для оцінювання частинних характеристик і динамічних параметрів АЦП, який використовується в інформаційної медичної системі.

Список літератури

1. N. Punchenko, O. Tsyra, and G. Kovalova, "The strategy of informative redundancy of necessary measurements in the ship navigation as the independent direction in the development of a high tech park", *IEEE 5th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC)*, pp. 110 – 113, 2018.

2. Г. Г. Бортник, Н. О. Пунченко, та О. Г. Бортник, "Швидкодійний аналого-цифровоий перетворювач з розширеним динаміческим діапазоном", *Вимірювальна та обчислювальна техніка в технологічних процесах*. № 3, с. 99–104, 2015.

УДК 338.24

О.В. Перепелюкова., Н.О. Пархоменко, А.О. Пастушенко

Lena.perepelukova@gmail.com, parkhomenko.na28@gmail.com., andrii.pastushenko@hneu.net.

Харківський національний економічний університет імені Семена Кузнеця, м. Харків

МІЖНАРОДНА ЕКОНОМІЧНА БЕЗПЕКА ДЕРЖАВИ В СУЧАСНИХ УМОВАХ

Для сучасного стану економіки України як самостійної незалежної держави, утвердження її як суб'єкта світового співтовариства особливо актуальними є проблеми забезпечення стійкого соціально-економічного розвитку, формування механізму протидії внутрішнім та зовнішнім загрозам, підвищення рівня життя населення, розвитку системи міжнародної економічної взаємозалежності. Сукупність цих проблем та алгоритм їх вирішення тісно пов'язані з категорією "безпека", що в перекладі з грецької мови означає "володіти ситуацією" [1, с. 7]. Зміна внутрішніх та зовнішніх чинників розвитку національної економіки актуалізує дослідження питання забезпечення економічної безпеки держави. Сьогодні питання національної безпеки набуло особливої актуальності, оскільки від його вирішення залежатимуть доля України, соціально-економічний добробут громадян, становлення їхньої національної самосвідомості та поваги до своєї держави, тому необхідно врахувати помилки, допущені під час здійснення економічних реформ, які призвели до руйнівних процесів в економіці та у свідомості людей.

Економічна безпека передбачає спроможність національної економіки забезпечити свій незалежний розвиток, стабільність інститутів громадянського суспільства, достатній оборонний потенціал держави за різних несприятливих умов і подій, а також здатність країни захистити власні інтереси від зовнішніх і внутрішніх загроз.

Висока фінансова залежність держави, проблеми внутрішнього характеру й будь-які інші дестабілізуючі фактори стають причинами зниження економічної та, відповідно, національної безпеки. Тому необхідною умовою для нормального стійкого розвитку країни стає забезпечення захисту життєво важливих інтересів громадян, суспільства та держави. Постійна зміна внутрішніх та зовнішніх чинників розвитку національної економіки актуалізує дослідження питання забезпечення економічної безпеки країни. Визначення стану її складових елементів у сьогоднішніх умовах має важливе значення, оскільки дозволяє своєчасно вжити заходів з організаційно-правового забезпечення економічної безпеки країни. Саме тому забезпечення національної безпеки України набуває все більшого значення. Особливо важливим є забезпечення економічної безпеки, яка гарантує державний суверенітет України, є умовою сталого розвитку і зростання добробуту громадян.

Різновекторні геополітичні впливи на Україну в умовах неефективності гарантій її безпеки, "заморожених" конфліктів біля її кордонів, а також критична зовнішня залежність національної економіки обумовлюють уразливість України, послаблюють її роль на міжнародній арені та виштовхують на периферію світової політики, у "сіру зону" безпеки. Результатом ситуації, що сформувалася під тиском як економічних, так і неекономічних чинників, стало критичне зростання рівня загроз економічній безпеці України насамперед за рахунок виникнення низки додаткових, принципово нових для нашої держави викликів [1]. Сучасними загрозами економічній безпеці є такі: критичне гальмування економічного розвитку України та погіршення основних макроекономічних показників (макроекономічне розбалансування за головними показниками); згортання промислового виробництва; зниження економічної активності, насамперед інвестиційної; погіршення добробуту населення (домогосподарств) та зростання рівня безробіття; посилення боргового тиску, насамперед у державному секторі; підвищення тінізації економічної діяльності [2].

