МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18–19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професо**р.**

Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.

Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.

Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень – завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.

Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024. – 238 с.

М34

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com

Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

СЕКЦІЯ 1. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

УДК 621.32

П. Когут, Д. Гавліч, М. Яворська, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ЗМІНИ ТЕМПЕРАТУРИ РОБОЧОГО СЕРЕДОВИЩА НА ІМІТАЦІЙНІЙ МОДЕЛІ

UDC 621.32

P. Kogut, D. Havlich, M. Yavorska, Ph.D., Assoc. Prof.

WORKING ENVIRONMENT TEMPERATURE CHANGE STUDY ON A SIMULATION MODEL

Якщо перебіг певного виробничого процесу може супроводжуватися відхиленнями деяких показників від номінальних значень, при прогнозуванні їх впливу не завжди доцільно використовувати складні математичні моделі. Простіше скористатися імітаційною моделлю, реалізованою в іншому фізичному середовищі. Найдоступнішим способом імітації фізичних явищ різної природи є процеси, що відбуваються в електричному колі. При побудові відповідної імітаційної моделі слід при дотримуватися певних аналогій (Табл. 1).

Таблиця 1

Теплова підсистема	Тепловий потік	Температура	Тепловий опір	Теплоємність	----------
Електрична підсистема	Струм	Напруга	Резистивний опір	Ємність	Індуктивність

Формальні правила переходу для імітування процесу, що відбувається в тепловій підсистемі до симулювання його в електричному колі наступні:

- кожному тілу, що приймає участь в теплообміні ставимо у відповідність ємність з номіналом C=cm, де c – питома теплоємність матеріалу, m – маса тіла;
- процеси теплообміну між контактними тілами імітуємо резисторами з номіналами рівними кондуктивним тепловим опорам, під'єднаним між відповідними ємнісними елементами,

$$R_{конд} = /(\mu S);$$

процеси теплообміну між тілами і середовищем імітуємо резисторами з номіналами рівними конвективним тепловим опорам, під'єднаними між базовим вузлом схеми і вузлом, відповідним даному елементу

$$R_{конв} = 1/Sa_{конв}.$$

Окремо вирішується питання моделювання джерела струму, що імітує зміну температури (нагрівання чи охолодження) тіла в процесі його функціонування.Приходимо до повної аналогії між тепловою підсистемою та електричним колом, зазначеної в табл. 1.

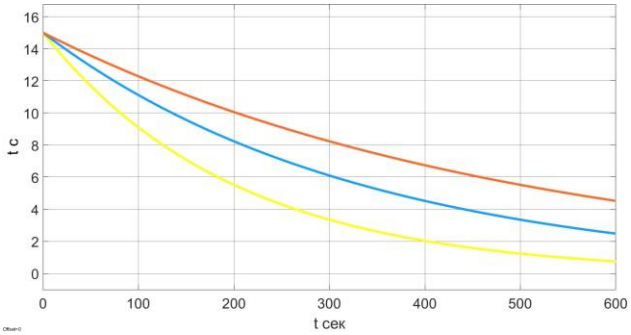


Рисунок 1. Криві охолодження робочого середовища холодоагентом холодоагентом

УДК 531:383
В. Кривень, докт. фіз.-мат. наук, проф.; Н. Балащак, канд. фіз.-мат. наук, доц.;
В. Валяшек, канд. фіз.-мат. наук, доц.; Л. Цимбалюк, канд. фіз.-мат. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОПТИМАЛЬНЕ КЕРУВАННЯ ЛІТАЛЬНИМ АПАРАТОМ ЗА НАЯВНОСТІ ОБМЕЖЕННЯ НА ТЯГУ

UDC 531:383
V. Kryven', Dr., Prof.; N. Blashchak, Ph.D., Assoc. Prof.;
V. Valiashek, Ph.D., Assoc. Prof.; L. Tsymbaljuk, Ph.D., Assoc. Prof.

OPTIMAL CONTROL OF THE AIRCRAFT IN THE PRESENCE OF THRUST LIMITATIONS

Розглянемо задачу про максимальну дальність польоту об'єкта з реактивним двигуном, за наявності обмеження на тягу двигуна.

Вважатимемо постійним прискорення сили тяжіння і нехтуватимемо аеродинамічними ефектами і обмежимося рухом в одній площині.

Динаміка об'єкта описується системою п'яти диференціальних рівнянь першого порядку:

$$\begin{cases} x'_1(t) = x_3 \\ x'_2(t) = x_4 \\ x'_3(t) = \dfrac{c}{x_5} u_1\, u_3, \\ x'_4(t) = \dfrac{c}{x_5} u_2\, u_3 - g, \\ x'_5(t) = -u_3. \end{cases}$$

у якій $x_1 = x_1(t)$, $x_2 = x_2(t)$ – координати об'єкта; $x_3 = x'_1(t)$, $x_4 = x'_2(t)$ – компоненти швидкості; $x_5 = x_5(t)$ – маса об'єкта; u_1, u_2 – напрямні косинуси вектора тяги; $u_3 = -x'_5(t)$ – швидкість втрати маси об'єкта; c – ефективна швидкість витікання палива; g – прискорення земного тяжіння.

З урахуванням обмеженості сили тяги $0 \le cu_3 \le cu_3^{max}$ множина керувань U визначається співвідношеннями:

$$\begin{cases} u_1^2+u_2^2 = 1, \\ 0 \le u_3 \le u_3^{max}. \end{cases}$$

За необхідності переведення об'єкта із заданих початкових координат, початкової маси і компонент швидкості у певне положення так, аби горизонтальне переміщення об'єкта було максимальним, задача зводиться до екстремуму функціонала

$$\int_{t_0}^{t_1} x_3(t)dt.$$

Його максимум забезпечується за умови

$$u_1(t) = \frac{-\mu_0}{\sqrt{\mu_0^2+\mu_2^2(t_1)}} = const,\ u_2(t) = \frac{\mu_2(t)}{\sqrt{\mu_0^2+\mu_2^2(t_1)}} = const$$

і досягається, коли вектор тяги кусково постійний за величиною і напрямком до моменту часу t_1 та нульовий коли $t > t_1$.

УДК 519.2:612.179
Т. В. Мельніченко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ ВЕЙВЛЕТ ПЕРЕТВОРЕННЯ ДОБЕШІ ДЛЯ ВИДІЛЕННЯ ЕЛЕКТРОКАРДІОСИГНАЛУ ПЛОДУ

UDC 519.2:612.179
T. V. Melnichenko

APPLICATION OF WAVELET TRANSFORM DOBESHI FOR SEPARATION OF FETAL ELECTROCARDIOLOGICAL SIGNAL

Моніторинг частоти серцевих скорочень плода (ЧСС) є однією з найважливіших процедур профілактики перинатальної захворюваності та смертності в галузі акушерства. Однак ефективність електронного моніторингу плода під час пологів постійно перебуває під сумнівами [1].

В порівнянні з електрокардіосигналом плоду, електрокардіосигнал матері має набагато більшу амплітуду за величиною [2]. В свою чергу це ускладнює вилучення фетальної електрокардіограми і збереження його морфології.

В даній магістерській роботі для виявлення електрокардіограми плоду було запропоновано Вейвлет перетворення з метою обробки електрокардіограми плода.

Для отримання електрокардіограми матері і електрокардіограми плоду було застосовано дискретне вейвлетне перетворення (DWT) з 10-рівневою декомпозицією. У цьому алгоритмі я використовувала вейвлет Добеші.

На рис. 1 показано витягнутий сигнал фетальної електрокардіограми плоду.

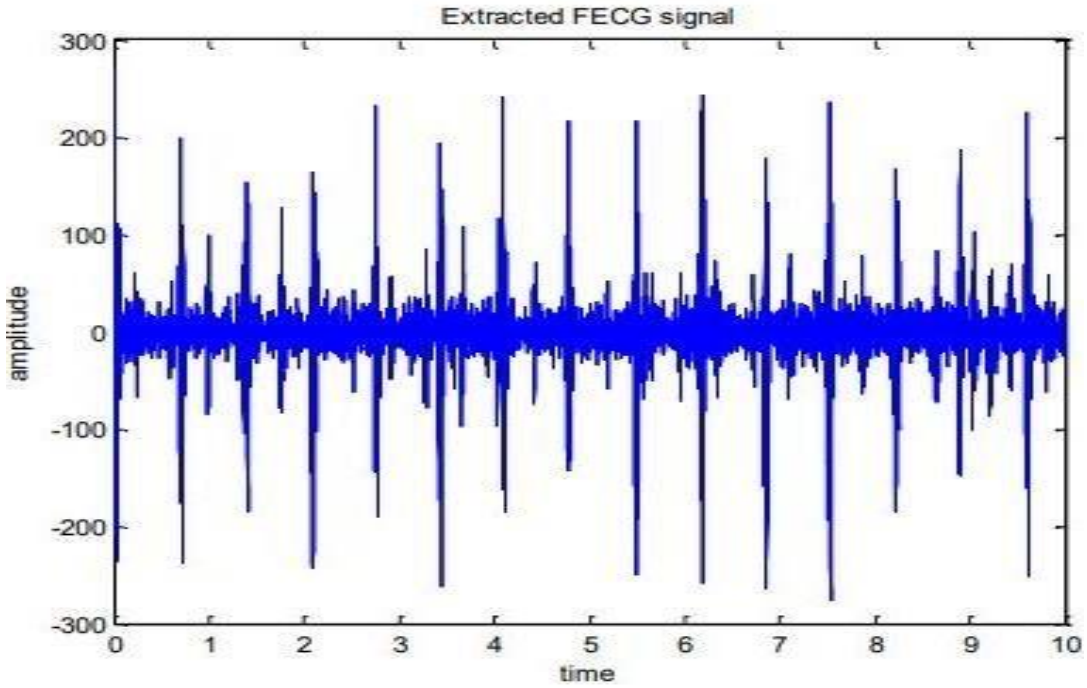


Рисунок 1. Витягнутий сигнал фетальної електрокардіограми

Рисунок 2. Блок-схема аналізу фетальної електрокардіограми

Література

1. Kwon JY, Park IY. Fetal heart rate monitoring: from Doppler to computerized analysis. ObstetGynecol Sci. 2016 Mar;59(2):79-84. doi: 10.5468/ogs.2016.59.2.79. Epub 2016 Mar 16. PMID: 27004196; PMCID: PMC4796090.
2. Франчевська Г. І. Застосування адаптивної фільтрації для виділення електрокардіосигналу плоду на фоні завад / Г. І. Франчевська, М. О. Хвостівський, В. Г. Дозорський // XI Міжнародна науково-практична конференція молодих учених та студентів „Актуальні задачі сучасних технологій“, 7-8 грудня 2022 року. – Т. : ТНТУ, 2022. – С. 172–173. – (Комп’ютерно-інформаційні технології та системи зв’язку).
3. Fetal ECG Extraction using Wavelet Transform Neha Para1, Dr. S. Wadhawani2 1M.E., Dept. of Electrical Engineering, MITS Gwalior, M.P., India 2Professor, Dept. of Electrical Engineering, MITS Gwalior, M.P., India Volume: 05 Issue: 07 | July 2018

УДК 621.32
П. Пархомець; М. Яворська, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ЗАЛЕЖНОСТІ ПРОЦЕСУ ВІДБРАКОВУВАННЯ ВИРОБІВ ЗА ВІДХИЛЕННЯМ ВІД ПАРАЛЕЛЬНОСТІ РОБОЧОЇ ПОВЕРХНІ ВІД ТОЧНОСТІ ПАРАМЕТРА ЕТАЛОНУ І МЕЖ ДОПУСКУ

UDC 621.32
P. Parkhomets, M. Yavorska, Ph.D., Assoc. Prof.

RESEARCH ON THE DEPENDENCE OF THE PRODUCT REJECTION PROCESS FOR DEVIATION FROM PARALLELISM OF THE WORKING SURFACE ON THE ACCURACY OF THE STANDARD PARAMETER AND THE TOLERANCE LIMIT

При виробництві деталей критерієм придатності виробу є умова:

$$| X - x_0 | < d$$

де x_0 – еталонне значення; d – допуск на відхилення контрольованого параметра від еталонного значення.

Нехай в процесі контролю певного параметра його біжучі значення X, орієнтовані на величину M, розподілені за нормальним законом з математичним сподіванням $M[X] = m$ і стандартним відхиленням $\sigma[X] = \sigma$:

$$P(X) = \frac{1}{2\sigma\sqrt{2\pi}} e^{-\frac{(X-M)^2}{2\sigma^2}}$$

Предметом дослідження є ймовірнісна оцінка знаходження вимірюваної величини X у дозволеному діапазоні значень при заданому допуску d: $P = p(x_0, d, m, \sigma)$. Ймовірність попадання значень випадкової величини з нормальним розподілом з параметрами m і σ в інтервал $[-d, d]$ можна оцінити за формулою Лапласа:

$$P\{x_0 - d < X < x_0 + d\} = \Phi\left(\frac{x_0 + d - m}{\sigma}\right) - \Phi\left(\frac{x_0 - d - m}{\sigma}\right)$$

де

$$\Phi(x) = \frac{1}{2\pi}\int_0^x e^{(-t^2/2)}\, dt$$

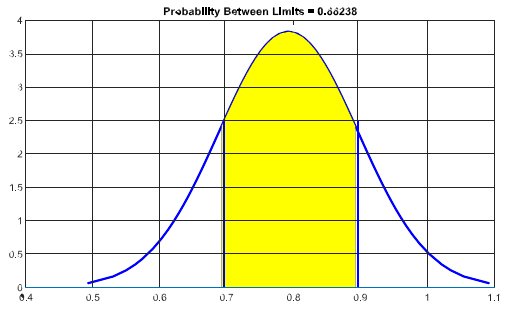


Рисунок 1. Обчислення імовірності попадання виміряної величини у межі допуску

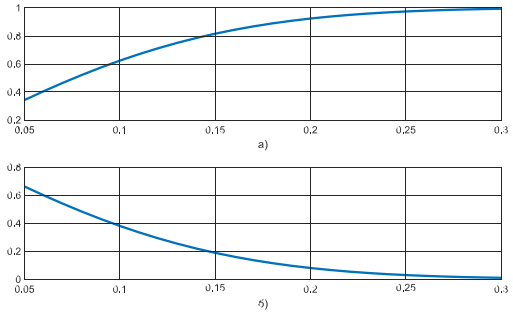


Рисунок 2. Залежність імовірності попадання виміря-
ної величини в межі допуску (а) контрольованого параметраі виходу за межі допуску (б)

Розроблене програмне забезпечення для імовірнісних оцінок фактів, що значення вимірюваного параметра, розподілені за нормальним законом із заданими характеристиками знаходитимуться в межах заданогодопуску (рис. 2 а), або випадатимуть за його межі (рис. 2 б).

УДК 519.6
В. В. Сумко; Я. В. Литвиненко, д.т.н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОГЛЯД МОДЕЛЕЙ ЦИКЛІЧНИХ СИГНАЛІВ ЯКІ ВРАХОВУЮТЬ РИТМ (РИТМІЧНУ СТРУКТУРУ)

UDC 519.6
V. V. Sumko; I. V. Lytvynenko, Dr., Prof.

REVIEW OF CYCLIC SIGNAL MODELS THAT ACCOUNT FOR RHYTHM (RHYTHMIC STRUCTURE)

Ритмічна структура циклічних сигналів визначає внутрішню організацію та закономірності повторюваних змін параметрів сигналу у часі (дискретна характеристика). Вона є ключовою характеристикою для їх аналізу, дозволяючи ідентифікувати природу процесу, оцінювати якість сигналу та прогнозувати його динаміку. Поруч з ритмічною структурою використовують поняття ритму циклічних сигналів.

Ритм циклічних сигналів - це характеристика, що визначає повторювану природу сигналів у часі (неперервна характеристика). Такий ритм може бути властивий як природним процесам (серцевий ритм, добові ритми), так і штучним системам (годинники, генератори сигналів). Оскільки це важлива характеристика циклічних сигналів тому розглянемо математичні моделі які їх описують.

Дана теза стосується огляду математичних моделей циклічних сигналів які дозволяють врахувати ритм (ритмічну структуру).

Математичні моделі, які враховують ритм циклічних сигналів, широко застосовуються в різних галузях науки і техніки. Вони дозволяють аналізувати, прогнозувати та описувати динаміку періодичних та циклічних процесів. Розглянемо основні підходи та моделі:

– Гармонічний аналіз (синусоїдальні моделі). Періодичний сигнал може бути описаний як сума синусоїдальних компонентів за допомогою ряду Фур'є, проте така модель дозволяє врахувати лише постійний ритм;

– Диференційні рівняння. Лінійні осцилятори та згасаючі коливання. Моделі які також не дозволяють врахувати змінний ритм.

– Автоколивальні системи. Сюди входить, наприклад, модель рівняння Ван дер Поля (Модель нелінійного осцилятора з саморегуляцією). Ця модель використовується для моделювання серцевих ритмів, нейронної активності та інших біологічних ритмів.

– Стохастичні моделі. В цю категорію входить багато математичних моделей які дозволяють врахувати випадковість форми та в деяких випадках змінність ритму (циклічний випадковий процес з подвійною стохастичністю).

– Моделі фазового портрету (динамічні системи). Такі моделі описують траєкторії коливань у фазовому просторі, наприклад, для маятника чи біологічних ритмів.

Мережеві моделі та теорія графів. Для аналізу складних взаємодій ритмічних сигналів у мережах (наприклад, в нейронних мережах). Наприклад, модель рівняння Куромото використовується для моделювання синхронізації.

– Фрактальні моделі. Для сигналів із ритмами, що демонструють масштабовану структуру (наприклад, для фінансових ринків чи біоритмів):

Математичні моделі для опису ритму є надзвичайно різноманітними і можуть бути адаптовані до конкретного сигналу з певним рядом припущень. Проте використання математичної моделі для моделювання різних циклічних сигналів з врахуванням, як постійного так і змінного ритму лишається відкритим для подальших наукових досліджень.

УДК 621.32

М. Франків; П. Когут
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ЗМІНИ ТЕМПЕРАТУРИ РОБОЧОГО СЕРЕДОВИЩА НА ІМІТАЦІЙНІЙ МОДЕЛІ

UDC 621.32

M. Frankiv; P. Kogut

WORKING ENVIRONMENT TEMPERATURE CHANGE STUDY ON A SIMULATION MODEL

Якщо перебіг певного виробничого процесу може супроводжуватися відхиленнями деяких показників від номінальних значень, при прогнозуванні їх впливу не завжди доцільно використовувати складні математичні моделі, як, наприклад, задачу нестаціонарної теплопровідності для симулювання охолодження робочого середовища. Простіше скористатися імітаційною моделлю, реалізованою в іншому фізичному середовищі. Умовою відповідності є аналогії між параметрами процесу та системи і подібність форми математичних співвідношень між ними. Зокрема, найдоступнішим способом імітації фізичних явищ різної природи є процеси, що відбуваються в електричному колі. При побудові відповідної імітаційної моделі слід дотримуватися певних аналогій (Табл. 1).

Таблиця 1

Теплова підсистема	тепловий потік	температура	Тепловий опір	теплоємність	----------
Електрична підсистема	струм	напруга	резистивний опір	ємність	індуктивність

Формальні правила переходу для імітування процесу, що відбувається в тепловій підсистемі до симулювання його в електричному колі наступні:

– нулю температурної шкали (за Цельсієм, Кельвіном чи просто умовна різниця температур) відповідає базовий вузол кола (земля);

– кожному тілу, що приймає участь в теплообміні ставимо у відповідність ємність з номіналом C=cm, де c – питома теплоємність матеріалу, m – маса тіла;

– процеси теплообміну між контактними тілами імітуємо резисторами з номіналами рівними кондуктивним тепловим опорам, під'єднаним між відповідними ємнісними елементами, $R_{конд}$= /(μS);

– процеси теплообміну між тілами і середовищем імітуємо резисторами з номіналами рівними конвективним тепловим опорам, під'єднаними між базовим вузлом схеми і вузлом, відповідним даному елементу, $R_{конв} = 1/Sa_{конв}$.

Окремо вирішується питання моделювання джерела струму, яке імітує зміну температури (нагрівання чи охолодження) тіла в процесі його функціонування і під'єднується між базовим вузлом схеми вузлом, відповідним даному елементу.

Таким чином приходимо до повної аналогії між тепловою підсистемою та електричним колом на рівні математичних моделей, як зазначено в табл. 1.

В результаті побудови імітаційної моделі у вигляді формальної електричної схеми із відповідними параметрами зміни температури охолоджуваного матеріалу чи продукту можемо спостерігати за моделюванням зміни напруги у відповідних вузлах імітаційної моделі що в результаті дає змогу ефективніше досліджувати температурні впливи для різних технічних задач засобами моделювання.

УДК 004.94+519.218
М. Фриз, канд. техн. наук, доц.; Б. Млинко, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЛІНІЙНИХ ТА УМОВНИХ ЛІНІЙНИХ ПРОЦЕСІВ

UDC 004.94+519.218
M. Fryz, Ph.D., Assoc. Prof.; B. Mlynko, Ph.D., Assoc. Prof.

COMPARATIVE ANALYSIS OF LINEAR AND CONDITIONAL LINEAR PROCESS

Лінійний випадковий процес (ЛВП) означено як стохастичний інтеграл виду [1]: $\xi(\omega,t)=\int_{-\infty}^{\infty}\varphi(\tau,t)d\eta(\omega,\tau),\ \omega\in\Omega,\ t\in\mathbb{R}$, де $\varphi(\tau,t),\ \tau,t\in\mathbb{R}$ – *невипадкова* функція (ядро), $\eta(\omega,\tau),\ \tau\in\mathbb{R}$ – стохастично неперервний процес із незалежними приростами.

Умовний лінійний випадковий процес (УЛВП) означено так [2]: $\xi(\omega,t)=\int_{-\infty}^{\infty}\varphi(\omega,\tau,t)d\eta(\omega,\tau),\ \omega\in\Omega,\ t\in\mathbb{R}$, де $\varphi(\omega,\tau,t),\ \tau,t\in\mathbb{R}$ – *випадкова* функція (ядро), причому випадкові функції $\varphi(\omega,\tau,t)$ і $\eta(\omega,\tau)$ є *стохастично незалежними*.

ЛВП з дискретним часом [1]: $\xi_t(\omega)=\sum_{\tau=-\infty}^{\infty}\varphi_{\tau,t}\zeta_\tau(\omega),\ \omega\in\Omega,\ t\in\mathbb{Z}$, де $\varphi_{\tau,t},\ \tau,t\in\mathbb{Z}$ – дійсна *невипадкова* функція (ядро), $\zeta_\tau(\omega),\ \tau\in\mathbb{Z}$ – породжуючий безмежно подільний білий шум у вузькому сенсі. Частинним випадком лінійного випадкового процесу з дискретним часом є модель авторегресії ковзної суми.

УЛВП з дискретним часом [3], [4]: $\xi_t(\omega)=\sum_{\tau=-\infty}^{\infty}\varphi_{\tau,t}(\omega)\zeta_\tau(\omega),\ \omega\in\Omega,\ t\in\mathbb{Z}$, де $\varphi_{\tau,t}(\omega),\ \tau,t\in\mathbb{Z}$ – дійсна *випадкова* функція (ядро), причому випадкові функції $\varphi_{\tau,t}(\omega)$ і $\zeta_\tau(\omega)$ є *стохастично незалежними*. Частинним випадком УЛВП з дискретним часом є модель авторегресії ковзної суми з випадковими коефіцієнтами.

У доповіді розглянуто також вирази для характеристичних та моментних функцій УЛВП, на основі яких доведено умови за яких УЛВП є стаціонарним, циклостаціонарним, періодично корельованим випадковим процесом, охарактеризовано властивості ергодичності та перемішування УЛВП.

Література

1. V. Babak, A. Zaporozhets, Y. Kuts, M. Fryz, and L. Scherbak, Noise signals: Modelling and Analyses, Cham: Springer Nature Switzerland, 2024. doi: https://doi.org/10.1007/978-3-031-71093-3.
2. M. Fryz and B. Mlynko, “Property Analysis of Conditional Linear Random Process as a Mathematical Model of Cyclostationary Signal,” in 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), Ternopil, Ukraine: CEUR Workshop Proceedings, 2022, pp. 77–82.
3. Mykhailo Fryz and Leonid Scherbak, “Properties of discrete-time conditional linear cyclostationary random processes in the problems of energy informatics,” System Research in Energy, no. 1 (72), pp. 72–79. doi: 10.15407/srenergy2023.01.072.
4. M. Fryz and B. Mlynko, “Determination of the characteristic function of discrete-time conditional linear random process and its application,” Scientific Journal of TNTU, vol. 109, no. 1, pp. 16–23, 2023, doi: https://doi.org/10.33108/visnyk_tntu2023.01.016.

УДК 621.38
М. Шевчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СТАТИСТИЧНИЙ АНАЛІЗ ПОХИБОК АВТОМАТИЗОВАНОГО ПРИЛАДУ ДЛЯ ВИМІРЮВАННЯ ЛІНІЙНИХ РОЗМІРІВ

UDC 621.38
M. Shevchuk

ERRORS STATISTICAL ANALYSIS OF AUTOMATED DEVICE FOR LINEAR DIMENSIONS MEASURING

Ефективність виготовлення та експлуатації технічних засобів значною мірою залежать від адекватних метрологічних оцінок як знарядь, так і продуктів виробництва. Запропоновано програмне забезпечення для тестування метрологічних характеристик удосконаленого автоматизованого приладу вимірювання лінійних розмірів. Похибки вимірювань визначаються при оцінці лінійних розмірів еталонних зразків або порівнянні зроблених вимірів з отриманими за допомогою більш точних приспосіблень. Отримані результати піддаються статистичному аналізу з використанням розробленого програмного забезпечення. Після обчислення середнього значення і квадратичного відхилення із вимірюваного ряду (рис. 1 а) відсіюються результати з екстремальними відхиленнями від середнього що перевищує трьохкратне квадратичне відхилення (Рис. 1 б).

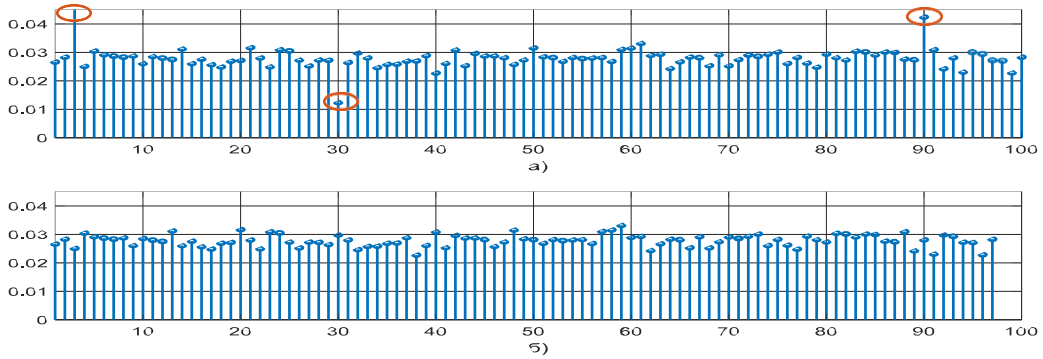


Рисунок 1. Вихідні дані: до відсіювання екстремальних значень (а) і після (б)

За гістограмами розподілу значень виміряних похибок (Рис. 2) відтворюємо параметри нормального розподілу: виправлене середнє значення і виправлену дисперсію.

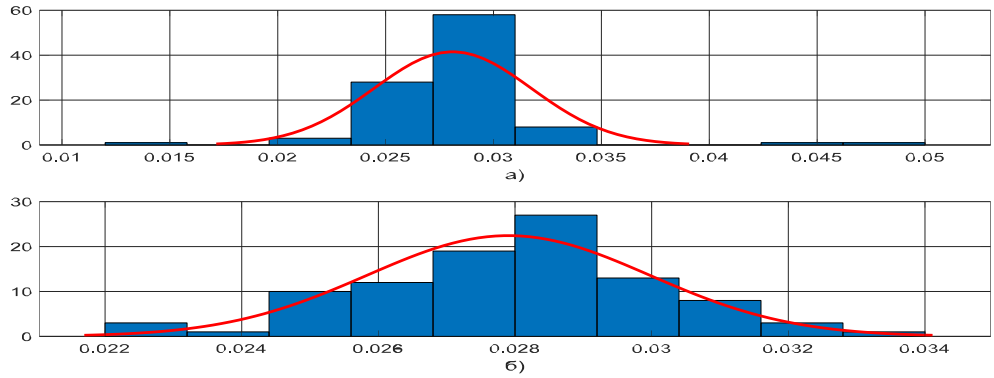


Рисунок 2. Гістограми: розподілу значень виміряних похибок до відсіювання екстремальних значень (а) і після (б)

УДК 621.38
М. Яворська, к.т.н., доц.; Ю. Наконечний; В. Соколовський; М. Соколовський
(Тернопільський національний технічний університет ім. Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ПЕРЕДАВАЛЬНОЇ ФУНКЦІЇ ВИМІРЮВАЛЬНОГО ЗАСОБУ

UDC 621.38
M. Yavorska, Ph.D., Assoc.Prof; Y. Nakonechnyi; V. Sokolovsky; M. Sokolovsky

STUDY OF THE TRANSFER FUNCTION OF A MEASURING INSTRUMENT

В роботі виконано дослідження чутливості індуктивного давача соленоїдного типу, який застосовується для вимірювання лінійних переміщень. Він являє собою циліндричну котушку намагнічування з рухомим феритовим осердям. Переміщення осердя визиває зміну індуктивності обмотки котушки. Якщо жорстко зв'язати переміщення осердя з вимірювальним параметром, то отримаємо пристрій для вимірювання лінійних переміщень. Передавальна функція такого пристрою приведена нижче.

$$L = L_O + A \cdot \left[\sqrt{(m+p_1)^2+1} + \sqrt{(m-p_1)^2+1} - \sqrt{(m+p_2)^2+1} - \sqrt{(m-p_2)^2+1} \right],$$

де

$$A = \frac{\pi \cdot r^2}{8} \cdot \mu_0 \cdot \left(\bar{\mu}_C - 1 \right) \cdot \frac{\omega^2 \cdot R}{p_C \cdot p_K}, \quad m = \frac{l}{R}; \quad p_1 = \frac{p_C + p_K}{R}; \quad p_2 = \frac{p_C - p_K}{R}$$

В цій формулі L_o – індуктивність котушки перетворювача при відсутності осердя, R – середній радіус витка, μ_0, μ_C – магнітна стала і магнітна проникність осердя відповідно, $p_к$, p_c – половина довжини котушки і осердя відповідно.

Для оцінки чутливості перетворювача лінійних переміщень запропоновано підхід на основі поліноміальної апроксимації фукції перетворення в середовищі MATLAB, (рис. 1).

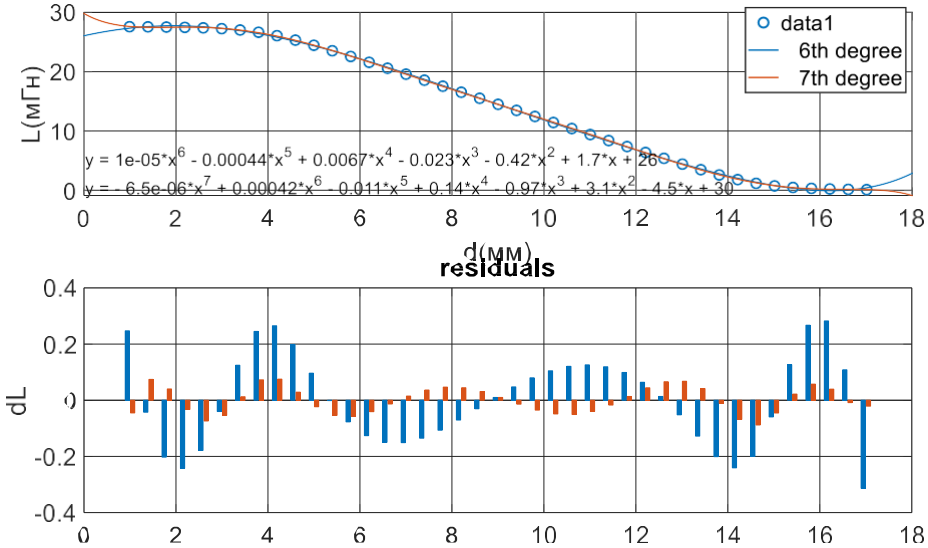


Рисунок 1. Передавальна функція для конкретних значень робочих параметрів, її апроксимація поліномами 6 і 7 порядків (верхній графік), і похибки апроксимації для вибраних значень (нижній графік)

З оцінки похибки апроксимації поліномами різних степеней вибраний олтимальний варіант – поліном 4-го степеня. У цьому випадку отримаємо без складних математичних перетворень наближену аналітичну форму чутливості засобу вимірювання у вибраному діапазоні переміщень із збереженням заданої точності вимірювань.

СЕКЦІЯ 2. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ, КІБЕРБЕЗПЕКА

УДК 355.45:316.658(477)
С. Базарний, Ph.D.; О. Терновий; О. Грищук
(НУОУ)

МЕТОД ВИКОРИСТАННЯ КОМП'ЮТЕРНОЇ ГРИ «STALKER», ЯК ІНСТРУМЕНТУ ІНФОРМАЦІЙНОЇ БОРОТЬБИ В УМОВАХ ШИРОКОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ

UDC 355.45:316.658(477)
Bazarny, Ph.D.; AT. Thorny; AT. Hryshchuk

THE METHOD OF USING THE COMPUTER GAME "STALKER" AS A TOOL OF INFORMATION WARFARE IN THE CONDITIONS OF LARGE-SCALE ARMED AGGRESSION OF THE RUSSIAN FEDERATION AGAINST UKRAINE

У дослідженні розглядаються можливості використання комп'ютерної гри STALKER, як інструменту інформаційної боротьби в умовах російсько-української війни. Особливу увагу приділено інтерактивному контенту та можливостям його інтеграції в психологічні операції для впливу на цільову аудиторію. Проаналізовано методологічні підходи до розробки контенту, оцінювання ефективності його впливу щодо використання комп'ютерних ігор під час проведення психологічних операцій. У роботі розглядається протистояння в інформаційному просторі українських спецслужб, зокрема Служби безпеки України та Головного управління розвідки МОУ, а також спецслужб російської федерації та іноземних держав. Зазначена роль НАТО у зміцненні інформаційної безпеки України та протидії російській інформаційній агресії. В умовах сучасної гібридної війни інформаційна боротьба стала одним із ключових інструментів досягнення стратегічних цілей. Суперечки за домінування в інформаційному просторі передбачають використання новітніх технологій, інтерактивних платформ для впливу на суспільну свідомість. Одним із таких інструментів є комп'ютерні ігри, які, завдяки своїй популярності, високому рівню залученості користувачів та емоційному впливу, мають великий потенціал у контексті психологічних операцій. Однак на сьогодні недостатньо досліджено, як інтерактивні платформи можуть бути адаптовані для ефективного використання в умовах широкомасштабної збройної агресії, зокрема для формування патріотичних настроїв, нейтралізації ворожої пропаганди та зміцнення національної безпеки. Це створює необхідність розробки науково обґрунтованих підходів до інтеграції комп'ютерних ігор, таких як STALKER, у стратегії інформаційної боротьби, а також вивчення їх впливу на різні цільові аудиторії.

Завдяки інтеграції наративів, які відображають героїзм українських військових, трагедії війни та важливість національних цінностей, гра може слугувати ефективним засобом формування патріотичних настроїв, підвищення мотивації та розвитку критичного мислення.

УДК 004.056
І. О. Баран, к.т.н., доц.; Ю. Р. Чорна
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТИПИ АНОМАЛІЙ

UDC 004.056
I. O. Baran, PhD; Yu. R. Chorna

TYPES OF ANOMALIES

У процесі інформатизації суспільства починають бурхливо розвиватися мережеві послуги і відбувається процес впровадження їх у майже всі верстви суспільства. Перед адміністраторами інформаційно-обчислювальних систем стоїть завдання забезпечити керованість цих систем, а також цілісність, доступність та конфіденційність даних. Зрештою забезпечити штатне функціонування системи за максимального виключення нестандартної поведінки системи (мережеві аномалії).

Стандартним видом аномалії трафіку є вихід інформативного параметра сигналу за його діапазон допустимих значень як за величиною, так і за швидкістю зміни часу [1].

У контексті мережевої безпеки аномалії можна поділити на точкові, контекстні та колективні [1]. Точкові аномалії характеризуються появою окремого об'єкта, який не узгоджується з рештою набору даних. Прикладом може бути ізольований екземпляр мережного трафіку, який відрізняється від нормальних екземплярів, на певному часовому відрізку. Контекстні аномалії характеризуються появою екземпляра даних, що є аномалією у цьому контексті. Контекст формується з урахуванням структур у наборах даних. Для його опису використовуються два основні набори змінних: контекстні та поведінкові. Перші використовуються визначення оточення кожному за екземпляра. Другі - визначають всі характеристики, що відносяться до конкретного примірника даних. Колективні аномалії характеризуються наявністю пов'язаних екземплярів даних, визнаних аномальними порівняно з іншими даними. Окремий екземпляр може і не бути відхиленням, однак спільна поява таких екземплярів є колективною аномалією. Прикладом може бути поява подій «переповнення буфера» і «копіювання файлів за протоколом ftp», які є звичайними подіями у певній системі, однак їхня спільна поява може слугувати про віддалену атаку на комп'ютерну систему.

Також має місце виявлення аномалій на основі продуктивності системи та зміни станів окремих додатків [1]. Аномалія у продуктивності. За ними можна судити про те, що поведінка програми, що спостерігається (наприклад, поточне використання ЦП) не може бути пояснено робочим навантаженням програми, що спостерігається (наприклад, тип і обсяг транзакцій, оброблюваних додатком, передбачає різний рівень використання ЦП). Зміна у продуктивності транзакцій програми. Як правило, мають на увазі істотну зміну (збільшення або зменшення) під час обробки транзакцій, наприклад, в результаті останнього оновлення програми.

Також важливо розрізняти аномалію продуктивності та зміну робочого навантаження. Аномалія продуктивності вказує на ненормальну ситуацію, яку необхідно досліджувати та вирішувати. Навпаки, зміна робочого навантаження (тобто зміни змішування транзакцій і навантаження) типова для веб-додатків. Тому вкрай бажано уникати помилкових тривог, викликаних алгоритмом через зміни робочого навантаження, хоча інформація про зміни робочого навантаження, що спостерігаються, може бути надана постачальнику послуг.

Література

1. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень: Автореф. дис..... докт. техн. наук: 05.13.21/НАУ. К., 2019. 42 с.

УДК 004.4
М. І. Богуцький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОПТИМІЗАЦІЯ АЛГОРИТМІВ ПОШУКУ ІНФОРМАЦІЇ НА ВЕБ-САЙТІ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

UDC 004.4
M. I. Boguzkiy

OPTIMIZATION OF INFORMATION SEARCH ALGORITHMS ON A WEBSITE USING MACHINE LEARNING METHODS

Обсяг інформації доступної в мережі Інтернет, зростає з неймовірною швидкістю, що створює нові виклики для ефективного пошуку даних та їх персоналізації. Розробка веб-сайту, який слугуватиме платформою для впровадження і тестування таких технологій, є важливим кроком у вивченні їх можливостей, особливостей та недоліків. Існує багато рішень для розробки такого проекту, одним з популярних та доволі оптимальних є Python та його фреймворки. Фреймворки Django та Flask дозволяють створити потужний та стабільний бекенд, здатний обробляти запити користувачів, виконувати пошукові операції та генерувати рекомендації в режимі реального часу [1].

Інтеграція пошукових алгоритмів на сайті забезпечується використанням індексованих баз даних, що значно скорочує час виконання запитів.[4] Наприклад, використання бібліотек як Whoosh або Elasticsearch дозволяє додатково оптимізувати процеси пошуку завдяки потужним інструментам для аналізу тексту, ранжування та врахування контексту запиту. Для підвищення якості пошуку впроваджуються алгоритми обробки природної мови (NLP), які допомагають розпізнавати значення запитів, аналізувати їх синтаксис та враховувати індивідуальні особливості користувачів [3].

Для зберігання даних про користувачів, товари, історію пошуку та взаємодії використовується база даних. Дані можуть бути попередньо структуровані та індексовані для забезпечення максимальної продуктивності пошукових алгоритмів [5]. Для інтеграції моделей машинного навчання та обробки даних використовуються бібліотеки, такі як TensorFlow або PyTorch, які дозволяють створювати гнучкі рішення для персоналізації пошуку та рекомендацій. Використовуючи технології обробки природної мови, запит обробляється для врахування контексту, після чого формується запит до бази даних [2].

Перевагою такого підходу є його гнучкість і масштабованість. Веб-сайт може адаптуватися до зростаючих вимог користувачів, підтримувати інтеграцію нових алгоритмів і обробляти великі обсяги даних. Інтеграція рекомендаційних систем дозволяє пропонувати користувачам товари чи контент, які максимально відповідають їхнім інтересам, підвищуючи задоволеність та залученість. Водночас існують певні недоліки, які потрібно враховувати під час розробки. Складність інтеграції алгоритмів, вимагає значних обчислювальних ресурсів, що може збільшити витрати на підтримку системи. Проблема конфіденційності даних, адже персоналізовані рекомендації потребують збору й обробки даних про користувачів. Крім того, система може зіткнутися з проблемою холодного старту, коли бракує даних для нових користувачів чи об’єктів, що впливає на якість пошуку та рекомендацій.

Література

1. Antonio Mele. Django 5 By Example - Fifth Edition: Build powerful and reliable Python web applications from scratch 5th ed. Edition / Antonio Mele, 2024 - с.820.
2. Структури даних та алгоритми [Електронний ресурс] : https://studfile.net/preview/10025806/page:21/. Доступ до ресурсу: 04.12.2024
3. К.М. Онищенко. Аналіз методів обробки природної мови / К.М. Онищенко, Я.І. Данієль, Р.О. Каманєв.
4. Charu C. Aggarwal. Recommender Systems: The Textbook / Charu C. Aggarwal, 2016 – с. 518 (Recommender Systems).
5. Cathy Tanimura. SQL for Data Analysis. Advanced Techniques for Transforming Data into Insights. 1st Ed. / Cathy Tanimura, 2021 – с. 350.

УДК 004.056
О. Борух; М. Карпінський, Ph.D
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РЕАЛІЗАЦІЯ АВТОМАТИЗОВАНОГО ІНСТРУМЕНТУ ДЛЯ ВИЯВЛЕННЯ ФІШИНГОВИХ ВЕБ-САЙТІВ

UDC 004.056
O. Borukh, student; M. Karpinskyi, Ph.D

IMPLEMENTATION OF AN AUTOMATED TOOL FOR DETECTING PHISHING WEBSITES

Фішингові веб-сайти становлять значну загрозу сучасному інформаційному суспільству, обманюючи користувачів і викрадаючи їхні конфіденційні дані. За даними Anti-Phishing Working Group, кількість фішингових атак щорічно зростає, охоплюючи фінансові установи, технологічні компанії та звичайних користувачів. У 2023 році частка фішингових інцидентів перевищила 36% усіх кіберзагроз, демонструючи потребу у впровадженні сучасних технологій для протидії таким атакам.

Сучасні методи боротьби з фішингом, такі як чорні списки, мають обмеження, пов’язані з їхньою реактивністю та неефективністю проти нових загроз. Це обумовлює потребу у впровадженні автоматизованих інструментів, які здатні виявляти нові патерни та мінімізувати затримки у реагуванні.

Машинне навчання відкриває нові можливості для активного та автоматизованого виявлення фішингових веб-сайтів. Алгоритми, такі як Random Forest, XGBoost і Support Vector Machines, дозволяють аналізувати структуру URL-адрес, вміст сторінок і поведінкові характеристики для ідентифікації потенційно небезпечних сайтів. У цій роботі розроблено інструмент на основі Python, який інтегрує методи машинного навчання для автоматизованого аналізу веб-ресурсів.

Для навчання моделі використано відкриті бази даних, зокрема PhishTank та OpenPhish, які містять актуальні фішингові сайти, а також легітимні ресурси з Alexa Top Sites. Попередня обробка даних включала виділення ключових ознак: довжина URL, наявність IP-адреси в домені, кількість спеціальних символів тощо. Модель була оцінена за допомогою метрик точності, повноти та F1-score.

Тестування продемонструвало високу точність інструменту, що перевершує ефективність традиційних методів, таких як чорні списки. Алгоритм Random Forest показав найкращі результати для задач класифікації URL-адрес. Додатково було протестовано XGBoost, який забезпечив найкращу швидкодію при роботі з великими обсягами даних.

Запропонований інструмент може бути використаний як окремий захисний механізм або інтегрований у загальні системи кібербезпеки, забезпечуючи своєчасне виявлення та блокування загроз. Для досягнення найвищої ефективності рекомендується регулярне оновлення навчальних даних та впровадження додаткових заходів, таких як багатофакторна автентифікація. Подальші дослідження можуть включати використання нейронних мереж для покращення точності, а також створення інтерактивного інтерфейсу для аналітиків із кібербезпеки.

Література

1. URL: https://phishtank.org/
2. URL: https://openphish.com/
3. Breiman L. Random Forests. Machine Learning, 2001.
4. Jason Brownlee. Machine Learning Mastery with Python, 2022.
5. Anti-Phishing Working Group (APWG) Report, 2023.

УДК 004.056.53
Н. Бурмістрова; Р. Козак, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ: ФРЕЙМВОРК SHENNINA

UDC 004.056.53
N. Burmistrova, student of gr. СБм-61; R. Kozak, Ph.D., Assoc. Prof.

USING MACHINE LEARNING FOR PENETRATION TESTING: SHENNINA FRAMEWORK

Автоматизація процесів пентесту із застосуванням машинного навчання відкриває нові можливості для досягнення цілей кібербезпеки. Фреймворк Shennina, що використовує машинне навчання для адаптивного виявлення та експлуатації вразливостей, є одним із новітніх рішень у цій сфері, що потребує дослідження його ефективності та можливостей. Автоматизоване тестування на проникнення не лише сприяє оперативності й ефективності тестування, але й дозволяє значно розширити його масштаби, що особливо важливо для комплексних систем, де необхідна всеосяжна безпекова перевірка [1].

Метою дослідження був аналіз можливостей та обмежень фреймворку Shennina для автоматизованого тестування на проникнення в порівнянні зі сканером вразливостей Nessus. Дослідження спрямоване на оцінку ефективності використання Shennina для реальної експлуатації вразливостей та визначення сценаріїв, у яких цей фреймворк є найбільш доцільним [2].

Для тестування та порівняння ефективності інструментів Shennina та Nessus було обрано віртуальну машину Metasploitable 2, яка є навмисно вразливою версією операційної системи Ubuntu Linux, спеціально створеною для навчальних цілей у сфері кібербезпеки та тестування на проникнення. Ця віртуальна машина дозволяє відпрацьовувати навички виявлення та експлуатації вразливостей у безпечному та контрольованому середовищі.