Одним із найважливіших завдань, які стоять перед нашою державою, є створення надійної системи забезпечення економічної безпеки як складової частини цілісної системи гарантування національної безпеки України. Держава як гарант захисту національних економічних інтересів повинна постійно досліджувати як реальні, так і перспективні загрози економічній безпеці та визначати механізми її захисту для забезпечення розвитку соціально орієнтованої національної економіки.

Список літератури

1. Ризики і загрози економічній безпеці України у 2015-2016 рр. та механізми їх мінімізації [Електронний ресурс]. Доступно: http://niss.gov.ua/content/articles/files/Risk-2ef8d.pdf. Дата звернення: Бер. 4, 2019.

2. В. В. Петрушевська, "Економічна безпека держави: зміст і класифікація загроз". *Збірник наукових праць "Ефективність державного управління",* Вип. 32, 2012, с. 441-448.

УДК 004.75:378

Л.М. Шемаєва

loraafanasieva@gmail.com

Харківський національний економічний університет ім. Семена Кузнеця, м. Харків

ДІГІТАЛІЗАЦІЯ ЯК ЧИННИК РОЗВИТКУ ВИЩОЇ ОСВІТИ

Окреслюючи майбутнє освіти, доцільним є визначення напрямів удосконалення, які вимагає інформаційне суспільство, роботодавці, викладачі, науковці, студентство. Спираючись на форсайт методику доцільно розробити карту змін університетів у контексті сучасних тенденцій, зокрема пов'язаних із дігіталізацією. Сьогодні, в умовах, де інформаційні технології стрімко розвиваються та змінюють усталений уклад усіх процесів життя, онлайн навчання стає дедалі актуальним і затребуваним.

З огляду на поширену думку в академічних колах провідних країн світу, "ера оффлайнових вишів" у найближчі 10–15 років може закінчитися. З цим твердженням складно погодитись, адже фундаментальні знання будуть надаватися студентам за класичною або формальною моделлю навчання. Тобто базові, обов'язкові, курси будуть забезпечуватися закладами вищої освіти (ЗВО). Додаткові або варіативні дисципліни можливо буде обрати на онлайн платформі. При цьому для зарахування курсу, сертифікат після проходження курсу на MOOC (Massive Open Online Course) платформі необхідно буде підтвердити складаючи фінальний іспит у ЗВО (в аудиторії). Також повний перехід до неформальної моделі (онлайнового навчання) неможливий у викладанні таких наук як хімія, фізика, медицина, де необхідним є наявність лабораторій для проведення експериментів, тестувань, набуття практичного досвіду.

Важливою і основною місією онлайн навчання у чистому вигляді є надання можливості навчатися тим, хто раніше не мав доступу до цього. В іншому випадку формальна модель є більш доцільною. Це легко довести спираючись на сутність природи процесів навчання та викладання. Навчання – це невпинний процес трансформації, набуття не тільки умінь та навичок, але й розширення меж мислення, сприйняття різних ситуацій через призму критичного мислення тощо. Отримати знання з дисципліни можна звертаючись до онлайн платформ, книг, електронних бібліотек, але тоді «опускається» така важлива опція як спілкування з ментором, наставником, який мотивує, направляє до ще більш визначних досягнень, формує світогляд нового формату, заточуючи на високий результат у навчанні, та на майбутнє. Тоді логічним є той факт, що процес викладання полягає не тільки у формальній підбірці цікавих матеріалів, кейсів, статистики, літератури, а й у менторстві, на важливість якого вказують останні дослідження.

Наступним чинником, що диктує зміни в освіті, є необхідність подолання розриву між вимогами ринку праці та знаннями, що дає університет. Сьогодні багато ЗВО залучають представників бізнесу до процесу оффлайн викладання, водночас це вирішує окреслену проблему лише частково. Беручи до уваги появу MOOC, а також поняття змішаного навчання (blended learning), що поєднує онлайн та оффлайн навчання, можна припустити, що започаткування практики зі створення курсу змішаного типу на партнерських засадах між роботодавцем та викладачем може стати ефективним інструментом наближення теорії і практики в рамках освітнього процесу.

Так, викладач відповідає за теоретичне наповнення курсу, узгоджуючи його із роботодавцем. При цьому викладач частково розвантажується через можливість подавати відео-лекції на платформі і проводити онлайн тести із контролю поточних знань. Звичайно, більша частина його навантаження розкривається у оффлайні в порівнянні із представником бізнесу, який відповідає виключно за онлайн частину курсу. Це надання ряду кейсів, розроблення завдань на основі реальних ситуацій, з якими стикається компанія на практиці. По закінченню курсу партнери можуть провести фінальні тренінги в оффлайні, де розставлять правильні акценти курсу та виступатимуть в активній ролі менторів.

З метою забезпечення якості такого курсу у технічному плані, питання фінансування доцільно покладати на роботодавця – приватного партнера. Університет зі свого боку має зацікавити роботодавця, створивши, наприклад, программу з відбору талановитої молоді, де на виході студент отримуватиме якісні знання, вміння та навички, орієнтовані на вимоги ринку праці, а роботодавець – молодого професійного робітника адаптованого до принципів та стандартів конкретної компанії.

Таким чином, майбутній університет – це майданчик змішаної форми навчання, що створений на партнерських засадах між викладачами та представниками бізнесу, серед основних завдань якого можна виділити: формування проактивної особистості, трансформація її світогляду та надання певних знань, умінь, навичок, що відповідають сучасним запитам ринку праці. Це в свою чергу не можливо реалізувати без застосування інформаційних технологій в освіті, таких, як наприклад десктоп-віджети, чат-боти, інтерактивні дошки, комп'ютерне моделювання тощо.

УДК 004.738.5

S. Syerov[1], С. С. Федушко[2], Ю. О. Сєров[2]

svyatsyerov@gmail.com, solomiia.s.fedushko@lpnu.ua, yurii.o.sierov@lpnu.ua

[1]*University of Illinois at Chicago, USA, Chicago*
[2]*Національний університет «Львівська політехніка», м. Львів*

ІНФОРМАЦІЙНА ЗАБЕЗПЕЧЕНІСТЬ СИСТЕМИ ВЕРИФІКАЦІЇ ПЕРСОНАЛЬНИХ ДАНИХ

Ефективне функціонування спільноти залежить від ряду чинників, як об'єктивних, так і суб'єктивних. Проте, наявні на сьогодні методи та засоби [1], що використовуються у глобальних сервісах, в повній мірі не виконують усіх завдань, які б задовольнили потреби власників та модераторів в управління віртуальними проектами, зокрема веб-спільнотами. Розроблення методів та засобів перевірки достовірності персональних даних у обліковому записі користувача [2] є одним з найбільш значимих факторів, які впливають на покращення функціонування веб-спільноти. До цієї комплексної проблеми належить і завдання розроблення методів визначення інформаційної забезпеченості системи верифікації персональних даних, що сприятиме вирішенню таких задач: брак якісного та достовірного контенту, анонімності користувачів, сприйняття спільноти, як платформи для довільної реалізації своїх бізнес ідей, низька рентабельність проектів, великі капіталовкладень у веб-спільнот, необґрунтовані затрати часу на веб-спільноту, інформаційної небезпеки учасників, низька конкурентоспроможність спільноти та проблеми в управлінні спільнотою (високий рівень конфліктів, низький авторитет модераторів).

Інформаційна забезпеченість системи верифікації персональних даних є ключовим завданням для якісного функціонування системи.