У процесі дослідження використовували два основних інструменти: Nessus і Shennina, які виконували сканування в контрольованому середовищі [3]. Алгоритм дослідження передбачав чітко структуровані етапи, що забезпечують повноту аналізу та можливість порівняння результатів між обраними інструментами.

З метою оцінки роботи Shennina та Nessus було сформовано метрики, які дозволяють провести об'єктивне порівняння цих інструментів: кількість виявлених вразливостей, час виконання сканування, глибина аналізу, покриття тестової системи, споживання системних ресурсів.

У результаті дослідження встановлено, що фреймворк Shennina, завдяки інтеграції з Metasploit і можливості автоматичної експлуатації, продемонстрував гнучкість у виявленні та використанні не лише стандартних, але й штучно створених вразливостей конфігураційного характеру. Однак охоплення виявлених уразливостей було вужчим, ніж сканера вразливостей Nessus. Це свідчить про необхідність комплексного підходу: використання Nessus для широкого виявлення вразливостей і аналізу відповідності до CVE, а Shennina – для перевірки можливості експлуатації та оцінки практичного ризику для інформаційних систем.

Література

1. Yaacoub J.-P. A., Noura H. N., Salman O., Chehab A. A Survey on Ethical Hacking: Issues and Challenges // A Preprint. American University of Beirut, Electrical and Computer Engineering Department, Beirut, Lebanon. 2020.
2. The Usage of Machine Learning on Penetration Testing Automation // Proceedings of the 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS). August 2023.
3. AI-Powered Penetration Testing using Shennina: From Simulation to Validation // Proceedings of the 2024 ACM Conference. July 2024.

.

УДК 004.7:8
А. Бучко; М. Стадник, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА СТРАТЕГІЙ РЕАГУВАННЯ НА ІНЦИДЕНТИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

UDC 004.7:8
A. Buchko, student of gr. СБм-62; M. Stadnyk, Ph.D.

DEVELOPMENT OF INCIDENT RESPONSE STRATEGIES IN INFORMATION SYSTEMS

Зважаючи на постійне зростання кількості кіберзагроз, розробка стратегій реагування є критично важливою для забезпечення та підтримання безпеки інформаційних систем. Особливу увагу варто приділяти швидкості виявлення інцидентів та мінімізації їх наслідків. Згідно з звітом IBM (2023 рік), вчасне реагування на інциденти дозволяє зменшити фінансові втрати компанії до 30%. У 2023 році середня вартість витоку даних досягла рекордного рівня в 4,88 мільйона доларів США, що на 10% більше порівняно з 2022 роком (4,45 мільйона доларів США). Це свідчить про зростання фінансових втрат, пов'язаних із кіберінцидентами, та підкреслює необхідність ефективних стратегій реагування для мінімізації їх наслідків [1].

Інциденти поділяються на мережеві атаки, компрометацію даних, відмову обладнання та збої програмного забезпечення. Така класифікація дозволяє більш ефективно розробляти стратегії для кожного типу інциденту [2].

Стратегія реагування на інциденти включає шість основних етапів: підготовку, виявлення, аналіз, стримування, ліквідацію та відновлення. Кожен з етапів супроводжується набором інструментів для автоматизації, таких як SIEM (Security Information and Event Management) – системи та SOAR (Security Orchestration, Automation and Response) – платформи [3].

Етап	Опис
Підготовка	Розробка політик, навчання персоналу, планування реагування на інциденти.
Виявлення	Виявлення загроз та аномальної активності за допомогою SIEM-систем.
Аналіз	Збір та аналіз даних для визначення джерела та масштабів загрози.
Стримування	Ізоляція уражених систем для запобігання подальшого поширення загрози.
Ліквідація	Видалення шкідливого програмного забезпечення та відновлення систем.
Відновлення	Повернення до нормальної роботи, оцінка ефективності реагування.

Рисунок 1. Етапи реагування на кіберзагрози

Використання SOAR(Security Orchestration, Automation and Response) платформ – дозволяє значно скоротити час реагування на інциденти, підвищити точність аналізу загроз і мінімізувати людський фактор. Згідно з Gartner (2023), автоматизація процесів знижує час усунення інцидентів у середньому на 40% [4].

Таким чином, запропонована стратегія реагування на інциденти довела свою ефективність під час тестування на прикладі моделювання реальних кіберзагроз. Вона дозволяє зменшити час простою систем, мінімізувати втрати даних та підвищити загальну стійкість інформаційних систем до інцидентів. Це підтверджує доцільність її впровадження в організаціях.

Література

1. IBM Security. Cost of a Data Breach Report 2023 // IBM Security Reports, 2023, URL: https://www.ibm.com.
2. NIST. Computer Security Incident Handling Guide (SP 800-61 Rev. 2) // NIST Special Publications, 2022, URL: https://csrc.nist.gov.
3. ENISA. Cybersecurity Incident Response Guidelines // ENISA Publications, 2023, URL: https://www.enisa.europa.eu. (https://www.enisa.europa.eu/)
4. Gartner. SOAR Market Guide // Gartner Reports, 2023, URL: https://www.gartner.com.

УДК 004.942:004.6
В. М. Вирста
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ РИЗИКІВ ВПРОВАДЖЕННЯ СИСТЕМ МОНІТОРИНГУ І КОНТРОЛЮ ЯКОСТІ ПОВІТРЯ НА БАЗІ ІОТ ДЛЯ РОЗУМНОГО БУДИНКУ

UDC 004.942:004.6
V. M. Vyrsta

RISK ANALYSIS OF IOT-BASED AIR QUALITY MONITORING AND CONTROL SYSTEMS FOR SMART HOMES

Актуальність проблематики аналізу ризиків впровадження систем моніторингу і контролю якості повітря на базі IoT для розумного будинку аргументується кількома факторами. Перший з них – популярність IoT. Можна побачити додатній приріст у відсотковому співвідношенні пристроїв, які підтримують IoT (станом на 2024 рік він становить близько 75%) [1].

Другою причиною є глобальні виклики, які постають в сьогоденні: чинники війн, природні та техногенні катастрофи тощо. Приблизні дані в загальному смертей від природніх катастроф за 2023 рік становить 95 000 людей [2].

По третє, прогноз ринку систем моніторингу якості повітря на 10 років. Даний ринок демонструє зріст сегменту IoT [3].

Було проведено аналіз ризиків впровадження систем моніторингу і контролю якості повітря на базі IoT для розумного будинку за допомогою вагового (Weighted) SWOT аналізу. Результат даного дослідження зведений у таблиці 1. Оцінено елементи SWOT аналізу були за п’ятибальною шкалою, де 1 – маловажлива характеристика, 5 – архіважлива характеристика для системи моніторингу і контролю якості повітря на базі IoT для розумного будинку.

Таблиця 1. Ваговий SWOT аналіз впровадження систем моніторингу і контролю якості повітря на базі IoT для розумного будинку (табличний формат)

№	Сильні сторони (оцінка)	Слабкі сторони (оцінка)	Можливості (оцінка)	Загрози (оцінка)
1	Точний контроль якості повітря (5)	Висока вартість впровадження (5)	Ріст ринку IoT (5)	Конкуренція на ринку (3)
2	Інтеграція з іншими системами (4)	Складність налаштування (4)	Підвищення обізнаності про екологію (4)	Регуляторні обмеження (4)
3	Персоналізація (3)	Вразливість до кіберзагроз (3)	Державні ініціативи та субсидії (3)	Енергетична нестабільність (3)
4	Економія ресурсів (4)	Обмежений термін служби обладнання (3)	Розвиток алгоритмів штучного інтелекту (4)	Недовіра до IoT (2)
5	Мобільний доступ (3)	-	Збільшення попиту серед алергіків (4)	Залежність від Інтернету (3)

Під точним контролем якості повітря (див. таблицю 1) мається на увазі, характеристика збору інформації з датчиків в режимі реального часу. Під персоналізацією – можливість налаштування системи під конкретні потреби мешканців (наприклад, активація очищувача повітря при досягненні певного рівня пилу), під мобільним доступом – керування і відстеження інформації з датчиків через смартфони, планшети тощо.

Однією з слабких сторін є висока вартість впровадження (складні датчики, програмне забезпечення є дорогим для початкового встановлення). Серед загроз – конкуренція на ринку даного продукту (див. рисунок 1). Це ускладнює вартість розробки та заробіток. Перебої зі світлом негативно впливають на статистичні характеристики даної системи.

Відображено результати вагового SWOT аналізу за допомогою кругової діаграми. Кругова діаграма вагового SWOT аналізу впровадження систем моніторингу і контролю якості повітря на базі IoT для розумного будинку наведена на рисунку 1.

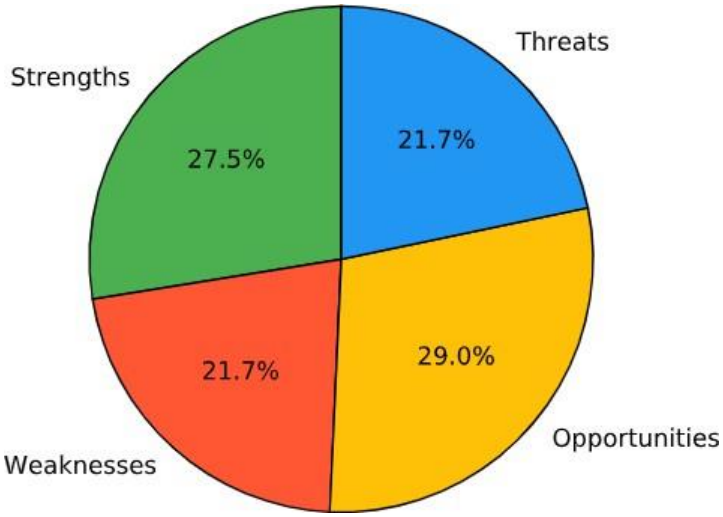


Рисунок 1. Кругова діаграма вагового SWOT аналізу впровадження систем моніторингу і контролю якості повітря на базі IoT для розумного будинку

З рисунку 1, ми можемо побачити, що найбільш вагомим показником є можливості (Opportunities) – 29 % (20 балів). Це говорить про високий потенціал даної тематики.

Висновки: в результаті проведення вагового SWOT аналізу було визначено, що загрози і слабкості мінімізуються сильними сторонами та можливостями. Впровадження IoT-систем моніторингу якості повітря має високий потенціал завдяки точності та інтеграції з іншими технологіями. Висока вартість і складність налаштування є основними перешкодами. Для успішного впровадження системи важливо мінімізувати кіберзагрози, забезпечити енергетичну стабільність.

Література

1. Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. statista. URL: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (date of access: 01.11.2024). https://www.iii.org/fact-statistic/facts-statistics-global-catastrophes.
2. Lörinc M., Hotový O., Podlaha A. 2023 Weather, Climate and Catastrophe Insight. AON. URL: https://www.aon.com/weather-climate-catastrophe/index.aspx (date of access: 05.11.2024).
3. Zoting S. Air Quality Monitoring System Market Size, Share and Trends 2024 to 2034. Precedence Research. URL: https://www.precedenceresearch.com/air-quality-monitoring-system-market (date of access: 14.11.2024).

УДК 621.38
В. В. Висоцький; М. І. Яворська, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ СТУПЕНЯ СТИСНЕННЯ НА ЯКІСТЬ ЗОБРАЖЕННЯ ТА ОБ'ЄМ ПАМ'ЯТІ, НЕОБХІДНИЙ ДЛЯ ЙОГО ЗБЕРІГАННЯ

UDC 621.38
V. V. Vysotskyi; M. I. Yavorska, Ph.D., Assoc. Prof.

THE EFFECT OF THE COMPRESSION RATIO ON THE IMAGE QUALITY AND THE MEMORY VOLUME REQUIRED FOR ITS STORAGE

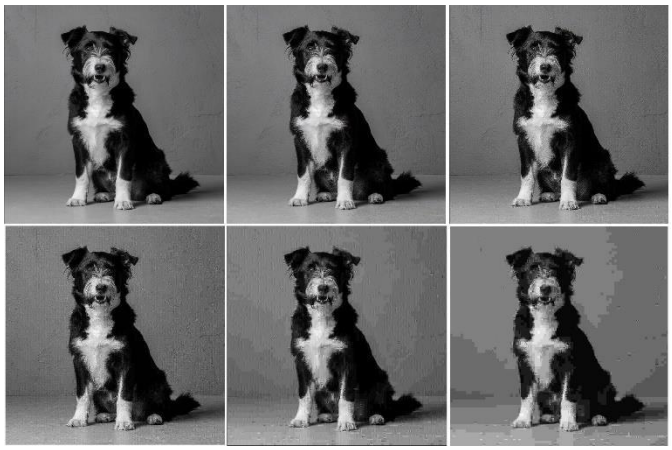


Рисунок 1. Вплив ступеня стиску на якість зображення

Стиск відеоінформації базується на тому факті, що при переході від одного кадру фільму до іншого на екрані звичайно майже нічого не змінюється. Тому стиснена відеоінформація може бути записом деяких базових кадрів і послідовності змін в них. тобто частина інформації може відкидатися. Основна ідея стиску графічної інформації з втратами опирається на такі міркування: стан кожного пікселя на дискретизованому зображенні характеризується трьома рівноважливими атрибутами: яскравістю, кольором і насиченістю. Але око людини не сприймає ці атрибути як рівні. Повністю сприймається тільки інформація про яскравість, в набагато меншій степені про колір і насиченість. Це дозволяє відкидати частину інформації про два останніх атрибути без втрати якості зображення (ця властивість зору використовується, зокрема, в кольоровому телевізорі, в якому на базове чорно-біле зображення наносять колірне розфарбовування). У форматі JPEG можна регулювати рівень стиску, задаючи ступінь втрати якості, як показано на рис.1. Проведені дослідження впливу показника стиску на коефіцієнт стиску і об'єм пам'яті, необхідний для збереження зображення.

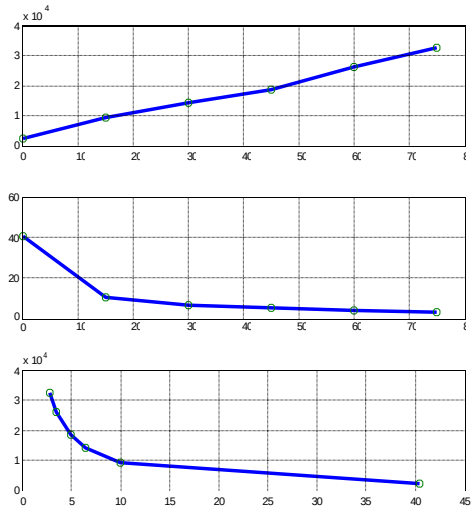


Рисунок 2. Залежності коефіцієнта стиску від показника стиску і об’єму пам’яті від коефіцієнта стиску

Верхній графік – залежність розміру стисненого зображення (в бітах) від заданого показника стиску. Середній графік – вплив параметра q на коефіцієнт стиску зображення.

Нижній графік – залежність об’єму пам’яті (в бітах), відведеної під запис зображення, від коефіцієнта стиску.

Попередній стиск із втратами дозволяє значно зекономити об’єм ресурсів. Причому після розпакування (декодування) файл може значно відрізнятися від оригіналу на рівні порівняння «біт у біт», але практично не відрізняється для сприйняття користувачем в більшості практичних застосувань.

УДК 004.056.53
М. Гладчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ АНОМАЛІЙ У ВЕЛИКИХ ДАНИХ ЯК ІНСТРУМЕНТ ПРОГНОЗУВАННЯ КІБЕРЗАГРОЗ

UDC 004.056.53
M. Hladchuk

DETECTION OF ANOMALIES IN BIG DATA AS A TOOL FOR CYBER THREAT PREDICTION

Виявлення аномалій у великих даних як інструмент прогнозування кіберзагроз

Сучасний стрімкий розвиток інформаційних технологій породжує як нові можливості, так і загрози, зокрема у сфері кібербезпеки. Основним завданням стає виявлення аномалій у великих даних, які часто сигналізують про можливі кіберзагрози. Зокрема, такі методи є ключовими для ідентифікації відхилень у поведінкових патернах мережевого трафіку або користувачів.

Аномалії у великих даних – це відхилення від нормальних патернів, які вимагають ефективних методів обробки. Використання алгоритмів машинного навчання, таких як кластеризація (K-means) та нейронні мережі, дозволяє аналізувати масиви інформації, які генеруються в реальному часі. Наприклад, кластеризація допомагає ідентифікувати точки даних, що не відповідають жодному кластеру, сигналізуючи про потенційні загрози. Методи на основі глибокого навчання забезпечують високу точність виявлення, проте є ресурсомісткими.

На практиці методи виявлення аномалій впроваджуються через платформи обробки великих даних, такі як Apache Spark. Наприклад, ізоляційні ліси (Isolation Forest) демонструють ефективність у реальному часі для виявлення рідкісних подій у фінансових та корпоративних системах. Водночас, проблеми шуму у даних або динамічних змін у поведінкових патернах можуть знижувати продуктивність алгоритмів.

Дослідження методів аналізу великих даних дозволяє ідентифікувати найефективніші алгоритми для різних задач кібербезпеки. Результати підтверджують, що поєднання традиційних підходів із сучасними алгоритмами забезпечує гнучкість та надійність системи. Подальший розвиток технологій, таких як квантові обчислення, відкриває нові можливості для вдосконалення прогнозування кіберзагроз.

Література

1. Xu, X., Wang, X. «Anomaly detection based on one-class SVM inwireless sensor networks» // Lecture Notes in Computer Science. – Berlin: Springer, 2005. – Vol. 3644. – P. 271–282.
2. Breunig, M.M. et al. «LOF: Identifying density-based local outliers» // ACM SIGMOD Record. – 2000. – Vol. 29, No. 2. – P. 93–104.
3. Song, X., Wu, M., Jermaine, C., Ranka, S. «Conditional anomalydetection» // IEEE Transactions on Knowledge and Data Engineering. – 2007. – Vol. 19, No. 5. – P. 631–645.
4. Pang, G. et al. «Deep learning for anomaly detection: A review» // ACM Computing Surveys. – 2021. – Vol. 54, No. 2. – P. 1–38.

УДК 004.056
І. Галанський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМА ЗАХИСТУ WEB-ЗАСТОСУНКІВ НА ОСНОВІ ДВОХФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

UDC 004.056
I. Halanskyi

WEB APPLICATION PROTECTION SYSTEM BASED ON TWO-FACTOR AUTHENTICATION

Двофакторна автентифікація (2FA) є важливим елементом сучасних систем безпеки, що забезпечує захист від несанкціонованого доступу за рахунок використання двох незалежних факторів перевірки. Її застосування дозволяє знизити ризик атак типу «людина посередник», фішингу та компрометації облікових даних, що є особливо актуальним для веб-додатків [1].

Під час виконання роботи було проаналізовано існуючі методи автентифікації. Традиційні паролі залишаються поширеним методом, однак їх низький рівень захисту через можливість перехоплення або підбору вимагає пошуку альтернатив. Біометричні методи пропонують високий рівень безпеки, але є дорогими у впровадженні та складними в інтеграції. Одноразові паролі (OTP), зокрема алгоритм TOTP (Time-based One-Time Password), було визначено як оптимальне рішення, яке поєднує високий рівень безпеки, простоту реалізації та доступність [2].

Впровадження системи двофакторної автентифікації включала кілька ключових етапів. Спочатку було визначено архітектуру системи з урахуванням сучасних вимог до безпеки та масштабованості. Для цього було обрано технології PHP як основну мову серверного програмування, MySQL як базу даних, а для надсилання одноразових паролів – бібліотеку PHPMailer.

На етапі реалізації було написано програмний модуль, який відповідає за генерацію одноразових паролів на основі алгоритму TOTP. Алгоритм працює за принципом генерації динамічних кодів, що змінюються з фіксованим часовим інтервалом, забезпечуючи високий рівень захисту за рахунок унікальності кожного пароля. Генеровані паролі надсилаються користувачам через електронну пошту, що є доступним і зручним каналом зв'язку.

Тестування системи показало її ефективність у протидії основним кіберзагрозам. Було перевірено стійкість до атак «людина посередник», перехоплення даних та фішингових атак. Отримані результати підтвердили, що запропоноване рішення відповідає сучасним вимогам до інформаційної безпеки та може бути використане у різних сферах, таких як електронна комерція, банківські системи або корпоративні мережі.

Впровадження двофакторної автентифікації на основі алгоритму TOTP є доступним і ефективним способом підвищення безпеки веб-додатків, що не потребує значних фінансових витрат, але забезпечує високий рівень захисту даних користувачів.

Література

1. Omwoyo R., Kamau J., Mvurya M. A review of Two Factor Authentication Security Challenges in the Cyberspace | International Journal of Advanced Computer Technology. *International Journal of Advanced Computer Technology*. URL: https://ijact.org/index.php/ijact/article/view/112 (дата звернення: 12.11.2024).
2. RFC 6238: TOTP: Time-Based One-Time Password Algorithm / D. M'Raihi et al. *IETF Datatracker*. URL: https://datatracker.ietf.org/doc/html/rfc6238 (дата звернення: 14.11.2024).

УДК 004.45
Д. В. Гемський; Б. В. Хоміцький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМА КОНТРОЛЮ КЛІМАТИЧНИХ ПОКАЗНИКІВ У ПРИМІЩЕННЯХ БАГАТОКВАРТИРНОГО БУДИНКУ

UDC 004.45
D. V. Hemsky; B. V. Khomitskyi

CLIMATE CONTROL SYSTEM IN THE PREMISES OF AN APARTMENT BUILDING

У сучасних умовах змін клімату та зростання енергоспоживання значущість ефективного контролю кліматичних показників у приміщеннях багатоквартирних будинків набуває все більшої актуальності. Забезпечення оптимальних мікрокліматичних умов не лише підвищує комфорт проживання, але й сприяє енергозбереженню та екологічній безпеці, що є критично важливим у контексті стійкого розвитку міської інфраструктури.

На даний момент існує кілька варіантів контролю кліматичних показників на рівні власників помешкань та керуючих компаній. Власники житлових приміщень можуть використовувати відкриті платформи для інтеграції побутових приладів, розроблених самостійно або створених іншими користувачами за допомогою відкритого API системи. Однією з таких платформ є Home Assistant, яка представляє собою відкриту екосистему, що дозволяє кожному користувачу додавати пристрої, підтримку яких можна переглянути на офіційному веб-сайті. Такий підхід забезпечує високу гнучкість та масштабованість системи, дозволяючи адаптувати її до специфічних потреб різних житлових приміщень.

У той же час, керуючі компанії зазвичай використовують власні розробки для контролю кліматичних показників. Однак ці системи часто мають закриту архітектуру, що обмежує можливості їхнього налаштування та інтеграції з іншими технологічними рішеннями. Через закритість розробки виникають труднощі у внесенні змін до системи, спостереженні за показниками в режимі реального часу та виявленні та усуненні проблем всередині системи. Це обмежує гнучкість управління та може призводити до менш ефективного використання енергоресурсів, а також до затримок у реагуванні на аварійні ситуації або відхилення від нормальних параметрів клімату.

Рисунок 1. Raspberry PI, на базі якого реалізовано Home Assistant

Ефективний контроль кліматичних показників у приміщеннях багатоквартирних будинків є критично важливим для забезпечення комфорту мешканців, енергозбереження та екологічної безпеки. Відкриті платформи надають високу гнучкість та можливості для інтеграції різноманітних пристроїв, що робить їх ідеальними для власників, які прагнуть до самостійного налаштування системи. У той же час, закриті системи, використовувані

керуючими компаніями, забезпечують стабільність та високий рівень безпеки, проте обмежують можливості налаштування та інтеграції.

Таблиця 1. Порівняльний аналіз відкритих та закритих систем контролю клімату

Критерії	Відкриті платформи	Закриті системи
Гнучкість та адаптивність	Висока: можливість додавання нових пристроїв	Низька: обмежені можливості налаштування
Інтеграція з іншими системами	Просторі можливості через відкриті API та стандарти	Обмежені можливості інтеграції
Безпека	Залежить від налаштувань користувача та спільноти	Високий рівень контролю та захисту
Підтримка та оновлення	Активна спільнота, регулярні оновлення	Регулярні оновлення від розробника
Можливості моніторингу в реальному часі	Високі завдяки гнучким інтеграційним можливостям	Можуть бути обмеженими через закритість системи

Найкращий варіант для реалізації системи контролю кліматичних показників може бути побудований на основі розробки ядра, яке може повторно використовуватись як спільнотою, так і керуючими компаніями. Такий підхід забезпечує баланс між гнучкістю та безпекою, дозволяючи адаптувати систему до різноманітних потреб користувачів та умов експлуатації. Перевикористання ядра сприятиме більшій сумісності між різними платформами та спрощенню процесу оновлення та модернізації системи, а також сприятиме розвитку спільноти користувачів, які можуть вносити власні покращення та інновації.

Вибір оптимальної системи контролю клімату залежить від конкретних потреб та ресурсів користувачів, а також від вимог до гнучкості, безпеки та інтеграції системи. Проте, впровадження універсального ядра, яке підтримує як відкриті, так і закриті моделі розробки, може стати ефективним рішенням, що об'єднає переваги обох підходів. Це дозволить створити більш адаптивні та стійкі системи контролю клімату, що відповідають сучасним викликам у сфері енергозбереження та екологічної безпеки.

Література

1. Стаценко, Д. В. (2022). Керування мікрокліматом у приміщеннях з системою «Розумний будинок».
2. Mistry, V. (2023). The Role of IoT in Enhancing HVAC Control Systems. Journal of Biosensors and Bioelectronics Research. SRC/JBBER-119. DOI: doi. org/10.47363/JBBER/2023 (1), 115, 2-5.
3. Documentation. Home Assistant. URL: https://www.home-assistant.io/docs/ (date of access: 21.11.2024).

УДК 621.855
Р. І. Гловяк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

НЕОБХІДНІСТЬ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ФОРМУВАННІ ТА ВИКОРИСТАННІ ЛАНЦЮГІВ ПОСТАЧАННЯ ТОВАРІВ І ПОСЛУГ

UDC 621.855
R. I. Hlovyak

THE NEED FOR THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE FORMATION AND USE OF GOODS AND SERVICES SUPPLY CHANNELS

У міжнародній логістиці одною з головних особливостей є транспортування товарів та послуг кількома видами транспорту при його доставці до кінцевого одержувача. Мультимодальні перевезення визначаються як перевезення, які використовують багато видів транспорту, але регулюються одним договором. При цьому не має значення, який вид транспорту використовується – залізничний, річковий, автомобільний тощо. Інтермодальні перевезення – це перевезення з використанням багатьох видів транспорту, в яких клієнт може укласти договір з кількома компаніями. У випадку інтермодальних перевезень може бути багато видів транспорту, а відповідальність розподіляється рівномірно між усіма учасниками [1]. На сьогоднішній день такі послуги надають ряд логістичних компаній в Україні.

З огляду на мультимодальні та інтермодальні логістичні особливості інтеграція сучасних ІТ-рішень набуває все ширшого застосування в діяльності логістичних компаній. Цього можна досягти за рахунок інтеграції цих технологій у існуючі логістичні системи, зокрема, таких як Інтернет речей (IoT), штучний інтелект (AI), аналітика великих даних (Big Data), блокчейн та автоматизація. Водночас ставить перед компаніями завдання, а саме: розробка програмного забезпечення для розумної логістики сприяє інтеграції сучасних технологій, забезпечуючи їх ефективне використання для оптимізації логістичних процесів, підвищення точності прогнозів та покращення управління ресурсами.

Іншим вагомим завданням, що потребує вирішення є підвищення ефективності та зменшення витрат. Традиційні методи управління логістикою часто є неефективними та затратними, що негативно впливає на конкурентоспроможність компаній. ІТ-рішення для розумної логістики дозволяють автоматизувати рутинні процеси, оптимізувати маршрути доставки, покращити управління запасами та знизити витрати на транспортування та зберігання товарів. Це сприяє підвищенню загальної ефективності логістичних операцій.

При застосуванні штучного інтелекту суттєво підвищується не тільки ефективність формування та використання ланцюгів постачання товарів і послуг, але й якість логістичних послуг. За допомогою аналізу великих даних і машинного навчання ми можемо постійно оптимізувати та вдосконалити існуючі процеси. З іншого боку, технологія штучного інтелекту може сприяти оптимізації шляху транспортування та підвищення ефективності доставки. Використання інформаційних систем надає можливість відстежити доставку, відповідно процес контролюється, а результат передбачуваний та виключає багато неконтрольованих факторів у роботі та забезпечення якості роботи.

Рисунок 1. Напрямки застосування штучного інтелекту в логістичних процесах, джерело [2]

Для уникнення потенційних ризиків при формуванні та використанні ланцюгів постачання товарів і послуг від негативних чинників, зокрема регуляторних змін при їх проєктуванні слід опиратись на стратегії управління регуляторними змінами. Моніторинг регуляторних змін – постійний моніторинг змін у законодавстві на місцевому, національному та міжнародному рівнях для своєчасного реагування. Внутрішній аудит та контроль відповідності – регулярні внутрішні аудити для перевірки відповідності чиним нормативно правовим актам та ідентифікації потенційних ризиків. Навчання та підвищення кваліфікації персоналу – навчання працівників новим регуляторним вимогам та забезпечення їхньої готовності до змін. Співпраця з регуляторними органами – активна взаємодія з регуляторними органами для отримання консультацій та рекомендацій щодо дотримання нових вимог. Адаптація бізнес-процесів – оновлення та адаптація бізнес-процесів, політик та процедур. Залучення експертів – співпраця з юридичними консультантами та експертами з регуляторних питань для отримання професійної допомоги в управлінні змінами.

Таким чином можемо обґрунтовано стверджувати, що впровадження технологічних змін у логістичних ланцюгах дозволяє підвищити ефективність, знизити витрати та покращити якість обслуговування клієнтів. Однак це вимагає ретельного планування, інвестицій та навчання персоналу для досягнення максимальних результатів.

Література

1. URL: https://www.searates.com/ua/blog/post/ntermodaln-ta-multimodaln-perevezennya-v-chomu-rznicya.
2. Кирлик Н. Ю. «Штучний інтелект» та його використання в логістичних процесах. Актуальні проблеми економіки. 2021. No. 243–244. С. 59–66.

УДК 004.046
Д. В. Граб
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА МОДУЛЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ОСНОВІ СТЕКУ MERN

UDC 004.046
D. V. Hrab

DEVELOPMENT OF AN INFORMATION SYSTEM MODULE BASED ON THE MERN-STACK

Сучасна веб-розробка вимагає інтеграції потужних технологій та інструментів для створення масштабованих, високопродуктивних інформаційних систем. MERN-стек, що складається з MongoDB, Express, React та Node.js, є одним із найпопулярніших підходів для розробки таких систем.

Розробка модуля інформаційної системи починається з проектування серверної частини, яка обробляє запити та забезпечує доступ до бази даних. Node.js надає можливість створення високопродуктивного сервера з асинхронною обробкою запитів, а Express.js спрощує розробку API завдяки своїм гнучким можливостям. MongoDB використовується як база даних для зберігання даних у JSON-подібному форматі, що дозволяє легко інтегрувати її із серверною логікою [2].

На наступному етапі створюється клієнтська частина за допомогою React. Ця бібліотека дозволяє розробляти багаторазові компоненти, які динамічно оновлюють інтерфейс у відповідь на зміни стану. React спрощує процес створення складних інтерфейсів завдяки використанню Virtual DOM, що покращує продуктивність додатків [3].

Завершальний етап полягає у забезпеченні інтеграції між серверною та клієнтською частинами через RESTful або GraphQL API. API, розроблений за допомогою Express.js, дозволяє клієнтській частині взаємодіяти з базою даних MongoDB для виконання CRUD-операцій (створення, читання, оновлення, видалення) [2].

Стек MERN пропонує значні переваги, включаючи однорідність використання JavaScript, високу продуктивність завдяки асинхронній обробці запитів і можливість створення динамічних інтерфейсів. Крім того, використання React дозволяє створювати інтерактивні додатки з високою швидкістю завантаження та перевикористовуваними компонентами. MongoDB забезпечує зберігання великих обсягів даних і динамічний дизайн схем, що робить її ідеальною для сучасних веб-додатків [1].

Використання стеку технологій та інструментів MERN для розробки модулів інформаційних систем є ефективним і сучасним підходом до створення масштабованих веб-додатків. Комбінація MongoDB, Express, React і Node.js забезпечує інтеграцію, продуктивність і адаптивність на всіх рівнях розробки. Дотримання передових практик розробки, включаючи планування, оптимізацію продуктивності та організацію робочих процесів, сприяє створенню високоякісних інформаційних систем, здатних задовольнити потреби сучасних користувачів [3].

Література

1. Vasan Subramanian (2019). Pro MERN Stack Development: Building Full-Stack React Apps with MongoDB, Express, and Node. Apress. ISBN 978-1484243909.
2. Shama Hoque (2018). Full-Stack React Projects: Modern web development using React 16, Node, Express, and MongoDB. Packt Publishing. ISBN 978-1788835534.
3. Kirupa Chinnathambi (2018). Learning React: A Hands-On Guide to Building Web Applications Using React and Redux. Addison-Wesley Professional. ISBN 978-0134843551.

УДК 004.4
В. Б. Гурський; Т. Р. Кульчицький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ ШИФРУВАННЯ НА ПРОДУКТИВНІСТЬ ВЕБСАЙТІВ: ПОРІВНЯЛЬНИЙ АНАЛІЗ СУЧАСНИХ АЛГОРИТМІВ

UDC 004.4
V. B. Hurskiy; T. R. Kulchytskyi

THE IMPACT OF ENCRYPTION ON WEBSITE PERFORMANCE: A COMPARATIVE ANALYSIS OF MODERN ALGORITHMS

1. Значення шифрування для сучасних вебсайтів

- **Забезпечення конфіденційності та безпеки даних**
  Шифрування є основою для захисту особистої інформації користувачів, особливо при передаванні даних через Інтернет (наприклад, HTTPS). Воно мінімізує ризик перехоплення та злому даних.

- **Обов'язковість у сучасних стандартах**
  Усі сучасні вебсайти мають використовувати HTTPS, що базується на TLS (Transport Layer Security), для відповідності вимогам пошукових систем і підвищення довіри користувачів.

- **Вплив на SEO**
  Пошукові системи (наприклад, Google) надають перевагу сайтам із шифруванням, підвищуючи їх у рейтингу.

2. Типи алгоритмів шифрування, що застосовуються у вебсайтах

- **RSA (Rivest–Shamir–Adleman)**
  - **Особливості:** Широко використовуваний алгоритм асиметричного шифрування для встановлення з'єднань.
  - **Недоліки:** Високе навантаження на процесор через складність обчислень, особливо з великими ключами (2048/4096 біт).
  - **Переваги:** Високий рівень захисту.
- **ECDSA (Elliptic Curve Digital Signature Algorithm)**
  - **Особливості:** Менші ключі зберігають такий самий рівень безпеки, як і RSA, але працюють швидше.
  - **Вплив на продуктивність:** Менше використання обчислювальних ресурсів.
- **AES (Advanced Encryption Standard)**
  - **Особливості:** Симетричний алгоритм, що забезпечує швидке шифрування. Зазвичай використовується у HTTPS після встановлення з'єднання.
  - **Переваги:** Енергоефективний, підходить для великих обсягів даних.
- **ChaCha20 + Poly1305**
  - **Особливості:** Більш ефективний для пристроїв із низькою продуктивністю, таких як мобільні телефони.
  - **Переваги:** Швидкий і сучасний, особливо для нестандартних умов з'єднання.

3. Як шифрування впливає на продуктивність вебсайтів

- **Затримки при встановленні з’єднання**
  Алгоритми асиметричного шифрування (RSA, ECDSA) впливають на швидкість першого встановлення TLS-з’єднання. Чим складніший алгоритм і більший ключ, тим більше часу потрібно.

- **Ресурси сервера**
  Використання складних алгоритмів шифрування збільшує навантаження на сервери. Це може бути критичним для сайтів із великим трафіком.

- **Затримки під час передачі даних**
  Симетричні алгоритми, такі як AES, швидше шифрують дані під час передачі, але все одно додають невеликі накладні витрати.

- **Оптимізація з'єднань**
  Використання HTTP/2 і TLS 1.3 значно зменшують накладні витрати шифрування, зменшуючи кількість «рукостискань» і оптимізуючи процес передачі.

4. Порівняльний аналіз продуктивності алгоритмів

- **RSA vs ECDSA**
  RSA забезпечує високу безпеку, але його повільніша продуктивність робить його менш ефективним порівняно з ECDSA, особливо в мобільних мережах.

- **AES vs ChaCha20**
  AES працює ефективніше на сучасних процесорах із підтримкою апаратного шифрування (AES-NI), тоді як ChaCha20 кращий для мобільних пристроїв і старіших процесорів.

- **TLS 1.2 vs TLS 1.3**
  TLS 1.3 швидший за TLS 1.2 завдяки меншій кількості рукостискань і оптимізованому алгоритму шифрування.

5. Шляхи оптимізації використання шифрування

- **Вибір правильного алгоритму для аудиторії сайту**
  Для мобільних користувачів варто використовувати ChaCha20, тоді як для стаціонарних серверів оптимальним є AES із апаратною підтримкою.

- **Використання TLS 1.3**
  Це новий стандарт, який дозволяє значно зменшити затримки й підвищити продуктивність.

- **Кешування та стиснення даних**
  Використання стиснення (наприклад, Brotli) зменшує обсяг переданих даних, а кешування TLS-з'єднань (Session Resumption) скорочує час повторного підключення.

6. Висновки

Шифрування є критично важливим компонентом сучасних вебсайтів, але воно має певний вплив на продуктивність. Правильний вибір алгоритму та технологій шифрування дозволяє забезпечити баланс між безпекою і швидкістю роботи вебсайту. У майбутньому, із розвитком обчислювальних технологій, продуктивність шифрування буде ще кращою.

УДК 004.056:629.331
М. Демчишин; В. Тимощук; В. Шиманська; Д. Тимощук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КІБЕРЗАГРОЗИ СЕНСОРНИМ ПІДСИСТЕМАМ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ

UDC 004.056:629.331
M. Demchyshyn; V. Tymoshchuk; V. Shymanska; D. Tymoshchuk

CYBER THREATS TO SENSOR SUBSYSTEMS OF AUTONOMOUS VEHICLES

Автономні транспортні засоби (АТЗ) є технологічним проривом, який обіцяє змінити сучасну транспортну інфраструктуру, забезпечивши підвищення ефективності, зниження кількості дорожньо-транспортних пригод та покращення якості перевезень. Завдяки використанню численних сенсорів, таких як LiDAR [1], камери, радари та ультразвукові датчики, АТЗ здатні аналізувати навколишнє середовище, ідентифікувати об'єкти, передбачати дії інших учасників руху та приймати рішення в реальному часі (рисунок 1).

Рисунок 1. Сенсори автономного транспортного засобу

Проте впровадження цієї технології супроводжується серйозними викликами в галузі кібербезпеки, особливо в контексті захисту критично важливих сенсорних підсистем. Ключовою складовою функціонування автономного транспорту є точне сприйняття навколишнього середовища. Залежність від сенсорних систем створює вразливості, які можуть бути використані зловмисниками для компрометації безпеки транспортного засобу. Такі атаки можуть включати викривлення даних, відтворення попередніх показників або повне відключення сенсорів. Найбільшу загрозу становлять атаки, спрямовані на сенсори, адже вони можуть створити небезпечні ситуації, що безпосередньо впливають на керування та прийняття рішень. Наприклад, маніпуляція даними LiDAR може привести до хибної ідентифікації об'єктів або створення «сліпих зон», що унеможливлює адекватне реагування транспортного засобу.

Зростаюча складність сучасних сенсорних систем вимагає розробки ефективних моделей захисту. Найбільш імовірними є атаки з частковою інформацією, коли зловмисник має обмежений доступ до системи та не може отримати повний огляд її роботи. У таких випадках атакуючий працює з мінімумом даних, наприклад, лише з вхідними показниками сенсора. Метою роботи був аналіз кіберзагроз сенсорним підсистемам АТЗ та розробка ефективних підходів до захисту.

Література

1. IBM. What is LiDAR? URL: https://www.ibm.com/topics/lidar (date of access: 07.12.2024).

УДК 004.056
В. Дячун; В. Ваврічен
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ВИЯВЛЕННЯ СПАМУ

UDC 004.056
V. Diachun; V. Vavrichen

METHODS OF SPAM DETECTION

Спам – це непотрібна, часто рекламна або шахрайська інформація, що надходить через електронну пошту, соціальні мережі або інші канали комунікації. Спам часто містить шкідливі посилання або вкладення, що можуть привести до зараження комп'ютерів вірусами, шкідливим програмним забезпеченням чи фішингом. Велика кількість спам-повідомлень засмічує поштові скриньки, що може ускладнювати роботу та знижувати продуктивність. Спам несе із собою нав'язливу рекламу, що може займати важливі ресурси пристроїв, наприклад, інтернет-трафік або пам'ять.

Боротьба зі спамом є однією з найстаріших проблем комп'ютерної безпеки, і, водночас, важливою складовою забезпечення безпеки та ефективності цифрового середовища сьогодення. Існує кілька підходів до виявлення та боротьби зі спамом. Традиційні методи виявлення спаму діляться на дві великі групи:

1. Методи, що базуються на аналізі повідомлення. Один з найпоширеніших методів – це фільтрація на основі ключових слів і шаблонів. Програми автоматично аналізують текст повідомлення на наявність певних слів або фраз, характерних для спаму. Крім того, аналіз контенту листа може здійснюватись з використанням сигнатур в оновленій базі даних, із застосуванням статистичних методів на основі теореми Байєса, за допомогою використання SURBL ((Spam URL Real-time Block Lists)
2. Репутаційні схеми. Їхнє завдання – виявляти розсилки однотипних листів серед великої кількості користувачів. Цей метод оцінює репутацію відправника, базуючись на історії його діяльності. Якщо адреса відправника була раніше пов'язана з великим обсягом спаму, система може позначити його повідомлення як спам.
3. Методи, засновані на визнанні відправника спамером. Ці методи спираються на різні чорні списки IP-адрес та адрес електронної пошти. Відомі адреси або IP-адреси, з яких часто надходить спам, можуть бути внесені в чорні списки, що допомагає блокувати подібні повідомлення ще на етапі їх надходження.
4. Методи, засновані на перевірці адреси електронної пошти та доменного імені відправника.

Крім цього фільтрація спам-листів може ґрунтуватись на аналізі поведінки користувачів. Якщо користувач отримує спам-повідомлення від незнайомих адрес чи в незвичний час, система може попередити про ймовірний спам. Це свого роду задача виявлення аномалій.

Сьогодні для фільтрації електронної пошти активно розробляються методи, що навчаються, або інтелектуальні методи, засновані на алгоритмах машинного навчання та техніках глибокого навчання. Підвищення точності роботи цих методів є актуальним науковим завданням.

Література

1. Saadat Nazirova. Survey on Spam Filtering Technique. Communications and Network, 2011, No. 3, P.153-160. doi:10.4236/cn.2011.33019
2. J, Rajesh & G, Mahalakshmi & P, Sudarshan. Email Spam Detection using Machine Learning Techniques. IARJSET, 2020, No 8, P.189-193.
3. AbdulNabi, Isra’a & Yaseen, Qussai. Spam Email Detection Using Deep Learning Techniques. Procedia Computer Science. 2021, No. 184 (2), P. 853-858

УДК 004.386.6
А. Іванюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОДЕЛЮВАННЯ СУДИННИХ МЕРЕЖ У 3D-ДРУКОВАНИХ ОРГАНАХ ІЗ ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

UDC 004.386.6
A. Ivanyuk

MODELING OF VASCULAR NETWORKS IN 3D-PRINTED ORGANS USING ARTIFICIAL INTELLIGENCE

В регенеративній медицині активно розвиваються технології 3D-друку органів, однак створення функціональних судинних мереж залишається актуальним викликом для науковців. З огляду на те, що судинна система забезпечує транспортування поживних речовин та кисню, і є життєво необхідним для функціонування органів. Особливо складний 3D-друк нирок, через їхню розгалужену судинну архітектуру, яка включає артерії, вени та капіляри.

Для аналізу судинної системи у дослідженні використовуються дані, отримані за допомогою **HiP-CT** (Hierarchical Phase-Contrast Tomography). HiP-CT – це метод візуалізації, що дозволяє отримувати тривимірні зображення реальних органів людини із високою роздільною здатністю. Він базується на фазовому контрасті, що забезпечує візуалізацію дрібних судин без застосування контрастних речовин. Зображення отримуються із зразків органів, наданих донорами або пацієнтами у межах відповідних біомедичних досліджень[1], [2].

Дані HiP-CT забезпечують деталізацію судинної системи на рівні капілярів, що робить їх ідеальними для дослідження судинної архітектури нирок. Перед обробкою дані проходять етап нормалізації, що усуває вплив шуму та варіацій інтенсивності у сканах:

$$I_{norm} = \frac{I - I_{\min}}{I_{\max} - I_{\min}},$$

де I – інтенсивність пікселів, $I_{\min}$ і $I_{\max}$ – мінімальне та максимальне значення інтенсивності [2].

Для сегментації судин використовується адаптована модель **U-Net**, яка має симетричну структуру для витягування ознак (contracting path) та відновлення просторової інформації (expanding path). Впроваджено мультикласову сегментацію, яка дозволяє розрізняти артерії, вени та фон. Розрахунок ймовірностей для кожного пікселя здійснюється за допомогою функції Softmax:

$$P(c|x) = \frac{e^{z_c}}{\sum_{i=1}^{C} e^{z_i}},$$

де c – клас (артерії, вени, фон), z_c – логіти, C=3 – кількість класів. Для мінімізації похибок використовується функція втрат крос-ентропії:

$$L = -\sum_{c=1}^{C} y_c \log(P(c|x)),$$

що дозволяє точно сегментувати зображення [3], [4].

Зображення HiP-CT подаються на вхід моделі U-Net, яка на виході генерує сегментовані дані у вигляді карти ймовірностей для кожного класу. Це дозволяє виділяти артерії, вени та виключати фонові області. Якість сегментації оцінюється за допомогою метрики Dice Score [4], [5].

Запропонований підхід забезпечує автоматизацію процесів аналізу та моделювання судинної архітектури, що є важливим кроком для створення функціональних 3D-друкованих нирок. У подальших дослідженнях передбачається вдосконалення підходу для роботи з іншими органами та інтеграція у системи біодруку, що відкриває нові перспективи для трансплантології [6].