Інформаційна забезпеченість (ІЗ) системи верифікації персональних даних – це зведений показник, який визначає повноту даних для коректної роботи системи верифікації персональних даних. ІЗ системи верифікації персональних даних залежить від таких параметрів: рівень заповнення облікового запису, рівень актуальності даних облікового запису та контенту, адміністративне повноваження, рівень активності веб-учасника та рівень дотримання правил спільноти. ІЗ системи верифікації персональних даних визначаємо як:

$$IPVer^{(User_j)} = k_1 * CA^{(User_j)} + k_2 * Actl^{(PD,C)} + k_3 * AP^{(User_j)} + k_4 * Actv^{(User_j)} + k_5 * RulVc^{(User_j)} \quad (1)$$

де $k_1, k_2, \ldots, k_5$ – вагові коефіцієнти кожного параметру ІЗ системи, які визначаються експертним шляхом з урахуванням комунікативної поведінки веб-учасника та сценарію розвитку веб-спільноти, при чому $\sum_i k_i = 1$, $k_i \geq 0$; $CA^{(User_j)}$ – рівень заповнення облікового запису; $Actl^{(PD,C)}$ – рівень актуальності даних облікового запису та контенту; $AP^{(User_j)}$ – адміністративне повноваження; $Actv^{(User_j)}$ – рівень активності веб-учасника; $RulVc^{(User_j)}$ – рівень дотримання правил веб-спільноти. Як наслідок, $IPVer^{(User_j)} \in [0,1]$.

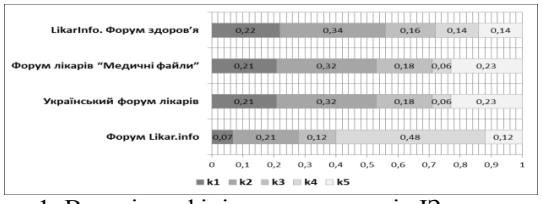


Рис. 1. Вагові коефіцієнти параметрів ІЗ медичних веб-спільнот

Визначення ІЗ системи верифікації даних віртуальних спільнот з медичної спеціалізації наведено на рис. 2.

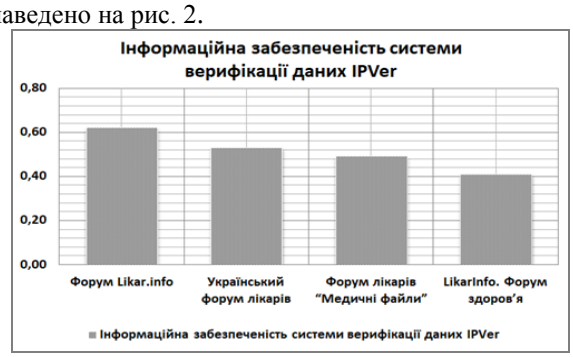


Рис. 2. Рівень ІЗ системи верифікації даних медичних веб-спільнот

Розроблені методи визначення інформаційної забезпеченості системи верифікації персональних даних веб-користувачів дозволяють збільшити ефективність функціонування веб-спільноти.

Список літератури

1. I. Korobiichuk, S. Fedushko, A. Juś, and Y. Syerov, "Methods of Determining Information Support of Web Community User Personal Data Verification System", *Automation 2017. ICA 2017. Advances in Intelligent Systems and Computing*, Volume 550, pp. 144–150, 2017.

2. Yu. Syerov, S. Fedushko, and Z. Loboda, "Determination of Development Scenarios of the Educational Web Forum", *XIth International Scientific and Technical Conference (CSIT 2016)*, pp. 73–76, 2016.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

СЕКЦІЯ 2 ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ 3 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

ТЕЗИ ДОПОВІДЕЙ
Міжнародної науково-практичної конференції
“Інформаційна безпека та інформаційні технології”

“Information Security and Information Technologies”

24–25 квітня 2019 р.

Відповідальний за випуск: *С.П. Євсеєв*

Комп`ютерна верстка: *А.А. Гаврилова*

Підписано до друку 30.03.2017. Формат 60×84/8. Папір офсетний.
Гарнітура «TimesNewRoman». Друк ризографічний. Ум.-друк. арк. – 8,6. Ціна договірна.
Наклад 250 прим.Зам. 0330/9-18

Видавництво «Цифрова друкарня №1»
Свідоцтво суб’єкта видавничої справи: серія ДК № 4354 від 06.07.2012 р.
61001, м. Харків, пл. Повстання, 7/8
e-mail: zebra-zakaz@mail.ru

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. **(057)778-60-34**e-mail: **bookfabric@rambler.ru**