Література

1. Wang, X., Li, Y., Zhao, H., et al. Kidney Blood Vessel Computed Tomography Image Segmentation. ResearchGate, 2023. Available at: https://www.researchgate.net/publication/376645882_Kidney_Blood_Vessel_Computed_Tomography_Image_Segmentation
2. Rahmani, S., Smith, T. J., Johnson, M., et al. Mapping the blood vasculature in an intact human kidney using hierarchical phase-contrast tomography. bioRxiv, 2023. Available at: https://www.biorxiv.org/content/10.1101/2023.03.28.534566v2.full
4. Ronneberger O., et al. "U-Net: Convolutional Networks for Biomedical Image Segmentation". MICCAI, 2015. URL: https://arxiv.org/abs/1505.04597
5. Hague, J. P. Simultaneous determination of interlocking arterial and venous network configurations for any tissue shape by global power optimization. ResearchGate, 2023. Available at: https://www.researchgate.net/publication/372962584_Simultaneous_determination_of_interlocking_arterial_and_venous_network_configurations_for_any_tissue_shape_by_global_power_optimization
6. Deep learning techniques for medical image segmentation: A survey. URL: https://arxiv.org/pdf/1703.00130
7. Murphy, D. J., Aghayev, A., & Steigner, M. L. Vascular CT and MRI: a practical guide to imaging protocols. Insights into Imaging, 2018. Available at: https://insightsimaging.springeropen.com/articles/10.1007/s13244-018-0597-2

УДК 004.7
Р. Калушка; М. Карпінський, докт. техн. наук, проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИЩЕНА КОРПОРАТИВНА КОМПЮТЕРНА МЕРЕЖА

UDC 004.7
R. Kalushka; M. Karpinskyi, Dr. Prof.

A SECURE CORPORATE COMPUTER NETWORK

В даний час базовим елементом корпорації є комп'ютерна мережа. Для створення захищеної комп’ютерної мережі використано різні компоненти, зокрема електропроводку. мережевий комутатор, маршрутизатор, сервер, комп'ютери тощо [1]. Сучасною нормою побудови комп’ютерних мереж в кожній корпорації є топологія «зірка», тому її застосовано в цій роботі. Засоби з кількома мережевими картами (сервери, дискові накопичувачі, бібліотеки) під’єднуються до обох комутаторів. Для випадку аварії одного з комутаторів сервери залишаються доступними в мережі, оскільки мережевий трафік автоматично перемикається на інший пристрій.

Одним з важливих елементів комп'ютерної системи корпорації застосовано мережу SAN (Storage Area Network). Це підмережа, фізично відокремлена від локальної мережі, яка з’єднує дискові ресурси (дискові масиви, стрічкову бібліотеку) із серверами. Завдяки цьому всі сервери мають виділений доступ до дискових ресурсів, що забезпечує можливість побудови високоефективної, масштабованої та стійкої до збоїв комп’ютерної системи.

У цій роботі застосовано віртуальне середовище VMware. В конфігурації, яку застосовано для створення віртуального середовища, використано два фізичні сервери, які названо хостами, та дисковий накопичувач, під’єднаний до фізичних серверів через мережу SAN. Ядра процесора та оперативна пам’ять для створення віртуальних машин використовують фізичні процесори та оперативну пам’ять обох хостів, а дисковий масив забезпечує дискові ресурси для цих віртуальних машин. Слід зазначити, що відмовостійкість є найбільшою перевагою віртуального середовища. Ще однією перевагою віртуального середовища є висока доступність і масштабованість.

У конкретному випадку нашої роботи створено 6 віртуальних машин, а саме: сервер DHCP, файловий сервер, сервер друку, контролер активного каталогу AD (Active Directory), сервер бази даних, сервер додатків. В роботі розроблено схему під’єднання серверів і дискового накопичувача до мережі LAN. Кожен сервер під’єднано чотирма портами. Це забезпечує резервування, так що для випадку збою порту в комутаторі або сервері буде забезпечена безперервна робота цих пристроїв. У той же час, для відповідної конфігурації комутаторів, два канали зв'язку між сервером і комутатором застосовано для розподілу трафіку між ними, використовуючи алгоритми балансування навантаження.

В роботі проведено конфігурації маршрутизатора, хоста, резервного сервера, дискового накопичувача, віртуальної машини контролера домену, DHCP, файлового сервера та сервера друку. Маршрутизатором застосовано TP-Link з бізнес-серії. Для проєкту було здійснено конфігурацію двох серверів компанії Lenovo.

Розроблене у цій роботі рішення надається для впровадження в корпорації середнього розміру. Його підготовлено за новітніми технологіями, що дає можливість подальшого розвитку проєкту.

Література

1. Peterson, L., Davie B. (2019). Computer Networks: A Systems Approach. Publisher: Larry Peterson and Bruce Davie.

УДК 621.855
І. М. Кіт
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ІНДИВІДУАЛЬНИХ ТЕРАПЕВТИЧНИХ СТРАТЕГІЙ

UDC 621.855
I. M. Kit

DEVELOPMENT OF ARTIFICIAL INTELLIGENCE ALGORITHMS FOR INDIVIDUALIZED THERAPEUTIC STRATEGIES

Персоналізована медицина спрямована на індивідуальний підхід до лікування пацієнтів, враховуючи їхні генетичні, клінічні та поведінкові характеристики. Інтеграція штучного інтелекту (ШІ) у цей процес дозволяє аналізувати великі масиви даних для створення алгоритмів, здатних прогнозувати ризики хронічних захворювань і формувати персоналізовані терапевтичні рекомендації. Такі алгоритми можуть не лише покращити результати лікування, але й знизити витрати на медичну допомогу. Запропоновано архітектуру алгоритму, яка поєднує аналіз часових рядів, інтерпретацію ключових факторів ризику та адаптацію до індивідуальних характеристик пацієнта.

Запропонований підхід передбачає послідовність етапів: збір та підготовку даних, врахування ваги для релевантних факторів ризику, індивідуалізація терапевтичних протоколів.

Дані отримані з електронних медичних записів (ЕМЗ), таких як результати лабораторних аналізів, діагнози, анамнез захворювань та генетичні маркери. Для масштабування даних застосовано Z-score нормалізацію [1]:

$$I_{\text{z-score}} = \frac{I - \mu}{\sigma}$$

де:

I – значення параметра,

μ – середнє значення вибірки,

σ – стандартне відхилення вибірки.

Цей підхід дозволяє стандартизувати різні типи даних для подальшого аналізу.

На наступному етапі розроблено гібридний алгоритм, який поєднує рекурентні нейронні мережі (RNN) з механізмами уваги (Attention Mechanisms) для роботи з часовими рядами. Механізм уваги обчислює ваги для релевантних факторів ризику [2]:

$$\alpha_t = \frac{e^{e_t}}{\sum_{i=1}^{T} e^{e_i}}, \quad e_t = f(s_{t-1}, h_t)$$

де:

α_t – вага для моменту часу t ,

$\boldsymbol{h_t}$ – прихований стан у момент часу t ,

s_{t-1} – попередній стан моделі,

f – функція подібності.

Механізм уваги дозволяє алгоритму фокусуватися на найбільш релевантних ознаках пацієнта.

Індивідуалізацію терапевтичних протоколів реалізовано завдяки запропонованому алгоритму, що враховує генетичні дані, такі як мутації, що впливають на реакцію організму на препарати, а також демографічні фактори (вік, стать, спосіб життя). Результати моделі представлені у вигляді ймовірностей кожного терапевтичного сценарію, які обчислюються за допомогою багатокласової функції активації Sigmoid [3]:

$$P(c|x) = \frac{1}{1 + e^{-z_c}}$$

де: z_c – логіт для класу c, що дозволяє прогнозувати ймовірності кожного класу незалежно.

В працях провідних науковців котрі займались даною тематикоюТеоретичний аналіз на базі синтетичних даних показує, що запропонована модель здатна досягати високих показників точності. Умовно очікувані метрики [4,5]:

- Точність: 85–90%;
- Чутливість: 80–85%;
- Специфічність: 88–92%.

Ці результати потребують підтвердження на реальних клінічних даних для перевірки узагальненості моделі.

Запропонована архітектура алгоритму має значний потенціал для персоналізованої медицини, проте потребує подальшого тестування. Наступні кроки дослідження передбачають перевірку результатів на реальних даних, інтеграцію механізмів Explainable AI для підвищення інтерпретованості прогнозів, а також адаптацію алгоритму для інших груп захворювань.

Література

1. Johnson, A. E. W., Pollard, T. J., Shen, L., et al. «MIMIC-III, a freely accessible critical care database». Scientific Data, 2016.
2. Bahdanau, D., Cho, K., Bengio, Y. «Neural machine translation by jointly learning to align and translate». arXiv, 2014.
3. Hochreiter, S., Schmidhuber, J. «Long short-term memory» Neural Computation, 1997.
4. Choi, E., Bahadori, M. T., Searles, E., et al. «RETAIN: An interpretable predictive model for healthcare using reverse time attention mechanism». NeurIPS, 2016.
5. Kingma, D. P., Ba, J. «Adam: A method for stochastic optimization». arXiv, 2014.

УДК 004.4
О. А. Ковальчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТИПИ ШКІДЛИВИХ ПРОГРАМ ДЛЯ ANDROID

UDC 004.4
O. A. Kovalchuk

TYPES OF ANDROID MALWARE

Системи виявлення шкідливих застосунків досить поширені, вони входять до складу антивірусних засобів, є частиною великих сервісів, що взаємодіють зі сторонніми програмами, наприклад, таких, як Google Play. Тому такі системи мають високу цінність як для дослідників, так і для компаній, що їх використовують.

Прийнято виділяти такі методи виявлення шкідливих застосунків: статичний; динамічний; гібридний.

Системи виявлення шкідливих застосунків, засновані на машинному навчанні, маючи можливість працювати як на основі результатів статичного, так і динамічного аналізу, а отже, і гібридного, є потужним, розширюваним і найефективнішим інструментом на даний момент. У зв'язку з цим такі системи активно розвиваються і вдосконалюються , а дослідники намагаються досягти їх найбільшої точності виявлення, застосовуючи різні методи машинного навчання.

При розгляді питання безпеки мобільних пристроїв не можна не згадати про типи шкідливих програм. Google виділяє 14 категорій, що стосуються Android пристроїв [1]. Вони входять як стандартні типи шкідливих застосунків:

- використовують чорні ходи;
- викликають відмову в обслуговуванні;
- завантажувачі;
- здійснюють фішинг;
- підвищують привілеї;
- здирники;
- розсилають спам;
- шпигунські програми;
- троянські програми

Так і типи, що стосуються конкретно платформи або мобільних пристроїв загалом:

- програми-шахраї з виставленням рахунків - це тип шахрайства з відправкою платних SMS- повідомлень, здійсненням дорогих дзвінків та підпискою на платні телефонні послуги;
- комерційне шпигунське програмне забезпечення - призначені для стеження за пристроєм, передачі особистої інформації з пристрою без повідомлення та згоди користувача;
- програми, що виконують рутинг, тобто отримання пристроєм прав суперкористувача root, без попередження;
- програми, що містять нестандартну для Android пристрою шкідливу функціональність, а також містять загрози для інших форм плат.

Література

1. Malware categories. [Електронний ресурс] - Режим доступу: https://developers.google.com/android/play-protect/phacategories (дата звертання: 03.11.24).

УДК 004.93
Н. М. Колачик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕТОДІВ РОЗРОБКИ ГОЛОСОВИХ АСИСТЕНТІВ ДЛЯ СМАРТ-СИСТЕМ ІЗ МОЖЛИВІСТЮ СПРИЙНЯТТЯ ЕМОЦІЙ КОРИСТУВАЧА

UDC 004.93
N. M. Kolachyk

RESEARCH ON THE DEVELOPMENT OF VOICE ASSISTANTS FOR SMART SYSTEMS WITH EMOTION RECOGNITION CAPABILITIES

У сучасному світі голосові асистенти стали невід'ємною частиною смарт-систем, забезпечуючи зручну взаємодію між користувачами і пристроями. Однак для підвищення ефективності та природності такої взаємодії важливо, щоб асистенти могли розпізнавати та реагувати на емоційний стан користувача. Це вимагає інтеграції методів обробки природної мови, машинного навчання та афективних обчислень.

Методи розробки голосових асистентів зі сприйняттям емоцій:

1) Обробка природної мови – дозволяє системам розуміти та генерувати людську мову. Для розпізнавання емоцій використовуються алгоритми, які аналізують тон, контекст та семантику висловлювань, визначаючи емоційне забарвлення повідомлень.

2) Машинне навчання та глибокі нейронні мережі – застосування моделей глибокого навчання, таких як рекурентні нейронні мережі та довготривала короткочасна пам'ять, дозволяє ефективно обробляти послідовності даних. Використання моделей машинного навчання на великих наборах даних покращує розуміння голосових команд та дозволяє точно виявляти емоційні патерни у мовленні.

3) Афективні обчислення – ця галузь спрямована на розробку систем, здатних розпізнавати, інтерпретувати та реагувати на людські емоції. Використання методів афективного аналізу для обробки акустичних характеристик мовлення (гучність, тональність, паузи) дозволяє підвищити ефективність голосових асистентів [1].

Для ефективного розпізнавання емоцій необхідне поєднання кількох методів збору даних. Голосові асистенти можуть аналізувати акустичні дані мовлення, але також можуть використовувати додаткові сенсори для збору інформації про мікровирази обличчя, біометричні показники (температура тіла, частота серцебиття) та невербальні сигнали. Такий мультиканальний підхід дозволяє досягти високої точності у визначенні емоцій користувача.

Застосування емоційного інтелекту дозволяє голосовим асистентам не лише ідентифікувати емоційний стан, а й адаптувати свою поведінку відповідно до ситуації. Наприклад, при виявленні стресу або незадоволеності у голосі користувача, система може запропонувати заспокійливу реакцію або допомогу. Важливим є також використання синтезованої мови, яка здатна передавати певний емоційний тон, щоб підтримати більш природний діалог.

Розробка голосових асистентів зі сприйняттям емоцій стикається з низкою викликів, включаючи: точність розпізнавання емоцій (індивідуальні особливості мовлення, діалектів та культурних відмінностей ускладнюють створення універсальних моделей), обчислювальні ресурси (емоційно чутливі системи вимагають великих обсягів даних та потужних обчислювальних ресурсів, що потребує оптимізації алгоритмів для роботи у реальному часі), етичні аспекти (збір та обробка емоційних даних піднімає питання конфіденційності та етики використання персональної інформації).

Незважаючи на ці виклики, впровадження емоційного інтелекту у голосові асистенти створює нові можливості для глибшого розуміння користувачів та побудови більш інтуїтивних систем. Такі асистенти мають потенціал для широкого застосування у медичній сфері, освіті, розважальних системах та в бізнес-середовищі [2].

Література

1. E-chat: Emotion-sensitive Spoken Dialogue System with Large Language Models. arXiv. URL: https://arxiv.org/abs/2401.00475.
2. Emotion Recognition in Voice Assistants Using Deep Learning and Affective Computing. IEEE Xplore. URL: https://ieeexplore.ieee.org/abstract/document/10226198.

УДК 338
В. Колижнюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ СУЧАСНОГО ЦИФРОВОГО ІНСТРУМЕНТАРІЮ ДЛЯ ПРОГНОЗУВАННЯ

UDC 338
V. Kolyzhniuk

USING MODERN DIGITAL TOOLS FOR FORECASTING

В період цифрових трансформацій важливо не лише розуміти сутність прогнозування, але й використовувати сучасні інструменти. На сьогодні створено та функціонує цифровий інструментарій для прогнозування, наприклад, платформа на основі штучного інтелекту Streamline для прогнозування попиту (рис. 1.)

Використання даної платформи дозволяє знизити рівень запасів до 50%, націлене на забезпечення довгострокового ROI із найвищим рівнем, знижує можливість відсутності потрібного виду запасу до 2%.

Для розробки прогнозів можна скористатися такими опціями:

- Вибір методу прогнозування;
- Вибір типу моделі;
- Включення/ігнорування періодів прогнозу;
- Врахування днів без торгів (для біржових прогнозів);
- Використання критерію цінової еластичності попиту;
- Врахування сезонності;
- Врахування вторинних чинників впливу.

Для врахування коливань бізнесу на сонові аналітики ланцюгів поставок та сценарної симуляції “What-IF” розроблено хмарний програмний сервіс SAP Integrated Business Planning for Supply Chain (SAP IBP). Також програма дозволяє встановити ряд припущень, які будуть враховані при розробці прогнозних сценаріїв та сформувати консенсус-прогноз, шляхом об’єднання прогнозованих даних, отриманих із використанням різних методик (рис. 1.6).

Дана програма дозволяє розробити прогнозні сценарії на основі методів моделювання із використанням ШІ із визначенням прогнозних значень обсягів попиту як загалом, так і за окремими сегментами, а також порівняти планові та досягнуті показники через візуалізацію даних Рис. 1.5 Програма SAP IBP, візуалізація з екрану

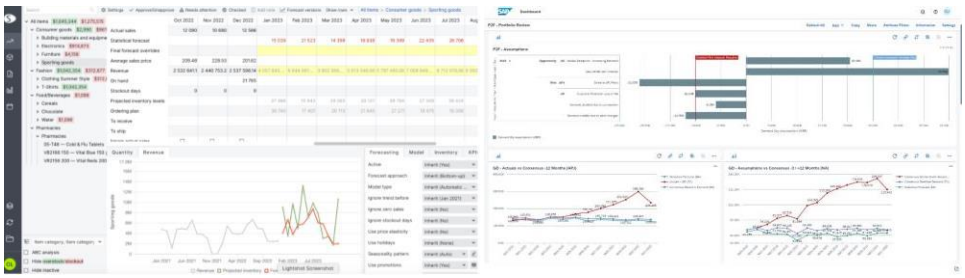


Рисунок 1. Платформа Streamline та програм SAP IBP, візуалізація з екрану

Література

1. Офіційний сайт Streamline. URL: https://gmdhsoftware.com/ua/
2. Офіційний сайт SAP IBP URL:https://www.sap.com/products/scm/integrated-business-planning. html

УДК 004.056.53
М. Кончак
(Тернопільський національний технічний університет імені Івана Полюя, Україна)

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВЕБ ДОДАТКІВ ВІД КІБЕРАТАК

UDC 004.056.53
M. Konchak

ANALYSIS OF METHODS FOR PROTECTING WEB APPLICATIONS FROM CYBER ATTACKS

З розвитком цифрових технологій веб-додатки стали важливою частиною сучасної інформаційної інфраструктури. Їх використання супроводжується ризиками кібератак, які можуть призвести до значних фінансових, репутаційних та інформаційних втрат.

Основні типи атак (згідно з рейтингом OWASP Top 10, 2024):

1. SQL-ін’єкції. Атаки, спрямовані на маніпулювання запитами до бази даних.
2. XSS-атаки (Cross-Site Scripting). Використовують уразливості для виконання шкідливих скриптів.
3. DDoS-атаки (Distributed Denial of Service). Перевантаження серверів з метою порушення їхньої роботи.

Методи захисту:

1. Валідація та фільтрація даних. Забезпечення коректної обробки вхідних даних.
2. Використання міжсайтових політик (CSP). Обмеження джерел виконання скриптів.
3. Шифрування даних. Захист переданої інформації за допомогою протоколів HTTPS.
4. Регулярні оновлення програмного забезпечення. Усунення відомих уразливостей.
5. Використання WAF (Web Application Firewall). Виявлення та блокування підозрілих запитів.

Аналіз сучасних методів захисту веб-додатків свідчить про необхідність комплексного підходу до кібербезпеки, який включає як технологічні рішення, так і організаційні заходи. Забезпечення безпеки веб-додатків є ключовим аспектом у захисті цифрових активів організацій.

Література

1. OWASP. *Top 10 Web Application Security Risks*. 2024.
2. Stallings W. *Network Security Essentials: Applications and Standards*. Pearson, 2022.
3. Symantec. *Internet Security Threat Report*. 2023.

УДК 004.056
М. Копач; Ю. Скоренький, к.ф.-м.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ ЦИФРОВИХ ДВІЙНИКІВ ВИРОБНИЧИХ ЛІНІЙ МЕТАЛООБРОБНИХ ПІДПРИЄМСТВ

UDC 004.056
M. Kopach; Yu. Skorenkyy, Ph.D., Assoc. Prof.

STUDY OF VULNERABILITIES OF DIGITAL TWINS OF THE METAL PROCESSING ENTERPRIZES

Ключові слова: інформаційна безпека, промисловий інтернет речей, вразливості.
Key words: information security, industrial internet of things, vulnerability.

Поява Інтернету речей (Internet of Things, IoT) проклала шлях до нових можливостей для вдосконалення промислових процесів за допомогою інтеграції та складного керування машинами та приводами, обладнаними датчиками. У технологічних процесах промисловий Інтернет речей дає виробникам можливість отримати всебічне уявлення про кожен етап виробничого процесу, сприяючи коригуванням у реальному часі для забезпечення безперебійного виробництва та зниження ймовірності дефектів і збоїв, спричинених людськими помилками, відповідно до принципів Індустрії 4.0. Позитивні наслідки інтелектуального виробництва виходять за рамки виробничих операцій, обладнання та оптимізації запасів. Цифрові близнюки (Digital Twin, DT), які широко використовуються в Індустрії 4.0 для моделювання та керування виробничими процесами [1], є віртуальними копіями фізичних об’єктів або систем. Перевага використання цифрових двійників для малого та середнього бізнесу полягає в можливості оптимізувати виробничі процеси, забезпечити навчання персоналу та розширити можливості моделювання, виправдовуючи розробку ресурсомісткого, але важливого програмного забезпечення, призначеного для моделювання та навчання.

Для металообробного виробництва з високим рівнем цифровізації промислове моделювання на основі даних дозволяє розробити відповідну архітектуру цифрового двійника. Зібрані дані та оброблена інформація є цінним бізнес-активом, тому необхідно розробити та вжити відповідних заходів безпеки.

В даній роботі представлено аналіз вразливостей [2] промислових цифрових двійників, які можуть суттєво вплинути на безпеку цих інформаційних систем.

Література

1. Skorenky Yu. et al. Development of digital twin interface for Industry 4.0 production line. CEUR Workshop Proceedings, 2024, 3742, pp. 358–369
2. R. Khan, K. McLaughlin, D. Laverty, S. Sezer. STRIDE-based Threat Modeling for Cyber-Physical Systems. In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings Institute of Electrical and Electronics Engineers Inc. (2018) 1-6. URL: https://doi.org/10.1109/ISGTEurope.2017.8260283

УДК 681.518.3
А. В. Кондратюк; Я. В. Литвиненко, д.т.н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОГРАМНІ ІНСТРУМЕНТИ ДЛЯ МОДЕЛЮВАННЯ ЦИКЛІЧНИХ СИГНАЛІВ

UDC 681.518.3
A. V. Kondratiuk; Ia. V. Lytvynenko Dr., Prof.

PROGRAMMING TOOLS FOR CYCLIC SIGNALS SIMULATION

Циклічні сигнали, відібрані від пацієнтів, які досліджуються в медицині є важливими для діагностики та моніторингу стану людини. При цьому вагомими факторами, які можуть впливати на коректність інтерпретації результатів діагностування є наявність певних артефактів, які можуть бути викликані: диханням пацієнта; електричними завадами мережі; рухом пацієнта під час їх відбору; втратою контакту електродів з тілом пацієнта та іншими чинниками. Програмне забезпечення, яке дозволяє проводити моделювання циклічних сигналів з врахуванням артефактів надає можливості для більш глибокого і якісного їх дослідження.

Дана теза стосується програмних інструментів для моделювання циклічних біомедичних сигналів. Розглянемо їх.

GNU Octave є, порівняно, низькорівневим відкритим програмним забезпеченням, сумісним з MATLAB, що дозволяє виконувати числові обчислення та моделювання сигналів з використанням скриптів на мові програмування MATLAB або з використанням спеціалізованого синтаксису – Octave. Ключовими можливостями є використання скриптів для моделювання та обробки, це дозволяє використовувати додаткові пакети, які розширюють можливості роботи з медичними сигналами.

ECGSIM - симулятор, який дозволяє генерувати реалістичні ЕКГ сигнали з можливістю налаштування параметрів та інтеграцією артефактів. Застосовується для перевірки ефективності методів обробки сигналів і дозволяє моделювати штучні данні.

Крім того існують спеціалізовані бібліотеки для моделювання медичних сигналів для різних мов і платформ. Наприклад, NumPy та SciPy: основні бібліотеки для наукових обчислень та обробки сигналів, BioSPPy: спеціалізована бібліотека для обробки біомедичних сигналів, включаючи ЕКГ та ЕЕГ. MNE: бібліотека для аналізу нейрофізіологічних даних, зокрема ЕЕГ та MEG сигналів. PyWavelets: для вейвлет-перетворень та великомасштабного аналізу сигналів.

Всі згадані бібліотеки і програмні інструменти є або низькорівневими для створення вузьконаправлених, спеціалізованих рішень або орієнтуються на конкретні типи сигналів. Тому, наявність універсального інструменту, який дозволятиме моделювати широке коло циклічних сигналів потребує розробки. Такий інструмент може спростити аналіз систем для діагностування стану здоров’я пацієнтів і сприятиме розвитку сфери їх опрацювання загалом. Адже моделювання таких сигналів з урахуванням можливих артефактів надасть більше інформації, візуалізуючи ключові аспекти і підвищить результативність і якість медицини вцілому.

Література

1. Стадник Н. Б. Моделювання та ефективні методи опрацювання циклічних сигналів на базі ізоморфних циклічних випадкових процесів. Дисертація, кандидат технічних наук, 01.05.02, Тернопільський національний технічний університет імені Івана Пулюя. Тернопіль, 2021.
2. Литвиненко Я.В. Методи ідентифікації сегментної та ритмічної структур циклічних сигналів в системах цифрової обробки даних: автореф. дис. … докт. техн. наук: 01.05.02. Тернопіль, 2019. 44 с.

.

УДК 004.92
В. І. Корнилів
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АВТОМАТИЗАЦІЯ ФОТОГРАММЕТРІЇ З AGISOFT METASHAPE

UDC 004.92
V. I. Kornyliv

AUTOMATION OF PHOTOGRAMMETRY USE AGISOFT METASHAPE

Фотограмметрія – це метод створення точних вимірювань та моделей 3D-об'єктів на основі фотографій. Автоматизація фотограмметрії - це використання сучасних технологій та інструментів, таких як штучний інтелект, машинне навчання та автоматична обробка зображень для автоматизації процесу створення цифрових моделей об'єктів на основі фотографій. Однією з основних переваг автоматизації фотограмметрії є прискорення процесу створення цифрових моделей об'єктів. Автоматична обробка зображень може бути використана для швидкого і точного виявлення ключових точок на фотографіях, що дозволяє прискорити процес створення моделей. Автоматизація фотограмметрії також може бути корисною для виявлення пошкоджень та деформацій об'єктів. Однак, незважаючи на переваги, автоматизація фотограмметрії також має обмеження. Наприклад, деякі об'єкти можуть мати складну форму або поверхню, які можуть бути важко оброблені автоматично. Крім того, автоматизація фотограмметрії може вимагати значних інвестицій у технології та навчання фахівців

Існують різне програмне забезпечення (ПЗ) для обробки зображень та створення тривимірних моделей. Деякі з них можуть автоматично обробляти зображення та створювати тривимірні моделі, використовуючи комп'ютерний зір та алгоритми комп'ютерного зору.

Одним з таких програмних комплексів є Agisoft Metashape – комерційне ПЗ, яке використовує методи SfM та multi-view стерео (MVS) для створення 3D-моделей. Він може обробляти великі набори даних та надає розширені функції, такі як фотореалістичне текстурування, інструменти вимірювання та інтеграція з геоінформаційною системою. Також пропонує зручний інтерфейс та велику документацію, що робить його популярним вибором для професіоналів у галузі фотограмметрії.

Agisoft також має досить складний інтерфейс користувача, який може бути корисний для складних проектів. Ще однією перевагою Agisoft є його здатність обробляти складніші умови освітлення та налаштування камери, що робить його ідеальним для проектів на відкритому повітрі.

Однак одним із недоліків Agisoft є його відносно висока ціна, що може стати перешкодою для деяких користувачів. Крім того, Agisoft може бути складнішим у використанні, порівняно з іншим ПЗ, і може знадобитися додаткове навчання та досвід, щоб максимально використовувати його функції.

Незважаючи на всі наведені переваги, функціонал програми може бути доповнений для більш швидкого та зрозумілого використання. Однак часто потрібно лише поліпшити або розширити функціонал існуючого програмного комплексу Agisoft Metashape. Хоча Agisoft Metashape, отже, містить у собі велику кількість інструментів для вирішення різноманітних задач фотограмметрії, все одно залишається поле для покращення та автоматизації процесів.

Література

1. Discover intelligent photogrammetry with Metashape [Електронний ресурс]. – Режим доступу: https://www.agisoft.com/ / (дата звертання: 04.12.2024)

УДК 004.4
А. Р. Комендат; Т. А. Лечаченко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ТЕХНОЛОГІЙ ЗАХИСТУ ВЕБ САЙТІВ

UDC 004.4
A. R. Komendat; T.A. Lechachenko

ANALYSIS OF WEB SITE PROTECTION TECHNOLOGIES

Веб-сайти є основою сучасного цифрового середовища, об'єднуючи бізнес, науку, освіту, розваги та інші сфери діяльності. Зі зростанням значення цифрової присутності для компаній і організацій, удосконалення веб-сайтів стало ключовим завданням для забезпечення їх ефективності, доступності та безпеки. Інформаційні технології (IT) виступають рушійною силою цих змін, забезпечуючи інструменти для всебічного аналізу, оптимізації та захисту веб-ресурсів.

Зростання кількості атак на веб-сайти, спрямованих на викрадення даних, злам систем або виведення ресурсів із ладу, вимагає впровадження сучасних рішень для забезпечення безпеки. Системи WAF (Web Application Firewall) дозволяють блокувати підозрілі запити в реальному часі, запобігаючи SQL-ін'єкціям, XSS-атакам та іншим загрозам. Використання SSL/TLS забезпечує шифрування даних, що передаються між сервером і клієнтом, запобігаючи їх перехопленню [1].

Одним із найбільш ефективних способів захисту користувачів веб-сайту – є впровадження багатофакторної автентифікації. Наприклад, користувач під час входу на сайт вводить свій логін і пароль, після чого система запитує одноразовий код, згенерований додатком Google Authenticator. У разі компрометації пароля зловмисник не зможе отримати доступ без цього додаткового коду [2].

Впровадження штучного інтелекту в системи кібербезпеки відкриває нові можливості для захисту веб-ресурсів. Алгоритми машинного навчання дозволяють виявляти нові типи загроз, аналізуючи поведінку трафіку та патерни атак. Наприклад, технології Deep Packet Inspection, що застосовуються у продуктах компаній, таких як Palo Alto Networks, здатні розпізнавати складні кіберзагрози [3].

Удосконалення захисту веб-сайтів за допомогою сучасних інформаційних технологій є основою їхньої стабільної роботи та довіри користувачів. Використання автоматизованих систем, машинного навчання, регулярний аудит і навчання персоналу забезпечують багаторівневий підхід до безпеки, що дозволяє запобігти більшості сучасних загроз. Тільки комплексні заходи зможуть гарантувати ефективність, надійність і захист веб-ресурсів у цифрову епоху.

Література

1. Гришина І. П., Коваленко А. С. «Сучасні методи забезпечення безпеки веб-додатків: теоретичний аналіз і практичні рекомендації». [Електронний ресурс]: journals.dut.edu.ua/index.php/dataprotect. Доступ: 05.12.2024. У статті розглядаються основні технології, включаючи SSL/TLS та WAF, як ефективні інструменти для запобігання сучасним кіберзагрозам
2. Добринін І.С., Пшеничних С.В. «Аналіз методів автентифікації для вебзастосунків та реалізація системи автентифікації». [Електронний ресурс]: ITSSI Journal. Доступ: 05.12.2024. У статті досліджуються сучасні технології багатофакторної автентифікації, включаючи Google Authenticator.
3. Савченко В. А., Шаповаленко О. Д. «Основні напрями застосування технологій штучного інтелекту у кібербезпеці». [Електронний ресурс]: journals.dut.edu.ua/index.php/sciencenotes. Доступ: 05.12.2024.

УДК 004.77
К. Костюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА МЕТОДОЛОГІЇ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ АГРОХОЛДИНГУ

UDC 004.77
K. Kostiuk

DEVELOPMENT OF A METHODOLOGY FOR INFORMATION SECURITY RISK ASSESSMENT FOR AN AGRICULTURAL HOLDING

Швидкий розвиток цифрових технологій в аграрному секторі відкриває нові можливості, але водночас збільшує вразливість до інформаційних загроз. Інциденти в інформаційній безпеці можуть мати серйозні наслідки для бізнесу: фінансові втрати, збої у виробничих процесах і погіршення репутації. У таких умовах постає необхідність розробки методології оцінки ризиків, яка враховувала б специфіку агрохолдингів, зокрема їхню залежність від технологій, сезонність операцій і широке використання автоматизованих систем.

Запропонована методологія побудована на основі аналізу сучасних підходів, таких як ISO/IEC 27005 [1], NIST [2], DoCRA [3] і інших визнаних стандартів, адаптованих до потреб аграрного бізнесу. Її мета – забезпечити системний підхід до управління ризиками, який дозволяє врахувати баланс між безпекою та ефективністю бізнес-процесів.

Особливістю методології є структурований підхід до ідентифікації активів, загроз і вразливостей, оцінки їхнього впливу та надання рекомендацій щодо пріоритетності заходів управління ризиками. Вона базується на принципах, що узгоджуються з міжнародними стандартами безпеки, та орієнтована на відповідальне управління ризиками з урахуванням бізнес-цілей організації [4].

Апробація методології на прикладі одного з провідних агрохолдингів України дозволила провести комплексну оцінку ризиків інформаційної безпеки. У результаті було ідентифіковано ключові загрози, визначено їхній вплив на критичні активи та надано рекомендації щодо пріоритетів у подальшому управлінні ризиками [5].

Запропонована методологія демонструє високу ефективність у контексті аграрного бізнесу, забезпечуючи можливість комплексної оцінки ризиків, оптимального планування заходів безпеки та підвищення стійкості інформаційних систем. Її впровадження сприяє мінімізації ризиків і забезпечує стабільність бізнес-процесів в умовах сучасних небезпек.

Таким чином, запропонована методологія демонструє високу ефективність у контексті аграрного бізнесу, забезпечуючи комплексний підхід до управління ризиками інформаційної безпеки. Її впровадження сприятиме мінімізації втрат від кіберзагроз, забезпеченню стабільності операційної діяльності та підвищенню конкурентоспроможності компанії.

Література

1. ISO/IEC 27005:2018 Information Security Risk Management. URL: https://www.iso.org/standard/75281.html.
2. NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments. URL: https://csrc.nist.gov/pubs/sp/800/30/r1/final.
3. The Duty of Care Risk Analysis Standard. URL: https://www.docra.org/.
4. Critical Asset Identification. URL: https://www.emagined.com/blog/critical-asset-identification.
5. CRR Implementation Guide Asset Management FINAL. URL: https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf.

УДК 004.4
Ю. Р. Курчак
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОДЕЛЮВАННЯ ТА АНАЛІЗ СИСТЕМИ РЕКОМЕНДАЦІЙ НА ВЕБ-САЙТІ НА ОСНОВІ ТЕОРІЇ ГРАФІВ І СТАТИСТИЧНИХ АЛГОРИТМІВ

UDC 004.4
Y. R. Kurchak

MODELING AND ANALYSIS OF A WEBSITE RECOMMENDATION SYSTEM BASED ON GRAPH THEORY AND STATISTICAL ALGORITHMS

Веб-сайти потребують інтеграції ефективних систем рекомендацій для персоналізації взаємодії користувачів. У цьому проекті основою є Python та його фреймворки Flask або Django, що забезпечують швидку розробку, гнучкість і потужні можливості інтеграції алгоритмів машинного навчання [1]. База даних буде на основі PostgreSQL або MySQL, що забезпечить зберігання та доступ до великих обсягів даних.

Система працює за рахунок обробки даних про взаємодії користувачів із контентом. Дані, такі як перегляди, оцінки чи історія покупок, зберігаються в базі та аналізуються [3]. Основою є методи колаборативної фільтрації, що порівнюють користувачів або об'єкти для пошуку схожостей. Для виявлення груп схожих об'єктів та користувачів використовуються графові алгоритми, наприклад, PageRank чи Louvain для кластеризації [2].

Гібридний підхід поєднує аналіз поведінкових даних із характеристиками контенту, що дозволяє покращити точність рекомендацій і зменшити проблему «холодного старту» [4]. Особливий акцент зроблено на впровадженні методів факторизації матриць, для пошуку прихованих взаємозв'язків між користувачами та контентом. Алгоритми реалізовуються за допомогою бібліотек, зокрема Scikit-learn, Pandas і NumPy.

Ключовими перевагами системи є її здатність підвищувати зручність користувачів і збільшувати конверсії завдяки точним рекомендаціям. Разом із тим, виклики включають обробку великих обсягів даних та забезпечення конфіденційності користувачів. Для вирішення цих завдань буде використано масштабовані обчислення за допомогою хмарних сервісів, таких як AWS або Google Cloud.

Проект демонструє, як інтеграція сучасних алгоритмів, таких як машинне навчання, графові моделі та кластеризація, дозволяє створити ефективну рекомендаційну систему. Завдяки цьому веб-сайт стає не лише інструментом доступу до контенту, а й платформою для глибшого розуміння потреб користувачів та їхньої поведінки [5].

Література

1. Ben Shaw. Web Development with Django: Learn to build modern web applications with a Python-based framework / Ben Shaw, 2021 – с. 826
2. Francesco Ricci, Lior Rokach, Bracha Shapira. Recommender Systems Handbook / Ricci, Lior Rokach, Bracha Shapira 2011 – с. 842 (Довідник по рекомендаційних системах).
3. Персональні рекомендації та як вони працюють [Електронний ресурс]: https: //brander.ua/blog/personalni-rekomendacii-yak-ce-pracyue. Доступ до ресурсу: 28.11.2024
4. Аналіз поведінки користувача на веб-сайті [Електронний ресурс]: https://www.promodo.ua/ blog/5-prostih-krokiv-z-analizu-povedinki-pokupciv-na-sayti. Доступ до ресурсу: 28.11.2024
5. Luis Serrano. Grokking Machine Learning / Luis Serrano, 2021 – с. 512.

УДК 004.6
В. А. Лабчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ MICROSOFT LINQ ДЛЯ ЗАДАЧ КОНСОЛІДАЦІЇ ДАНИХ

UDC 004.6
V. A. Labchuk

RESEARCHMENT OF THE DATA CONSOLIDATION TASKS' OPPORTUNITIES WITH THE HELP OF USING MICROSOFT LINQ TECHNOLOGY

При консолідації даних з різних ресурсів постає питання роботи з даними різних форматів і приведення їх до єдиного. LINQ вміє працювати з різними джерелами даних, зокрема отриманих у вигляді наборів даних (зокрема з CSV-файлів), сутностей (описуються класами), баз даних, xml-файлів тощо. Для цього існують відповідні імплементації LINQ to SQL, LINQ to XML, LINQ to Dataset, LINQ to Entities. Хоча на сьогодні велика частина інформації зберігається у базах даних, однак звісно далеко не вся. До того ж дані можуть бути як структурованими, так і напівстрктурованими, і нестрктурованими взагалі [1].

Для роботи з LINQ може використовуватися два C# інтерфейси – IEnumerable та IQueryable. Перший підходить для ітерації колекцією об'єктів, другий – для зовнішніх ресурсів, наприклад роботи з базою даних. В даному випадку LINQ не обмежується лише Microsoft SQL Server, але й може працювати з іншими постачальниками даних. Тобто фактично LINQ створює абстракцію рівня доступу до даних. При цьому запити можна створювати в SQL-подібному стилі або ж за допомогою методів розширення. Microsoft рекомендує застосовувати саме методи розширення в ситуаціях коли це можливо [2].

Насправді на цьому можливості LINQ не закінчуються і є можливість інтегруватися і з іншими технологіями для отримання даних. Однак деякі зі специфічних розширень можуть постачатися третіми сторонами. Зокрема можна згадати LINQ to Twitter для взаємодії з відповідною соцмережею, LINQ to Result (для підтримки залізнично-орієнтованого програмування в мові C#), LINQ to Anything. Останній варіант дозволяє перетворити будь-яке джерело даних у IQueryable для зручної взаємодії з ним [3].

Висновок. Досліджено можливості застосування технології Microsoft LINQ для задач консолідації даних. Ця мова дозволяє нам абстрагуватися від різноманіття форм даних, що надходять на вхід і сконцентруватися безпосередньо на роботі з даними, а отже може бути доцільним інструментом для використання в задачах консолідації даних. Для кращої продуктивності при об'єднанні великих масивів даних краще використовувати паралельну версію даного інструменту – PLINQ, однак це не варто робити при роботі на 1-ядерних пристроях та коли масиви даних незначні за обсягом.

Література

1. John Paul Mueller. LINQ for dummies. P.105-210. URL: https://srikanthkamuju.wordpress.com/wp-content/uploads/2011/05/free-ebooks-download-org-for-dummies-linq-for-dummies.pdf.
2. Marian Rusek, Jakub Maguza, Waldemar Karwowski. Integration of queries to heterogeneous data sources using LINQ technology. URL: https://www.infona.pl/resource/bwmeta1.element.baztech-4e4868a0-984f-4a92-8427-e08bcf08c1b4/content/partContents/c62cd082-38a8-387a-a04c-c481345a5313.
3. Harry McIntyre, Luke McGregor. LINQ to anything library. URL: https://github.com/mcintyre321/LinqToAnything.

УДК 004.6
В. А. Лабчук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПЕРЕВАГИ ТА НЕДОЛІКИ LINQ В ПОРІВНЯННІ З SQL-КОДОМ

UDC 004.6
V. A. Labchuk

PROS AND CONS OF USING LINQ INSTEAD OF RAW-SQL

Використання LINQ надає багато переваг в порівнянні з аналогічними запитами SQL. Такі запити більш високорівневі та інтегровані в мову програмування. Звідси слідує, що такий код компільований, а отже виявлення помилок відбувається під час компіляції, а не під час виконання. Крім того ризик SQL-ін'єкцій, тобто вставок, значно послаблюється, оскільки не використовується звичайне об'єднання значень рядків, значення дозволяється передавати в якості параметрів. А для вибірки даних з різних таблиць чи сутностей непотрібно з'єднувати таблиці, а достатньо викликати відповідну властивість цього об'єкту, що скорочує код. До того ж LINQ може працювати не лише зі структурованими даними з баз даних, але й наприклад зі слабкоструктурованими, що робить цю мову запитів універсальнішою [1].

Мова запитів LINQ зокрема застосовується і в інших інструментах MIcrosoft, наприклад, Entity Framework Core. Хоча дана технологія дозволяє використовувати і чистий SQL-код, однак необхідно враховувати доцільність цього в конкретній ситуації, а також пам'ятати про архітектуру програмного продукту. Враховуючи переваги мови запитів, в контексті архітектури в більшості випадків доцільніше використовувати саме її. Крім того її застосування підходить для здійснення архітектурних припущень, аналізу патернів використання та антипатернів [2].

Однак у мови запитів є і недоліки та ситуації, коли доцільніше використовувати код SQL. Наприклад, швидкість виконання запитів LINQ може бути нижчою ніж у запитів SQL. Крім того використання коду SQL потенційно може знадобитися для деяких складних запитів, а також його доведеться застосовувати для того, щоб використовувати тригери, тобто реакцію на якусь подію. Однак відсоток випадків, коли дійсно потрібно застосовувати SQL, є незначним, близько 5% [3].

Література

1. Harun Cerim. Extendind C# with a library of functional programming concepts.Md. Rashedul Islam, Aloke Kumar Shah, Md. Rofiqul Islam. Experimental evaluation of parallelism in real time execution. P. 15-22. Dspace. URL: https://dspace.cuni.cz/bitstream/handle/20.500.11956/121344/120370216.pdf?sequence=1&isAllowed=y.
2. Bartosz Frackowiak, Robert Dabrowski. Using LINQ as an universal tool for defining architectural assertions. Federated conference of computer science and information systems. URL: https://annals-csis.org/Volume_8/pliks/pliks/587.pdf.
3. Joseph Albahari. Why LINQ beats SQL. URL: https://www.linqpad.net/WhyLINQBeatsSQL.aspx.

УДК 519.6
С. В. Литвиненко, к.т.н., доц.; М. Є. Фриз
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МАТЕМАТИЧНЕ ЗАБЕЗПЕЧЕННЯ ТАРГЕТОВАНОЇ РЕКЛАМИ

UDC 519.6
S. V. Lytvynenko, Ph.D., Assoc. Prof.; M. E. Friz

MATHEMATICAL SUPPORT OF TARGETED ADVERTISING

Математичне забезпечення таргетованої реклами базується на використанні алгоритмів машинного навчання, оптимізації, статистики та теорії ймовірностей. Воно дозволяє ефективно аналізувати поведінку користувачів, сегментувати аудиторію та приймати рішення про покази рекламного контенту. Проведемо огляд ключових аспектів:

1. Сегментація аудиторії:

– Кластеризація. Використовується для поділу користувачів на групи за схожими характеристиками, застосовують наприклад метод K-середніх;

– Ієрархічна кластеризація (алгоритми агломерації чи поділу);

– DBSCAN: знаходить кластери за щільністю точок;

– Факторний аналіз: Метод зменшення кількості змінних для виявлення ключових факторів, що впливають на поведінку користувачів (наприклад, PCA).

2. Рекомендаційні системи:

– Матричний факторинг. Метод розкладання матриці взаємодії користувачів із контентом (лайки, перегляди);

– Колаборативна фільтрація: Метод користувачів використовує рекомендації які базуються на схожих користувачах. Метод предметів використовує схожість між елементами контенту. Гібридні методи поєднують в собі контентний аналіз та колаборативної фільтрації для точніших рекомендацій.

3. Алгоритми прогнозування:

– Регресійні моделі. Лінійна регресія та логістична регресія (для бінарних цілей, наприклад, кліки);

– Моделі класифікації. Тут застосовують: Дерева рішень, Random Forest; Градієнтний бустинг (XGBoost, LightGBM);

– Нейронні мережі (глибоке навчання для аналізу великих наборів даних).

4. Оптимізація реклами:

– Моделі аукціонів. Модель Generalized Second Price (GSP): У аукціонах типу Google Ads. – Програматик-аукціони (RTB). Використовується модель Vickrey-Clarke-Groves (VCG), де виграш залежить від ставки та внеску реклами в ефективність кампанії;

– Бюджетна оптимізація. Максимізація ROI (Return on Investment).

5. Моделювання поведінки користувачів:

– Аналіз часових рядів. Тут використовуються моделі для вивчення змін активності користувачів у часі;

– ARIMA: моделювання сезонних і трендових компонент;

– LSTM (рекурентні нейронні мережі): прогнозування поведінки користувачів у довгостроковій перспективі;

– Моделі Маркова. Описують імовірність переходів користувачів між різними станами (наприклад, клік, покупка).

6. Глибоке навчання для таргетованої реклами:

– Word2Vec та Doc2Vec для текстового аналізу (наприклад, опису товарів чи поведінкових патернів);

– Transformer-архітектури (BERT, GPT) для персоналізації та прогнозування текстової реклами;

– Графові нейронні мережі (GNN) для аналізу зв’язків між користувачами та контентом у соціальних мережах.

Математичне забезпечення таргетованої реклами використовує складні моделі аналізу та прогнозування поведінки користувачів, вибору оптимальних стратегій і максимізації прибутку. Основні акценти ставляться на персоналізації, прогнозуванні результатів і оптимізації бюджету, що базується на даних.

УДК 004.9
О. Ловчук; В. Дубельт; А. Лисий
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

KUBERNETES В ОБЧИСЛЮВАЛЬНІЙ ІНФРАСТРУКТУРІ РОЗУМНИХ МІСТ

UDC 004.9
O. Lovchuk; V. Dubelt; A. LYSYI

KUBERNETES IN THE SMART CITIES COMPUTING INFRASTRUCTURE

Розумні міста інтегрують обширні множини IoT-пристроїв. Це супроводжується зростанням навантаження обчислювальних і мережевих систем для забезпечення функціонування різнотипових «розумних» систем, як от моніторинг транспортних потоків, оперативне управління процесами енергоспоживання, контроль параметрів довкілля, інтелектуальні системи відеоспостереження та інші «розумні» служби. Інтеграція Kubernetes в обчислювальну інфраструктуру розумних міст дає змогу забезпечити гнучкість та масштабованість «розумних» цифрових сервісів, сприяючи при цьому підвищенню їх стійкості та надійності. Алгоритми планування в системах класу «розумне місто» здатні автоматично перемикати обчислювальні навантаження в разі відмови окремих вузлів або при виникненні непередбачуваних навантажень.

Kubernetes використовує декларативний підхід до керування програмно-алгоритмічними засобами, коли адміністратори чи користувачі вказують бажані стани програм, а система автоматично їх підтримує. Він також надає обширний перелік інструментів для моніторингу та керування застосунками, зокрема, програмно-алгоритмічні засоби для автоматичного виявлення збоїв та самовідновлення. Загалом Kubernetes пропонує гнучкі алгоритмічні рішення для керування контейнерними програмами у виробничих обчислювальних середовищах. Kubernetes підходить для веб-застосунків на основі мікросервісів. При цьому кожен компонент веб-систем можна запускати в окремому контейнері [1]. Завдяки легкості розгортання контейнерів, їх можна легко створювати та знищувати, забезпечуючи оперативне та високоефективне використання обчислювальних ресурсів. Kubernetes автоматизує процеси розгортання, масштабування та керування контейнерами в обчислювальному кластері, покращуючи використання ефективність і гнучкість виділення, використання та вивільнення різнотипових ресурсів. Це спрощує процедури створення та підтримки складних програмно-алгоритмічних комплексів. Крім стандартних стратегій планування Kubernetes, як от BestEffort або Burstable, для «розумних міст» можна використовувати спеціалізовані оригінальні стратегії планування, які базуються на характеристиках міської обчислювальної інфраструктури та його сервісних потребах [2]. Наприклад, планувальники можуть бути оперативно налаштовані для вибору окремих обчислювальних вузлів на основі географічного положення для забезпечення мінімального часу затримки або підвищення ефективності процесів обміну даними між регіонами. Водночас, алгоритми масштабування Kubernetes можуть бути модифіковані для інтеграції з системами прогнозування обчислювального навантаження.

Література

1. Senjab, Khaldoun, et al. «A survey of Kubernetes scheduling algorithms». Journal of Cloud Computing 12.1 (2023): 87.
2. Li, Hongjian, et al. «Cost-efficient scheduling algorithms based on beetle antennae search for containerized applications in Kubernetes clouds». The Journal of Supercomputing 79.9 (2023): 10300-10334.

УДК 004.032
О. Ловчук; Р. Катрич; В. Дуда
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АКТУАЛЬНІСТЬ ХМАРНОГО МАСШТАБУВАННЯ ТА KUBERNETES

UDC 004.032
O. Lovchuk; R. Katrych; V. Duda

THE RELEVANCE OF CLOUD SCALATION AND KUBERNETES

На даний час в процесі розширення хмарних платформ та послуг зростає потреба в підвищенні продуктивності інфраструктур центрів обробки даних. Високопродуктивні обчислення, передові мережеві рішення та стратегії динамічної оптимізації обчислювальних ресурсів зможуть допомогти персоналу центрів хмарного опрацювання даних забезпечувати високу швидкість та ефективність, що необхідні для надання високоякісних послуг [1]. При цьому однією з ефективних стратегій оптимізації хмарних обчислювальних процесів є запуск контейнерних програм. Він забезпечує покращення портативності програмно-алгоритмічних засобів, підвищення безпеки, прискорення перебігу процесів використання ресурсів, пришвидшення процедур розгортання та масштабування, а також покращення процесів інтеграції та взаємодії. Зазначені переваги зможуть допомогти установам та організаціям покращити протікання процесів розгортання застосунків, їх супроводу, обслуговування та керування, даючи змогу оперативніше та ефективніше реагувати на динамічні потреби бізнес-процесів.

Kubernetes – це система оркестровки контейнерів. Вона призначена для автоматизації процесів розгортання, масштабування та управління контейнерними програмно-алгоритмічними засобами. Однією з ключових її особливостей є функціональні можливості планувати процедур розгортання та виконання контейнерів у кластерах обчислювальних вузлів за допомогою алгоритмів планування [2]. Ці алгоритми визначають найкраще розміщення контейнерів на доступних обчислювальних вузлах у кластері. Система оркестрації контейнерів Kubernetes, пропонує можливість автоматизованого керування та масштабування цих розумних служб, забезпечуючи високі показники надійності та стійкості роботи за допомогою динамічного планування обчислювального навантаження. Тому алгоритми планування в Kubernetes для розумних міст є ключовими компонентами ефективного управління та розподілу ресурсів в міській обчислювальній інфраструктурі.

Тому актуальним напрямком сучасних досліжень є вичерпний аналітичний огляд різнотипових алгоритмів планування Kubernetes [1]. При дослідженні характеристик алгоритмів планування Kubernetes їх можна згрупувати у чотири підкатегорії:

- загальне планування;
- планування з підтримкою автоматичного масштабування;
- планування на основі багатоцільової оптимізації;
- орієнтоване на штучний інтелект планування.

Алгоритми планування Kubernetes функціонують на основі різнотипових параметрів, як от обчислювальні ресурси, мережеві вимоги, характеристики зв’язку та інші критерії.

Література

1. Senjab, Khaldoun, et al. «A survey of Kubernetes scheduling algorithms». Journal of Cloud Computing 12.1 (2023): 87.
3. Wen, Shilin, et al. «K8sSim: A Simulation Tool for Kubernetes Schedulers and Its Applications in Scheduling Algorithm Optimization». Micromachines 14.3 (2023): 651.

УДК 004.056
П. Луговський; І. Фалендиш
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИБІР ІНФОРМАТИВНИХ ОЗНАК ДЛЯ ЗАДАЧІ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ANDROID

UDC 004.056
P. Lugovskyi; I. Falendysh

SELECTION OF INFORMATIVE FEATURES FOR THE TASK OF ANDROID MALWARE DETECTION

Шкідливе програмне забезпечення для Android – це будь-яке шкідливе програмне забезпечення або код, призначений для завдання шкоди мобільному пристрою користувача Android, наприклад, віруси, трояни, програми-вимагачі, рекламне, шпигунське та інше. Таке шкідливе програмне забезпечення може бути завантажене або встановлене з різних джерел. Після проникнення шкідливого програмного забезпечення на мобільний телефон користувача Android, воно може виконати різні шкідливі дії, такі як крадіжка та продаж конфіденційної інформації, шпигунство за активністю на телефоні (наприклад, текстовими повідомленнями, дзвінками тощо) або вимагання викупу.

Загалом методи виявлення шкідливого програмного забезпечення діляться на три великі групи: статичні, динамічні та гібридні [1]. Як показує дослідження [2], методи машинного навчання виявились дуже перспективними для виявлення шкідливого програмного забезпечення для Android, оскільки вони можуть розпізнавати складні шаблони даних і навчатися на великих масивах даних. Алгоритми машинного навчання ідеально підходять для виявлення шкідливого програмного забезпечення для Android.

Вибір інформативних і незалежних ознак є вирішальним елементом ефективних алгоритмів розпізнавання образів, класифікації та регресії, а ознаки, як правило, є числовими. У нашому дослідженні з виявлення шкідливого програмного забезпечення для Android за допомогою динамічного методу ML на рівні API (Application Programming Interface), інтерфейс прикладного програмування було обрано як ознаку для навчання моделей машинного навчання, які будуть використані для класифікації того чи іншого додатка Android як шкідливого програмного забезпечення чи ні. Наприклад, якщо під час роботи мобільного додатку було викликано один API, то для цього API буде зазначено значення один для ознаки, що стосується цього додатку, або ж буде надано значення нуль. Специфікація API - це детальний опис, який допомагає розробнику використовувати такий інтерфейс для виконання певних вимог або функцій.

Інженерія ознак полягає у визначенні ознак для кращого представлення цільової задачі, яку розв’язує машинне навчання, і подальшого підвищення його точності. Зазвичай для цього використовуються знання з певної галузі або автоматизовані методи для вилучення, вибору або побудови правильних ознак. Для цього сценарію використання для виявлення шкідливого програмного забезпечення на Android ключовим фактором досягнення високої точності є вибір ознак, який, по суті, є вибором API в підході.

Література

1. Ashawa, Moses & Morris, Sarah. (2019). Analysis of Android Malware Detection Techniques: A Systematic Review. International Journal of Cyber-Security and Digital Forensics. No. 8. P. 177-187. 10.17781/P002605.
2. Chowdhury, Naseef & Haque, Ahshanul & Soliman, Hamdy & Hossen, Mohammad Sahinur & Ahmed, Imtiaz & Fatima, Tanjim. (2023). Android Malware Detection using Machine learning: A Review. 10.36227/techrxiv.22580881.v1.

УДК 004.77
В. Мазур
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ЗАХИСТУ ВІД КІБЕРАТАК НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

UDC 004.77
V. Mazur

AI-BASED METHODS FOR PROTECTION AGAINST CYBERATTACKS

У сучасному цифровому середовищі інформаційна безпека стає все більш важливою через стрімке зростання кількості та складності кіберзагроз. Особливою проблемою є атаки на основі штучного інтелекту (ШІ), які використовують потужні алгоритми машинного навчання, нейронні мережі та інші передові технології для обходу традиційних захисних систем. Ці атаки стають більш витонченими та адаптивними, що ускладнює завдання захисту інформаційних систем [1].

У результаті проведеного дослідження було здійснено глибокий аналіз сучасних методів атак на основі ШІ, таких як генеративні змагальні мережі (GANs), машинне навчання для DDoS-атак та нейронні мережі для обходу CAPTCHA [2]. Було встановлено, що ці інструменти дозволяють зловмисникам створювати реалістичні моделі атак, які можуть обходити традиційні системи захисту, що підвищує загрозу для критичної інфраструктури, корпоративних систем та персональних даних.

Для протидії таким атакам були розроблені ефективні методи захисту, що включають використання систем машинного навчання та глибокого навчання для виявлення аномалій у мережевому трафіку та поведінці користувачів [3]. Зокрема, було запропоновано застосування алгоритмів Random Forest та Support Vector Machines (SVM) для класифікації та виявлення DDoS-атак, а також впровадження генеративних моделей для розпізнавання підроблених фішингових листів та обходу CAPTCHA [4].

Експериментальні дослідження показали, що запропоновані методи забезпечують високу точність виявлення загроз, швидку адаптацію до нових типів атак та зниження кількості хибних спрацьовувань. Наприклад, інтеграція моделей машинного навчання дозволила зменшити ризик простою серверів на 95% та скоротити час реакції на атаки до 30 секунд [5].

Отримані результати дозволили створити гнучкі та ефективні системи захисту, здатні оперативно реагувати на еволюцію кіберзагроз на основі ШІ. Це підвищило загальний рівень безпеки інформаційних систем, забезпечуючи надійний захист від сучасних та майбутніх атак [6]. Таким чином, дослідження продемонструвало важливість використання штучного інтелекту для вдосконалення кіберзахисту та надання ефективних рішень у боротьбі з новими формами кіберзагроз.

Література

1. Аленічев, І.В. Штучний інтелект у кібербезпеці: сучасні підходи, 2015.
2. Бабенко, О.В. Методи захисту інформаційних систем на основі машинного навчання, 2021.
3. Барановський, П.О. Захист від DDoS-атак у мережах на основі штучного інтелекту, 2020.
4. Kim, J., Kim, H., & Kim, J. Deep Neural Networks for Cybersecurity, 2020.
5. Kshetri, N. Artificial Intelligence in Cybersecurity, 2021.
6. Li, W., et al. Network Intrusion Detection Using Machine Learning 2020.

УДК 004.02
М. Маланчук; Г. Козбур, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОГЛЯД ВІТЧИЗНЯНИХ АВТОМАТИЗОВАНИХ СИСТЕМ ДЛЯ НАДАННЯ ПЕРШОЇ МЕДИЧНОЇ ДОПОМОГИ З ВИКОРИСТАННЯМ ЧАТ-БОТІВ

UDC 004.02
M. Malanchuk; H. Kozbur, Ph.D., Assoc. Prof.

REVIEW OF DOMESTIC AUTOMATED SYSTEMS FOR FIRST AID USING CHATBOTS

У сучасному цифровому середовищі існує безліч чат-ботів, орієнтованих на надання медичних рекомендацій, що спрощують доступ до інформації в надзвичайних ситуаціях. Особливої уваги потребують рішення, здатні оперативно реагувати на симптоми користувача та надавати рекомендації щодо першої допомоги. Оскільки такі чат-боти є доступними цілодобово та забезпечують швидкий доступ до інформації, вони стають цінним інструментом у кризових ситуаціях.

Чат-бот «Друг. Перша допомога» орієнтований на надання першої психологічної допомоги, спираючись на науково обґрунтовані протоколи для підтримки ментального здоров'я [1]. Він забезпечує зручний у користуванні інтерфейс, що дозволяє оперативно заспокоїти користувача після стресових подій або травматичних ситуацій. Функціонування бота організовано в режимі 24/7, що надає користувачам безперешкодний доступ до рекомендацій у будь-який час. Однак цей бот фокусується винятково на психологічній підтримці, не охоплюючи питання фізичної допомоги чи базових медичних дій. Це обмеження може знижувати його корисність у ситуаціях, коли потрібна негайна фізична допомога.

Чат-бот «Турбота» виконує функцію посередника між пацієнтами та медичними працівниками, допомагаючи користувачам швидко знаходити фахівців для консультацій [2]. Він надає зручний спосіб пошуку медичних послуг, включаючи інформацію про доступні медичні заклади та лікарів. Проте чат-бот не пропонує миттєвих рекомендацій щодо першої допомоги; для отримання консультації користувачеві необхідно пройти кілька кроків, що може бути не зручним в екстрених ситуаціях, коли потрібна швидка медична порада.

Чат-бот «MedicalForUA_bot» також спрямований на надання медичних рекомендацій та допомогу у пошуку лікарів для користувачів. Його основна функція полягає у забезпеченні інформації з питань здоров'я та наданні консультацій з медичних тем [3]. Основний акцент робиться на допомозі у пошуку спеціалістів для подальшого лікування, тоді як функціонал не включає негайних інструкцій з надання першої допомоги. Таке обмеження може впливати на ефективність бота у критичних випадках, коли потрібна швидка реакція.

Пропонується розробка чат-боту для надання першої медичної допомоги, який поєднує в собі переваги існуючих рішень та має такі функціональні особливості: доступність у популярному месенджері Telegram, що забезпечує швидкий доступ до необхідної інформації; персоналізація, що здійснюється на основі використання сучасної класифікаційної моделі для точного аналізу симптомів; а також безкоштовність та відсутність реклами, що робить його зручним і доступним для користувачів.

Література

1. В Україні створили чатбот психологічної допомоги «Друг». URL: https://speka.media/v-ukrayini-stvorili-catbot-psixologicnoyi-dopomogi-drug-v53yzp (дата звернення 23.10.2024).
2. Як отримати медичну консультацію. Запрацював безкоштовний бот «Турбота». URL: https://ain.ua/2022/03/01/yak-otrymaty-medychnu-konsultacziyu-zapraczyuvav-bezkoshtovnyj-bot-turbota/ (дата звернення 23.10.2024).
3. Охорона здоров’я онлайн під час війни в україні. URL: http://amer.org.ua/wp-content/uploads/2023/E-Health-та-онлайн-сервіси-для-ВПО.pdf (дата звернення 23.10.2024).

УДК 004.02
М. Маланчук; Г. Козбур, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ДЛЯ НАДАННЯ ПЕРШОЇ МЕДИЧНОЇ ДОПОМОГИ З ВИКОРИСТАННЯМ ЧАТ-БОТА

UDC 004.02
M. Malanchuk; H. Kozbur, Ph.D., Assoc. Prof.

DEVELOPMENT OF AN AUTOMATED SYSTEM FOR PROVIDING FIRST AID USING A CHATBOT

В умовах сучасного суспільства оперативність надання першої медичної допомоги є критичною для збереження здоров'я та життя постраждалих. Інформаційна система, побудована на основі моделей класифікації, дозволить забезпечити автоматичне надання рекомендацій користувачам, що робить процес першої медичної допомоги швидким та доступним, особливо в екстрених випадках, коли важлива кожна хвилина.

Мета дослідження полягає у розробці системи надання автоматизованих рекомендацій з першої медичної допомоги реалізовану у формі чат-бота, для швидкого і доступного вирішення медичних потреб користувачів.

За основу роботи автоматизованої системи вибрано модель багатокласової класифікації з використанням методу стохастичного градієнтного спуску для максимальної ентропії (СГСМЕ, SDCA Maximum Entropy). Цей підхід забезпечує високу точність і стабільність при класифікації медичних симптомів, що вводяться користувачем, та дозволяє моделі ефективно аналізувати різні варіанти відповідей, знаходячи найбільш релевантну.

Метод СГСМЕ обрано завдяки його здатності ефективно вирішувати багатокласові задачі, що є особливо корисним у медичних класифікаціях. На основі введених користувачем симптомів модель прогнозує можливий стан здоров'я, враховуючи складні взаємозв’язки між симптомами. Це сприяє підвищенню точності у визначенні стану користувача.

Чат-бот на основі СГСМЕ аналізує введені користувачем симптоми як окремо, так і в комбінації з іншими симптомами. Це дозволяє системі передбачати можливі варіанти стану здоров'я та визначати найбільш імовірний діагноз. Модель класифікації використовує числові ознаки, що відповідають введеним симптомам, для прогнозування потенційних станів здоров'я.

Метод максимізації ентропії допомагає моделі враховувати невизначеність і складність даних, що підвищує точність класифікації в умовах відсутності чітких або комбінованих симптомів. Застосування стохастичного градієнтного спуску забезпечує ефективне навчання та оновлення моделі, що є важливим у випадках з обмеженими ресурсами, як у випадку Telegram-бота.

Для навчання моделі були зібрані та впорядковані дані з відкритих джерел, таких як посібники з надання першої допомоги та матеріали сайту «Рецептіка». Ці дані були об'єднані в єдиний файл, що містить інформацію для побудови класифікаційної моделі. На основі цього навчального набору модель досягла високих результатів точності, що відображають її ефективність у наданні медичної допомоги.

Бот досяг таких метрик на навчальному наборі даних: Log-loss – 4,02%, що вказує на низький рівень похибок; макроточність – 98,00%, яка підтверджує загальну якість класифікації для кожного класу; мікроточність – 98,00%, що відображає точність для всього набору, враховуючи дисбаланс між класами.

УДК 621.120.30
К. Марущак; В. Макар; А. Макар; П. Марущак, докт. техн. наук, проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЛАБОРАТОРНА АПРОБАЦІЯ МЕТОДУ ДЕФЕКТОСКОПІЇ ПОВЕРХНІ МЕТАЛОПРОКАТУ З ЗАСТОСУВАННЯМ ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖ

UDC 621.120.30
K. Marushchak; V. Makar; A. Makar; P. Maruschak, DSc., Prof.

LABORATORY TESTING OF THE METHOD OF DEFECTOSCOPY ON THE SURFACE OF ROLLED METAL PRODUCTS USING CNN

При діагностування металопрокату з допомогою оптико-цифрових методів слід враховувати відбиття, розсіювання, поглинання і ін. явища, пов’язані із взаємодією поверхні металопрокату із світловим випромінюванням. Важливим аспектом є врахування впливу умов освітлення металевої поверхні на фунціональність оптичної системи, зміну співвідношення «сигнал/шум» одержаних фотозображень, вплив на індикатрису розсіювання дефектів. Ще одним технологічним чинником впливу на якість контролю дефектності металопрокату є вібрація. Незважаючи на малі амплітуди та високі частоти вібрації поверхні металопрокату, на нашу думку вони вливають на точність діагностування розмірів дефектів, оскільки виникають «стрибання» зображення.

Під час даного дослідження розвинуто програмно-апаратний метод оцінювання впливу освітленості на ефективність розпізнавання дефектів металевої смуги з допомогою нейронних мереж, який ґрунтується на розробленій лабораторній установці та алгоритмах штучного інтелекту. Пропонований метод у поєднанні з цифровою зйомкою та обчислювальною технікою, дозволяє тестувати параметри систем технічного контролю дефектів металопрокату та оцінювати їх роботоздатність.

Розглянемо основні функціональні можливості експериментальної установки. На рухому котушку вібростенда, подавали синусоїдальну напругу амплітудою 0-30В від генератора низькочастотних коливань через аналоговий підсилювач класу АВ з вихідною потужністю до 100Вт та частотою 10-1000 Гц. При потребі, змінна напруга може мати трикутну чи пилкоподібну форму або форму прямокутних імпульсів. Це забезпечило циклічне вібрування досліджуваного металевого листа.

Сигнал вертикального циклічного переміщення металевого листа знімали та записували екстензометром моделі Bi-06-308 на ПК, які з’єднано з допомогою контролера моделі B1-07-005 (TESTRESOURSES ASIA BiSS, Індія). Наявність на ПК програмного забезпечення MTL32 Base Module дозволило візуалізувати сигнал та оцінити його параметри. Виявлення дефектів на поверхні металевої пластини було здійснено нейронною мережею з архітектурою U-net із енкодером на основі ResNet152, яка дозволяє сегментувати зображення, відносячи всі пікселі зображення до одного з двох класів ("пошкодження" чи "фон") [1].

Виявлено вплив низькоамлітудних циклічних вібрацій на параметри обчислених дефектів металопрокату. Проте, для дослідженої амплітуди (0,045 мкм) він мав випадковий характер, що на наш думку зумовлено малою амплітудою вібрування дослідженого металевого листа. В подальших працях автори спробують оцінити вплив вібрацій у широкому діапазоні значень амплітуд досліджуваного циклічного переміщення.

Література

1. І. Коноваленко, П. Марущак, Г. Козбур, О. Ясній Вплив частоти вібрацій та якості освітлення на кількісні показники дефектів, виявлених на поверхні металопрокату з застосуванням глибоких нейронних мереж // Праці Міжнародної науково-технічної конференції присвяченої 70-річчю від дня народження член-кореспондента НАН України, проф. Яснія Петра Володимировича «Міцність і довговічність сучасних матеріалів та конструкцій» 10–11 листопада 2022 року. – Тернопіль: ФОП Паляниця В. А., 2022. – С. 240–242.

УДК 004.62
С. Р. Миськів
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОГНОЗУВАННЯ ОБСЯГІВ СТВОРЕНИХ, ЗІБРАНИХ, СКОПІЙОВАНИХ І СПОЖИТИХ ДАНИХ У СВІТІ

UDC 004.62
S. R. Myskiv

FORECASTING THE AMOUNT OF DATA CREATED, COLLECTED, COPIED AND CONSUMED IN THE WORLD

Прогнозування обсягів даних – це критично важливе завдання в епоху цифрової трансформації. Воно дозволяє підготуватися до викликів, які супроводжують швидке зростання інформаційних потоків, і максимально ефективно використовувати потенціал великих даних для розвитку суспільства та економіки [1].

В середньому, у світі, за секунду створюється 29 терабайтів даних, за хвилину – 1736 терабайтів, за годину – 104000 терабайтів, за день – 2,5 мільйонів терабайтів [2].

Вхідні дані для прогнозування обсягів даних, створених, зібраних, скопійованих і спожитих в світі сумарно наведено у таблиці 1 [3].

Таблиця 1. Вхідні дані для прогнозування обсягів даних, створених, зібраних, скопійованих і спожитих в світі сумарно

Рік	Обсяг даних	Зміна у % порівняно з попереднім роком
2024	147 zettabytes	22.5%
2023	120 zettabytes	23.71%
2022	97 zettabytes	22.78%
2021	79 zettabytes	23.05%
2020	64.2 zettabytes	56.59%
2019	41 zettabytes	24.24%
2018	33 zettabytes	26.92%
2017	26 zettabytes	44.44%
2016	18 zettabytes	16.13%
2015	15.5 zettabytes	24%

Аналіз вибірки: найбільші зміни у відсотках припали на роки COVID-19 – 2020 рік.

Для задачі прогнозування було використано метод поліноміальну регресії (2-го ступеня). Аргументація вибору даного методу наступна: дані про обсяги даних у світі показують нелінійний, прискорений ріст.

Python-скрипт реалізує задачу прогнозування. Основні етапи реалізації:

Імпорт бібліотек – бібліотеки pandas, numpy, matplotlib, sklearn для аналізу та візуалізації даних.

Дані – обсяги даних (у зетабайтах) за 2015–2024 роки.

Модель – застосовано поліноміальну регресію 2-го степеня..

Прогноз – обчислюється прогноз на 2025–2030 роки.

Візуалізація – будується графік з фактичними даними, трендом і прогнозами.

Результати – виводиться графік та таблиця з прогнозованими значеннями.

Результат прогнозування обсягів даних, створених, зібраних, скопійованих і спожитих в світі сумарно графічно наведено на рисунку 1.

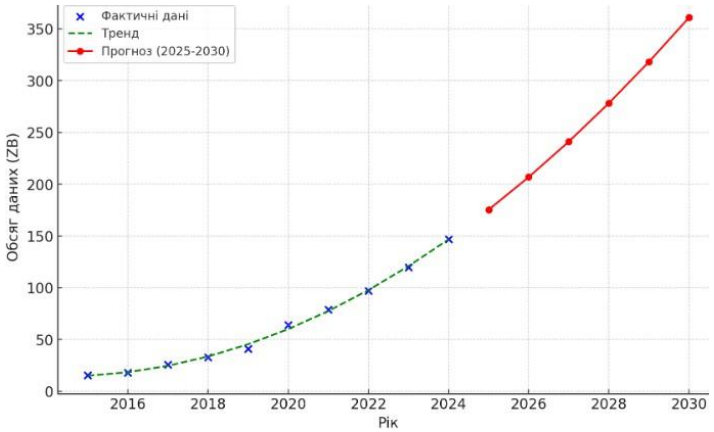


Рисунок 1. Результат прогнозування обсягів даних, створених, зібраних, скопійованих і спожитих в світі сумарно (графічне представлення)

Результат прогнозування обсягів даних, створених, зібраних, скопійованих і спожитих в світі сумарно представлених в табличному форматі наведено у таблиці 2.

Таблиця 2. Результат прогнозування обсягів даних, створених, зібраних, скопійованих і спожитих в світі сумарно представлених в табличному форматі

Рік	Прогнозований обсяг даних (ZB)
2025	175.46
2026	206.96
2027	241.27
2028	278.40
2029	318.34
2030	361.09

Висновки: аналіз показує, що обсяги інформації зростають прискореними темпами, особливо помітно під час пандемії COVID-19 у 2020 році. За прогнозом, дані створені, зібрані, скопійовані і спожиті в світі сумарно у 2030 році буде у 23,296 раз більше порівняно з 2015.

Література

1. Kumar N. Big Data Statistics 2024: Growth and Market Data. Demandsage. URL: https: //www.demandsage.com/big-data-statistics/ (date of access: 19.01.2024)
2. Marr B. How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Forbs. 2021. URL: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/ (date of access: 30.01.2024).
3. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2023, with forecasts from 2024. Statista. URL: https://www.statista.com/statistics/871513/worldwide-data-created/ (date of access: 05.02.2024).

УДК 004.416.2
А. Мельник; П. Скалецький; Н. Гарматюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕСТУВАННЯ МОБІЛЬНИХ ЗАСТОСУНКІВ СМАРТ СИСТЕМ

UDC 004.416.2
A. Melnyk; P. Skaletskyi; N. Harmatiuk

TESTING SMART SYSTEMS MOBILE APPLICATIONS

Для успішного впровадження мобільних застосунків смарт систем важливо, щоб вони відповідали усім вимогам зручності використання. Застосунки мають бути не лише високоефективними, але й практично функціонально повними. Це означає, що усі множини користувачів мобільних застосунків смарт систем повинні швидко та без зайвих складнощів отримувати бажані результати. Для забезпечення високих показників якості застосунки такого класу проходять декілька етапів тестування. При цьому ручне тестування мобільних застосунків має ряд недоліків, зокрема особливо виділяються повторюваність та трудомісткість процедур тестування [1]. Незважаючи на це, значна частина тестування все ще проводиться вручну, що часто стає причиною помилок, низької ефективності та високих витрат. Це створює очевидну потребу у впровадженні автоматизації в процеси тестування.

Автоматизоване тестування дає змогу комп'ютерним системам імітувати роботу тестувальників під час ручного запуску тестових кейсів. Завдяки цьому великі компанії, розробники мобільних застосунків, активно впроваджують автоматизовані методи тестування програмного забезпечення такого класу. Автоматизація процесів тестування мобільних застосунків смарт систем набуває популярності в колах розробників програмного забезпечення та тестувальників, оскільки вона суттєво прискорює робочі процеси та дає змогу досягнути кращі та надійніші результати [2]. Автоматизоване тестування мобільних застосунків смарт систем дає можливість швидко та ефективно їх тестувати, підвищує надійність та прийнятність інформаційних продуктів загалом. Використовуючи інструменти автоматизованого тестування, розробники програмного забезпечення смарт систем можуть скоротити період запуску тестових кейсів. Інформаційно-технологічні інструменти допомагають відтворювати попередньо записані тестові процедури та визначені дії, водночас порівнювати результати з очікуваною поведінкою користувачів та оперативно надавати результати інженерам-тестувальникам [3]. Системи автоматизованого тестування мобільних застосунків смарт систем мають значний потенціал, але потребують подальшої адаптації до викликів сучасного ринку. Найефективніші напрямки досліджень в цій галузі базуються на гібридних підходах та спрямовані на комплексне підвищення масштабованості, сумісності та функціональності процесів тестування.

Література

2. Berihun, Natnael Gonfa, Cyrille Dongmo, and John Andrew Van der Poll. «The Applicability of Automated Testing Frameworks for Mobile Application Testing: A Systematic Literature Review.» Computers 12.5 (2023): 97.
3. Kumar, Sarvesh. «Reviewing software testing models and optimization techniques: an analysis of efficiency and advancement needs.» Journal of Computers, Mechanical and Management 2.1 (2023): 43-55.
4. Wang, Junjie, et al. «Software testing with large language models: Survey, landscape, and vision.» IEEE Transactions on Software Engineering (2024).

УДК 004.056.55
Т. Микитюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ІОТ ПРИСТРОЇВ

UDC 004.056.55
T. Mykytiuk

PENETRATION TESTING OF IOT DEVICES

З кожним днем Інтернет речей все більше інтегрується у повсякденне життя. Перевагами які надають IoT пристрої користуються не лише різного розміру бізнес а я звичайні люди які використовують IoT для різних повсякденних задач. Разом з всіма перевагами які пропонує IoT, користувачі ризикують отримати низку ризиків пов'язаних з вразливостями IoT систем як-от слабкі паролі, відсутність шифрування чи відсутність оновлень. Гучні інциденти зі залученням IoT зайвий раз підкреслюють небезпеку цих вразливостей і гостру необхідність їхнього своєчасного виявлення і оперативного виправлення. З боку розробників, вони повинні зробити все щоб кінцевий продукт був максимально захищеним, з боку користувачів, вони повинні забезпечити систематичне тестування на проникнення IoT-пристроїв щоб запобігти використання вразливостей зловмисником.

Дослідження спрямоване на аналіз реальних випадків атак на IoT-пристрої з метою визначення основних причин їх успіху та методів ідентифікації вразливостей. Зокрема, було проаналізовано такі інциденти:

- DDoS-атаки з використанням IoT-пристроїв, спричинені слабкими паролями;
- Компрометація IP-камер через незахищені веб-інтерфейси.

Методи аналізу включали розгляд відкритих джерел даних, стандартів OWASP IoT Top 10 та рекомендацій ENISA. Для кожного інциденту було запропоновано підходи, які дозволили б виявити вразливості під час тестування на проникнення. Наприклад:

- Для атак ботнету Mirai доцільним є використання сканерів паролів та автоматизованих засобів для виявлення відкритих портів;
- Для компрометації камер — аналіз мережевих конфігурацій і прошивок.

Результати дослідження демонструють, що інтеграція стандартів OWASP і ENISA дозволяє створити системний підхід до безпеки IoT. Запропоновані методики можна адаптувати до різних середовищ: від домашніх мереж до критичної інфраструктури. Практичні рекомендації включають посилення шифрування, регулярне оновлення прошивок та ізоляцію IoT-пристроїв у сегментованих мережах.

Дослідження показує, як використання сучасних інструментів тестування та аналізу може допомогти вчасно ідентифікувати ризики, зменшуючи ймовірність майбутніх інцидентів.

Література

1. Integrity360. «What is IoT Penetration Testing and Why Do You Need It?». URL: https://insights.integrity360.com/what-is-iot-penetration-testing-and-why-do-you-need-it. (дата перегляду 04.12.2024).
2. OWASP. «OWASP Internet of Things Project». URL: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10. (дата перегляду 04.12.2024).

УДК 004.932
Р. Р. Митулинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОЖЛИВОСТІ МАНІПУЛЯЦІЇ ТА МЕТОДИ ВИЯВЛЕННЯ ФАЛЬШИВИХ ЗОБРАЖЕНЬ І ВІДЕО

UDC 004.932
R. R. Mytulinskyi

POSSIBILITIES OF MANIPULATION AND METHODS OF DETECTION FAKE IMAGES AND VIDEOS

Анотація. У доповіді висвітлюються можливості маніпуляцій зображеннями та відео за допомогою сучасних алгоритмів, таких як DeepFake. Описано ключові принципи створення фальшивок, їхній вплив на суспільство, а також актуальні методи виявлення фальшивих матеріалів. Проаналізовано приклади використання таких технологій у різних сферах – від розважальної індустрії до політичних маніпуляцій. Окрема увага приділяється сучасним методам боротьби з фальшивими зображеннями, які включають аналіз фізичних закономірностей, використання метаданих та алгоритмів машинного навчання.

Ключові слова: DeepFake, маніпуляція зображеннями, фальшиві відео, цифрова безпека, машинне навчання, штучний інтелект, виявлення фальшивок.

Вступ. DeepFake – технологія, що використовує генеративно-змагальні нейронні мережі (GAN) для створення реалістичних фальшивих відео та зображень. Її поширення впливає на політику, бізнес і приватність, підкреслюючи важливість методів виявлення маніпуляцій.

Матеріали та методи. Дослідження базувалося на аналізі наукових статей, звітів компаній і матеріалів міжнародних конференцій. Розглянуто три основні підходи:

- Аналіз фізичних закономірностей. Наприклад, розбіжності в освітленні, неправильне відображення тіней або аномальні рухи очей і губ.
- Аналіз метаданих. Вивчення інформації, що міститься у файлах зображень і відео, наприклад, змінені параметри зйомки.
- Методи машинного навчання. Використання алгоритмів, які аналізують тисячі зображень і відео для виявлення специфічних артефактів, властивих фальшивим матеріалам.

Також вивчено автоматизовані рішення для виявлення фальшивок у реальному часі, які можуть бути інтегровані у платформи соціальних мереж.

Результати. Технології створення: GAN дозволяють генерувати високоточні фальшивки.

Сфери застосування: Розваги, освіта, кінематограф; маніпуляції, дискредитація.

Методи виявлення: Аналіз моргання, рухів губ, піксельних аномалій; моделі машинного навчання із точністю понад 90%.

Висновки. DeepFake є серйозною загрозою для інформаційного середовища. Для протидії необхідно розвивати адаптивні моделі виявлення, посилювати співпрацю між експертами та підвищувати цифрову грамотність.

Література

1. Deepfake detection using deep learning methods: A systematic and comprehensive review https://wires.onlinelibrary.wiley.com/doi/10.1002/widm.1520 (дата звернення 02.12.2024).
2. Діпфейки: як розпізнати та захиститися? https://netfreedom.org.ua/article/dipfejki-yak-rozpiznati-ta-zahistitisya (дата звернення 02.12.2024).
3. Synthetic Media & Deepfakes https://innovating.news/article/synthetic-media-deepfakes/ (дата звернення 02.12.2024).

УДК 004.38
Р. Р. Митулинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КВАНТОВІ КОМП'ЮТЕРИ: ЯК ВОНИ ПРАЦЮЮТЬ І ЯКІ МОЖЛИВОСТІ ВОНИ ДАЮТЬ

UDC 004.38
R. R. Mytulinskyi

QUANTUM COMPUTERS: HOW THEY WORK AND WHAT OPPORTUNITIES THEY PROVIDE

Анотація. У доповіді досліджуються принципи роботи квантових комп'ютерів, основні технології, що стоять за ними, а також їхні можливості та потенціал для різних галузей. Розглядаються відмінності між квантовими та класичними комп'ютерами, зокрема, використання кубітів для зберігання та обробки інформації, що дозволяє значно прискорити виконання обчислень. Також розглянуто перспективи використання квантових комп'ютерів у таких сферах, як криптографія, штучний інтелект та моделювання складних систем. Підкреслюється важливість подальших досліджень у цій галузі для досягнення практичного застосування квантових технологій.

Ключові слова: квантові комп'ютери, кубіти, квантова механіка, криптографія, штучний інтелект, обчислювальні технології.

Вступ. Квантові комп'ютери, використовуючи принципи квантової механіки, є революцією в обчислювальних технологіях. Вони працюють з кубітами, здатними до суперпозиції, що значно прискорює вирішення задач у криптографії, оптимізації та моделюванні фізичних систем. Однак їх практичне застосування стримується низкою технічних і теоретичних викликів.

Матеріали та методи. Дослідження базувалося на аналізі наукових статей та монографій з квантової фізики та комп'ютерних наук. Основну увагу було приділено концепціям кубітів, суперпозиції, квантової інтерференції та алгоритмам.

Результати. Кубіти дозволяють виконувати паралельні обчислення, підвищуючи продуктивність. Квантова інтерференція оптимізує результати, а алгоритми Шора (факторизація) та Гровера (пошук) перевершують класичні аналоги. Основні застосування включають криптографію, моделювання хімічних і фізичних процесів, що сприяє прогресу в матеріалознавстві та медицині.

Одним з основних застосувань квантових комп'ютерів є криптографія. Квантові комп'ютери здатні ефективно розв'язувати задачі, які є надто складними для класичних комп'ютерів, що має важливі наслідки для безпеки інформації. Крім того, квантові комп'ютери можуть бути використані для моделювання складних хімічних та фізичних процесів, що відкриває нові можливості для розвитку матеріалознавства, медицини та інших наукових дисциплін.

Висновки. Квантові комп'ютери відкривають нові можливості в науці та технологіях, але їх впровадження ускладнене технічними бар'єрами. Подальші дослідження, спрямовані на покращення стабільності кубітів і створення нових алгоритмів, є ключовими для розвитку цієї галузі.

Література

1. Квантовий комп’ютер: що це та що зможе робити. URL: https://gigacloud.ua/blog/navchannja/kvantovij-kompjuter-scho-ce-ta-scho-zmozhe-robiti (дата звернення 02.12.2024).
2. Рахують за 200 сек те, що класичні ПК рахували б 10 тис. років: як працюють квантові комп’ютери. URL: https://robotdreams.cc/uk/blog/392-yak-pracyuyut-kvantovi-komp-yuteri (дата звернення 02.12.2024).
3. Як працює квантовий комп'ютер. URL: https://www.fizykaua.com/post/chatgptyak-tse-pratsyuye-kvantovyy-kompyuter (дата звернення 02.12.2024).

УДК 621.391.7:004.056.5
В. Новосад; О. Оробчук, Ph.D
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ВРАЗЛИВОСТЕЙ ПРОТОКОЛУ SS7, ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ

UDC 621.391.7:004.056.5
V. Novosad, student; O. Orobchuk Ph.D

ANALYSIS OF SS7 PROTOCOL VULNERABILITIES, THREATS, AND PROTECTION METHODS

Протокол SS7 (Signaling System No. 7) є фундаментальною технологією для телекомунікаційних мереж другого і третього поколінь (2G та 3G), та взаємодії між різними мережами, особливо між 4G і попередніми поколіннями. Він забезпечує передачу сигналів для маршрутизації викликів, передачі SMS та підтримки роумінгу.

Однак, архітектура SS7 побудована на принципі довіри між вузлами мережі, що створює значні ризики безпеки. Вразливості цього протоколу вже неодноразово використовувалися для таких атак, як перехоплення повідомлень, визначення місцезнаходження користувачів, шахрайство у роумінгу та перенаправлення викликів.

Актуальність даної теми обумовлена тим, що попри впровадження сучасніших протоколів, таких як LTE та 5G, SS7 залишається у використанні. Його широке застосування у мобільних мережах створює загрози для конфіденційності мільйонів користувачів, фінансової стабільності операторів та національної безпеки. У роботі проведено дослідження ключових вразливостей SS7, оцінка їх впливу на телекомунікаційні мережі та розробка рекомендацій щодо їх мінімізації. У ході дослідження систематизовано основні вразливості, зокрема відсутність шифрування даних між вузлами мережі, недостатня автентифікація запитів, а також відсутність ефективної фільтрації трафіку. Серед можливих заходів захисту розглянуто впровадження SS7 Firewall, який блокує небезпечні запити, систем моніторингу для аналізу мережевого трафіку та попередження атак у реальному часі, а також впровадження автентифікації вузлів. Крім того, важливим рішенням є перехід до сучасного протоколу Diameter, що забезпечує вищий рівень безпеки завдяки вбудованому шифруванню та автентифікації.

Ці результати можуть бути використані операторами мобільного зв’язку для забезпечення комплексного підходу до захисту їхніх мереж, включаючи впровадження сучасних технологій моніторингу, шифрування даних та багаторівневої автентифікації. Завдяки цьому оператори зможуть ефективніше виявляти та запобігати атакам, знижувати ризики витоку конфіденційної інформації та мінімізувати фінансові втрати, спричинені шахрайством у роумінгу чи іншими видами атак.

Література

1. 3GPP TS 29.002. Mobile Application Part (MAP) Specification. Version 15.6.0. Sophia Antipolis: 3GPP, 2020. 250 с.
2. Engel T. SS7: Locate. Track. Manipulate. Presentation at 31st Chaos Communication Congress (31C3). 2014. 58 с.
3. GSM Association. SS7 Interconnect Security Monitoring and Firewall Guidelines. London: GSM Association, 2017. 45 с.
4. Positive Technologies. SS7 Security: Threats and Vulnerabilities. [Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ (дата звернення: 04.12.2024). 25 с.
5. RFC 6733. Diameter Base Protocol. [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc6733 (дата звернення: 04.12.2024). 160 с.

УДК 004.056.55
Ю. Олійник; О. Оробчук, Ph.D
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

UDC 004.056.55
Y. Oliynyk.; O. Orobchuk, Ph.D

METHODS OF PROTECTING INFORMATION AND TELECOMMUNICATION SYSTEMS AND NETWORKS FROM UNAUTHORIZED ACCESS USING VPN TECHNOLOGY

У сучасному цифровому світі питання захисту інформації стає дедалі важливішим. Інформаційно-телекомунікаційні системи є вразливими до кіберзагроз, що можуть спричиняти витік даних чи несанкціонований доступ. Одним із ефективних рішень є використання VPN, який створює захищені з'єднання навіть через публічні мережі. Це дозволяє забезпечити конфіденційність та цілісність даних, що передаються, знижуючи ризики для користувачів.

Розвиток кібератак, таких як «людина посередині» (MITM), вимагає застосування складних технологій безпеки. VPN забезпечує шифрування даних і мінімізує ризик їх перехоплення, що є важливим як для корпоративних систем, так і для приватних осіб. Це підвищує загальний рівень довіри до мережевих комунікацій.

У роботі проведено дослідження ефективності VPN-протоколів, таких як OpenVPN та WireGuard. Аналіз включав тестування продуктивності під час різного навантаження та вивчення стійкості до кібератак. Такий підхід дозволив визначити оптимальні технічні параметри для захисту мережевих ресурсів. Додатково, було розглянуто вплив різних конфігурацій на швидкість з'єднання та загальну безпеку системи.

WireGuard показав вищу продуктивність, тоді як OpenVPN забезпечив більшу гнучкість налаштувань. Надійність шифрування залежить від довжини ключів і обраних алгоритмів. Розроблено рекомендації для налаштування VPN-систем у контексті запобігання типових уразливостей. Важливо також враховувати специфічні потреби організації для оптимізації безпеки та ефективності мережі.

VPN є ключовим інструментом для захисту інформаційно-телекомунікаційних систем. Однак для максимального ефекту потрібно інтегрувати VPN у загальну стратегію кібербезпеки, забезпечуючи регулярні оновлення та оптимізацію налаштувань. Це включає впровадження додаткових заходів безпеки, таких як двофакторна автентифікація та моніторинг мережевої активності.

Література

1. RFC 7296 – Internet Key Exchange Protocol Version 2 (IKEv2).
2. Jason A. Donenfeld. WireGuard Cryptokey Routing Protocol.
3. OpenVPN Community. OpenVPN Protocol Documentation.

УКД 004.056
З. В. Олекшій
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

«ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ»

UDC 004.056
Z. V. Olekshii

«PROTECTION OF CONFIDENTIAL INFORMATION IN CONDITIONS OF MARTIAL LAW»

В умовах ввоєнного стану гостро постала необхідність посилення захисту інформації з обмеженим доступом в автоматизованих системах. Кіберзагрози зі сторони агресора зумовили впровадження нових підходів до створення систем захисту. Особливо цінним є збереження конфіденційності в роботі державних підприємств оборонної сфери, оскільки інформація, що має стратегічне значення для безпеки країни, може бути використана для організації кібератак. Невдалі спроби захистити таку інформацію можуть мати катастрофічні наслідки для національної безпеки.

Невід'ємною складовою захисту конфіденційної інформації є швидка адаптація існуючих систем до умов воєнного часу. Підвищений рівень кіберзагроз вимагає впровадження більш ефективних засобів криптографії, антивірусного захисту, а також технологій моніторингу та виявлення аномальної активності в реальному часі. Такі заходи здатні зменшити ризики витоків важливої інформації та несанкціонованого доступу до державних систем [1].

В умовах военного стану значну роль у захисті інформації відіграють як організаційні, так і технічні заходи. Першочерговим завданням є забезпечення безпеки на всіх етапах обробки даних – від їх створення та збереження до передачі та використання в межах організацій. Це включає створення багаторівневих систем контролю доступу, впровадження шифрування на всіх рівнях, а також обмеження доступу до інформації для мінімальної кількості осіб.

Окремо варто зазначити важливість навчання персоналу, особливо в умовах екстремальних ситуацій. Підвищення обізнаності про сучасні загрози та правильне поводження з конфіденційними даними є важливою частиною стратегії захисту інформації. Адже людський фактор, зокрема помилки або недбалість співробітників, часто є основною загрозою для витоку інформації. Крім того, на тлі воєнного стану зростає значення захисту інформації від впливу зовнішніх загроз, таких як кібератаки або спроби знищення критичної інфраструктури [2].

Актуальним є створення систем, здатних автоматично виявляти й блокувати несанкціоновані спроби доступу до систем, а також запобігати можливим атакам з використанням шкідливого програмного забезпечення. У цьому контексті застосування сучасних технологій, таких як блокчейн для забезпечення цілісності даних і штучний інтелект для автоматичного виявлення аномальних дій, є важливими елементами захисту [3].

Не менш важливим є адаптація державних нормативно-правових актів до умов воєнного часу. Потрібно запровадити нові підходи до класифікації інформації, враховуючи специфіку загроз, що виникають в умовах війни. Врахування військових стандартів, наказів захисту інформації, що вже використовуються в країнах, де інформаційна безпека є пріоритетом, дозволяє удосконалити національні регуляції й привести їх у відповідність до сучасних вимог [4].

Таким чином, захист конфіденційної інформації в умовах воєнного стану є комплексним завданням, яке включає в себе технічні, організаційні та правові заходи. Це дозволяє забезпечити не лише захист критично важливої інформації від зовнішніх загроз, але й зберегти її цілісність, доступність і конфіденційність у найскладніших умовах.

Література

1. Шкварчук, В. В. Кіберзагрози та заходи їх мінімізації в умовах війни. – Київ: Національний університет оборони України, 2021. – 280 с.
2. Smith, J. Cybersecurity in Times of Crisis: Emerging Technologies and Practices. New York: Tech Press, 2022. – 180 p.
3. The Role of Blockchain in Enhancing Information Security in Wartime» – Journal of Cybersecurity Research, 2023.
4. Харченко, Ю. М. Інформаційна безпека в умовах сучасних загроз. – Київ: Літера, 2019.

УДК 630,247
О. Оробчук, Ph.D; А. Мазяр
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

«АНАЛІЗ ВРАЗЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА МЕТОДІВ ЇХНЬОГО ВИКОРИСТАННЯ В КІБЕРЗАГРОЗАХ»

UDC 630,247
O. Orobchuk, Ph.D; A. Maziar

«ANALYSIS OF ARTIFICIAL INTELLIGENCE VULNERABILITIES AND METHODS OF THEIR USE IN CYBER THREATS»

Стрімкий розвиток штучного інтелекту (ШІ) відкриває нові горизонти для інновацій, проте разом із цим створює потенційні ризики кібербезпеки. Зловмисники активно досліджують і використовують вразливості ШІ для реалізації складних кіберзагроз, що вимагає поглибленого вивчення цієї проблематики.

У сучасному середовищі штучного інтелекту існує кілька типів вразливостей, які можуть використовуватися зловмисниками. Перш за все, варто зазначити, що одним із поширених видів атак є вплив на вхідні дані. Це може проявлятися у вигляді отруєння даних, коли до системи вводяться некоректні або навмисно шкідливі дані, що порушують її роботу, або створення спеціальних шкідливих прикладів, які вводять моделі в оману. Додатково, моделі ШІ самі можуть мати внутрішні слабкі сторони, як-от перенавчання чи нездатність коректно працювати з неточними чи некоректними даними. Ще однією серйозною загрозою є використання моделей для викрадення конфіденційної інформації, що може реалізуватися через атаки інверсії моделей.

Такі вразливості вже активно використовуються у реальних кіберзагрозах. Генеративні моделі, наприклад, можуть допомагати у проведенні фішингових кампаній та здійсненні атак із використанням соціальної інженерії. Ще одним небезпечним застосуванням є створення deepfake-контенту, що використовується для маніпуляцій і поширення дезінформації. Окрім того, автономні системи, зокрема дрони та транспортні засоби, також мають свої вразливі місця, які можуть бути використані зловмисниками для створення загроз.

Таким чином, проблема вразливостей ШІ потребує системного підходу для забезпечення кібербезпеки. Запропоновані рекомендації можуть бути інтегровані у сучасні стратегії безпеки.

Література

1. Papernot, N., McDaniel, P., & Goodfellow, I. (2016). Practical black-box attacks against machine learning. Proceedings of the ACM on Artificial Intelligence.
2. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition.
3. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

УДК 004.056.55
О. Оробчук, Ph.D; М. Демчишин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОСНОВНІ КІБЕРЗАГРОЗИ ТА МЕТОДИ ШИФРУВАННЯ ДАНИХ ДЛЯ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ

UDC 004.056.55
O. Orobchuk, Ph.D; M. Demchyshyn

MAIN CYBER THREATS AND DATA ENCRYPTION METHODS FOR AUTONOMOUS VEHICLES

У сучасному світі автомобільні транспортні засоби (АТЗ) дедалі більше інтегруються з цифровими технологіями. В них використовують комбінацію датчиків, камер, радарів і лідарів для сканування навколишнього середовища та навігації. АТЗ створюють тривимірну карту місцевості, виявляють інші транспортні засоби, пішоходів, дорожні знаки тощо. Бортові комп'ютери використовують ці дані разом з високоточними картами для планування безпечного маршруту, керування гальмами, газом, кермом тощо. Впровадження автономних систем керування, сенсорних мереж та підключення до Інтернету відкриває нові можливості, але й водночас ця цифровізація створює нові виклики у сфері кібербезпеки, які потребують впровадження ефективних методів захисту даних.

Хакери можуть використовувати вразливості в програмному забезпеченні транспортного засобу, мережах або системах зовнішнього зв'язку [1].

Основні кіберзагрози з якими можуть стикнутися автомобільні транспортні засоби це:

1. Загрози, пов'язані з комунікаціями:

– атаки на V2V (зв'язок «транспорт-транспорт») та V2I (зв'язок «транспорт-інфраструктура»);

– перехоплення та підробка даних;

– DDoS-атаки на управління мережею.

2. Загрози для сенсорів та систем управління:

– підміна даних GPS, LiDAR, або камери, що призводить до неправильного аналізу дорожнього розташування;

– впровадження шкідливих даних у системи обробки сигналів.

3. Несанкціонований доступ до бортових систем:

– злом інтерфейсів управління;

– атаки на OTA (оновлення «по повітрю»).

4. Порушення конфіденційності даних:

– крадіжка персональної інформації, включаючи дані про маршрути.

АТЗ залежать від складних систем збору, обробки та передачі даних. Це робить їх вразливими до кібератак, які можуть порушити їх функціонування, знизити безпеку та поставити під загрозу конфіденційність. Для захисту інформації від несанкціонованого доступу запроваджено різні алгоритми, які стосуються цілісності, доступності, автентифікації та авторизації інформації на серверах, включаючи інформацію у файлах і базах даних.

Шифрування даних відіграє ключову роль у забезпеченні захисту конфіденційної інформації від хакерів і кіберзагроз. За допомогою шифрування таких критично важливих даних, як інформація про місцезнаходження, режими водіння та діагностика транспортних засобів, виробники і користувачі знижують ризик несанкціонованого доступу та потенційних кібератак [2].

Для забезпечення конфіденційності та цілісності конфіденційної інформації використовуються наступні методи захисту даних в АТЗ:

1. Криптографічні методи:

– симетричне шифрування (алгоритми: AES). Використовується для захисту даних у пам'яті автомобіля. В АТЗ симетричне шифрування зазвичай використовується через ефективність і швидкість обробки великих обсягів даних;

– асиметричне шифрування (алгоритми: RSA, ECC). Використовується для захисту ключів та зв'язку між автомобілями й інфраструктурою. Цей метод підвищує безпеку в АТЗ, дозволяючи безпечно передавати дані через загальнодоступні мережі без необхідності ділитися особистим ключем;

– хешування (алгоритми: SHA-256, SHA-3). Використовується для забезпечення цільності даних, зокрема при перевірці оновлень програмного забезпечення.

2. Протоколи захищеного зв'язку:

– використання TLS забезпечує захищений канал між транспортним засобом та хмарними сервісами, DTLS для реального часу в системах V2X;

– впровадження VPN або IPSec для мережевої ізоляції, забезпечують захист даних між транспортними засобами та серверами.

3. Безпека оновлень програмного забезпечення:

– використання цифрових підписів для перевірки справності оновлень;

– виявлення механізмів втручання під час ОТА.

4. Моніторинг та виявлення загроз:

– системи виявлення аномалій на основі штучного інтелекту (ШІ).

5. Стійкість до майбутніх загроз:

– інтеграція квантово-стійких алгоритмів шифрування.

Щоб знизити ризики, пов’язані з кібератаками, і забезпечити стабільну роботу автономних транспортних засобів потрібно дотримуватись наступних рекомендацій:

✓ Постійне оновлення систем. Регулярні ОТА-оновлення із застосуванням криптографічної верифікації.

✓ Сегментація мережі. Розділення критичних систем, таких як управління, від вторинних (мультимедіа, навігація).

✓ Моніторинг аномалій. Використання AI/ML для виявлення нетипової поведінки в системах.

✓ Залучення стандартів. Дотримання міжнародних стандартів, таких як ISO 26262, для безпеки в автомобільній галузі.

✓ Навчання користувачів. Інформування власників про важливість безпечного підключення.

Виклики щодо кіберзагроз залишаються актуальними для всіх учасників автомобільної галузі, від виробників до споживачів. Тому, автомобільні транспортні засоби вимагають комплексного підходу до кібербезпеки. Поєднання сучасних криптографічних методів, захищених протоколів зв’язку та системи моніторингу є ключем до мінімізації ризиків та забезпечення надійної роботи автономних транспортних засобів у різних умовах.

Література

1. Meyer, S.F., Elvik, R. & Johnsson, E. Risk analysis for forecasting cyberattacks against connected and autonomous vehicles. *J Transp Secur* 14, 227–247 (2021). URL: https://doi.org/10.1007/s12198-021-00236-4.
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації : навч. посіб. (2-ге видання, стереотипне). Львів : Новий Світ-2000, 2024. 678 с.

УДК 629.01
С. М. Осів; М. О. Стрембіцький, к.т.н., А. В. Чайковський, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ ОДНОПЛАТНИХ МІКРОКОМП'ЮТЕРІВ В СФЕРІ ВЕНДІНГОВИХ АПАРАТІВ

UDC 629.01
S. Osiv; M. Strembitskyi; A. Chaikovs'kyi

THE USE OF SINGLE-BOARD MICROCOMPUTERS IN THE FIELD OF VENDING MACHINES

Ключові слова: вендінговий апарат, мікрокомп'ютер, універсальність
Key words: vending machine, microcomputer, universality

Сучасний розвиток вендінгових апаратів характеризується необхідністю забезпечення надійності, доступності та масштабованості їх функціоналу. Найкращою платформою для розробки торгових апаратів є одноплатні мікрокомп'ютери.

Завдяки розмірам кредитної картки, низькому енергоспоживанню, наявністю великої кількості портів взаємодії – цю платформу все частіше використовують від малих автоматів з водою до апаратів з забезпечення роботизованої автомийки. Універсальність цієї платформи забезпечується наявність GPIO(англ. General-purpose input/output) портів які дають змогу використовувати велику кількість давачів, таких як давачів тиску, температури, різноманітних клапанів, монето приймачів та купюро приймачів.

Дану платформу використано при розробці вендінгового апарату з фіксованою подачею рідини в рамках дипломної праці. Пристрій, при отриманні коштів в купюро приймач, дає сигнал на мікрокомп'ютер та надає користувачеві фіксовану кількість рідини. Завдяки раніше згаданих GPIO у пристрої є змога керувати електромагнітними клапанами і подавати рідини з декількох різних шлангів, забезпечувати відображення інформації на LCD моніторі, а також використовувати кнопки для взаємодії з ним.

Усе це легко поєднується в компактному корпусі та завдяки лише одному мікрокомп'ютеру дає змогу легко поєднувати усі згадані модулі і навіть безперервно виводити інформацію в мережу інтернет для власників апарату. Одноплатний комп'ютер легко опрацьовує великі потоки даних, здійснює безготівковий розрахунок клієнтів і все завдяки універсальній операційні системі.

Література

1. Пушкар, М.С. П 91 Проектування систем автоматизації : навч. посібник / М.С. Пушкар, С.М. Проценко – Д.: Національний гірничий університет, 2013. – 268 с. ISBN 978-966-350-423-0
2. Могильний С.Б. – Мікрокомп'ютер Raspberry Pi – інструмент дослідника: посібник.– К.: 2014. –340 с. ISBN 978-617-7133-48-2
3. URL: https://www.raspberrypi.com/for-home/.
4. URL: https://www.raspberrypi.com/documentation/computers/raspberry-pi.html.

УДК 004.49
Б. Петльовий
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СПОСОБИ ТА ЗАСОБИ ЗАХИСТУ БАЗ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

UDC 004.49
B. Petlovyi

METHODS AND TOOLS TO PROTECT DATABASES FROM UNAUTHORIZED ACCESS

Захист баз даних від несанкціонованого доступу є одним із ключових аспектів інформаційної безпеки, що забезпечує конфіденційність, цілісність та доступність даних. У сучасному світі інформаційних технологій бази даних стають важливим елементом роботи різних організацій, а ризики втрати чи компрометації даних зростають разом із розвитком кіберзагроз. У зв'язку з цим важливим є дослідження способів та засобів захисту баз даних від потенційних атак.

Одним із найефективніших підходів до захисту є використання механізмів аутентифікації та авторизації. Автентифікація забезпечує перевірку особи користувача, який запитує доступ до бази даних, тоді як авторизація встановлює рівні доступу до конкретних ресурсів системи. Сучасні технології пропонують багатофакторну аутентифікацію MFA, яка поєднує кілька елементів для підвищення рівня безпеки.

Важливим способом захисту є шифрування даних, що забезпечує збереження конфіденційності інформації навіть у разі її перехоплення. Використання симетричних алгоритмів таких як AES, DES та асиметричних алгоритмів шифрування до прикладу RSA, дає змогу захистити як дані, що зберігаються, так і ті, що передаються в мережі. Особливого значення набуває технологія управління ключами SSL/TLS, яка гарантує надійне зберігання та обмін ключами.

Моніторинг активності в базах даних і аудит дозволяють своєчасно виявляти підозрілі дії, такі як несанкціоновані спроби доступу чи аномалії в поведінці користувачів. Аналітичні системи на основі штучного інтелекту здатні такі як IBM Guardium, Splunk, Elastic Security, та інші здатні розпізнавати складні шаблони атак і забезпечувати оперативну реакцію на інциденти. Системи захисту баз даних також використовують методи виявлення вторгнень, які базуються на аналізі мережевого трафіку та поведінкових характеристик користувачів.

Таким чином, ефективний захист баз даних від несанкціонованого доступу є багаторівневим процесом, що включає поєднання технічних, організаційних та процедурних заходів. Постійний розвиток інформаційних технологій та кіберзагроз вимагає впровадження новітніх підходів до безпеки, що базуються на інноваційних технологіях та інструментах.

Література

1. Bishop, M., & Venkatramanayya, S. Introduction to Computer Security. Addison-Wesley, 2022.
2. Kim, H., & Solomon, M. G. Database Security and Auditing. Jones & Bartlett Learning, 2023.
3. Elmasri, R., & Navathe, S. Fundamentals of Database Systems. Pearson, 2021.
4. Mirkovic, J., & Reiher, P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM Computing Surveys, 2022.
5. O’Reilly Media. Defensive Security Handbook: Best Practices for Securing Systems and Organizations, 2023.

УДК 004.02
О. Ю. Петрик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ

UDC 004.02
O. Y. Petryk

UI/UX EFFECTIVENESS IN OPTIMIZING THE USER EXPERIENCE OF ONLINE-STORES

Дослідження користувацького досвіду є основним етапом у створенні ефективних онлайн-магазинів. Комфортна взаємодія з інтерфейсом сприяє зростанню конверсії та лояльності клієнтів.

Статистика показує, що добре продумана система кошиків та інтуїтивно зрозуміла навігація можуть зменшити рівень відмов і заохотити клієнтів завершити свої покупки. Коли користувачі можуть легко прокручувати продукти та знаходити те, що вони шукають, вони, швидше за все, повернуться, незалежно від того, чи здійснюють покупки в Інтернеті, чи переходять на взаємодію офлайн.

Поширені проблеми UX на платформах електронної комерції можуть перешкодити вашій здатності підтримувати лояльність споживачів і стимулювати продажі. Наприклад, відсутність соціальних доказів , таких як відгуки клієнтів або рейтинги, може змусити потенційних покупців вагатися у прийнятті рішення про покупку. Крім того, розуміння важливості багатоканального досвіду, коли клієнти можуть плавно переходити між онлайн-покупками та офлайн -магазинами, є життєво важливим для підтримки взаємодії та задоволення**.**

Успіх діяльності онлайн магазину залежить від кількох факторів, зокрема:

- Якість пропонованого продукту або послуги
- Якість контенту, що представляє пропозицію клієнтам
- Якість дизайну електронної платформи — веб-сайту та/або мобільного додатку — за допомогою якої здійснюються продажі.

Тож, очевидно, що UI/UX дизайн є важливим: продумана логіка та переходи, інтуїтивно зрозумілі мікровзаємодії, швидкий зворотній зв’язок із системою, приваблива презентація продукту та плавні потоки платежів – усе це безпосередньо впливає на прибутковість бізнесу в конкурентному середовищі онлайн продажів.

Дизайнери та бізнес-експерти повинні співпрацювати, щоб покращити взаємодію з користувачами, що зрештою принесе користь цільовій аудиторії.

Література

1. Optimizing Online Stores With Essential UX Design Best Practices [Electronic resource] – 2024**.** URL: https://finch.com/blog/optimizing-online-stores-with-essential-ux-design-best-practices.
2. E-commerce UX and UI Design Guide for Best Practices [Electronic resource]. 2024. URL: https://orthoplexsolutions.com/web-development/e-commerce-ux-and-ui-design-best-practices-a-full-guide/.

УДК 681.519.6
М. Петрошук; Я. Литвиненко, д.т.н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДОЛОГІЧНІ ОСНОВИ ОЦІНЮВАННЯ РІВНЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

UDC 681.519.6
M. Petroshuk; I. Lytvynenko, Dr., Prof.

METHODOLOGICAL FRAMEWORK FOR ASSESSING THE LEVEL OF DIGITAL TRANSFORMATION IN HIGHER EDUCATION INSTITUTIONS

Цифрова трансформація закладів вищої освіти (ЗВО) є важливим чинником підвищення їх конкурентоспроможності та ефективності. Розробка методології оцінювання рівня цифрової трансформації є необхідною для визначення поточного стану цифровізації та стратегічного планування подальших змін.

Дані тези стосуються основних понять методологічних основ оцінювання рівня цифрової трансформації ЗВО та можуть бути використанні в освіті, зокрема в ТНТУ.

Цифрова трансформація визначається як інтеграція сучасних цифрових технологій у всі аспекти діяльності ЗВО: навчання, управління, дослідницьку діяльність. Основними складовими цифрової трансформації є:

- розвиток цифрової інфраструктури;
- використання інформаційно-комунікаційних технологій (ІКТ) у навчанні;
- цифрова компетентність викладачів і студентів.

Запропонована методологія ґрунтується на системному підході та включає:

- використання моделі зрілості цифрової трансформації (Digital Maturity Model) для класифікації ЗВО за рівнем цифрової зрілості;
- аналіз із урахуванням технічних, організаційних і освітніх показників;
- визначення ключових показників ефективності (KPI) для кількісного вимірювання цифровізації.

Ключові індикатори. Сформовано набір індикаторів:

- інтеграція цифрових технологій у навчальний процес;
- рівень автоматизації адміністративних процесів;
- цифрова грамотність персоналу.

Системний підхід до аналізу цифрової зрілості дає змогу керівництву закладів:

- приймати обґрунтовані стратегічні рішення щодо подальшого розвитку цифрової інфраструктури;
- підвищувати рівень цифрової компетентності викладачів і студентів;
- інтегрувати сучасні інформаційно-комунікаційні технології для оптимізації освітнього процесу.

Впровадження системи оцінювання цифрової трансформації може стати основою для моніторингу прогресу у цифровізації вищої освіти в Україні. Подальші дослідження мають бути зосереджені на розробці автоматизованих аналітичних систем для моніторингу цифрової трансформації в режимі реального часу та інтеграції цих рішень у загальнодержавні стратегії цифровізації освіти.

Література

1. Harvard Business Review. Digital Transformation in Education. URL: https://hbr.org.
2. OECD (2019). Digitalisation in Education: A Key to 21st Century Skills. URL: https://oecd.org.
3. Morze N., Buinytska O. Digital Transformation of Higher Education Institutions: Challenges and Opportunities. ICT in Education Journal, 2021.

УДК 004.65
Р. В. Пітух; Р. І. Королюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОРГАНІЗАЦІЯ УПРАВЛІННЯ БАЗАМИ ДАНИХ В IoT ВУЛИК

UDC 004.65
R. V. Pituh; R. I. Koroliuk

ORGANIZATION OF DATABASE MANAGEMENT IN IoT HIVE

Метою стартапу IoT Вулик є створення системного підходу до бджолярства з єдиною системою збору даних, аналізу їх професійними та науковими кадрами, а також надання послуг з рекомендаціями по веденню ефективного бджільництва, а не створення системи інформування про окремий вулик. Зокрема, запропоновано інтегрувати в програмну складову стартапу базу даних для збереження та обробки даних про стан бджолосімей та пасік. Тому ефективне збереження і обробка таких даних є важливими для автоматизованої роботи системи.

Розглянувши сучасні підходи до зберігання інформації з IoT-пристроїв – розумний вулик [1], проаналізовано різні типи баз даних для інтеграції в систему. Основними критеріями відбору була простота використання, продуктивність, масштабованість і можливість роботи з великими обсягами даних. Тому у процесі аналізу розглянуто MySQL [2], PostgreSQL [3] та SQLite [4] та основні характеристики, котрі наведено в табл. 1. Розміщення бази даних планується в хмарі Amazon Web Services (AWS).

Таблиця 1. Характеристики баз даних

Характеристика	MySQL	PostgreSQL	SQLite
Тип	Реляційна	Реляційна	Реляційна
Продуктивність	Висока для читання та складних запитів	Висока для складних запитів	Середня для великих обсягів
Масштабованість	Висока	Хороша	Низька
Легкість інтеграції	Висока	Висока	Дуже висока
Споживання ресурсів	Помірне	Вище середнього	Низьке

Загалом, за результатами аналізу, MySQL є найбільш придатною базою даних для збереження даних IoT Вулик, котрий забезпечує баланс між продуктивністю, масштабованістю та простотою інтеграції в систему. MySQL дозволяє легко структурувати дані, створюючи таблиці для показників датчиків, часових міток та даних роєвого стану.

Література

1. Rostyslav Koroliuk, Vyacheslav Nykytyuk, Vitaliy Tymoshchuk, Veronika Soyka and Dmytro Tymoshchuk. Automated monitoring of bee colony movement in the hive during winter season. Proceedings of the 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024). Zboriv, Ukraine, October 02-04, 2024. CEUR Workshop Proceedings, 2024, 3842, pp. 147-156.
2. MySQL Documentation. MySQL 8.0 Reference Manual. URL: https://dev.mysql.com/doc/ (дата звернення 8.12.2024).
3. What’s the Difference Between MySQL and PostgreSQL. URL: https://aws.amazon.com/compare/ the-difference-between-mysql-vs-postgresql/ (дата звернення 8.12.2024).
4. DigitalOcean. SQLite vs MySQL vs PostgreSQL: A Comparison Of Relational Database Management Systems. URL: https://www.digitalocean.com/community/ tutorials/sqlite-vs-mysql-vs-postgresql-a-comparison-of-relational-database-management-systems (дата звернення 9.12.2024).

УДК 004.056:004.9
П. В. Пилипів; Т. А. Лечаченко, канд. техн. наук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РИЗИКИ КІБЕРБЕЗПЕКИ NFT-ТЕХНОЛОГІЇ ТА МЕТОДИ ЇХ ВИРІШЕННЯ

UDC 004.056:004.9
P. Pylypiv; T. Lechachenko, Ph.D

SECURITY RISKS OF NFT TECHNOLOGY AND METHODS FOR ADDRESSING THEM

NFT (невзаємозамінні токени) стрімко завоювали популярність у різних галузях – від цифрового мистецтва та ігор до фінансів і управління інтелектуальною власністю. Ключовими причинами цього є їх можливість надання підтвердження права власності та походження активу. NFT досі розглядаються як шлях до створення прозорої та підзвітної цифрової екосистеми. Проте разом із поширенням даної технології збільшилась кількість випадків шахрайства та фішингу, зломів гаманців, використання вразливостей смарт-контрактів та атак на мережу блокчейн. Згідно зі звітами, щорічні втрати через кіберзагрози у блокчейн-екосистемах сягають мільйонів доларів.

Проте, попри зростання популярності NFT, наразі немає усталених підходів для мінімізації ризиків. Це робить дослідження у цій сфері необхідними для подальшого розвитку екосистеми.

Аналіз ризиків технології NFT включає аналіз вразливостей смарт-контрактів, пов’язаних з ними атаки, атаки на мережу блокчейн, зокрема атаки маршрутизації, атаки 51%, атаки на протоколи блокчейну[1] та криптографічні атаки.

Мінімізація можливих ризиків невзаємозамінних токенів досягається підвищенням безпеки смарт-контрактів, зокрема їх аудитом, вирішенням вразливостей згідно OWASP Smart Contract Top 10 [2], а також впровадженням використання звернень до стороннього джерела інформації, відомого як оракул, для отримання інформації про транзакції. Дана реалізація здійснена за допомогою Chainlink API, яке дозволяє отримати рівень довіри до адреси та історію його попередніх транзакцій для подальшої оцінки ризиків транзакції.

Важливим аспектом пом’якшення ризиків є методи боротьби з поширеними атаками на блокчейн-мережі, зокрема атакою затемнення, атаками 51% та атаками пов’язаними з подвійною витратою. Також одною з основних сторін захисту є використання децентралізованих та мультифакторних рішень для підвищення безпеки гаманців та орієнтованих на безпеку платформ для створення та торгівлі NFT.

У підсумку, рішення повинні бути спрямовані на комплексний підхід до ідентифікації, аналізу та вирішення ризиків, забезпечуючи більш надійну та безпечну інфраструктуру для використання невзаємозамінних токенів, що є ключовим в умовах зростання популярності NFT у різних сферах життєдіяльності.

Література

1. Framework for Determining the Suitability of Blockchain: Criteria and Issues to Consider. URL: https://www.researchgate.net/publication/353073634_Framework_for_Determining_the_Suitability_of_Blockchain_Criteria_and_Issues_to_Consider.
2. OWASP Smart Contract Top 10. URL: https://owasp.org/www-project-smart-contract-top-10/.

УДК 004.77
В. Поліщук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ НА ОСНОВІ АНАЛІЗУ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

UDC 004.77
V. Polishchuk

DEVELOPMENT OF AN ANOMALY-BASED INTRUSION DETECTION SYSTEM USING MACHINE LEARNING FOR NETWORK TRAFFIC ANALYSIS

Сучасні інформаційні системи стикаються з низкою проблем, серед яких зростання кількості кібератак, еволюція методів атак, а також недостатня адаптивність традиційних систем виявлення вторгнень (IDS). Традиційні IDS здебільшого базуються на сигнатурному або евристичному аналізі, що дозволяє ефективно виявляти лише добре відомі атаки. Їх основним недоліком є нездатність розпізнавати нові, невідомі загрози і частота хибнопозитивних (false positive) спрацьовувань, що ускладнює роботу аналітиків безпеки. Тому розробка системи виявлення вторгнень на основі аналізу аномалій у мережевому трафіку з використанням машинного навчання є надзвичайно актуальною. Такий підхід дозволяє забезпечити адаптацію до нових загроз та ефективне виявлення невідомих атак [1].

Використання машинного навчання для обробки мережевого трафіку дозволяє побудувати моделі, які навчаються розпізнавати відхилення від нормальної поведінки. Алгоритми, такі як кластеризація (наприклад, DBSCAN) чи метод опорних векторів (SVM), успішно застосовуються для аналізу великих обсягів мережевих даних [2].

Система виявлення вторгнень була реалізована з використанням TensorFlow, Snort та Python-бібліотеки Scikit-learn для обробки даних. Тестування системи виконано на основі набору даних CICIDS2017, який містить як звичайні сесії, так і сесії з атаками, які відображає відповідний мережевий трафік. Розроблена система дозволила ефективно виявляти аномалії у мережевому трафіку, зокрема атаки типу Brute Force, DoS та DDoS, з високою точністю, забезпечуючи адаптивний підхід до нових загроз.

Загалом, розвиток технологій обробки даних і штучного інтелекту відкриває нові можливості для галузі кібербезпеки та вирішення її основних завдань щодо захисту. Зокрема, автоматизація аналізу мережевого трафіку дозволяє значно скоротити час реакції на загрози, підвищуючи ефективність роботи IT-фахівців. Такі системи можуть працювати як у локальних мережах, так і в хмарних середовищах, що робить їх універсальними для різних типів організацій [3].

Завдяки використанню таких систем у корпоративних мережах різного масштабу можна підвищити загальний рівень безпеки, зменшити ризики витоку даних і забезпечити стабільну роботу інформаційних ресурсів. Інтеграція алгоритмів машинного навчання дозволяє адаптувати системи до нових загроз, виявляючи аномалії навіть у разі невідомих атак. Реалізація подібних рішень сприяє підвищенню ефективності моніторингу мереж і забезпечує довготривалий захист від новітніх кіберзагроз.

Література

1. Xie Y., Yu S. A deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computing. 2015.
2. Kim D. Y., Kang H. Anomaly detection in network traffic using unsupervised deep learning methods // IEEE Access. 2020.
3. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection // IEEE Symposium on Security and Privacy. 2010.

УДК 004.056
О. Прокопенко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА НАВЧАЛЬНОЇ СИСТЕМИ ДЛЯ ЗБОРУ ПЕРСОНАЛЬНИХ ДАНИХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

UDC 004.056
O. Prokopenko

DEVELOPMENT OF A TRAINING SYSTEM FOR COLLECTING PERSONAL DATA USING AI AND SOCIAL ENGINEERING

Сучасні конфлікти, зокрема війна між Україною та Росією, демонструють, що кіберпростір стає одним із ключових фронтів. Збір персональних даних через соціальну інженерію та їх використання для інформаційних атак став важливим інструментом агресора. Розробка навчальних систем із використанням штучного інтелекту допоможе не лише дослідити ці методи, але й підготувати фахівців для протидії таким загрозам [1].

Штучний інтелект пропонує нові інструменти для збору та аналізу персональних даних, але водночас створює виклики, пов'язані з етикою та конфіденційністю. Навчальні системи, що симулюють сценарії соціальної інженерії, дозволяють зрозуміти поведінкові моделі та розробити механізми захисту. Це особливо актуально для країн, які перебувають у зоні геополітичної нестабільності, як Україна [2].

Актуальність теми зумовлена масштабним використанням соціальної інженерії для маніпуляції громадською думкою, збору конфіденційної інформації та проведення інформаційних операцій. В умовах війни, такі дії можуть мати катастрофічні наслідки для безпеки держави. Навчальні системи на основі штучного інтелекту допоможуть моделювати реальні загрози, формувати критичне мислення та вдосконалювати розуміння стосовно цього. Україна вже кілька років стикається з інформаційними атаками, що є частиною гібридної війни з Росією. Розуміння механізмів збору даних допоможе протистояти таким загрозам [3].

Основна робота зосереджена на створенні телеграм-бота, який імітує один із можливих методів збору інформації для соціальної інженерії. Telegram є популярним месенджером в Україні, що робить його ефективним середовищем для моделювання потенційних загроз і навчання користувачів реагувати на них. Цей бот демонструє вразливість до фішингових атак і навчає користувачів розпізнавати загрози. За допомогою цього бота, також можна продемонструвати анонімний збір персональних даних користувачів.

Сучасний світ дедалі більше залежить від цифрових технологій, що робить суспільство вразливим до атак, які використовують персональні дані. Тому запропонована модель демонстрації загрози має високий потенціал для вивчення цієї теми та в подальшому використанні методів захисту на основі запропонованого навчального бота.

Література

1. Roles and Implications of AI in the Russian-Ukrainian Conflict URL:Warfarehttps://www.cnas.org/publications/commentary/roles-and-implications-of-ai-in-the-russian-ukrainian-conflict.
2. RAND CorporationURL: https://www.rand.org/pubs/commentary/2022/11/ukraines-lessons-for-the-future-of-hybrid-warfare.html.
3. Oxford Academic. URL: https://academic.oup.com/book/56111/chapter-abstract/442747673?redirectedFrom=fulltext&login=false.

УДК 004.62
І. Р. Ралік
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

CRM-СИСТЕМА ДЛЯ АВТОМАТИЗАЦІЇ ТОРГІВЛІ НА ПІДПРИЄМСТВАХ

UDC 004.62
I. R. Ralik

CRM-SYSTEM FOR RETAIL AUTOMATION AT ENTERPRISES

Станом на теперішній час задача автоматизації торгівлі на підприємствах вирішуються за допомогою сучасних інформаційних систем. Водночас використання програмних засобів іноземного походження може викликати труднощі у впровадженні через їхню високу вартість та складність адаптації до специфіки різних бізнесів, не менш важливим є питання кібербезпеки. Це підкреслює актуальність дослідження та розробки CRM-систем для автоматизації торгівлі.

Для вирішування завдань автоматизації торгівлі на підприємстві пропонується проект CRM-системи з такою архітектурою, де реалізована клієнтська частина із графічним інтерфейсом, що реалізує функції системи та забезпечує зручність роботи користувачів. Також база даних, яка виконує роль сервера з значною частиною бізнес-логіки, реалізованою в більшій мірі за допомогою збережених процедур.

Для реалізації CRM-системи використано стек технологій від Microsoft, такі як: система управління базами даних Microsoft SQL Server, мова програмування C# та платформа .NET[1]. Основний функціонал CRM-системи складатиме з себе: управління клієнтами (збереження інформації про клієнтів, історія взаємодій, аналітика продажів), управління товарами (облік товарів, формування залишків, генерація замовлень), документообіг (автоматизація операцій, пов’язаних із продажем, постачанням та поверненням товарів), звіти та аналітика (динамічні звіти про продажі, стан складу, фінансові результати). З метою захисту даних впроваджено автентифікацію SQL Server, резервне копіювання даних відбувається кожні 24 години (повна копія) та кожні 10 хвилин (бекап транзакцій). Збережені процедури бази даних в CRM-системі забезпечують виконання складних обчислень і формування звітів безпосередньо на сервері, що підвищує продуктивність системи.

Перспектива подальших досліджень та розробок: розширення функціональних можливостей CRM-системи, зокрема інтеграція із зовнішніми сервісами (платіжні системи тощо); впровадження додаткових рівнів захисту даних, зокрема шифрування з використанням сучасних алгоритмів, аналізу загроз і моніторингу аномальної активності в системі; реалізація модулів штучного інтелекту для прогнозування попиту, персоналізації пропозицій клієнтам, а також автоматичного виявлення відхилень у поведінці користувачів чи транзакціях; адаптація системи для роботи в хмарних середовищах, що дозволить спростити масштабування, забезпечити відмовостійкість і оптимізувати витрати; додаткові функції для персоналізації клієнтського досвіду (аналітика поведінки клієнтів, рекомендаційні системи).

Пропонована CRM-система сприяє підвищенню ефективності торговельної діяльності підприємства, знижує витрати на управління процесами та забезпечує гнучкість у прийнятті бізнес-рішень.

Література

1. Rahayu, S., Cakranegara, P. A., Simanjorang, T. M., & Syobah, S. N. «Implementation of Customer Relationship Management System to Maintain Service Quality for Customer», Enrichment: Journal of Management, 12(5), с. 38-39.

УДК 004.77
М. Ратишин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА ОСНОВІ БЛОКЧЕЙНУ

UDC 004.77
M. Ratyshyn

DEVELOPMENT OF A DECENTRALIZED ELECTRONIC VOTING SYSTEM BASED ON BLOCKCHAIN

Сучасні виборчі процеси стикаються з низкою проблем, серед яких маніпуляції результатами голосування, недостатня прозорість, а також обмежена довіра з боку виборців. Тому розробка децентралізованої системи електронного голосування є надзвичайно актуальною, особливо у світі, що прагне до цифрової трансформації та забезпечення безпеки виборчих процесів [1].

Розробка децентралізованої системи електронного голосування може бути реалізована на основі технології блокчейн. Блокчейн забезпечує надійність, прозорість і незмінність даних, завдяки збереженню інформації у вигляді ланцюга блоків, які пов'язані криптографічними хешами [2]. Це дозволяє запобігти будь-яким фальсифікаціям і забезпечити повну прозорість виборчого процесу.

Використання смарт-контрактів на платформі Ethereum дозволяє автоматизувати правила та процес голосування. Смарт-контракти відповідають за обробку голосів і збереження результатів у децентралізованій мережі, що виключає можливість зовнішнього впливу чи маніпуляцій з даними [3].

Реалізація системи здійснена з використанням таких технологій, як Spring Boot для серверної частини, бібліотеки Web3j для інтеграції з блокчейн-мережею та React.js для клієнтського інтерфейсу. Система протестована у локальному середовищі за допомогою Ganache – інструменту для імітації мережі Ethereum, що дозволило перевірити взаємодію між клієнтом, сервером та блокчейном.

Алгоритм голосування в системі побудований з використанням смарт-контрактів, які виконують функції створення голосування, додавання кандидатів, перевірки користувача, та запису голосу. Смарт-контракт отримує запит від авторизованого користувача на голосування, перевіряє, чи користувач вже проголосував, та у разі позитивного результату записує голос у блокчейн. Цей процес побудований на основі функцій Solidity, що забезпечують всі етапи від створення голосування до його завершення. Таким чином, алгоритми системи гарантують, що кожен користувач може проголосувати лише один раз, а результати зберігаються в незмінному вигляді у блокчейн-мережі.

Таким чином, запропонована система має високий потенціал для застосування в умовах виборчих процесів, забезпечуючи анонімність, надійність і прозорість голосування, що є важливими вимогами для сучасних демократичних систем. Використання блокчейн-технології разом із криптографією робить цю систему безпечною та важко зламною, що є ключовою перевагою для демократичних процесів.

Література

1. Anil Kumar M. «Blockchain for Securing E-Voting.» International Journal of Computer Applications, 2020.
2. Wood G. Ethereum: A Secure Decentralized Generalized Transaction Ledger. URL: https://ethereum.org/en/whitepaper/
3. Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.

УДК 004.7:8
Д. Ревура; Р. Козак, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕРПРЕТАЦІЯ СИСТЕМИ ОЦІНКИ ВРАЗЛИВОСТЕЙ, ЯК МЕТОДУ ДЛЯ ОЦІНКИ РИЗИКІВ

UDC 004.7:8
D. Revura; R. Kozak, Ph.D.

INTERPRETATION OF A VULNERABILITY ASSESSMENT SYSTEM AS A METHOD FOR RISK EVALUATION

У сучасному кіберсередовищі стрімко зростає кількість вразливостей та загроз, що створює потребу в простих і доступних методах оцінювання ризиків. Одним із ключових інструментів для оцінювання вразливостей є система CVSS (Common Vulnerability Scoring System). CVSS широко використовується в різних організаціях для визначення пріоритетності усунення вразливостей, але її потенціал для оцінки ризиків залишається недостатньо розкритим [1].

Метою роботи є дослідження можливості застосування характеристик системи оцінки вразливостей CVSS для оптимізації процесу оцінювання ризиків, використовуючи наявні в CVSS показники впливу та ймовірності. Для досягнення мети виконано наступні завдання:

- Проаналізовано систему CVSS 3.0, включаючи формули, їхню специфіку, визначення та обґрунтування коефіцієнтів.
- Проаналізовано наукові дослідження, присвячені вдосконаленню процесів оцінки та управління ризиками за допомогою нормалізації CVSS для стандартизації оцінок ризиків, а також методології OWASP, яка забезпечує структуровану класифікацію ризиків та прозорість у їх інтерпретації
- Досліджено методології нормалізації даних, що використовуються для аналізу ризиків.
- Розроблено алгоритм оцінки ризиків на основі CVSS та побудувано блок-схему для його впровадження.

Аналіз літератури охоплює наукові праці, присвячені вдосконаленню процесів управління ризиками [2], а також OWASP Risk Rating Methodology. Було досліджено математичні підходи до нормалізації даних для полегшення інтерпретації метрик CVSS. Результати аналізу показали, що нормалізація може бути ефективним інструментом для автоматизації процесу оцінювання ризиків.

На основі отриманих даних запропоновано інтерпретацію CVSS методом нормалізації на прикладі вразливостей компаній малого бізнесу, що дозволяє адаптувати підхід до їхніх потреб і обмежених ресурсів.

Результати дослідження демонструють, що інтеграція CVSS у процеси оцінки ризиків дає змогу створити системний підхід для управління безпекою. Нормалізація даних підвищує точність інтерпретації, а автоматизований алгоритм оцінки зменшує потребу в залученні експертів. Запропонована методологія є перспективним напрямом у розвитку підходів з управління ризиками кібербезпеки та може бути адаптована до умов малого та середнього бізнесу.

Література

1. SAM'11. «Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics». Presented at the International Conference on Security Assessment and Management.
2. IEEE FiCloud. «Normalization Framework for Vulnerability Risk Management in Cloud». Presented at the International Conference on Internet of Things and Cloud Technologies (FiCloud).

УДК 004.8
Я. Роган
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ МЕТОДУ GRAD-CAM ДЛЯ ДІАГНОСТИКИ ХВОРОБИ АЛЬЦГЕЙМЕРА

UDC 004.8
Ya. Rohan

USE OF THE GRAD-CAM METHOD FOR DIAGNOSIS OF ALZHEIMER'S DISEASE

Метод Gradient-weighted Class Activation Mapping (Grad-CAM) є сучасним інструментом штучного інтелекту, що дозволяє візуалізувати роботу глибинних нейронних мереж (ГНМ). У контексті медичної діагностики, зокрема діагностики хвороби Альцгеймера, Grad-CAM допомагає виявляти патологічні особливості на медичних зображеннях, таких як МРТ головного мозку.

Діагностика хвороби Альцгеймера базується на аналізі нейродегенеративних змін, що відображаються у вигляді зменшення об'єму кори головного мозку. Grad-CAM додає прозорості, накладаючи теплові карти уваги на вихідні зображення, що показують, які області мали найбільший вплив на прийняте рішення.

Основний алгоритм Grad-CAM полягає у вирахуванні градієнтів виходу моделі по відношенню до активацій на останньому згортковому шарі. Це дозволяє визначити просторову значущість кожного пікселя. У випадку хвороби Альцгеймера Grad-CAM може ідентифікувати зони атрофії які корелюють із ступенем розвитку хвороби. Поетапний опис роботи методу Grad-CAM:

1. **Отримання передбачення**. Вхідне зображення пропускається через модель (наприклад, ResNet, VGG), щоб отримати прогноз або класову оцінку y^c для цільового класу c.

2. **Обчислення градієнтів**. Вираховуються градієнти передбачення y^c відносно активацій нейронів у вибраному згортковому шарі. Градієнти показують, наскільки зміни в активаціях цього шару впливають на вихідний клас.

3. **Агрегація градієнтів.** Градієнти усереднюються за просторовими вимірами (ширина та висота карти активацій) для кожного фільтра:

$$a_k^c = \frac{1}{Z} \sum_i \sum_j \frac{\delta y^c}{\delta A_{ij}^k}$$

де:
a_k^c – вага фільтра k для класу c;
A_{ij}^k – значення активації фільтра k у позиції (i, j);
Z – кількість просторових позицій;

4. **Побудова теплової карти**. Карти активацій A^k зважуються коефіцієнтами a_k^c і підсумовуються:

$$L_{Grad-CAM}^c = ReLU(\sum_k a_k^c A^k)$$

При цьому Функція ReLU використовується, щоб залишити тільки позитивні впливи, ігноруючи негативні

5. **Інтерполяція теплової карти**. Отримана карта $L_{Grad-CAM}^c$ має розмірність згорткових активацій. Її масштабують до розмірів початкового зображення за допомогою інтерполяції.

6. **Накладення на зображення**. Теплова карта накладається на вхідне зображення щоб показати області, які найбільше вплинули на прогноз.

На рисунку 1 наведено приклад реалізації методу Grad-CAM для діагностики хвороби Альцгеймера:

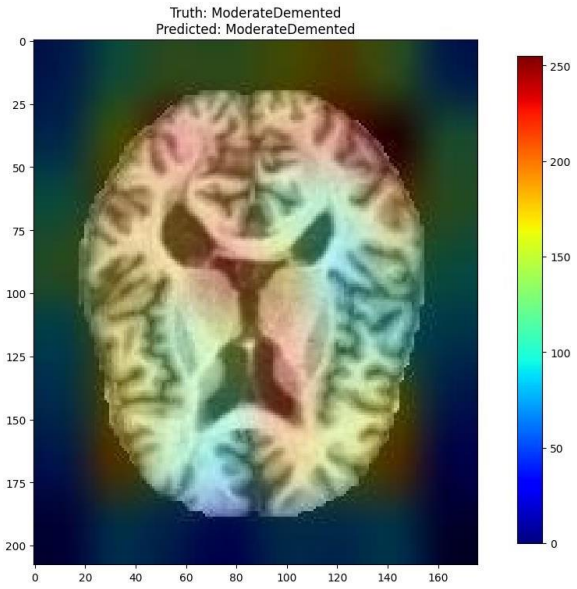


Рисунок 1. Реалізація методу Grad-CAM

Проаналізувавши рисунок бачимо, що вхідне зображення покривається картою-градієнтом, показуючи на яких ділянках зображення найбільше було зосереджено уваги для винесення діагнозу нейронною мережею. Червоним кольором позначені ділянки, які маю велике значення важливості для передбачення, сині ділянки позначають ділянки, які мать найменше значення важливості. Таким чином ми бачимо відносно яких ділянок мозку робились передбачення про наявний діагноз і його клас. Зокрема можна помітити високу активність в центральній зоні головному мозку, в місці так званих «шлуночків», а також в закінченнях кори мозку, оскільки дані зони надають найбільше інформації про наявність хвороби Альцгеймера та її складність.

Ефективність Grad-CAM для діагностики хвороби Альцгеймера підтверджується кількома ключовими аспектами. По-перше, метод дозволяє лікарям не лише отримувати результат, але й розуміти, чому модель прийняла певне рішення. Це підвищує довіру до системи. По-друге, Grad-CAM може допомогти у виявленні ранніх змін, що складно помітити при візуальному аналізі. Це відкриває можливості для розробки інтерпретованих рішень у сфері діагностики на основі глибокого навчання, забезпечуючи лікарям корисний інструмент для прийняття рішень.

Література

1. Selvaraju R. R. Grad-cam: visual explanations from deep networks via gradient-based localization / R. R. Selvaraju, M. Cogswell, A. Das, [et al.] // International Journal of Computer Vision. 2020. Vol. 128, No. 2. P. 336–359.

УДК 004.8
Я. Роган
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ АНАЛІЗУ МЕДИЧНИХ ЗОБРАЖЕНЬ

UDC 004.8
Ya. Rohan

USE OF NEURAL NETWORKS FOR MEDICAL IMAGE ANALYSIS

Нейронні мережі стали революційним інструментом в аналізі медичних зображень. Їх здатність до автоматичного виділення ознак, навчання на великих обсягах даних та виконання складних завдань робить їх незамінними у сучасній медицині.

Основними застосуваннями нейронних мереж у цій сфері є діагностика захворювань, сегментація зображень, виявлення патологій, класифікація медичних знімків та прогнозування результатів лікування. Наприклад, згорткові нейронні мережі успішно використовуються для аналізу рентгенівських знімків, комп'ютерної томографії (КТ) та магнітно-резонансної томографії (МРТ). Вони демонструють високу точність у виявленні ракових утворень, пошкоджень кісток та інших патологій.

Основні етапи аналізу медичних зображень за допомогою нейронних мереж:

1. **Збір даних**. Медичні зображення отримують із пристроїв візуалізації, таких як МРТ чи КТ. Ці дані можуть бути представлені в різних форматах.
2. **Попередня обробка зображень**. Попередня обробка потрібна для покращення якості зображень та видалення артефактів. Вона включає фільтрацію шумів, контрастну обробку, нормалізацію та сегментацію.
3. **Аналіз зображень**. Спочатку визначаються ознаки зображень, тобто кількісні характеристики, які використовуються для ідентифікації аномалій, наприклад форма, текстура та інтенсивність. Згодом створюються та навчаються моделі нейронних мереж, які шукають закономірності у зображеннях.
4. **Класифікація**. В залежності від завдання може виконувати двоїсту (наявність або відсутність хвороби) або множинну класифікацію (відсутність хвороби, легка стадія, середня, важка)
5. **Валідація та інтерпретація**. Результати аналізу зображень повинні бути перевірені лікарями. Це гарантує, що модель працює коректно, і її висновки мають практичне застосування.

Переваги використання нейронних мереж включають швидкість обробки зображень, можливість обробки великих обсягів даних та високу точність результатів. Крім того, такі системи можуть працювати як інструменти підтримки прийняття рішень, допомагаючи лікарям уникати людських помилок.

З подальшим розвитком методів навчання, доступу до великих баз даних та зростанням обчислювальних можливостей, нейронні мережі зможуть ще ефективніше допомагати у ранній діагностиці захворювань, розробці індивідуалізованих планів лікування та моніторингу стану пацієнтів.

Література

1. Mehmood A. A deep siamese convolution neural network for multi-class classification of alzheimer disease / A. Mehmood, M. Maqsood, M. Bashir, Y. Shuyuan // Brain Sciences. 2020. Vol. 10. No. 2. P. 84.

УДК 004.89
М. М. Рокош
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЗАХИСТУ КОРПОРАТИВНИХ КОМУНІКАЦІЙ

UDC 004.89
M. Rokosh

APPLICATION OF GENERATIVE ARTIFICIAL INTELLIGENCE FOR THE PROTECTION OF CORPORATE COMMUNICATIONS

Генеративний штучний інтелект (ГШІ) пропонує передові рішення для забезпечення безпеки корпоративних комунікацій, які є критично важливими для збереження інформаційної цілісності сучасних організацій. ГШІ дозволяє автоматизувати процеси виявлення та запобігання кіберзагрозам, таким як фішингові атаки, витоки даних та спроби соціальної інженерії. Це досягається завдяки інтеграції технологій обробки природної мови (NLP) та моделей глибокого навчання, здатних аналізувати зміст та контекст повідомлень. Armorblox є прикладом ефективного застосування ГШІ для захисту електронної пошти та інших каналів корпоративної комунікації. Використовуючи лексичний, синтаксичний та семантичний аналіз тексту, платформа автоматично виявляє потенційно небезпечні повідомлення, ідентифікує неправомірні запити доступу до даних та запобігає випадковим витокам інформації. Такий підхід мінімізує залежність від людського фактору, автоматизуючи виявлення загроз та значно знижуючи ризик помилок, спричинених недосвідченістю або недбалістю співробітників.

На технічному рівні Armorblox використовує моделі на основі трансформерів, такі як GPT (Generative Pre-trained Transformer) або їх модифіковані варіанти. Ці моделі проходять попереднє навчання на великих наборах даних, а потім донавчаються з урахуванням специфічних потреб у сфері кібербезпеки. У процесі розробки та впровадження систем захисту комунікацій на основі ШІ ці інструменти створюють багатовимірні представлення даних, що дозволяє ідентифікувати приховані зв’язки між контекстом повідомлення, його відправником і отримувачем. Наприклад, платформа може виявити підозрілий запит на зміну банківських реквізитів від імені фінансового директора, якщо аналіз історії комунікацій покаже аномалії у стилі письма або характері запиту.

Інтеграція генеративного ШІ у захист корпоративних комунікацій охоплює кілька технічних етапів. Спершу система здійснює попередню обробку даних, аналізуючи їх, видаляючи шум та нормалізуючи текст, наприклад, виправляючи помилки або стандартизуючи форматування. Далі система генерує контекстуальні вектори для кожного повідомлення, використовуючи архітектури трансформерів, такі як BERT чи GPT, що дозволяє враховувати як значення слів, так і їх контекст у загальному потоці комунікацій. Наступним етапом є виявлення аномалій за допомогою моделей машинного навчання, таких як LSTM (Long Short-Term Memory) чи GRU (Gated Recurrent Units), які відстежують поведінкові патерни, виявляючи аномалії у часі, форматі або змісті повідомлень, які можуть свідчити про загрозу. Нарешті, алгоритми ГШІ приймають рішення та здійснюють реагування, використовуючи механізми раннього попередження для автоматичного блокування підозрілих повідомлень або передачі їх на перевірку відповідальним працівникам. Наприклад, якщо система виявляє лист, схожий на фішингову атаку, вона ізолює його та сповіщає користувача, пояснюючи ризики.

Розгортання та оцінка систем безпеки на основі ШІ часто передбачають тестування у контрольованих умовах, таких як імітація фішингових кампаній або інших кіберзагроз, що дозволяє вдосконалити функціональні можливості системи та забезпечити її надійність. Такі симуляції допомагають оцінити здатність моделі виявляти нові загрози та адаптувати алгоритми до змін у патернах атак. Крім того, масштабованість і надійність цих систем забезпечуються за допомогою передових фреймворків розгортання, включаючи інструменти контейнеризації, такі як Docker і Kubernetes, які підтримують обробку в реальному часі та моніторинг роботи системи у хмарних або гібридних середовищах.

Реалізація таких рішень демонструє значні переваги у зниженні ризиків кіберзагроз, оптимізації витрат на безпеку та покращенні управління потоками комунікацій. Проте важливо вирішувати питання конфіденційності даних, етичного використання технологій та адаптації персоналу до роботи з новими інструментами. Збалансоване поєднання технічних та організаційних заходів дозволяє максимально ефективно використовувати потенціал генеративного ШІ у корпоративній кібербезпеці.

Література

1. Dhoni P., Ravinder K. Synergizing Generative Artificial Intelligence and Cybersecurity: Roles of Generative Artificial Intelligence Entities, Companies, Agencies and Government in Enhancing Cybersecurity, Authorea Preprints, Journal of Global Research in Computer Sciences, 2023. doi:10.4172/2229-371X.14.3.005.
2. Krishnamurthy O. Enhancing Cyber Security Enhancement Through Generative AI, International Journal of Universal Science and Engineering 9, pp. 35-50, 2023. URL: https://ijuse.org/admin1/upload/06%20Oku%20Krishnamurthy%2001155.pdf.
3. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. doi:10.48550/arXiv.1810.

УДК 514.18

С. В. Романський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДЕТЕКТУВАННЯ ОСОБЛИВОСТЕЙ НА ЗОБРАЖЕННЯХ

UDC 514.18

S. V. Romanskyi

FEATURE DETECTION IN IMAGES

У комп'ютерному зорі снує важливий напрямок - детекція особливостей (feature detection) на зображеннях, з яких, власне, ключові точки і визначаються як такі. Під цим можна мати на увазі не просто точки, як пару координат, а деякі області на зображеннях, для знаходження яких і існують різні методи та алгоритми.

Власне особливості зображення може бути різних видів:

- ребра (edges) – межі між двома областями зображень, це можуть бути випадкові контури та стики різних об'єктів; практично часто набір точок, які мають велику величину градієнта;
- кути/точки інтересу, ключові точки (corners / interest points, фактично синоніми). Спочатку продукт аналізу ребер з метою знаходження різких змін у напрямку (тобто кутів), потім були розроблені алгоритми, що не потребують явного обчислення ребер (наприклад, шукають сильне викривлення градієнта зображення). Зазначимо, що знайдені ключові точки зовсім не обов'язково є кутами об'єктів сцен у прямому розумінні, проте вони – особливості, які враховуються;
- сфери / ключові області, ключових точок (blobs / regions of interest or interest points). Фактично опис областей зображення. Так само як і кути вважаються ключовими точками (і мають фактичний центр), однак вони мають свої алгоритми розрахунків.

Різні алгоритми знаходження особливостей завжди схожі в одному – як тільки особливість знайдена, відбувається витяг (extraction) невеликої області навколо неї. Результат – дескриптор або векторні особливості. Це стосується і кутів і сфер. Різні алгоритми пошуку особливостей пропонують різні дескриптори.

Методи зіставлення дескрипторів (matchers) ключових точок на різних зображеннях – наріжний камінь знаходження шаблонів на сцені, можливість комп'ютерного зору для вирішення задачі розпізнавання образів.

І ці способи зіставлення можуть бути відмінними для різних алгоритмів пошуку ключових точок та різних дескрипторів.

Для виділення ключових точок існує кілька основних методів, які вже реалізовані в різних програмних засобах і широко використовуються на практиці. Методи як мінімум включають алгоритми пошуку, що повертають список ключових точок, а також зазвичай (але не завжди) мають вбудовані алгоритми вилучення дескрипторів. Якщо вбудованих алгоритмів вилучення немає, то існують реалізовані окремо, здатні витягувати із зображення дескриптори певних форматів за знайденими ключовими точками.

Основні методи пошуку ключових точок на зображеннях, що мають доступну, готову для використання програмну реалізацію, це SIFT, SURF, ORB, BRISK та AKAZE. Алгоритмічно це різні методи, що тяжіють до різних особливостей зображень.

Ці методи пошуку ключових точок найбільш популярні і поширені (є й інші, зазвичай модифікації вказаних), крім того, важливо те, що їх реалізації є в одній відкритій бібліотеці комп'ютерного зору OpenCV, що робить неактуальним їх реалізацію з нуля (або використання різних джерел/бібліотек) і дає можливість порівнювати їхню роботу в ідентичних умовах.

УДК 004.056.53
Б. Слупський; Р. Козак, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АВТОМАТИЗОВАНІ ІНСТРУМЕНТИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА ЇХ ЕФЕКТИВНІСТЬ

UDC 004.056.53
B. Slupskyi; R. Kozak, Ph.D., Assoc. Prof.

AUTOMATED PENETRATION TESTING TOOLS AND THEIR EFFECTIVENESS

Автоматизоване тестування на проникнення є складовою комплексного підходу до забезпечення кібербезпеки [1]. Постійне зростання кількості кібератак, швидкий розвиток веб-додатків та динамічні зміни у їх архітектурі та функціоналі вимагають систематичного моніторингу й оперативного виявлення вразливостей. Веб-додатки часто стають ціллю зловмисників через відкритий доступ, розгалужену функціональність і велике коло користувачів. Використання автоматизованих інструментів дає змогу суттєво скоротити час на ідентифікацію вразливих місць, мінімізує вплив людського фактору та підвищує загальну ефективність тестування [2].

У дослідженні розглянуто інструменти автоматизованого тестування на проникнення з акцентом на їхнє застосування до веб-додатків. Проведено оцінку точності виявлення різноманітних типів вразливостей, швидкодії сканування та зручності взаємодії користувача з інструментами. Також проаналізовано можливості інтеграції інструментів у процеси розробки та супроводу програмних продуктів. Враховано потреби малих організацій, для яких питання оптимального вибору інструментів та зниження витрат на спеціалізованих фахівців є особливо актуальним [2], [3].

На основі отриманих даних сформовано практичні рекомендації щодо оптимального вибору засобів автоматизованого тестування відповідно до конкретних вимог та ресурсів організації. Зокрема, визначено, які інструменти здатні найкраще виявляти критичні вразливості веб-додатків, а які забезпечують більш широкий, але менш глибинне ооплення потенційних загроз.

Перспективним напрямом подальших досліджень є удосконалення методик оцінювання ефективності інструментів, застосування штучного інтелекту для інтелектуального аналізу результатів тестування та розробка адаптивних систем автоматизованого тестування, що динамічно адаптуються до особливостей цільових веб-додатків.

Література

1. Guo W., Jin G. Automated Penetration Testing: An Overview. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/325030351_Automated_Penetration_Testing_An_Overview.
2. Aloul, F., Al-Azani, S. Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/381847814_Adopting_Automated_Penetration _Testing_Tools_A_Cost-Effective_Approach_to_Enhancing_Cybersecurity_in_Small_Organizations.
3. Shah, M.P. Automated Vulnerability Scanning and Testing. Master Thesis, National College of Ireland, 2019. [Електронний ресурс]. – Режим доступу: https://norma.ncirl.ie/4165/1/mandarprashantshah.pdf.

УДК 004.7
О. В. Смик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ВІД ВНУТРІШНІХ ЗАГРОЗ

UDC 004.7
O. V. Smyk

METHODS AND MEANS OF PROTECTING THE INFORMATION AND COMMUNICATION SYSTEM OF AN INFORMATION ACTIVITY OBJECT FROM INTERNAL THREATS

Сучасні інформаційно-комунікаційні системи (ІКС) є основою функціонування організацій та підприємств, але водночас стають мішенню для внутрішніх загроз, які залишаються одними з найскладніших для ідентифікації. Залежність організацій від ІКС збільшує потенційні ризики, що пов'язані як із людським фактором, так і з технічними недоліками [1]. Внутрішні загрози можуть виникати через ненавмисні помилки співробітників, порушення правил роботи із системою, або навмисні дії, що мають на меті завдання шкоди.

Мета дослідження полягає у створенні системи, яка забезпечить виявлення внутрішніх загроз в ІКС за допомогою аналізу поведінки користувачів та класифікації їх дій із застосуванням методів машинного навчання.

За основу роботи системи захисту ІКС взято модель класифікації, що дозволяє аналізувати взаємозв'язки між різними параметрами поведінки користувачів. Для навчання та тестування моделі було обрано датасет Data Leakage Detection із відкритої платформи Kaggle [2]. Датасет містить інформацію про активність користувачів у комп'ютерній мережі або системі, охоплюючи такі показники, як методи автентифікації, рівень доступу до даних, операції з файлами, рівень чутливості даних та ознаки аномальної поведінки. Використання цього датасету обґрунтоване його відповідністю специфіці задачі та наявністю збалансованого розподілу класів для «нормальної» та «аномальної» активності.

Розроблена система включає функціонал моніторингу поведінки користувачів у реальному часі, що дозволяє виявляти аномалії у діях співробітників. Алгоритм класифікує дії як нормальні або аномальні, спираючись на заздалегідь визначені параметри, такі як частота доступу до конфіденційної інформації, час входу в систему, кількість запитів тощо.

Застосування розробленої системи дозволяє вчасно виявляти потенційні загрози, знижуючи ризики витоку інформації, а також фінансових і репутаційних збитків.

Важливою особливістю запропонованого підходу є використання машинного навчання для моніторингу поведінкових патернів та автоматичного аналізу аномалій. Це дозволяє адаптувати розроблену систему до потреб різних галузей, що підкреслює її практичну цінність у забезпеченні безпеки інформаційно-комунікаційних систем.

Література

1. Insider Threats: From Malicious to Unintentional. URL: https://www.sentinelone.com/blog/insider-threats-from-malicious-to-unintentional/?utm_source=chatgpt.com (дата звернення: 05.12.2024).
2. Data Leakage Detection. URL: https://www.kaggle.com/datasets/syedmarslanalvi /data-leakage-detection (дата звернення: 05.12.2024).

УДК 004.9
Р. Ставицький; Р. Катрич; А. Лисий
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ШТУЧНИЙ ІНТЕЛЕКТ В РОЗУМНИХ МІСТАХ

UDC 004.9
R. Stavytskyi; R. Katrych; A. Lysyi

ARTIFICIAL INTELLIGENCE IN SMART CITIES

Штучний інтелект має значний потенціал для аналітичного опрацювання зібраних та інтегрованих в середовищі «розумних міст» великих за обсягом наборів та колекцій даних, що дає змогу ефективно використовувати отримані інсайти для оперативної оптимізації витрат ресурсів та забезпечення високоефективної взаємодії з громадянами. Як зазначено в [1], програмно-алгоритмічні засоби на основі штучного інтелекту можуть сприяти підвищенню безпеки та захисту громадськості завдяки використанню вдосконалених технологій спостереження, моніторингу аварійних та надзвичаних ситуацій, поєднанню баз даних. Розподілене та високоефективне управління процесами постачання ресурсів, зокрема енергії та води, є ще однією актуальною сферою використання штучного інтелекту [2]. Аналітичне опрацювання соціальних джерел для розуміння потреб громадян у режимі реального часу та використання інтерактивних чат-ботів на основі штучного інтелекту для повсякденної комунікації з «розумними» міськими системами та послугами також показали високу ефективність [3].

На даний час у середовищах «розумних міст» продукуються обширні множини різнотипових даних. З часом зростатиме їх різноманіття: від зображень і відео до сенсорних даних, показників споживання ресурсів, а саме електроенергії та води, даних із соціальних джерел, текстів тощо. Важливим фактором є те, що в «розумних» середовищах можуть виникати нескінченна множина потенційних ситуацій [4]. Хоча використання технології хмарних обчислень, штучного інтелекту, машинного навчання та аналітичного опрацювання принесло значну користь «розумним містам», існують ключові обмеження, які стримують реалізацію переваг від таких інформаційно-технологічних досягнень. Зокрема обмеження полягає в тому, що використання штучного інтелекту наразі відбувається ізольовано, у вигляді окремих застосунків, через відсутність ефективних механізмів інтеграції та обміну інформацією.

Література

1. Guelzim, T., & Obaidat, M. S. (2016). Cloud computing systems for smart cities and homes. In M. S. Obaidat & P. Nicopolitidis (Eds.), Smart Cities and Homes (pp. 241–260). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-803454-5.00012-2.
2. De Silva, D., Sierla, S., Alahakoon, D., Osipov, E., Yu, X., & Vyatkin, V. (2020). Toward intelligent industrial informatics: A review of current developments and future directions of artificial intelligence in industrial applications. IEEE Industrial Electronics Magazine, 14(2), 57–72. https://doi.org/10.1109/MIE.2019.2952165.
4. Adikari, A., De Silva, D., Alahakoon, D., & Yu, X. (2019). A cognitive model for emotion awareness in industrial Chatbots. 2019 IEEE 17th international conference on industrial informatics (INDIN), 1, 183–186.
5. Mohammad, N., Muhammad, S., Bashar, A., & Khan, M. A. (2019). Formal analysis of human-assisted smart city emergency services. IEEE Access, 7, 60376–60388.

УДК 004.9
Р. Ставицький; В. Дубельт; Х. Дуда
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗУМНІ МІСТА ТА ПРОГРАМНО-АЛГОРИТМІЧНІ ЗАСОБИ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

UDC 004.9
R. Stavytskyi; V. Dubelt; K. Duda

SMART CITIES AND SOFTWARE AND ARTIFICIAL INTELLIGENCE-BASED ALGORITHMIC TOOLS

Міграція в міста є зростаючим трендом двадцять першого століття, і, за прогнозами ООН, до 2050 року понад 70% населення світу житиме в міському середовищі [1]. Ці міграційні процеси спричинятимуть зростаючий тиск на здатність міст справлятися із викликами, що продукує нагальну потребу розробки «розумніших» підходів до процесів управління міськими проблемами, як-от зростання міського населення, транспортні затори, зростання рівня злочинності, соціальні виклики, підвищена потреба та розподіл ресурсів тощо. На даний час ефективні рішення у цій царині пропонують інформаційно-технологічні концепти «розумне місто».

Бурхливий розвиток інформаційних технологій актуалізує оперативне управління великими обсягами різнотипових структурованих та неструктурованих даних. Світ наповнюється IoT-пристроями та сенсорами, які здатні відслідковувати характеристики навколишнього середовища та обмінюватися даними між собою, формуючи при цьому цифрове середовище «розумних міст» з великими за обсягом наборів та колекцій мінливих та різноманітних даних. Традиційні методи штучного інтелекту та машинного навчання, розроблені на даний час для детерміністичних ситуацій, не підходять для таких швидкоплинних умов та ситуацій [2]. Завдяки великій кількості різноманітних параметрів, що потребує кожен IoT-пристрій у «розумному» міському цифровому середовищі, бажано, щоб програмно-алгоритмічні засоби на базі штучного інтелекту мали змогу оперативно адаптуватися. Тобто здійснювати процедури самоструктурування, самоналаштовування та самонавчання, а не обмежуватися попередньо заданою структурою та параметрами. Тому актуальним напрямком сучасних досліджень є дослідження процесів автоматизованого формування «розумних» міських систем на базі штучного інтелекту та алгоритмів машинного навчання для розширення аналітичних можливостей при опрацюванні великих даних в обчислювальному середовищі розумних міст. Впродовж останнього періоду часу інформаційні системи такого класу формуються за допомогою моделей самоорганізуючих карт, які дають можливість усунути обмеження традиційних підходів до систем на основі штучного інтелекту та забезпечити своєчасну обробку даних у динамічних обчислювальних середовищах розумних міст. Вони можуть інтегрувати аналітичні програмно-алгоритмічні засоби з використанням хмарних обчислювальних платформ.

Література

1. World population projection by UN. (2018). UN DESA | United Nations Department of Economic and Social Affairs. URL: https://www.un.org/ development/desa/en/news/population/2018-revision-of-worldurbanization-prospects.html.
2. Alahakoon, Damminda, et al. «Self-building artificial intelligence and machine learning to empower big data analytics in smart cities». Information Systems Frontiers (2023): 1-20.

УДК 004.8
О. Стець
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ОПТИМІЗАЦІЇ SWAP ПОКАЗНИКІВ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ПІДМІНИ ОБЛИЧЬ

UDC 004.8
O. Stets

SWAP METRICS OPTIMIZATION METHODS FOR MOBILE FACE ANTI-SPOOFING NEURAL NETWORKS

Виявлення підміни обличчя (FAS) має вирішальне значення для захисту систем розпізнавання обличчя, особливо на мобільних пристроях, де обчислювальні ресурси, пам'ять та енергія є обмеженими. Традиційні нейронні мережі FAS часто занадто великі та вимогливі до ресурсів для мобільного розгортання, що робить їхню оптимізацію важливою. Завдання полягає в збереженні високої точності виявлення при дотриманні строгих вимог до розміру, швидкодії та енергоефективності (SWAP) моделі, щоб забезпечити продуктивність у реальному часі та ефективність на мобільних платформах.

Оптимізація моделей FAS для мобільних пристроїв передбачає кілька методів. «Квантування моделі» (Model Quantization) є широко використовуваною технікою, яка знижує точність вагових коефіцієнтів моделі та активації з 32-розрядного числа з плаваючою точкою до нижчого розряду, наприклад 8-розрядного цілого числа. Цей підхід значно зменшує розмір моделі та прискорює роботу з мінімальним впливом на точність. Метод «Виключення ваг» (Pruning) видаляє зайві ваги, щоб мінімізувати використання обчислень і пам'яті. «Дистиляція знань» (Knowledge Distillation) тренує компактну модель учня, щоб імітувати роботу більшої моделі-вчителя, фіксуючи основні шаблони з меншою складністю. Полегшені архітектури, такі як MobileNet, ShuffleNet та EfficientNet, оптимізують дизайн моделі для мобільних платформ. «Пошук нейронної архітектури» автоматизує виявлення ефективних архітектур. «Навчання зі змішаною точністю» поєднує різні числові точності, наприклад, 16-бітні та 32-бітні числа з плаваючою комою, під час навчання та роботи моделі, з ціллю зменшення споживання пам'яті та прискорення обчислення без значної втрати точності.

Аналіз методів оптимізації SWAP показників показав, що підхід «Дистиляція знань», зокрема «дистиляція карти ознак», ідеально підходить для мобільного розгортання, дозволяючи малій моделі-учню на полегшеній архітектурі відтворювати точність великої моделі-вчителя, яка працює на непридатних для мобільних платформ архітектурах, наприклад ResNet. Такий змішаний підхід дозволяє учню імітувати активації проміжного рівня вчителя, покращуючи його здатність захоплювати дрібні деталі, необхідні для захисту від підробки обличчя. Окрім того, це покращує доменне узагальнення моделі-учня щодо невідомих атак підміни обличь.

Література

1. Yu Z., Wan J., Li X., Li S., Zhao G. NAS-FAS: Static-Dynamic Central Difference Network Search for Face Anti-Spoofing. URL: https://doi.org/10.1109/TPAMI.2020.3036338.
2. Cheng T., Zhang Y., Yin Y., Zimmermann R., Yu Z., Guo B. A Multi-Teacher Assisted Knowledge Distillation Approach for Enhanced Face Image Authentication. URL: https://doi.org/10.1145/3591106.3592280.
3. Kong Z., Zhang W., Wang T., Zhang K., Li Y., Tang X., Luo W., Dual Teacher Knowledge Distillation with Domain Alignment for Face Anti-spoofing. URL: https://arxiv.org/html/2401.01102v1.

УДК 004.7
П. С. Стрийвус; Р. І. Королюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СПОСОБИ БЕЗДРОТОВОЇ ПЕРЕДАЧІ ДАНИХ І ЇХ ЗАСТОСУВАННЯ

UDC 004.7
P. S. Struvyus; R. I. Koroliuk

METHODS OF WIRELESS DATA TRANSMISSION AND THEIR APPLICATION

Стартап IoT Вулик передбачає збір інформації з вуликів, як розміщених на стаціонарних пасіках, так і з окремо розташованих вуликів та вуликів розміщених на пересувних пасіках. Універсального оптимального методу бездротової передачі даних для вказаних умов не існує, тому у IoT-пристроях пропонується інтегрувати різні технології залежно від вимог до швидкості, дальності передачі та енергоспоживання.

При проведенні порівняння різних технологій бездротової передачі даних були проаналізовані методи, що використовуються в ряді промислових і побутових пристроїв, зокрема у сфері моніторингу, автоматизації та зв'язку. На основі цього аналізу, використовуючи рекомендації робіт [1, 2] вибір був зупинений на технологіях та їх застосуваннях в конкретних умовах, які подані в табл. 1.

Таблиця 1. Технології бездротової передачі даних та їх застосування

Технологія	Швидкість передачі	Дальність	Енерго-споживання	Застосування
Wi-Fi	До 1 гбіт/с	До 100 м	Високе	В межах стаціонарної пасіки
Bluetooth LE	До 3 мбіт/с	До 100 м	Низьке	В межах пересувної пасіки
LoRa	До 50 кбіт/с	До 15 км	Дуже низьке	Між окремо розміщеним вуликом та стаціонарною пасікою
GSM	До 200 кбіт/с	До 35 км	Помірне	Між стаціонарними та пересувними пасіками

Висновок. Для стаціонарних пасік найкраще використовувати Wi-Fi, бо ця система бездротової передачі даних вмонтована в контролери Raspberry Pico та можливе розгортання стаціонарної мережі Wi-Fi, яка покриватиме всю пасіку. У випадку пересувної пасіки, де відсутнє зовнішнє енергопостачання та довільне розташування вуликів, яке може змінюватися, оптимальне використання системи Bluetooth LE, що дозволяє зв'язати Raspberry Pi Pico з іншими Bluetooth-пристроями як вузол обміну даними. Між окремо розміщеним вуликом та стаціонарною пасікою передачу даних доцільно проводити використовуючи LoRa, через дуже низьке енергоспоживання та дальність передачі даних до 15 км. GSM може бути використано для глобально віддаленого моніторингу, але має значне енергоспоживання та витрати на зв'язок.

Література

1. Rostyslav Koroliuk, Vyacheslav Nykytyuk, Vitaliy Tymoshchuk, Veronika Soyka and Dmytro Tymoshchuk. Automated monitoring of bee colony movement in the hive during winter season. Proceedings of the 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024). Zboriv, Ukraine, October 02-04, 2024. CEUR Workshop Proceedings, 2024, 3842, pp. 147-156.
2. Королюк Р. І. Специфіка розроблення електронного курсу дисципліни «Сучасні пошукові системи та бібліографія» для вищих навчальних закладів. Імідж сучасного педагога. 2024. №1 (214). С. 26-30. DOI: 10.33272/2522-9729-2024-1(214)-26-30.

УДК 621.38
М. Стрембіцький, к.т.н., доцент; А. Кондратюк; Р. Мудрак
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНФОРМАЦІЙНА СИСТЕМА РОЗПІЗНАВАННЯ ТА ПРОГНОЗУВАННЯ ТРАЄКТОРІЇ ПОВІТРЯНИХ ЦІЛЕЙ

UDC 621.38
M. Strembitskyi, Ph.D., associate professor; A. Kondratyuk; R. Mudrak

INFORMATION SYSTEM FOR RECOGNITION AND PREDICTION OF TRAJECTORY OF AIR TARGETS

Метою роботи є створення інформаційної системи комп’ютерного сприйняття сцен шляхом розробки моделей комп’ютерного сприйняття, методів та архітектур адаптивної обробки відеопотоків у системах комп’ютерного зору, спрямованих на інтелектуальну обробку даних та їх розпаралелювання. Основні результати: розробка методології розпізнавання погано формалізованих об'єктів у неоднорідному полі уваги в реальному часі; метод поділу частково перекриваються об'єктів; дослідження методології оцінки якості та її розробка, зокрема, вибір найбільш ефективного методу та вдосконалення існуючого для оцінки якості в системах комп’ютерного зору, а також розробка апаратно-орієнтованого методу розпаралелювання відеопотоків на основі теплового представлення зображення.

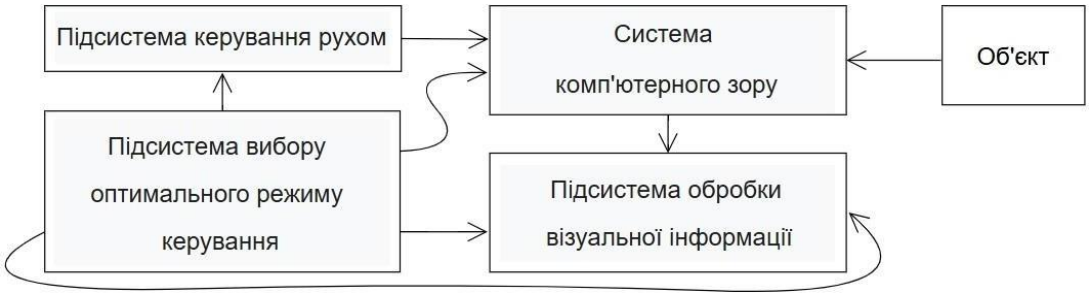


Рисунок 1. Структура адаптивної системи керування поворотом платформи

Адаптивна система складається з: об’єкту керування (поворотна платформа), системи комп’ютерного зору, підсистеми вибору оптимального режиму керування, системи обробки візуальної інформації, підсистеми керування рухом.

Наукова новизна даного дослідження полягає в прийнятті рішень в інтелектуальній інформаційній системі, що враховує багатоетапність вирішення задач маніпулювання об’єктами та навігації в системі. Зазначений вище підхід вимагає появи нової властивості систем прийняття рішень щодо виявлення та підтримки об’єктів, а саме здатності гнучко перебудовувати (адаптувати) роботу залежно від змін зовнішнього середовища, зміни мети чи окремих підцілей, у стані самої інформаційної системи. Застосування методів візуального контролю дозволяє адаптувати роботу приладів за рахунок широкого використання візуальної інформації про стан низьколітаючих повітряних цілей і прогнозування опорної траєкторії.

Література

1. Паламар М.І., Стрембіцький М.О., Паламар А.М. Проектування комп’ютеризованих вимірювальних систем і комплексів. Навчальний посібник. Тернопіль: ТНТУ. 2019. 150 с.
2. Батюк В.В, Стрембіцький М.О., Чайковський А.В. Розрахунок траєкторії безпілотних літаючих об ‘єктів у просторі. Матеріали VII Міжнародної студентської науково-технічної конференції «Природничі та гуманітарні науки. Актуальні питання». Тернопіль: ТНТУ. 2024. 5-6 с.

УДК 519.6
Т. С. Срогий; д.т.н., проф. Я. В. Литвиненко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОГЛЯД МАТЕМАТИЧНИХ МОДЕЛЕЙ ДЛЯ МОДЕЛЮВАННЯ ЦИКЛІЧНИХ СИГНАЛІВ В ЕКОНОМІЦІ

UDC 519.6
T. S. Srogy; Dr., Prof. I. V. Lytvynenko

REVIEW OF MATHEMATICAL MODELS FOR SIMULATING CYCLICAL SIGNALS IN THE ECONOMY

Математичні моделі циклічних сигналів в економіці використовуються для аналізу, прогнозування та управління коливаннями в економічних системах. Такі сигнали в економіці відображають повторювані зміни ключових показників, таких як ВВП, зайнятість, ціни або інвестиції.

Дана теза присвячена огляду математичних моделей циклічних сигналів в економіці. Розглянемо основні математичні моделі:

1. Класичні моделі економічних циклів:

- Модель Гаррода-Домара. Ця модель базується на співвідношенні між заощадженнями, інвестиціями та економічним зростанням;
- Модель Самуельсона-Хікса. Заснована на концепції мультиплікатора-акселератора. Вона описує регулярні коливання економічної активності.

2. Стохастичні моделі економічних циклів:

- ARIMA (AutoRegressive Integrated Moving Average). Це стохастична модель аналізу часових рядів, яка враховує автокореляцію між попередніми значеннями;
- Моделі випадкових процесів (наприклад, Браунівський рух). Економічний сигнал описується як комбінація тренду та стохастичних варіацій (адитивна модель).

3. Нелінійні динамічні моделі:

- Модель Гудвіна (хижак-жертва). Відображає взаємодію між зарплатами та зайнятістю;
- Рівняння Лотки-Вольтерри. Описує циклічну динаміку між різними економічними факторами;
- Модель Кальдора. Це нелінійна модель інвестиційних циклів.

4. Фрактальні та хаотичні моделі:

- Фрактальні моделі (Hurst exponent) Викорирстовують для аналізу економічних часових рядів для виявлення довгострокової залежності;
- Теорія детермінованого хаосу. Використовують для аналізу складних економічних систем через атрактори та чутливість до початкових умов.

5. Спектральний аналіз циклічності:

- Перетворення Фур'є. Використовується для аналізу частотних компонент економічних циклів. Представлення економічного сигналу у вигляді гармонік дозволяє виділяти домінуючі цикли;
- Вейвлет-аналіз. Дозволяє аналізувати цикли, які змінюють свою амплітуду чи частоту у часі.

6. Мережеві та агентно-орієнтовані моделі:

- Моделі взаємодії агентів. Економічні агенти моделюються як вузли мережі, між якими виникають циклічні процеси;
- Системна динаміка. Моделюються причинно-наслідкові зв'язки, які викликають економічні цикли (наприклад, підйоми та спади через попит та пропозицію).

Математичні моделі циклічних сигналів в економіці охоплюють як детерміновані, так і стохастичні підходи. Проте вибір моделі залежить від даних, наявності в них шуму, а також залежать від мети аналізу (прогнозування, оптимізація чи опис закономірностей).

УДК 004.9
А. А. Титжинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАХИСТ БЛОКЧЕЙНУ ВІД КВАНТОВИХ ОБЧИСЛЕНЬ

UDC 004.9
A. A. Tytzhynskyi

PROTECTION OF BLOCKCHAIN FROM QUANTUM COMPUTING

Блокчейн-технологія забезпечує прозорість і захищеність даних у багатьох сферах, таких як фінанси, логістика та охорона здоров'я. Однак із розвитком квантових обчислень постає загроза для існуючих криптографічних механізмів, які є основою безпеки блокчейну. Дослідження спрямоване на аналіз методів захисту блокчейну від квантових обчислень.

Квантові комп'ютери здатні значно прискорити виконання задач, які вважаються складними для класичних комп'ютерів. Алгоритм Шора дозволяє розв'язувати задачі факторизації та обчислення дискретного логарифма за поліноміальний час, що ставить під загрозу криптографічні алгоритми, такі як RSA та ECC, які широко використовуються в блокчейні. Для вирішення цих проблем досліджуються квантово-стійкі алгоритми, що включають криптографію на основі граток, хешів, кодів та багаточленів. Ці алгоритми забезпечують новий рівень захисту від атак квантових комп'ютерів[1].

Окрім криптографічних змін, модернізація механізмів консенсусу є важливим напрямом для посилення безпеки. Існуючі механізми, такі як Proof of Work, можуть бути замінені або модифіковані із врахуванням можливостей квантових обчислень. Досліджуються альтернативи, включаючи Proof of Stake з додатковим захистом і механізми Byzantine Fault Tolerance, що дозволяють підвищити стійкість системи до квантових атак. Гібридні системи, які поєднують класичні та квантово-стійкі алгоритми, забезпечують перехідний етап до більш безпечних стандартів [2].

Було проведено дослідження впливу квантових обчислень на найбільш поширені алгоритми блокчейну, такі як SHA-256 та ECDSA. Встановлено, що квантові комп'ютери можуть значно скоротити час підбору хешів або приватних ключів, що підвищує ймовірність атак на блокчейн-мережі. Це робить актуальним розробку нових стандартів і протоколів, які враховують можливості квантових технологій [3].

Для збереження безпеки блокчейну в умовах розвитку квантових обчислень необхідно впроваджувати квантово-стійкі криптографічні методи, адаптувати існуючі протоколи та підвищувати рівень досліджень у цій сфері. Стандартизація нових криптографічних алгоритмів та їх інтеграція в існуючі блокчейн-системи є пріоритетними завданнями для забезпечення довготривалої безпеки даних. Масштабованість і швидкодія нових рішень також повинні бути враховані при розробці цих систем, щоб вони могли відповідати сучасним вимогам [4].

Таким чином, розвиток квантових обчислень вимагає переосмислення основ безпеки блокчейну. Лише активні дослідження та інноваційні підходи дозволять зберегти довіру до технологій розподіленого реєстру в умовах квантової ери.

Література

1. Procedia Computer Science. Vol. 177, pp. 183-191. ArXiv. URL: https://arxiv.org/abs/2011.03460.
2. Allende M., López León D., Cerón S., Leal A., Pareja A., Da Silva M., Pardo A., Jones D., Worrall D., Merriman B., Gilmore J., Kitchener N., Venegas-Andraca S. E., 2021. Quantum-resistance in blockchain networks. International Journal of Quantum Information. Vol. 19, No. 7, pp. 1-15. ArXiv. URL: https://arxiv.org/abs/2106.06640.
3. Gate.io Research Team, 2023. Post-Quantum Cryptography in Blockchain Security. Blockchain Technology Research Journal. No. 12, pp. 45-52. Gate.io. URL: https://www.gate.io/uk/learn/articles/post-quantum-cryptography-in-blockchain-security/1061.
4. Cryptomus Editorial Team, 2022. Quantum Computers and Cryptocurrencies: Impact and Solutions. Journal of Blockchain Applications. Vol. 8, No. 3, pp. 27-34. Cryptomus. URL: https://cryptomus.com/uk/blog/quantum-computers-and-cryptocurrencies.

УДК 004.9
А. А. Титжинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПОРІВНЯЛЬНИЙ АНАЛІЗ КОНСЕНСУСНИХ АЛГОРИТМІВ У КОНТЕКСТІ ЇХНЬОЇ СТІЙКОСТІ ДО АТАК

UDC 004.9
A. A. Tytzhynskyi

COMPARATIVE ANALYSIS OF CONSENSUS ALGORITHMS IN THE CONTEXT OF THEIR RESISTANCE TO ATTACKS

Консенсусні алгоритми є ключовими елементами технології блокчейн, забезпечуючи узгодженість і безпеку розподіленого реєстру. Різні алгоритми мають унікальні підходи до вирішення завдань забезпечення стійкості до атак, таких як атаки 51%, сибіл-атаки та інші види порушень. Дослідження спрямоване на порівняльний аналіз таких алгоритмів, як Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS) та Practical Byzantine Fault Tolerance (PBFT) [1].

Proof of Work забезпечує безпеку через складність обчислювальних задач, що ускладнює реалізацію атак. Проте висока енергозатратність та можливість централізації через пул майнінгу є серйозними недоліками. Proof of Stake покладається на підтвердження транзакцій учасниками з найбільшими ставками. Це дозволяє зменшити енергозатрати, але підвищує ризики концентрації влади у великій кількості активів [2]. У контексті DPoS пропонується модель делегованої участі, що зменшує кількість валідаторів, роблячи мережу швидшою, але створює ризики, пов’язані з довірою до делегатів. PBFT спрямований на мінімізацію впливу зловмисників у мережах, які мають до однієї третини недобросовісних вузлів. Це робить його ефективним для приватних мереж, але малопридатним для масштабованих публічних мереж [3].

Дослідження показало, що стійкість до атак значною мірою залежить від механізмів вибору валідаторів, моделі винагороди та архітектури мережі. Наприклад, PoW ефективно протистоїть сибіл-атакам, але вразливий до атак 51% через можливість централізації майнінгу. PoS має нижчу ймовірність таких атак, але ризикує через економічну нерівність. DPoS забезпечує високу швидкість транзакцій, але залежність від обраних делегатів може стати слабким місцем. PBFT демонструє високий рівень стійкості в умовах обмеженої кількості учасників, проте його ефективність падає з ростом масштабів мережі [4]. Таким чином, вибір консенсусного алгоритму має базуватися на специфіці використання блокчейн-мережі, її розмірі, рівні довіри між учасниками та потенційних ризиках. Для публічних децентралізованих мереж найбільш підходять PoW і PoS, тоді як приватні мережі можуть використовувати PBFT для досягнення високої швидкості та безпеки [5].

Подальші дослідження мають зосереджуватися на розробці гібридних моделей, які поєднують переваги різних підходів, мінімізуючи їхні недоліки. Це дозволить забезпечити більшу стійкість блокчейн-систем до атак та підвищити їхню ефективність у різних умовах використання.

Література

1. Zhebka S. V., Vlasenko V. O., Aronov A. O., Kolodiuk A. V., 2024. Solution to the dilemma of choosing a consensus algorithm in distributed systems. TIT: Telecommunications and Information Technology. No. 3, pp. 25-34. tit.dut.edu.ua.
2. Hilevskyi O. M., 2023. Comparative analysis of existing cryptocurrencies with the PoS consensus algorithm from the perspective of effective implementation reserves in terms of speed. Diploma work. Kyiv Polytechnic Institute. ela.kpi.ua.
3. Albrecht J., Andreina S., Armknecht F., Karame G., Marson G., Willingmann J., 2024. Larger-scale Nakamoto-style Blockchains Don't Necessarily Offer Better Security. ArXiv. URL: https://arxiv.org/abs/2404.09895.
5. «Analysis of consensus mechanisms in decentralized systems», 2023. A review of various consensus algorithms, including Proof of Work, Proof of Stake, Delegated Proof of Stake, and Practical Byzantine Fault Tolerance. PeerDH. peerdh.com.
6. «Performance benchmarks of consensus algorithms for decentralized oracles», 2023. Evaluation of key performance metrics of consensus algorithms such as throughput, latency, scalability, and fault tolerance, with comparisons of PoW, PoS, DPoS, and PBFT. PeerDH. peerdh.com.

УДК 355.:316.(477)
В. Федорієнко, канд. техн. наук; О. Жук, канд. техн. наук, доцент
(НУОУ)

ПІДХІД ДО МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ІНТЕРЕСАХ СИЛ ОБОРОНИ УКРАЇНИ

UDC 355.:316.(477)

V. Fedorienko, Ph.D. technical sciences; O. Zhuk, Ph.D. technical Sciences, associate professor

APPROACH TO MONITORING THE INFORMATION SPACE IN THE INTERESTS OF THE DEFENSE FORCES OF UKRAINE

В сучасних конфліктах інформація використовується як ефективна зброя, здатна маніпулювати громадською думкою, підривати довіру до влади, дестабілізувати ситуацію в країні та навіть провокувати соціальні заворушення. Саме тому, моніторинг інформаційного простору (далі – МІП) набуває все більшої важливості в умовах сучасних гібридних воєн, для отримання інформаційної переваги. Сили оборони України, як ніколи раніше, потребують ефективних інструментів для виявлення, аналізу та нейтралізації інформаційних загроз. Сучасні війни ведуться гібридними методами, що поєднують військові дії з інформаційними операціями, кібератаками, економічним тиском та іншими формами впливу. МІП допомагає розпізнавати та аналізувати ці гібридні загрози, адекватно реагувати на них та мінімізувати їхній негативний вплив. Інтернет та соціальні мережі забезпечують миттєве поширення інформації, що використовується для поширення дезінформації та ворожої пропаганди. За допомогою МІП можливо оперативно відстежувати та аналізувати інформаційні потоки, виявляти фейкові новини та протидіяти поширенню шкідливого контенту. Інформація є ключовим фактором для прийняття рішень на всіх рівнях, від військового командування до громадянського суспільства. МІП забезпечує достовірною інформацією, необхідною для адекватного реагування на загрози та прийняття ефективних рішень. Інформаційні атаки можуть бути спрямовані на критичну інфраструктуру, таку як енергетичні мережі, транспортні системи, фінансові установи тощо. Завдяки МІП можливо завчасно виявити такі атаки та забезпечити стабільність та функціонування життєво важливих об'єктів. МІП в умовах сучасних війн та гібридних загроз є невід'ємною складовою національної безпеки. Він дозволяє вчасно виявляти та протидіяти інформаційним атакам, захищати критичну інфраструктуру, забезпечувати громадян достовірною інформацією та підтримувати стабільність в країні.

Ситуація щодо підходу до моніторингу інформаційного простору України, який кардинально мав би змінитися з початком широкомасштабної збройної агресії російської федерації проти України з лютого 2022 року, на жаль, і досі потребує усвідомлення та є теоретичним та практичним завданням, яке потребує вирішення.

УДК 004.056
В. Р. Цвігун; М. В. Деркач, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ БЕЗПЕКИ МОБІЛЬНИХ ДОДАТКІВ ЗА ДОПОМОГОЮ MOBSF

UDC 004.056
V. R. Tsvihun; M. V. Derkach, Ph.D., Assoc. Prof.

SECURITY ANALYSIS OF MOBILE APPLICATIONS USED BY MOBSF

За останні роки мобільні додатки стали невід'ємною частиною нашого повсякденного життя. Ми використовуємо їх для комунікації, розваг, фінансових операцій та багатьох інших цілей. Тим не менш, зі зростанням популярності мобільних додатків зростає і ризик їхньої безпеки, тепер доступ до цінної інформації можна отримати, зламавши програму на смартфоні користувача. У зв'язку з цим аналіз захищеності та безпеки мобільних додатків стає надзвичайно важливим завданням.

Для вирішення цього завдання, перш за все необхідно визначити потенційні загрози та ризики, які можуть вплинути на безпеку програми, що включає оцінку потенційних вразливостей програмного забезпечення, аналіз мережевих потоків та перевірку на виток інформації. Також необхідно провести тестування на SQL-ін'єкції, перехоплення даних та інші атаки. Важливо перевірити, як програма перевіряє ідентифікацію користувача та надає доступ до функцій.

MobSF (Mobile Security Framework) – це один із найкращих інструментів для аналізу мобільних додатків. MobSF — комплексне автоматизоване середовище оцінки безпеки мобільних додатків для Android, iOS та Windows, яке виконує як статичний, так і динамічний аналіз безпеки мобільних додатків.

Для аналізу безпеки було запущено MobSF у Docker-контейнері, налагоджено сканування мобільного додатку, зроблено аналіз результатів та створено звіт. Результати включають інформацію про знайдені вразливості, ступінь їх серйозності та рекомендації щодо усунення; перевірку маніфестів; відстеження дозволів, які потрібні додатку для роботи; аналіз мережної безпеки; перевірку актуальності сертифікатів. Сервіс оцінює загрози за міжнародним загальновизнаним стандартом в інформаційній безпеці Common Vulnerability Scoring System (CVSS). MobSF надає оцінку безпеки кожному відсканованому додатку, вказуючи відсоток дотримання рекомендацій щодо безпеки.

Було проаналізовано 20 мобільних додатків, 17 з яких мають щонайменше один сумнівний дозвіл, це свідчить про поширену практику зловживання рекламними дозволами та потенційній передачі даних стороннім компаніям, звідки і отриманні оцінки в діапазоні 40-48 з 100 на середньому рівні ризику, в разі якщо конфіденційні дані будуть використовуватись не за призначенням.

Підсумовуючи, зазначимо, що MobSF дійсно дозволяє сканувати мобільні програми на предмет вразливостей у коді та конфігурації; використовує різні статичні та динамічні аналізатори для виявлення вразливостей; може вилучати дані з мобільних програм, такі як рядки, URL-адреси, ключі API та іншу конфіденційну інформацію; генерує докладні звіти про знайдені вразливості та рекомендації щодо усунення проблем безпеки; може інтегруватися з іншими інструментами безпеки, такими як Burp Suite, ZAP та Metasploit, що дозволяє підвищити ефективність тестування.

Література

1. Деркач, М. В., Хомишин, В. Г., & Гудзенко, В. О. Тестування безпеки вебресурсу на базі інструментів для сканування та виявлення вразливостей. Наукові вісті Далівського університету. Електронне видання. 2023. №25.

УДК 628.8
В. Фецак; Є. Тиш, к.т.н., доц
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕТОДІВ ІНТЕГРАЦІЇ СИСТЕМ АДАПТИВНОГО УПРАВЛІННЯ МІКРОКЛІМАТОМ ТА ОПТИМІЗАЦІЇ ЕНЕРГОВИТРАТ У РОЗУМНОМУ БУДИНКУ

UDC 628.8
V. Fetsak; I. Tysh, Ph.D., Associate Prof.

RESEARCH OF ALGORITHMS FOR ADAPTIVE CONTROL OF MICROCLIMATE QUALITY AND ENERGY CONSUMPTION OPTIMIZATION IN A SMART HOME

Сучасні системи розумного будинку інтегрують автоматизовані методи управління мікрокліматом, що дозволяє оптимізувати енергоспоживання та покращити комфорт для мешканців. Одним із ключових завдань таких систем є підтримання комфортного середовища для мешканців за мінімальних енерговитрат. У даному дослідженні основна увага приділена адаптивному управлінню мікрокліматом у житлових приміщеннях [3].

Адаптивне управління дозволяє системі автоматично підлаштовуватися до змін зовнішніх та внутрішніх умов, таких як температура, вологість та якість повітря [1]. Для досягнення цієї мети було розроблено та протестовано алгоритми, що забезпечують динамічне корегування параметрів мікроклімату, включаючи прогнозування змін умов на основі зібраних даних з сенсорів таких як DHT22 для контролю температури, AM2302 для вологості, MQ-135 для якості повітря, освітлення забезпечується через модулі BH1750, інтегровані з LED-лампами [2].

Особливістю запропонованого підходу є використання адаптивного PID-регулювання з елементами машинного навчання, що дозволяє прогнозувати зміну параметрів мікроклімату та оптимізувати роботу виконавчих механізмів [4]. Наприклад, якщо прогнозується підвищення температури через сонячне нагрівання, система автоматично знижує інтенсивність роботи нагрівачів, зберігаючи комфортні умови [5]. Функція управління задається рівнянням:

$$u(t) = K_p e(t) + K_i \int e(t)dt + K_d \frac{de(t)}{dt}, \quad (1)$$

де $e(t)$ – відхилення поточного значення параметра від заданого, K_p, K_i, K_d – коефіцієнти PID-регулятора.

Для оптимізації енерговитрат використовується цільова функція:

$$E_{opt} = \min \left(\sum_{i=1}^{n} P_i \cdot t_i \right), \quad (2)$$

де P_i – потужність пристрою, t_i – час його роботи, n – кількість пристроїв.

Прототип системи був протестований у реальних умовах, і результати експериментів підтвердили її ефективність [6]. Встановлено, що адаптивне управління дозволяє значно підвищити енергоефективність будинку, одночасно забезпечуючи комфортні умови проживання [3].

На рисунку 1 представлено графік зміни температури та вологості, і зниження енергоспоживання під час роботи алгоритму системи.

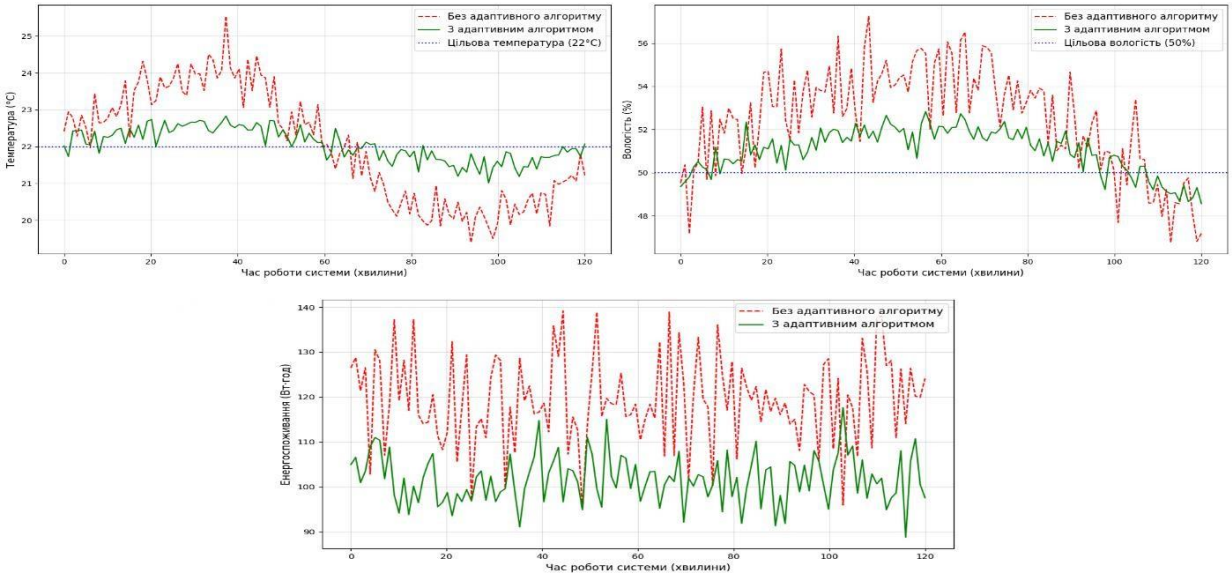


Рисунок 1. Графіки зміни температури та вологості, і зниження енергоспоживання під час роботи алгоритму системи

Експериментальні випробування показали:

– Точність підтримання параметрів мікроклімату: ±0.5°C для температури, ±2% для вологості;

– Зниження енергоспоживання на 15% порівняно зі стандартними алгоритмами;

– Висока стабільність роботи навіть за умов раптових змін температури та вологості.

Висновок. Розроблені алгоритми забезпечують адаптивне управління параметрами мікроклімату, мінімізуючи енерговитрати. Подальший розвиток системи передбачає інтеграцію додаткових сенсорів та впровадження більш складних алгоритмів машинного навчання для прогнозування довготривалих змін.

Література

1. Angelopoulos C., Gondchawar S., Kawitkar R. IoT for Microclimate Monitoring in Greenhouses. *Jurnal FP Unila*, 2020. – No 34, PP. 50-60. – Режим доступу: https://jurnal.fp.unila.ac.id.
2. IEEE Xplore. IoT-Based Weather Monitoring System Using Arduino UNO. *IEEE Conference Publication*, 2024. – Vol. 12, No 3, PP. 120-130. – Режим доступу: https://ieeexplore.ieee.org/document/9357748.
3. MDPI. IoT-Enhanced Decision Support System for Real-Time Microclimate Monitoring and Control. *MDPI Sensors Journal*, 2024. – Vol. 22, No 10, PP. 985-1001. – Режим доступу: https://www.mdpi.com.
4. WebbyLab. Automated Greenhouse Management with IoT. *WebbyLab Insights*, 2023. – Режим доступу: https://webbylab.com.
5. IJSTE. IoT-Based Environmental Monitoring System Using Arduino UNO and Thingspeak. *IJSTE Journal of Engineering Science*, 2023. – Vol. 4, Issue 9, PP. 65-72. – Режим доступу: https://www.ijste.org.
6. Hafiz R., Alam T., Dwiratna W. Efficient Use of IoT for Energy Management in Residential Spaces. *Sustainable Energy Journal*, 2021. – Vol. 18, No 4, PP. 45-53.

УДК 004.94
В. Фецак; Є. Тиш, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕТОДІВ ІНТЕГРАЦІЇ МУЛЬТИСЕНСОРНИХ СИСТЕМ ДЛЯ АДАПТИВНОГО МОНІТОРИНГУ ТА ОПТИМІЗАЦІЇ МІКРОКЛІМАТУ В РОЗУМНОМУ БУДИНКУ

UDC 004.94
V. Fetsak; I. Tysh, Ph.D., Associate Prof.

RESEARCH OF MULTI-SENSOR SYSTEM INTEGRATION METHODS FOR ADAPTIVE MONITORING AND MICROCLIMATE OPTIMIZATION IN A SMART HOME

Розумні будинки інтегрують мультисенсорні системи, які підвищують ефективність моніторингу мікроклімату. Мультисенсорні системи забезпечують не лише збір даних, але й їхню інтеграцію для динамічного адаптивного управління мікрокліматом у приміщенні забезпечуючи персоналізацію і оптимізацію енерговитрат [1], [3].

У даному дослідженні основна увага приділена інтеграції сенсорів для створення єдиної адаптивної системи. Впровадження таких систем дозволяє адаптувати управління системою що враховуватиме зовнішні та внутрішні фактори, включаючи освітлення, вологість, температуру та якість повітря [4].

Особливістю запропонованого підходу є використання алгоритмів кластеризації для об’єднання даних від сенсорів у кластери, що дозволяє оптимізувати обробку інформації та маршрутизацію сигналів. Інтеграція алгоритмів машинного навчання забезпечує точніше прогнозування змін мікроклімату, враховуючи коливання параметрів, таких як температура, вологість і якість повітря. Для стабілізації параметрів використовуються інтелектуальні підходи до PID-регулювання, які адаптуються до отриманих сенсорних даних. Це дозволяє враховувати зовнішні фактори, наприклад, зміну температури від сонячного нагрівання або підвищення вологості під час приготування їжі [2].

На рисунку 1 представлено графіки зміни температури, вологості та енергоспоживання в реальних умовах роботи системи.

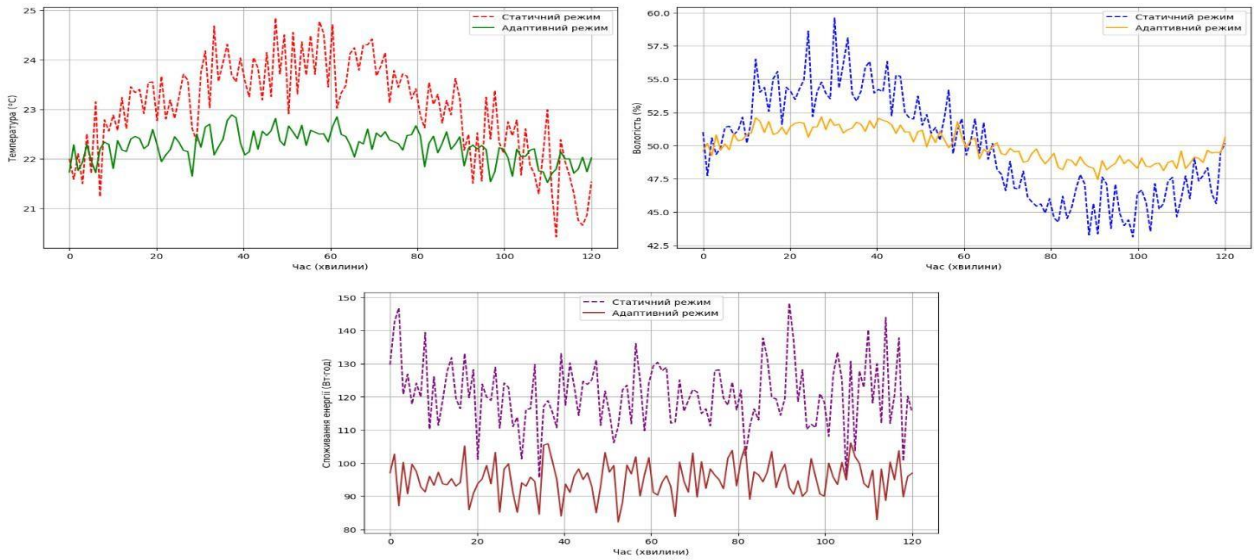


Рисунок 1. Графіки зміни температури, вологості та енергоспоживання в реальних умовах роботи системи

Регулювання мікроклімату базується на прогнозуванні параметрів, використанні кластеризації даних і функції оптимізації роботи системи, формула:

$$U = \frac{1}{n} \sum_{i=1}^{n} \left(\frac{W_i \cdot \Delta P_i}{T_i} \right), \quad (1)$$

де *U* - ефективність роботи системи, *Wi* – ваговий коефіцієнт сенсора *i*, Δ*Pi* – зміна параметра мікроклімату (температура, вологість тощо), *Ti* – час реакції системи, *n* – кількість активних сенсорів [1], [5].

Прототип системи був протестований у приміщенні площею 50 м² із симуляцією реальних умов.

Експериментальні випробування показали:

– Покращення точності підтримання параметрів: ±0.4°C для температури, ±1.2% для вологості;

– Зниження енергоспоживання до 20%;

– Час реакції системи скоротився до 7 секунд.

Висновок. Інтеграція мультисенсорних систем у комбінації з інтелектуальними алгоритмами управління демонструє значне покращення ефективності роботи системи мікроклімату. Подальші дослідження спрямовані на вдосконалення алгоритмів кластеризації та впровадження штучного інтелекту [6].

Література

1. IoT-Enhanced Decision Support System for Real-Time Greenhouse Microclimate Monitoring and Control. Sensors (Switzerland), 2020. – Vol. 20, No. 7, PP. 1–16. – Режим доступу: https://www.mdpi.com.
2. Development of a Low-Cost Microclimate Monitoring System through IoT. Archive, 2022. – Режим доступу: https://archive.org.
3. Sensor Systems for Greenhouse Microclimate Monitoring and Control: A Review. Journal of Biosystems Engineering, 2020. – Vol. 45, No. 3, PP. 12–34. – Режим доступу: https://link.springer.com.
4. An IoT-Based System to Control the Greenhouse’s Microclimate. Springer, 2019. – Режим доступу: https://link.springer.com.
5. Development and Verification of Microclimate Control System. Sciendo, 2023. – Vol. 22, No. 1, PP. 10–25. – Режим доступу: https://sciendo.com.
6. Evaluating Models for Predicting Microclimatic Parameters in Greenhouses. Applied Ecology and Environmental Research, 2020. – Vol. 18, No. 2, PP. 2141–2161. – Режим доступу: https://doi.org.

УДК 004.9
А. Хом'як
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ СИНТЕТИЧНИХ СИГНАЛІВ ДЛЯ ПОКРАЩЕННЯ КЛАСИФІКАЦІЇ МЕГ СИГНАЛІВ

UDC 004.9
A. Khomiak

IMPROVEMENT OF MEG SIGNAL CLASSIFICATION VIA THE USAGE OF SYNTHETIC SIGNALS

Для підвищення ефективності класифікації сигналів магнітоенцефалограм (МЕГ), особливо у випадках, коли обсяг доступних розмічених даних обмежений, пропонується застосувати стратегію попереднього навчання, яка базується на відновленні коефіцієнтів перетворення Фур'є. Цей підхід спрямований на формування надійних та узагальнених представлень сигналів у частотній області, що може покращити точність класифікації.

Процес починається з генерації різноманітного набору синтетичних даних, що імітують характеристики реальних МЕГ-сигналів. Для цього використовуються методи моделювання, такі як системи ітераційних функцій та фрактальний броунівський рух, які дозволяють створювати складні та реалістичні патерни сигналів[1]. Кожен згенерований сигнал піддається перетворенню Фур'є, що дозволяє представити його у вигляді спектра частот.

На наступному етапі задіюється модель кодувальника-декодувальника, побудована на архітектурі Transformer[2], яка попередньо навчається на цих синтетичних даних. Кодувальник, аналізуючи вхідний МЕГ-сигнал, витягує з нього найважливіші ознаки, використовуючи механізм самостійної уваги. Цей механізм дозволяє моделі ефективно враховувати взаємозв'язки між різними частинами сигналу, навіть якщо вони знаходяться на значній відстані одна від одної. Декодувальник, в свою чергу, намагається відновити початкові коефіцієнти перетворення Фур'є на основі інформації, отриманої від кодувальника.

Для навчання моделі використовується метод мінімізації середньоквадратичної помилки (MSE) між передбаченими та фактичними коефіцієнтами Фур'є. Такий підхід спонукає модель до формування максимально точного та стиснутого представлення інформації про частотний спектр сигналу.

Після завершення попереднього навчання кодувальник використовується як ефективний витягувач ознак для класифікації реальних МЕГ-сигналів[3]. Вивчені представлення частотної області передаються до класифікатора, побудованого на основі повністю зв'язаної нейронної мережі (FCNN).

Очікується, що використання такої стратегії попереднього навчання дозволить значно покращити продуктивність класифікатора FCNN, особливо в умовах обмеженого доступу до розмічених МЕГ-даних. Завдяки здатності моделі узагальнювати знання, отримані на синтетичних даних, вона зможе ефективніше розпізнавати важливі патерни в реальних сигналах та підвищити точність класифікації.

Література

1. H. Kataoka *та ін.*, «Pre-Training without natural images», *Int. J. Comput. Vis.*, т. 130, № 4, с. 990–1007, лют. 2022. Дата звернення: 11 груд. 2024. [Онлайн]. Доступно: https://doi.org/10.1007/s11263-021-01555-8.
2. A. Vaswani *та ін.* «Attention is all you need». [Онлайн]. Доступно: https://arxiv.org/abs/1706.03762.
3. H. Ismail Fawaz, G. Forestier, J. Weber, L. Idoumghar та P.-A. Muller, «Transfer learning for time series classification», у *2018 IEEE Int. Conf. Big Data (Big Data)*. 2018, с. 1367–1376. [Онлайн]. Доступно: https://doi.org/10.1109/BigData.2018.8621990.

УДК 004.056

І. С. Цимбрак
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РЕАЛІЗАЦІЯ КРИПТОАЛГОРИТМУ ХЕШУВАННЯ SHA256

UDC 004.056

I. S. Tsymbrak

IMPLEMENTATION OF THE SHA256 HASHING CRYPTO ALGORITHM

Реалізація мовою Python містить чотири модулі: «binary_operations», «encoding», «SHA256», «main». Їх призначення такі:

– в першому модулі реалізовані операції над двійковими рядками (векторами) - операція побітового виключного або, циклічного зсуву вправо, логічного зсуву вправо, двійкового додавання двох векторів за модулем 2^{32} , операція побітового «І», операція побітового заперечення;

– у другому модулі були реалізовані методи кодування - перетворення текстового рядка в бінарний рядок кодування UTF8, переведення цілого десяткового числа в двійкове подання у вигляді рядка, переведення рядка двійкового подання у рядок шістнадцяткового подання;

– у третьому модулі було реалізовано клас, що містить функціонал хеш-функції. При створенні екземпляра класу відбувалася ініціалізація констант. Було реалізовано метод «hash_data», який приймає вхідний текстовий рядок. У ньому відбувалося початкове скидання констант (щоб забезпечити правильне хешування за нового виклику даного методу), після чого проводився алгоритм хешування, описаний у попередньому розділі. Наприкінці отриманий результат переводився в шістнадцяткову форму і повертався;

– в останньому модулі знаходиться точка входу в програму, в якій створювався рядок і подавався на вхід функції хешування.

Для перевірки коректності алгоритму було здійснено порівняння для пробного тексту, що містить 7965 символів. Як «еталонна» реалізація використовувалася реалізація SHA256 у бібліотеці «hashlib» [1]. Результати наведено на рис. 1. На ньому зображені підсумкові значення змінних у шістнадцятковій і двійковій формі. Далі вказана їхня конкатенація – результат алгоритму SHA256. В останньому рядку вказано результат хешування ««hashlib.sha256».

```
h0 = 082012D9 = 00001000001000000001001011011001
h1 = 52CBDDD3 = 01010010110010111101110111010011
h2 = 03728F4B = 00000011011100101000111101001011
h3 = 7AAF36FF = 01111010101011110011011011111111
h4 = 698496A9 = 01101001100001001001011010101001
h5 = 20B4E904 = 00100000101101001110100100000100
h6 = 599F1BA5 = 01011001100111110001101110100101
h7 = 8F28EE76 = 10001111001010001110111001110110
082012D952CBDDD303728F4B7AAF36FF698496A920B4E904599F1BA58F28EE76
082012D952CBDDD303728F4B7AAF36FF698496A920B4E904599F1BA58F28EE76
```

Рисунок 1. Результати роботи власної реалізації SHA256 та бібліотеки «hashlib»

Література

1. Hashlib — Secure hashes and message digests. [Електронний ресурс] – Режим доступу: https://docs.python.org/3/library/hashlib.html (дата звертання: 08.11.24).

УДК 004.65
А. Б. Чекановський; К. Б. Швирло
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СТРАТЕГІЇ ПОКРАЩЕННЯ ПРОДУКТИВНОСТІ РЕЛЯЦІЙНИХ СИСТЕМ КЕРУВАННЯ БАЗАМИ ДАНИХ

UDC 004.65
A. B. Chekanovskyi; K. B. Shvyrlo

STRATEGIES FOR IMPROVING PERFORMANCE OF RELATIONAL DATABASE MANAGEMENT SYSTEMS

У сучасних інформаційних системах продуктивність баз даних є критичною, адже затримки у виконанні запитів, надмірне споживання ресурсів та ускладнення масштабування можуть впливати на швидкість обробки інформації, зручність роботи користувачів та загальну продуктивність бізнесу. З огляду на це, виникає потреба у впровадженні рішень, які дозволять не лише покращити швидкість і надійність доступу до даних, але й забезпечити гнучкість та стійкість баз даних в умовах підвищених навантажень.

Індексація є основною технікою для прискорення пошуку та вибірки даних. Вона включає одиночні індекси для прискорення виконання запитів, що здійснюють фільтрацію чи сортування на основі одного стовпця, складені індекси, що забезпечують оптимізацію складніших запитів, а також спеціалізовані структури, такі як GIN (Generalized Inverted Index) та GiST (Generalized Search Tree) індекси, які забезпечують ефективну роботу з нетиповими даними або специфічними типами пошуку [1].

Грамотна побудова SQL-запитів, а також використання відповідних інструментів для аналізу та оптимізації коду також дозволяють скоротити час виконання складних запитів і зменшити навантаження на базу даних. Правильне налаштування кешу дозволяє суттєво знизити затрати на обчислення і скоротити час виконання запитів, зменшуючи навантаження на сервер бази даних. Кешування є ефективним способом зменшення кількості звернень до бази даних при однотипних запитах, забезпечуючи швидкий доступ до часто використовуваних даних.

Нормалізація бази даних допомагає уникнути надлишковості даних та оптимізувати структуру. Проте, в деяких випадках, денормалізація може бути також доцільною, особливо коли потрібно мінімізувати кількість JOIN-операцій у запитах для прискорення їх виконання [2].

Реплікація та фрагментування (шардінг) допомагають розподіляти дані між кількома вузлами або серверами, забезпечуючи балансування навантаження та зменшення часу доступу до даних [3]. Апаратні ресурси, зокрема об’єм пам'яті, потужність процесора, тип дискової підсистеми, також грають важливу роль в оптимізації, а для систем з інтенсивним використанням дискової підсистеми, використання різних рівнів RAID може істотно підвищити продуктивність баз даних.

Отже, впровадження вищенаведених стратегій покращення продуктивності реляційних баз даних дозволяє суттєво підвищити ефективність роботи систем.

Література

1. Recommendations for optimizing data. Microsoft Learn. URL: https://learn.microsoft.com/en-us/azure/well-architected/performance-efficiency/optimize-data-performance.
2. Udasi A. Denormalized Data Explained. Zenduty Blog. URL: https://www.zenduty.com/blog/data-denormalization.
3. Learn When to Use Database Replica and Database Sharding for Systems Design. Java Challengers. URL: https://javachallengers.com/database-replica-and-sharding.

УДК 658.8
О. Чорновол
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНФОРМАЦІЙНА СИСТЕМА ДЛЯ МЕРЧАНДАЙЗИНГУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ КОМП'ЮТЕРНОГО ЗОРУ

UDC 658.8
O. Chornovol

INFORMATION SYSTEM FOR MERCHANDISING USING COMPUTER VISION TECHNOLOGIES

Мерчандайзинг – це важливий елемент маркетингу, спрямований на підвищення привабливості товару на полицях магазинів та стимулювання продажів. Він передбачає раціональне розміщення продукції, щоб вона виглядала максимально помітною для покупця. У сучасному світі, де конкуренція серед брендів надзвичайно висока, якість представлення товару на полицях може стати ключовим фактором успіху [1].

Проте оцінка розміщення товару залишається складним і часозатратним завданням, яке залежить від людського фактора. Мерчендайзери повинні вручну перевіряти полиці магазинів, що забирає багато часу та не гарантує високої точності. Особливо це актуально для великих торговельних мереж, де потрібно аналізувати велику кількість магазинів.

Для вирішення цієї проблеми у проєкті була розроблена інформаційна система для автоматизації оцінки якості представлення товару. Основною функцією цієї системи є обчислення кількості одиниць товару на фотографії. Мобільний додаток, створений у рамках проєкту, дозволяє мерчендайзерам швидко отримувати дані про наявність продукції та оцінювати її представлення, а також порівнювати з конкурентами.

Для реалізації системи використовувалися сучасні технології, які забезпечують її ефективність та точність. Основними інструментами стали мови програмування Python і Swift. Python використовувався для серверної частини системи та реалізації алгоритмів обробки зображень, завдяки своїй гнучкості та багатству бібліотек. Бібліотека комп’ютерного зору OpenCV дозволила реалізувати основні етапи обробки зображень, включаючи попередню підготовку даних і фільтрацію. Для розпізнавання об’єктів застосовувалася одна з найсучасніших моделей – YOLO (You Only Look Once), яка забезпечує високу точність і швидкість виявлення товарів на зображеннях [2].

Розроблена система спрощує роботу мерчендайзерів, зменшує ймовірність помилок та дозволяє швидко приймати управлінські рішення на основі отриманих даних. Вона є перспективним інструментом для підвищення ефективності мерчандайзингу та створення конкурентної переваги для брендів.

Література

1. Котлер Ф., Армстронг Г. «Принципи маркетингу» 2021 – 101с.
2. Szeliski, R. «Computer Vision: Algorithms and Applications» 2010 – 69с.

.

УДК 004.77
К. Чурбаков
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ МОВИ LUA ДЛЯ РОЗШИРЕННЯ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ IDS/IPS

UDC 004.77
K. Churbakov

USING LUA LANGUAGE TO EXTEND THE FUNCTIONALITY OF IDS/IPS

Інформаційна безпека є важливим напрямком у сучасних технологіях, а системи виявлення та попередження вторгнень (IDS/IPS) відіграють ключову роль у захисті мереж. Однак стандартні функціональні можливості таких систем можуть бути недостатніми для специфічних потреб, що створює попит на інструменти їхньої адаптації. Використання мови Lua дозволяє створювати гнучкі налаштування та розширювати функціонал IDS/IPS, забезпечуючи адаптивність до нових загроз та підвищення ефективності їх роботи [1].

Впровадження Lua в системи виявлення вторгнень дозволяє ефективно інтегрувати специфічні сценарії аналізу мережевого трафіку, що важливо для виявлення складних і невідомих типів атак. Можливість використання користувацьких скриптів розширює функціональність базових механізмів IDS/IPS, роблячи систему більш гнучкою до змін у кіберзагрозах [2].

Метою дослідження є розробка і тестування інтеграції мови Lua з існуючими IDS/IPS для створення динамічних модулів, здатних забезпечити більш точне виявлення загроз і зменшення кількості хибних спрацьовувань. У роботі застосовувалася мова Lua для створення користувацьких скриптів, які інтегруються із платформою Suricata, що забезпечує обробку мережевого трафіку з дотриманням специфічних правил. Локальне тестування показало підвищення точності і надійності системи виявлення [3].

Особливістю мови Lua є її легкість і висока продуктивність, що робить її ідеальним вибором для інтеграції у реальному часі в умовах великих обсягів мережевого трафіку. Lua дозволяє створювати правила та логіку, які працюють паралельно з основними алгоритмами аналізу без зниження загальної продуктивності системи.

Результати роботи демонструють, що впровадження мови Lua у роботу IDS/IPS може суттєво розширити функціональні можливості цих систем, зокрема шляхом динамічного налаштування правил та адаптації до сучасних викликів у сфері інформаційної безпеки.

Література

1. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. URL: https://www.usenix.org/legacy/events/sec99/full_papers/paxson/paxson.pdf.
2. Roesch M. Snort: Lightweight Intrusion Detection for Networks. URL: https://www.snort.org/downloads/snort/white_paper.pdf.
3. Schlueter K. Lua Programming for Real-World Security. O'Reilly Media, 2020.

УДК 004.7:8
О. Швець; М. Стадник, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ ПІДОЗРІЛИХ ДІЙ ТА СПРОБ АТАК З ВИКОРИСТАННЯМ АНАЛІЗУ ТРАФІКУ З AMAZON CLOUD WATCH

UDC 004.7:8
O. Shvets; M. Stadnyk, Ph.D.

DETECTION OF SUSPICIOUS ACTIVITIES AND ATTACK ATTEMPTS USING TRAFFIC ANALYSIS FROM AMAZON CLOUD WATCH

Штучний інтелект (ШІ) покращує традиційний підхід до аналізу мережевого трафіку. Завдяки своїм можливостям обробки великих обсягів даних і виявлення складних патернів, ШІ стає незамінним інструментом у боротьбі з кіберзагрозами, включаючи атаки типу «отруєння кешу», DoS, DDoS, аналіз вмісту трафіку (вміст пакетів для виявлення шкідливого коду, фішингових атак), детекцію ботнетів, що використовуються для розповсюдженню спаму [1].

ШІ-системи можуть визначати відхилення від шаблону нормального трафіку, які можуть вказувати на атаку. Наприклад, раптовий сплеск запитів до незвичайного домену або зміни в поведінці користувача. Також системи штучного інтелекту створюють детальний профіль кожного користувача, включаючи звички перегляду, географічне розташування, браузер для використання. Будь-які відхилення від цього профілю можуть свідчити про компрометацію облікового запису. Також ШІ системи можуть прогнозувати потенційні атаки на основі аналізу історичних даних та трендів .

Amazon Cloud Watch – це потужний інструмент, який дозволяє не лише збирати дані про вашу інфраструктуру в AWS, але й проводити глибокий аналіз мережевого трафіку. Завдяки цій функціональності можливим є наступне:

- Виявлення аномалії. З використанням Amazon CloudWatch можливо достатньо швидко виявити піки трафіку, незвичайні шаблони або різкі спади, що можуть свідчити про проблеми з веб-сервісом або атаку.
- Оптимізувати витрати: Проаналізувавши обсяги трафіку, можливо оптимізувати розмір інстансів та інших ресурсів, знизивши таким чином витрати.
- Усунути проблеми з продуктивністю: Виявивши вузькі місця в мережі, можливо покращити загальну продуктивність сервісу чи додатку.
- Забезпечити безпеку: Аналізуючи трафік, можливо виявити підозрілу активність, яка може свідчити про спробу хакерської атаки.

Набір даних містив записи веб-трафіку, зібрані через AWS CloudWatch, спрямовані на виявлення підозрілих дій і потенційних спроб атак. Дані були згенеровані шляхом моніторингу трафіку до робочого веб-сервера з використанням різних правил виявлення для ідентифікації аномальних шаблонів. Первинний набір даних складався із 16 параметрів (час створення, час закриття зв'язку, IP джерела, кількість байтів отриманих, кількість надісланих байтів, країна, код відповіді HTTP, IP отримувача). Для класифікації трафіку було використано моделі Random Forest, CNN, Dense. Також було виявлено позитивну кореляцію між вхідними та вихідними байтами. Це свідчить про те, що більші байти на вході зазвичай відповідають вищим байтам на виході, що вказує на двонаправлений зв'язок між сервером і клієнтами.

Література

1. Abbasi M., Shahraki A., Taherkordi A. Deep learning fornetwork traffic monitoring and analysis (NTMA): A survey. Computer Communications 170, 2021, p. 19–41.

УДК 004.42
С. Шиндеровський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ЗАХИСТУ ДЛЯ СЕРВЕРНОЇ ЧАСТИНИ НА NODE.JS

UDC 004.42
S. Shinderovskiy

RESEARCH ON PROTECTION MECHANISMS FOR THE SERVER SIDE ON THE NODE.JS

Безпека веб-додатків є однією з ключових проблем сучасної кібербезпеки, враховуючи стрімке зростання кількості цифрових сервісів та обсягів оброблюваних ними даних. У зв'язку з розвитком технологій і збільшенням інтеграції веб-додатків у різні сфери життя – від банківської справи до соціальних мереж – забезпечення їх захищеності стає критично важливим. Будь-яка вразливість у веб-додатку може бути використана зловмисниками для крадіжки конфіденційної інформації, порушення роботи сервісу чи навіть компрометації цілих інформаційних систем [1].

Особливу увагу приділено вивченню загроз для серверної частини веб-додатків, які систематизовано за методологією STRIDE [3]. На основі цієї методології визначено шість основних категорій загроз: підробка, втручання в дані, відмова від авторства, розголошення інформації, відмова в обслуговуванні та підвищення привілеїв. Кожна із загроз детально проаналізована з огляду на її особливості, реальні приклади атак та сучасні методи запобігання [2].

Було проаналізувано основні загрози для серверної частини веб-додатків, використовуючи методологію STRIDE, яка охоплює підробку, втручання в дані, відмову від авторства, розголошення інформації, відмову в обслуговуванні та підвищення привілеїв. Для кожного типу загроз були запропоновані ефективні механізми захисту, такі як впровадження аутентифікації через JWT-токен та бібліотеки хешування, зокрема bcrypt, захист від XSS-атак, використання rate limiting та розмежування прав доступу на основі ролей. Також було додано журналювання дій користувачів, що забезпечує прозорість операцій на сервері. Інтеграція цих механізмів у серверну частину забезпечила багаторівневий підхід до мінімізації ризиків.

Практична значущість дослідження полягає у створенні універсального підходу до захисту серверної частини веб-додатків, який може бути використаний для реалізації надійних систем, стійких до сучасних загроз. Запропоновані механізми та методи дозволяють підвищити рівень безпеки даних, які передаються між клієнтом і сервером, зберігаються у базі даних або обробляються сервером.

У результаті проведеного дослідження доведено, що інтеграція заходів безпеки у процесі реалізації серверної частини дозволяє знизити ризики витоку даних, перехоплення запитів та несанкціонованого доступу до інформації. Це забезпечує надійність веб-додатків та підвищує їхню стійкість до кібератак. Таким чином, результати дослідження є цінним внеском у розвиток безпеки веб-технологій та можуть бути використані у подальших дослідженнях у сфері інформаційної безпеки.

Література

1. What is a Web Application?[електронний ресурс] / AWS Amazon – URL: https://aws.amazon.com/what-is/web-application/.
2. STRIDE Threat Modelling: What You Need to Know[електронний ресурс] / Alex Hewko – URL: https://www.softwaresecured.com/post/stride-threat-modelling.
3. Threat Modeling Methodology: STRIDE[електронний ресурс] / Claire Allen-Addy – URL: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.

УДК 004.9
В. Шендрик, к. т. н., доцент; Ю. Парфененко, к. т. н., доцент; І. Захарченко
(Сумський державний університет, Україна)

РЕІНЖИНІРИНГ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДТРИМКИ УПРАВЛІННЯ ЕНЕРГЕТИЧНИМИ МІКРОМЕРЕЖАМИ З ВІДНОВЛЮВАЛЬНИМИ ДЖЕРЕЛАМИ ЕНЕРГІЇ

V. Shendryk, Ph.D., Assoc. Prof.; Y. Parfenenko, Ph.D., Assoc. Prof.; I. Zakharchenko

RE-ENGINEERING OF THE INFORMATION SYSTEM TO SUPPORT THE MANAGEMENT OF ENERGY MICROGRIDS WITH RENEWABLE ENERGY SOURCES

Відновлювані джерела енергії (ВДЕ) є важливим інструментом у боротьбі з кліматичними змінами. Мікромережі на основі ВДЕ забезпечують автономне енергопостачання для підприємств і житлових будинків, підвищуючи надійність енергозабезпечення. Впровадження таких мікромереж активно триває, зокрема в Сумському державному університеті. Для моніторингу та управління мікромережою з використанням ВДЕ було створено веборієнтовану інформаційну систему [1]. Однак, для підвищення гнучкості та надійності, потрібно провести її реінжиніринг.

Проаналізувавши наявну інформаційну систему, встановлено, що при її реінжинірингу необхідно застосувати об’єктно-орієнтоване програмування (ООП). Використання ООП забезпечить створення модульного та гнучкого коду, що значно покращить його структуру та спростить підтримку і подальше розширення системи. Також для реінжинірингу найбільш доцільним є використання патерну MVC, який забезпечує чітке розділення даних, логіки та інтерфейсу користувача. Такий підхід покращує зручність розробки, спрощує підтримку та забезпечує масштабованість системи. MVC є одним із найпоширеніших стандартів у веброзробці та оптимальним вибором для створення сучасного та гнучкого вебзастосунку [2].

В рамках реінжинірингу було створено нову архітектуру інформаційної системи підтримки управління енергетичними мікрмережами з ВДЕ з використанням патерну MVC. Оновлено інтерфейс, покращено безпеку системи для захисту від потенційнх загроз, а також проведено Unit-тестування функціоналу для перевірки якості коду. Це дозволило значно підвищити зручність розробки та забезпечити більш ефективну підтримку системи. Як результат, система стала більш гнучкою, безпечною та масштабованою, що покращило її загальну ефективність і стабільність.

Література

1. В. Шендрик, Ю. Парфененко, В. Майковський, Д. Юрченко, С. Шендрик, «Підсистема збору, зберігання та візуалізації оперативних даних системи підтримки прийняття рішень для управління мікрогід», *Computer systems and information technologies,* no. 2, pp. 69–77, Jun. 2022, doi: 10.31891/csit-2022-2-8.
2. L. A. T. Nguyen, T. S. Huynh, D. T. Tran, and Q. H. Vu, «Design and Implementation of Web Application Based on MVC Laravel Architecture», *European Journal of Electrical Engineering and Computer Science,* vol. 6, no. 4, 2022, doi: 10.24018/ejece.2022.6.4.448.

УДК 004.6
Т. Щур; Г. Осухівська, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЕФЕКТИВНЕ УПРАВЛІННЯ ІНВЕНТАРЕМ ЗА ДОПОМОГОЮ ДРОНІВ І ШТУЧНОГО ІНТЕЛЕКТУ

UDC 004.6
T. Shchur; H. Osukhivska, Ph.D., Assoc. Prof.

EFFECTIVE INVENTORY MANAGEMENT USING DRONES AND ARTIFICIAL INTELLIGENCE

Поєднання технології дронів та штучного інтелекту, а саме систем розпізнавання, відкриває нові можливості для автоматизації систем інвентаризації, які раніше було виконати складніше. Системи з використанням штучного інтелекту дозволяють збирати, обробляти та аналізувати дані у режимі реального часу, що покращує системи управління процесом інвентаризації, що є важливим фактором для ефективного управління. Дрони забезпечуватимуть швидке та точне відстеження товарів на складах та їх ідентифікацію при використанні технологій розпізнавання для виявлення штрих-кодів і QR-кодів та їх читання. Ці системи використовують комп'ютерне бачення та алгоритми машинного навчання для ідентифікації, декодування та обліку товарів [1]. Завдяки цьому дрони можуть вільно переміщатися складським приміщенням для моніторингу товарів. Це зменшує потребу в безпосередній участі людини в процесах інвентаризації та мінімізує помилки.

Системи комп’ютерного бачення для виявлення об’єктів працюють шляхом розпізнавання шаблонів в сирих даних (значенях пікселів для зображень). Такі системи використовують згорткові нейронні мережі (CNN), які здатні аналізувати зображення в режимі реального часу. При цьому в системах інвентаризації можуть бути використані для розпізнавання та класифікації кодів чи самих товарів на складі.

Окрім автоматизації пошуку товару для його ідентифікації та інвентаризації у системі, для ефективного управління інвентарем також можна автоматизувати чи оптимізувати процес формування маршрутів для дронів [2]. Представлення схеми топографії приміщень складу у вигляді графу, дозволить використовувати такі алгоритми як метод Дейкстри чи Беллмана-Форда у виборі найшвидшого (відповідно найменш енергозатратного) шляху переміщення. Це дозволяє дронам швидко охоплювати великі ділянки складу, точно оновлювати інформацію про наявний товар, що вагомо зменшує час на інвентаризацію та підвищує її точність.

Отже, системи управління інвентарем, що використовують дрони з технологіями розпізнавання та моделі штучного інтелекту, є великим кроком вперед у автоматизації процесів. Використання сучасних алгоритмів дозволяють розпізнавати об’єкти в режимі реального часу, будувати шлях переміщення дрону та керувати ним.

Література

1. Cho Hyeon, et al. 2D barcode detection using images for drone-assisted inventory management. In: 2018 15th International Conference on Ubiquitous Robots (UR). IEEE, 2018. p. 461–465.
2. Maweni, Thabisa; Setati, Tiro; Botha, Natasha. Optimized path planning of a UAV for inventory management applications. In: MATEC Web of Conferences 388, 04021, 2023.

УДК 004.056
О. С. Юречко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНСАМБЛЕВІ МЕТОДИ МАШИННОГО НАВЧАННЯ

UDC 004.056
P. S. Yurechko

ENSEMBLE METHODS OF MACHINE LEARNING

Ансамблеві методи – це галузь машинного навчання, яка на вирішення завдання навчає множину моделей про «слабких учнів» і поєднує їх задля отримання кращого результату.

Можна виділити три категорії ансамблевих алгоритмів [1].

1. Bagging або Bootstrap Aggregation. У цій категорії паралельно та незалежно навчаються кілька «слабких учнів», результат класифікації визначається голосуванням. Для організації майже повної незалежності дані для навчання слабких учнів вибираються з навчальної вибірки за допомогою статистичного методу bootstrap. Суть методу можна описати так: виробляється генерація вибірок розміру B з вихідного набору даних розміру N здійснюється шляхом випадкового вибору з повтореннями елементів у кожному з B разів.

2. Boosting. У цій категорії алгоритмів група «слабких учнів» навчається послідовно, кожен новий «слабкий учень» навчається на даних, які були погано класифіковані попереднім учнем. Результат передбачення визначається кожним слабким учнем, ними накладається вага моделі, та, скомбінувавши результати передбачень, визначається результат. Даний вид навчання дозволяє отримувати точні передбачення на всіх типах даних.

3. Stacking. У цій категорії алгоритмів «слабкі учні» навчені різними методами, а результати їх прогнозів навчають мета-модель, яка визначає кінцевий результат прогнозу. Властиво «слабким учнем» може бути і сама мета-модель.

Для досягнення поставленої мети було обрано два ансамблеві алгоритми машинного навчання - Random Forest та AdaBoost.

Random Forest – представник ансамблевих алгоритмів машинного навчання категорії bagging. Модель, навчена за допомогою алгоритму, є колекцією дерев вибору, кожне з яких навчається незалежно і паралельно, а результат класифікації визначається загальним голосуванням. Серед переваг цього алгоритму варто відзначити його простоту, швидкість порівняно з іншими алгоритмами бегінга та бустингу та високу точність.

AdaBoost – ансамблевий алгоритм машинного навчання категорії boosting. Схема його є ітераційним алгоритмом, у якому після кожної епохи навчання ваги «слабких учнів» індивідуально перераховуються. Ваги збільшуються для некоректно передбачених екземплярів та зменшуються для коректно передбачених. На першій ітерації слабкі учні навчаються на оригінальному наборі даних, із кожною наступною ітерацією набір даних змінюється. Результат класифікації визначається загальним голосуванням навчених «слабких учнів».

Література

1. Ensemble methods: bagging, boosting and stacking. URL: https://towardsdatascience.com/ensemble-methods-bagging-boosting-and-stacking-c9214a10a205 (дата звертання 11.11.2024).

УДК 004.6

В. В. Юрчак
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕХНОЛОГІЇ ПОБУДОВИ BI-СИСТЕМ ДЛЯ АНАЛІЗУ ВЕЛИКИХ ДАНИХ

UDC 004.6

V. V. Yurchak

TECHNOLOGIES OF BUILDING BI-SYSTEMS FOR BIG DATA ANALASYS

При побудові BI (Business Intelligence) - систем для аналізу великих даних для різних завдань, зазвичай використовується технологія ROLAP. Реляційна онлайн-аналітична обробка (Relational OLAP, ROLAP) - це форма OLAP (online analytical processing – аналітична обробка у реальному часі), яка виконує динамічний багатовимірний аналіз даних, що зберігаються в реляційній базі даних, а не в багатовимірній базі даних.

Принцип роботи такої моделі досить простий: при активізації аналітичної функції формується SQL – запит, який йде на той чи інший бекенд. При цьому BI -система може бути інтегрована з будь-якою СУБД, що підтримує мову SQL (наприклад, реляційні СУБД MySQL, PostgreSQL та інші).

Перевага даної технології у тому, що для роботи BI- системи немає обмежень за обсягом даних. Недолік – відносно невисока швидкість виконання запитів, що негативно впливає на продуктивність BI -системи.

Для вирішення цієї проблеми використовуються різні підходи, у тому числі застосування спеціалізованих колонкових СУБД, наприклад ClickHouse або Vertica. Однак колонкові СУБД використовують власний обрізаний діалект SQL, що суттєво знижує функціональні можливості такого рішення.

Більш перспективним є рішення, засноване на застосуванні СУБД, в яких реалізована технологія In-Memory, що є технологією виконання комп'ютерних обчислень повністю в пам'яті комп'ютера, наприклад, в оперативному запам’ятовучому пристрої (ОЗП).

Цей термін, зазвичай, має на увазі великомасштабні складні обчислення, які вимагають спеціального системного програмного забезпечення для виконання обчислень на комп'ютерах, що працюють разом у кластері. Як кластер комп'ютери об'єднують свою оперативну пам'ять, тому розрахунок, по суті, виконується між комп'ютерами і використовує загальний простір ОЗП всіх комп'ютерів разом. Обробка в пам'яті усуває всі повільні звернення до даних і покладається виключно на дані, що зберігаються в ОЗП [1]. Загальна продуктивність обробки не знижується через затримку, яка зазвичай спостерігається при доступі до жорстких дисків або твердотільних накопичувачів. Обробка в пам'яті часто виконується за допомогою технології відомої як мережі даних у пам'яті.

Такі СУБД мають перевагу у швидкості порівняно з традиційними дисковими СУБД. Багато існуючих реляційних СУБД підтримують механізм In Memory, наприклад, пізні версії MS SQL Server, Oracle Database та інші.

За результатами представленого аналізу вибираємо як технологію побудови BI -системи для аналізу великих даних технологію, засновану на застосуванні реляційної СУБД, що підтримує механізм In-Memory.

Література

1. In-Memory Processing [Електронний ресурс]. – Режим доступу: https://hazelcast.com/glossary/in-memory-processing/ (дата звертання: 04.12.2024).

УДК 004.056.55
О. Ярема
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЕВРИСТИЧНІ МЕТОДИ ГЕНЕРАЦІЇ S-БЛОКІВ ТА ЇХ ПРОГРАМНА РЕАЛІЗАЦІЯ

UDC 004.056.55
O. Yarema

PRACTICAL ASPECTS OF RESEARCH ON THE RESISTANCE OF S-BLOCKS TO DIFFERENTIAL CRYPTANALYSIS

S-блоки (блоки підстановки), як один з елементів симетричних блокових шифрів, є основним методом забезпечення нелінійності шифрів. Існують багато способів генерації S-блоків, але в загальному всі вони входять до одної з трьох категорій: евристичні, алгебраїчні та комбіновані методи [1].

Евристичні методи є найпростішими та найбільш поширеними за рахунок своєї простоти. Ці методи використовують псевдовипадковості для генерації S-блоків, які потім перевіряються на відповідність заданим критеріям стійкості. За рахунок використання псевдовипадковостей такий спосіб просто реалізувати програмно і використовувати його для генерації великої кількості блоків. Проте евристичні методи не гарантують криптографічної стійкості і сильно залежать від того, які саме критерії оцінки стійкості обрані в конкретній реалізації [2].

Алгебраїчні методи використовують теорію груп, полів та інших алгебраїчних структур для генерації блоків. Такі блоки можуть мати високу криптографічну стійкість за рахунок використання доведених математичних властивостей. Недоліком таких методів є їх складність в реалізації та потреба в великих обчислювальних ресурсах.

Комбіновані методи, як очевидно з назви, комбінують підходи обох попередніх типів в певних пропорціях і дозволяють отримати дещо середні результати – блоки з непоганою криптографічною стійкістю та відносно простою реалізацією алгоритму генерації.

Варто окремо зауважити, що евристичні методи мають набагато вищу популярність серед шифрів, які використовують динамічні S-блоки [3], які генеруються на основі ключа. Таким шифрам зазвичай не підходять алгебраїчні методи через необхідність в швидкодії [4], що не притаманна алгебраїчним методам генерації S-блоків.

Література

1. Menezes A. J., van Oorschot P. C., Vanstone S. A. Overview of cryptography. Handbook of applied cryptography. 2018. С. 1–48. URL: https://doi.org/10.1201/9780429466335-1 (дата звернення: 01.12.2024).
2. Cryptanalytic attacks on IDEA block cipher / H. K. Sahu та ін. Defence science journal. 2016. Т. 66, № 6. С. 582. URL: https://doi.org/10.14429/dsj.66.10798 (дата звернення: 01.12.2024).
3. Agarwal P., Singh A., Kilicman A. Development of key-dependent dynamic S-Boxes with dynamic irreducible polynomial and affine constant. Advances in mechanical engineering. 2018. Т. 10, № 7. С. 168781401878163. URL: https://doi.org/10.1177/1687814018781638 (дата звернення: 25.11.2024).
4. Sharma S., Patel K. N., Siddhath Jha A. Cryptography using blowfish algorithm. 2021 3rd international conference on advances in computing, communication control and networking (ICAC3N), м. Greater Noida, India, 17–18 груд. 2021 р. 2021. URL: https://doi.org/10.1109/icac3n53548.2021.9725661 (дата звернення: 01.12.2024).

СЕКЦІЯ 3. КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

УДК 004.45

В. С. Бондаренко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ДОДАТКУ ВІДЕОТРАНСЛЯЦІЇ ПІД МОБІЛЬНІ ПРИСТРОЇ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

UDC 004.45

V. S. Bondarenko

DEVELOPMENT OF A VIDEO BROADCASTING APPLICATION FOR MOBILE DEVICES BASED ON THE ANDROID OPERATING SYSTEM

Розроблений мобільний додаток забезпечує відеотрансляцію в реальному часі із використанням технології WebRTC. Основне призначення системи – захоплення відео через камеру мобільного пристрою та його передача іншому пристрою або серверу з мінімальними затримками. Система інтегрує функціонал WebRTC для передачі відео та аудіо, адаптивно підлаштовуючись до якості мережевого з'єднання [2].

Основні функції розробки включають захоплення та обробку медіаданих. Додаток отримує відеопотік із камери та, за потреби, аудіопотік із мікрофона[1]. Вхідні дані обробляються із застосуванням сучасних відеокодеків (наприклад, VP8, H.264) для забезпечення високої ефективності стиснення. Використання WebRTC дозволяє створювати прямі з'єднання точка-точка, використовуючи STUN/TURN сервери для пробивання NAT і забезпечення стабільного зв'язку [4].

До основних переваг розробки належать низька затримка передачі даних, що досягає 50–200 мс, адаптивність до змін у мережі, підтримка шифрування для забезпечення конфіденційності та можливість масштабування для багатокористувацького використання. Крім того, система має інтуїтивно зрозумілий інтерфейс, що спрощує її інтеграцію в різні сфери застосування.

Недоліками розробки є високе споживання обчислювальних ресурсів, залежність від якості мережі, а також складність масштабування WebRTC для великих стрімінгів. Окрім цього, не всі пристрої підтримують сучасні кодеки, що може обмежувати функціонал додатка.

Інтеграція WebRTC з платформою Android забезпечує ефективну передачу медіаданих за рахунок використання нативних бібліотек та API, оптимізованих для цієї операційної системи[3]. Це дозволяє застосунку стабільно працювати на різноманітних мобільних пристроях, надаючи високу якість відео та мінімальні затримки. Крім того, Android дозволяє тонко налаштовувати параметри WebRTC, такі як управління енергоспоживанням та оптимізація ресурсів, що підвищує надійність роботи додатку у різних мережевих умовах. Таким чином, застосунок пропонує зручний інтерфейс для реального часу відео- та аудіокомунікацій, відповідаючи сучасним вимогам мобільних технологій.

Результати тестування продемонстрували стабільну роботу системи у різних мережевих середовищах, включаючи Wi-Fi, 4G та 3G. Якість відео залишалася задовільною навіть за низької швидкості з'єднання (1–2 Мбіт/с). Система досягла високого рівня сумісності з веб-клієнтами, побудованими на основі WebRTC API. Аналіз отриманих результатів підтвердив ефективність розробки для реального часу відеотрансляцій із мінімальними затримками. У подальшому рекомендується оптимізувати використання ресурсів, розширити функціонал (наприклад, додати можливість запису відео на сервері) та вдосконалити моніторинг мережевого стану. Розробка має значний потенціал для застосування у відеоспостереженні, дистанційному навчанні та інших сферах.

Література

1. WebRTC [Електронний ресурс]. Режим доступу: https://webrtc.org.
2. Johnston, A. B., & Burnett, D. C. (2014). WebRTC: APIs and protocols of the HTML5 real-time web (3rd ed., pp. 1-10). Digital Codex LLC. ISBN-13: 978-0-9859788-7-7.
3. Android documentation. https://developer.android.com/reference.
4. Emmanuel, E. A., & Dirting, B. D. (2017). A Peer-To-Peer Architecture For Real-Time Communication Using WebRTC. *Journal of Multidisciplinary Engineering Science Studies (JMESS).*

УДК 004.41
І. Бородій; Г. Осухівська, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АРХІТЕКТУРА ПРОГРАМНОЇ СИСТЕМИ ПРОГНОЗУВАННЯ СТАНУ ЯКОСТІ АТМОСФЕРНОГО ПОВІТРЯ

UDC
I. Borodii; H. Osukhivska, Ph.D., Assoc. Prof.

ARCHITECTURE OF A SOFTWARE SYSTEM FOR FORECASTING THE STATE OF ATMOSPHERIC AIR QUALITY

Розробка програмної системи прогнозування якості атмосферного повітря є важливим етапом для контролю екологічної безпеки. Ця система повинна опрацьовувати великі об'єми даних, передбачати зміни показників і мати здатність швидко реагувати на ризики. На рисунку 1 зображена архітектура системи стану якості атмосферного повітря. Інформація надходить із кількох джерел, зокрема метеорологічні API, платформи відстеження якості повітря, дані про наявність пожеж та об'єктів промисловості. Для збору, паралельної обробки та завантаження надвеликих обсягів даних використовується Apache Spark [1]. Дані зберігаються у сховищі формату Apache Iceberg, оптимізованому для аналітики та машинного навчання [2]. Прогнози формуються за допомогою алгоритмів машинного навчання та візуалізовані в інструменті Power BI через інтерактивні мапи та інформаційні панелі, які відображають рівень забруднення. Усі компоненти системи контейнеризовані за допомогою Docker з метою стабільності та масштабованості. Інструмент Apache Airflow координує процеси та забезпечує автоматизоване функціонування системи.

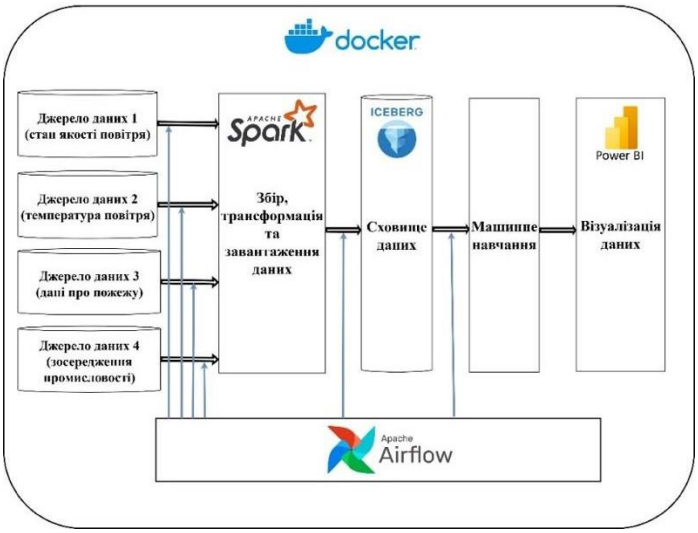


Рисунок 1. Архітектура програмної системи прогнозування стану якості атмосферного повітря

Запропонована система є комплексним рішенням для моніторингу та прогнозування стану повітря, яка може знайти застосування з метою контролю екологічної безпеки.

Література

1. Palamar A., Karpinski M., Palamar M., Osukhivska H., Mytnyk M. Remote Air Pollution Monitoring System Based on Internet of Things. CEUR Workshop Proceedings, 2nd International Workshop on Information Technologies: Theoretical and Applied Problems, Ternopil, Ukraine, November 22–24, 2022. Vol. 3309. P. 194–204.
2. Бородій І., Осухівська Г. Проєктування програмної системи формування агрегованих надвеликих масивів даних. Матеріали XI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології», Тернопіль: ТНТУ. 2023. С. 137.

УДК 004.451:656.025.2
В. Бражніков
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АКТУАЛЬНІСТЬ ЗАСОБІВ ОПТИМІЗАЦІЇ CRM-СИСТЕМ ДЛЯ ЛОГІСТИКИ

UDC 004.451:656.025.2
V. Brazhnikov

RELEVANCE OF CRM SYSTEM OPTIMIZATION TOOLS FOR LOGISTICS

Сучасна логістика – це складний механізм, де кожна деталь має значення. Зростаючі обсяги перевезень, різноманітність маршрутів та вимоги клієнтів до швидкості доставки ставлять перед логістичними компаніями значні виклики. У цьому контексті ефективне управління взаємовідносинами з клієнтами є одним з ключових факторів успіху. Саме тут на допомогу приходять CRM-системи, оскільки вони дозволяють автоматизувати, аналізувати і планувати всі процеси взаємодії з клієнтами [1, 2].

Однак з розвитком технологій і збільшенням обсягу даних традиційний підхід до використання CRM-системи виявляється недостатнім. Величезні обсяги інформації про клієнтів, замовлення, маршрути та транспортні засоби необхідно аналізувати швидко і точно. Крім того, сучасні логістичні компанії використовують різноманітні інформаційні системи, такі як ERP і WMS, які необхідно інтегрувати з CRM для створення єдиного інформаційного середовища [1, 2]. Все це ставить перед логістичними компаніями нові виклики і вимагає пошуку інноваційних рішень.

Одним з найбільш перспективних напрямків оптимізації CRM-систем є використання машинного навчання та штучного інтелекту. Ці технології дозволяють аналізувати великі обсяги даних, виявляти закономірності та прогнозувати майбутні тенденції. Наприклад, машинне навчання можна використовувати для оптимізації маршрутів доставки, прогнозування попиту на певні послуги та персоналізації пропозицій для клієнтів. Крім того, штучний інтелект може взяти на себе рутинні завдання, такі як обробка замовлень або відповіді на запити клієнтів, дозволяючи співробітникам зосередитися на більш складних завданнях.

Ще одним важливим аспектом оптимізації CRM-системи є інтеграція аналітичних інструментів. Інформаційні панелі та звіти дають змогу менеджерам отримувати детальну інформацію про результати діяльності компанії, виявляти вузькі місця та приймати обґрунтовані рішення. Візуалізація даних дозволяє швидко оцінити ситуацію і вжити необхідних заходів.

Таким чином, оптимізація CRM-систем в логістиці є необхідною умовою для підвищення ефективності бізнесу. Використовуючи новітні технології, такі як машинне навчання, штучний інтелект і аналітичні інструменти, логістичні компанії можуть значно поліпшити якість обслуговування, знизити витрати і підвищити задоволеність клієнтів. Інвестуючи в розвиток CRM-систем, компанії роблять крок до успіху в конкурентному середовищі.

Література

1. 5 benefits of CRM for Logistics Service Providers. URL: https://www.workbooks.com/resources/blog/5-benefits-of-crm-for-logistics-service-providers/.
2. CRM for logistics: importance, advantages and features. URL: https://www.customerization.ca/best-crm-logistics-industry/.

УДК 004.451:656.025.2
В. Бражніков; Г. Осухівська, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ ПЕРСОНАЛІЗАЦІЇ КЛІЄНТСЬКИХ ВЗАЄМОВІДНОСИН НА ЕФЕКТИВНІСТЬ CRM-СИСТЕМ У ЛОГІСТИЦІ

UDC 004.451:656.025.2
V. Brazhnikov; H. Osukhivska, Ph. D., Assoc. Prof.

THE IMPACT OF CUSTOMER RELATIONSHIP PERSONALIZATION ON THE EFFICIENCY OF CRM SYSTEMS IN LOGISTICS

Сьогодні логістика все більше орієнтується на клієнта, пріоритезуючи індивідуальні підходи до кожного замовника. Такий підхід потребує персоналізованих рішень у взаємовідносинах з клієнтами, які допомагають підвищити якість обслуговування та задоволеність клієнтів. У цьому випадку CRM-системи є ключовим інструментом, який дозволяє ефективно керувати відносинами з клієнтом завдяки збору, аналізу та використання даних [1, 2].

Персоналізація клієнтських взаємовідносин у логістичних операціях стикається з низкою викликів. Важливим аспектом є необхідність обробки великої кількості даних про клієнтів, зокрема, їх вподобання, історію замовлень та особливості поведінки. Такі дані повинні бути доступними в режимі реального часу для забезпечення адаптації послуг до потреб замовників. Тому CRM-системи мають бути не тільки потужними, але й гнучкими та інтегрованими з іншими інструментами інтернету речей та автоматизованими системами підтримки для забезпечення високого рівня персоналізації.

У реалізації персоналізованого підходу вирішальну роль відіграють технології. Штучний інтелект, машинне навчання, аналітика великих обсягів даних і алгоритми кластеризації дозволяють розподілити клієнтів за їх характеристиками та прогнозувати майбутні потреби. Для прикладу це можуть бути індивідуальні рекомендації та пропозиції або попередження щодо доставки, які допомагають покращити досвід клієнта. До того ж, автоматизовані рішення, такі як чат-боти, забезпечують цілодобову підтримку, яка відповідає конкретним запитам клієнтів.

Персоналізація підходу приносить значні переваги як для клієнтів, так і для компанії. Клієнт отримує кращий досвід взаємодії, швидке вирішення проблем та відчуття індивідуального підходу. Перевагою для компанії є підвищення лояльності клієнтів та збільшення обсягів повторних замовлень. До того ж, персоналізація допомагає оптимізувати витрати, спрямовуючи ресурси на цільові сегменти аудиторії. Одночасно, це дозволяє зміцнити репутацію компанії, що важливо у конкурентному середовищі сьогодення.

Отже, персоналізація клієнтських відносин через CRM-системи є корисною не лише як інструмент підвищення ефективності, але й як стратегічна перевага. Вона дозволяє адаптовувати бізнес до мінливості ринку, дозволяючи забезпечувати високий рівень довіри та задоволення клієнтів. Сучасні технології дозволяють логістичним компаніям не просто реагувати на потреби клієнтів, але й передбачати їх, створюючи довгострокові та взаємовигідні відносини.

Література

1. Переваги використання CRM систем для ефективної роботи компаній. URL: https://firtka.if.ua/blog/view/perevagi-vikoristannia-crm-sistem-dlia-efektivnoyi-roboti-kompanii.
2. Впровадження CRM-системи: роль CRM-технологій у підвищенні ефективності бізнесу. URL: https://tqm.com.ua/ua/likbez/crm-systemy/rol-vprovadzhennia-crm.

УДК 681.518.3
А. М. Паламар, канд. техн. наук, доц.; Р. О. Жаровський, канд. техн. наук; Ю. С. Гарбіч
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМА МОНІТОРИНГУ АТМОСФЕРНОГО ТИСКУ ЗА ДОПОМОГОЮ ІОТ-ТЕХНОЛОГІЙ

UDC 681.518.3
A. M. Palamar, Ph.D, Assoc. Prof.; R. O. Zharovskyi, Ph.D.; Y. S. Harbich

SYSTEM FOR MONITORING ATMOSPHERIC PRESSURE USING IOT TECHNOLOGIES

Погодні аномалії можуть мати серйозний вплив на різні сфери життя, такі як сільське господарство, транспорт і енергетика. Саме тому актуальним питанням є підвищення точності прогнозування погоди. Атмосферний тиск є одним із ключових параметрів, які визначають формування та рух циклонів і антициклонів.

Традиційні методи моніторингу атмосферного тиску, які базуються на використанні стаціонарних метеостанцій, обмежені локальним охопленням і часом оновлення даних. Це створює необхідність у використанні розподілених мереж моніторингу на основі технологій інтернету речей (IoT), які забезпечують гнучкість, масштабованість і доступність даних у реальному часі [1].

Метою цього дослідження є розробка системи моніторингу атмосферного тиску на основі IoT, яка дозволяє не лише забезпечити оперативний доступ до даних, але й підвищити точність прогнозування погоди завдяки інтеграції з хмарними платформами та алгоритмами обробки даних.

Запропонована система складається з сенсора BMP280 для вимірювання атмосферного тиску, мікроконтролера ESP32 для обробки даних і передачі їх на IoT-платформу, а також хмарної інфраструктури для зберігання та аналізу отриманих результатів.

Після зчитування даних сенсор передає їх на мікроконтролер ESP32, який формує інформаційне повідомлення для передачі на хмарну платформу. Використання IoT-платформи Thinger.io дозволяє зберігати дані, аналізувати їх у реальному часі та візуалізувати результати у вигляді графіків і діаграм. Це сприяє більш детальному аналізу динаміки змін атмосферного тиску та його впливу на погодні умови. Такий підхід також відкриває можливість інтеграції з метеорологічними платформами для створення комплексних систем прогнозування.

Перевагами розробленої системи є її висока точність, гнучкість у використанні та можливість інтеграції з іншими системами моніторингу. Крім того, доступ до даних через веб-інтерфейс значно розширює можливості використання системи в різних галузях. Запропонований метод на основі IoT є перспективним інструментом для забезпечення точного моніторингу атмосферного тиску та покращення процесу прогнозування погодних умов. Використання розподілених систем і хмарних технологій відкриває нові горизонти у сфері метеорології та кліматичних досліджень.

Література

1. Оконський М.В., Лупенко С.А., Паламар А.М. Інформаційно-вимірювальна система для контролю метеорологічних параметрів на основі Інтернету речей. Матеріали IX науково-технічної конференції "Інформаційні моделі, системи та технології" Тернопільського національного технічного університету імені Івана Пулюя (Тернопіль, 8–9 грудня 2021 року), Тернопіль: ТНТУ, 2021. С. 118.

УДК 004.738.5
С. Вінтонів; Є. Тиш, канд. техн. наук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОПТИМІЗАЦІЯ КІЛЬКОСТІ ЗАПИТІВ ДО БАЗИ ДАНИХ ДЛЯ GRAPHQL-API З ВИКОРИСТАННЯМ DATALOADER

UDC
S. Vintoniv; Ie. Tysh, Ph.D.

OPTIMIZING THE NUMBER OF DATABASE QUERIES FOR GRAPHQL-API USING DATALOADER

Оптимізація запитів до бази даних є важливим аспектом сучасної розробки інформаційних платформ особливо для систем, що використовують GraphQL. На відміну від REST API, GraphQL дозволяє клієнтам запитувати точні підмножини даних, що часто призводить до множинних запитів до бази даних («проблема N+1»). Ця проблема може призвести до зниження продуктивності та неефективного використання ресурсів. Щоб вирішити цю проблему, використовується DataLoader - утиліта пакетної обробки та кешування для оптимізації виконання запитів для GraphQL API. DataLoader дозволяє об'єднувати запити до бази даних в один запит, мінімізуючи надлишкові операції і скорочуючи час відгуку.

На додаток до пакетної обробки запитів, розширені функціональні можливості, такі як реалізація користувацьких обгорток над базою даних, можуть ще більше підвищити продуктивність. Ці обгортки попередньо обробляють запити, ефективно використовують індекси бази даних і структурують конвеєри для агрегації. Поєднуючи пакетну обробку запитів з оптимізованими обгортками запитів, можна значно зменшити навантаження на базу даних і підвищити загальну продуктивність системи.

Цей підхід відповідає сучасним практикам GraphQL, де виконання запитів і оптимізація продуктивності є ключовими для обробки великих наборів даних і високого рівня паралелізму. Інтеграція цих методів з базами даних на основі документів, такими як MongoDB, забезпечує масштабований та ефективний пошук даних.

Вивчення таких інструментів і методів дає цінну інформацію для розробки GraphQL API, підкреслюючи необхідність добре структурованих стратегій пакетної обробки, кешування та оптимізації запитів.

Література

1. Optimizing GraphQL Queries with DataLoader. URL: https://moldstud.com/articles/p-optimizing-graphql-queries-with-dataloader.
2. Declarative Data Fetching with GraphQL. URL: https://css-tricks.com/declarative-data-fetching-graphql/.
3. How to solve the GraphQL N+1 problem. URL: https://hygraph.com/blog/graphql-n-1-problem.

УДК 681.518.3

А. М. Паламар, канд. техн. наук, доц.; Ю. С. Гарбіч
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ДЛЯ IOT-МОНІТОРИНГУ АТМОСФЕРНОГО ТИСКУ

UDC 681.518.3

A. M. Palamar, Ph.D, Assoc. Prof.; Y. S. Harbich

COMPUTERIZED SYSTEM FOR IOT MONITORING OF ATMOSPHERIC PRESSURE

Розвиток технологій Інтернету речей (IoT) відкриває нові можливості для моніторингу навколишнього середовища, зокрема атмосферного тиску, який є важливим параметром для прогнозування змін погоди. Традиційні методи моніторингу, що базуються на стаціонарних метеостанціях, мають обмежене покриття та не забезпечують оперативного доступу до даних у режимі реального часу. Це створює необхідність у розробці розподілених комп'ютеризованих систем моніторингу на основі IoT, які поєднують сучасні сенсори, мікроконтролери та хмарні технології. Метою дослідження є створення такої системи для забезпечення точного, ефективного та масштабованого моніторингу атмосферного тиску.

Запропонована система складається з сенсора BMP280, мікроконтролера ESP32 та IoT-платформи (рис. 1). Сенсор зчитує дані про тиск і температуру, які передаються на мікроконтролер для обробки. Після цього дані у реальному часі відправляються на хмарну платформу, де вони зберігаються, аналізуються і візуалізуються у вигляді графіків.

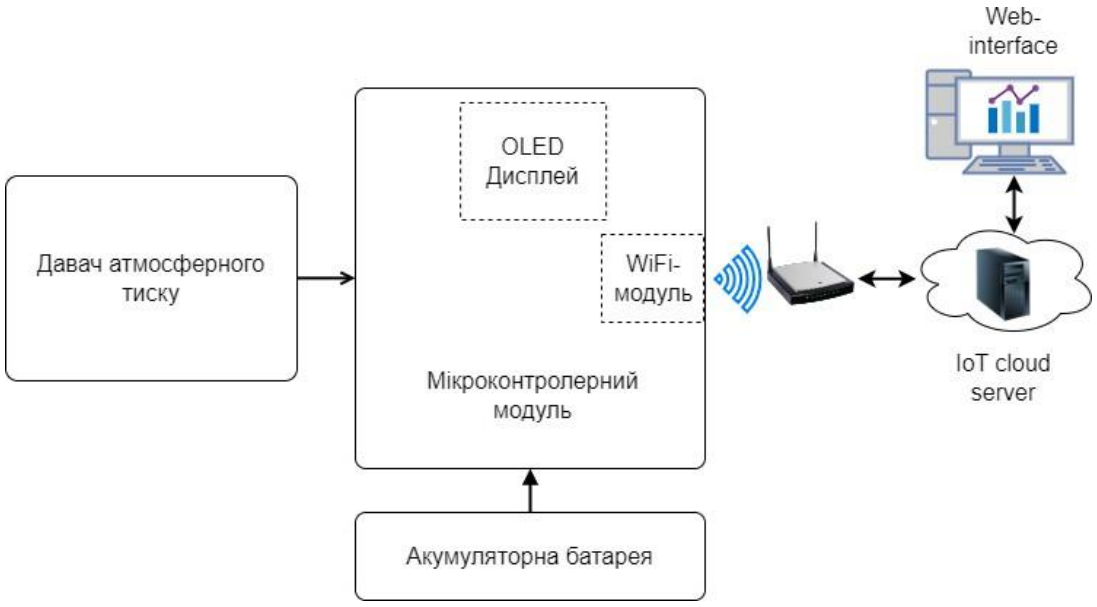


Рисунок 1. Структурна схема проєктованої системи

Перевагами запропонованої системи є її автономність, низьке енергоспоживання, висока точність вимірювань та можливість інтеграції з IoT платформами. Крім того, система забезпечує оперативний доступ до даних через веб-інтерфейс.

Розроблена система демонструє високу ефективність у задачах моніторингу атмосферного тиску, забезпечуючи надійний збір, передачу та візуалізацію даних. Це підтверджує перспективність використання IoT-технологій для розв'язання актуальних задач у сфері метеорології.

УДК 004.45
Н. О. Гладовський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОГРАМНІ РІШЕННЯ МОНІТОРИНГУ СИСТЕМ ТА МЕРЕЖ

UDC 004.45
N. M. Holovetskyi

SYSTEM AND NETWORK MONITORING SOFTWARE SOLUTIONS

Системи моніторингу (СМ) дозволяють усувати незначні несправності, що становлять основну масу інцидентів, автоматично або за допомогою підключення віддаленим доступом до обладнання, що адмініструється.

Graphite. ПЗ застосовує тільки свою БД Whisper, а також є складним для налаштування. Проте є компенсація за рахунок високої продуктивності за великих даних обробки. Graphite створено моніторингу системних та бізнес-метрик, котрі реалізовані із використанням надбудов, у т.ч. і для прогнозування. Недолік продукту полягає у специфіці реалізації функцій під чітко визначені бізнес-процеси., відсутність автоматичного відтворення сервісів вслід за виявленням відмови. В цілому існують суб'єктивні та суперечливі думки про незручний інтерфейс додатків Graphite та вимушено високі витрати дуже великої кількості моніторингових серверів Graphite.

New Relic. Відома як програмний засіб відстеження та оцінювання застосунків, проте містить рішення також і для системних індексів із вбудованим сприянням фільтрації помилкових повідомлень та передбачення відмов. Біля 20 млн осіб застосовують розробки New Relic, котрі є доступними у хмарних середовищах, зокрема Amazone і Azure. Проте, безпекові умови компаній не дають змогу збереження даних, хоча б зашифрованих, на зовнішніх хмарних сховищах. Для вирішення цього New Relic дозволив під’єднювати свої модулі через JSON HTTP POST, і одержувати дані від серверів New Relic через API функцій та будувати власні екрани візуалізації даних.

Nagios. Проводить моніторинг за введеними вузлами та сервісами, та повідомляє мережевого адміністратора, якщо деякий сервіс чи вузол припиняють (або відновлюють) свою роботу. СМ має можливість створення карти мережі, із зазначенням детальної інформації про об'єкти. Особливості продукту: моніторинг стану робочих станцій (завантаження процесора, застосування простору жорсткого диска); інтуїтивно зрозуміла архітектура модулів розширень дає змогу застосовуючи будь-яку мову програмування, досить просто і легко створювати свої способи перевірки сервісів; є можливість інтеграції з іншими системами для покращення надійності і побудови розподіленої системи відстеження та оцінювання.

Prometheus. Є ще однією СМ різних сервісів та систем, при допомозі котрої сисадміни здатні збирати дані щодо метрик систем, налаштовувати додаткові функції для налаштування додаткових повідомлень (наприклад, повідомлення про те, коли виникають проблеми). Prometheus здобув популярність серед розробників, оскільки це проект з відкритим вихідним кодом, більшість компонентів якого написана мовою програмування Golang, а частина мовою Ruby. Виходячи з цього можна вивести, що у користувача даною системою буде лише один бінарний файл, який необхідно буде завантажити і встановити разом з компонентами системи Prometheus,

Zabbix. Універсальна СМ, що дозволяє спостерігати різні параметри на віддалених машинах. Параметри заносяться в БД, які при необхідності можна витягти, наприклад, для побудови графіків, налаштування оповіщення при переході значень параметрів через межу та ін. який знаходиться під моніторингом, опис проблеми, тривалість несправного стану та резолюція щодо усунення несправності. Оповіщення можуть здійснюватися як електронною поштою, так і через SMS.

УДК 004.94

Н. О. Гладовський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИЯВЛЕННЯ НЕСПРАВНИХ ПАРАМЕТРІВ У ХОДІ МОНІТОРИНГУ МЕРЕЖІ

UDC 004.94

N. M. Holovetskyi

DETECTION OF FAULTY PARAMETERS DURING NETWORK MONITORING

Розглянемо постановку задачі моніторингу комп'ютерної мережі. Загалом завдання моніторингу можна описати в такий спосіб: події, що відбуваються в комп'ютерних мережах та інформаційних системах, мають випадковий характер. У зв'язку з цим для їх вивчення найбільше підходять ймовірнісні математичні моделі теорії масового обслуговування, наприклад теорія марковських ланцюгів [1].

Для моделювання спочатку необхідно визначити вхідні дані. Розглянемо події, пов'язані з детектуванням аномалій у процесі діагностики та контролю досліджуваних системою параметрів обладнання в мережі, як стан аналізованої системи моніторингу мережі. Виходячи з викладеного вище, виведемо можливі стани в процесі моніторингу метрик (параметрів) мережного обладнання: S_0 – відсутність несправностей; S_1 – навантаження мережі; S_2 – зниження пропускної спроможності; S_3 – відсутність мережного порту; S_4 – фізична недоступність пристрою; S_5 – фрагментація пакета; S_6 – повна відмова системи.

Описаний ланцюг подій під час моніторингу мережі можна подати у вигляді графа станів, як показано на рис. 1.

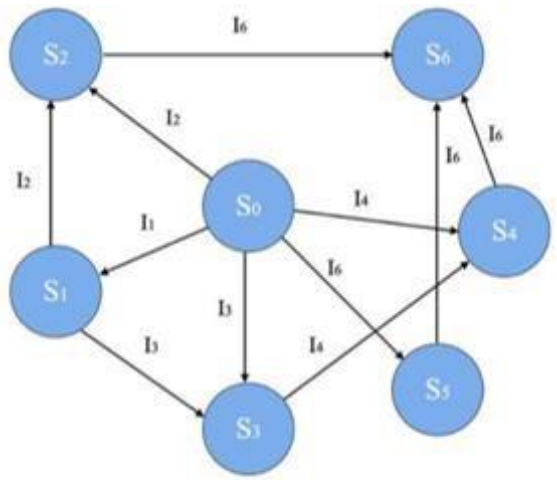


Рис. 1 - Граф виявлення несправних параметрів у ході моніторингу мережі

Імовірність виявлення несправного параметра в мережі визначається в даному випадку як ймовірність знаходження системи в стані S_i.

На графі кожна стрілка відповідає інтенсивності потоку подій, який переводить систему з одного стану в інший. Послідовність опитування визначається призначеним системним адміністратором пріоритетом. Чим вищий пріоритет у параметра мережного пристрою, тим вище інтенсивність його опитування. За інтенсивності переходів у разі приймається I_i – інтенсивність опитування i -го параметра у системі моніторингу.

Зважаючи на описані вище метрики роботи, система моніторингу виходить, що вона зі стану S_0 при виконанні опитування мережевих пристроїв при відмові будь-якого компонента переходить у стан виявлення несправностей S_i з інтенсивністю I_i. За графом можна скласти математичну модель процесу моніторингу мережі з урахуванням ймовірностей p_i як системи рівнянь. Її розв’язок дозволяє відстежити динаміку діагностування несправних параметрів у процесі мережного моніторингу через відстеження ймовірностей у певні проміжки часу.

Література

2. Погоруй А. О., Чемерис О.А. Вступ до теорії випадкових процесів : навчальний посібник. Житомир : Вид-во ЖДУ ім. І. Франка, 2020. 70 с.

УДК 004.45

Н. М. Головецький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

УПРАВЛІННЯ ПРИСТРОЯМИ В ЛОКАЛЬНІЙ M2M МЕРЕЖІ

UDC 004.45

N. M. Holovetskyi

DEVICE MANAGEMENT IN A LOCAL M2M NETWORK

У локальній бездротовій мережі M2M (machine-to-machine) поєднуються всі домашні електричні прилади та системи на базі мережі радіодоступу Wi-Fi. За допомогою програми M2M, що здійснює моніторинг та керування домашньою електромережею, забезпечується взаємодія всіх елементів. Для домашніх електроприладів можна організувати вихід на зв'язок із зовнішніми програмами M2M за допомогою маршрутизатора Wi-Fi, який в даному випадку стає аналогом шлюзу M2M.

До переваг застосування мереж радіодоступу Wi-Fi, в плані об'єднання домашніх електричних приладів, можна віднести широку поширеність технології, просте і швидке її розгортання і використання на безоплатній основі без необхідності ліцензування, на відміну від мереж радіодоступу операторів мобільного зв'язку.

У розподільних електричних мережах пристрої M2M потрібні, для того щоб збирати дані з «розумних» лічильників і відправляти отриману інформацію в спеціалізований центр обробки даних, який, у разі необхідності, може відправити команду у відповідь на цей «розумний» лічильник. Налагоджений обмін даними в розподільчих електромережах відкриває безліч нових можливостей у вимірюваннях споживання енергії, управлінні навантаженням та вимірюванні в режимі реального часу таких енергетичних характеристик, як напруга, сила струму, потужність та частота, тим самим перевіряючи якість та безперервність електроживлення. Для організації взаємодії між пристроями та програмами M2M у розподільній мережі також можна використовувати мобільні мережі доступу 3GPP та M-3GPP.

Як приклад, збирання необхідної інформації можна реалізувати за допомогою M2M-пристрою, який запрограмовано відправляти на сервер M2M дані своїх вимірювань в інтервалом, заданим мережею Smart Grid на основі мережі доступу GSM. Зроблені виміри можна надсилати за допомогою SMS -повідомлень або через канал GPRS за протоколом TCP/IP. Вибір каналу надсилання звітності часто робиться, спираючись на вимоги постачальника програм M2M, а також виходячи з обмежень, пов'язаних із мережею радіодоступу, розгорнутою в зоні дії мережі Smart Grid. У системах генерації та передачі електроенергії на пристрої M2M покладаються керування та контроль за рядом електричних пристроїв та систем: перемикачі з віддаленим керуванням, індикатори несправностей, захисні реле, системи автоматизації електричних підстанцій, відновлювані джерела енергії та ін.

Якщо виник розрив, пристрій керування електричною підстанцією за допомогою технології Circuit Switched Data (CSD) передає на пристрій M2M керування вітряною турбіною сигнал про відключення через мобільну мережу 3GPP. Отримавши цей сигнал, пристрій керування вітряною турбіною відключає подачу електроенергії, потім надсилає зворотний підтверджуючий сигнал на пристрій керування електричною підстанцією. У порівнянні з каналом GPRS, основний плюс застосування для передачі команд управління CSD-каналу полягає у першочерговому виділенні ресурсів мережі. Крім цього, CSD -канал має гарантований стандарт і оператор смуги пропускання 9,6 Кбіт/с (у випадку HSCSD – 57,6 Кбіт/с), а також йому властиві стабільність і стійкість, а комутація каналу проводиться за телефонним номером.

УДК 621.855
Л. П. Дмитроца, канд.техн.наук, доц.; О. Т. Старицький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОПТИМІЗАЦІЯ ПРОДУКТИВНОСТІ ТА SEO ПРИ МАСШТАБУВАННІ ПРОЄКТІВ НА ОСНОВІ REACT І NEXT.JS

UDC 621.855

L. P. Dmytrotsa, Ph.D., Assoc. Prof.; O. T. Starytskyi

OPTIMIZING PERFORMANCE AND SEO WHEN SCALING PROJECTS BASED ON REACT AND NEXT.JS

Оптимізація продуктивності та SEO відіграють ключову роль у сучасній розробці веб-додатків. В умовах зростаючої конкуренції в онлайн-середовищі та підвищених очікувань користувачів щодо якості веб-ресурсів, ці аспекти стають особливо важливими.

Метою роботи було дослідити доступні підходи до оптимізації продуктивності та SEO в проєктах, створених на основі React і Next.js, а також оцінити їхню ефективність і практичну користь для розробників.

Для аналізу методів було підібрано три види рендеру, які по різному впливають на оптимізацію сайту. Було визначено їх основні функції, переваги та недоліки (таблиця 1).

Таблиця 1. Аналіз доступних рендерів

Характеристики	SSR	SSG	CSR
Швидкість завантаження	Помірна	Найвища	Залежить від JS
SEO	Висока	Висока	Низька (без оптимізації)
Динамічність контенту	Найвища	Низька (статичний)	Найвища
Час до відображення	Середній	Найнижчий	Найвищий
Складність реалізації	Середня	Низька	Найнижча

Провівши порівняння та ознайомившись із функціоналом кожного з рендерів, ми обрали SSR, оскільки цей підхід дозволяє ефективно вирішувати задачі SEO та працювати з динамічним контентом. Він забезпечує генерацію готового HTML на сервері для кожного запиту, що покращує індексацію сторінок і створює кращий користувацький досвід завдяки швидкому завантаженню основного контенту. SSR також надає гнучкість у реалізації, що робить його оптимальним вибором для проєктів із динамічними даними.

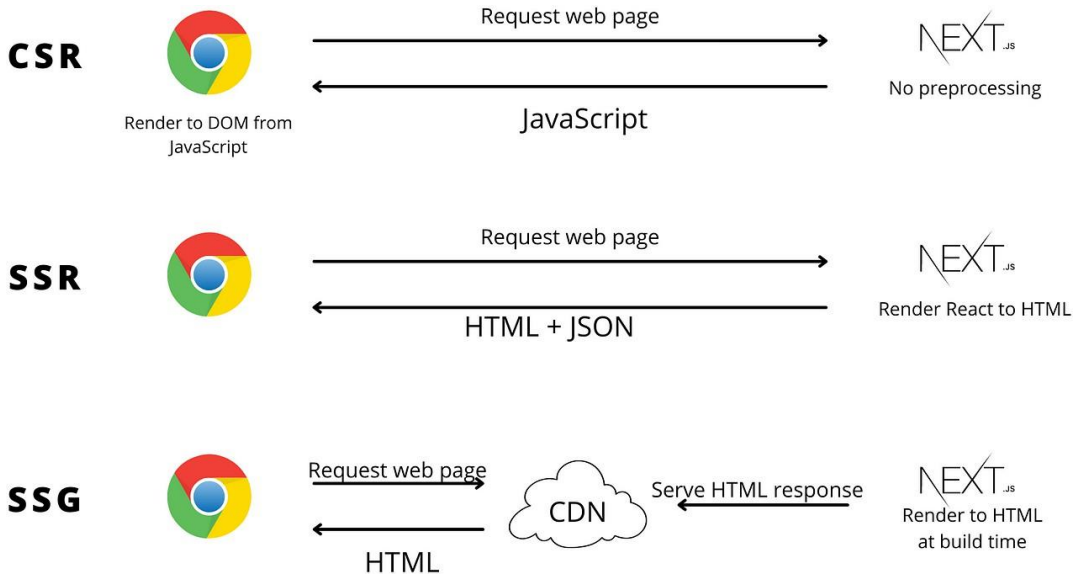


Рисунок 1. Як працюють види рендеру

Висновок: досліджено наявні підходи до рендеру та обрано оптимальний варіант для нашої роботи. На основі вибраної стратегії було обрано основний напрямок для оптимізації. Обраний рендер допоможе нам покращити динамічність та SEO та автоматизувати роботу в певних аспектах коду.

Література

1. React Performance Optimization Techniques // Режим доступу: https://supertokens.com/blog/5-tips-for-optimizing-your-react-apps-performance. [дата звернення 12.11.2024].
2. Next.js SEO Optimization: Practical Techniques for Better Ranking. // Режим доступу: https://nextjs.org/learn-pages-router/seo/introduction-to-seo. [дата звернення 12.11.2024].
3. Server-Side Rendering and Static Site Generation in Next.js. // Режим доступу: https://nextjs.org/docs/pages/building-your-application/rendering/static-site-generation [дата звернення 12.11.2024].
4. Using Google Analytics and Search Console with Next.js. // Режим доступу: https://nextjs.org/docs/messages/next-script-for-ga. [дата звернення 12.11.2024].
5. Enhancing Mobile Responsiveness for Better SEO in Next.js. // Режим доступу: https://nextjs.org/learn-pages-router/seo/web-performance/seo-impact [дата звернення 12.11.2024].

УДК 004.75
М. В. Дрогобицький; А. І. Фіялка; Н. С. Луцик, Ph.D, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ВИКОРИСТАННЯ МЕРЕЖ MICROGRID ДЛЯ ДИНАМІЧНОГО БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ЗАГАЛЬНИХ ЕЛЕКТРИЧНИХ МЕРЕЖ

UDC 004.75
M. V. Drohobytskyi; A. I. Fiialka; N. S. Lutsyk, Ph.D, Assoc. Prof.

METHODS OF USING MICROGRID NETWORKS FOR DYNAMIC LOAD BALANCING OF GENERAL ELECTRICAL GRIDS

Сучасна енергетична система стикається з численними викликами, зумовленими технічними, економічними та екологічними факторами. Усе частіше електромережі стикаються з проблемою дисбалансу через непередбачувані обставини, такі як пікові навантаження, аварійні ситуації або раптові зміни в обсягах генерації електроенергії. Усі ці фактори ускладнюють управління енергосистемою та створюють необхідність пошуку нових рішень для забезпечення її стабільності, надійності та гнучкості. Одним із перспективних підходів до розв'язання цих проблем є впровадження та вдосконалення методів інтеграції локальних мереж MicroGrid у загальні електричні мережі[1].

Відсутність децентралізованої системи управління, яка б дозволяла оптимізувати потоки енергії між локальними мережами та загальною системою, є ще однією перешкодою для інтеграції MicroGrid у загальні електромережі[2].

Запропоновано системний підхід спрямований на комплексне вирішення проблем інтеграції мікромереж (MicroGrid) у загальні електричні системи. Він охоплює технічні, економічні та аналітичні аспекти, сприяючи ефективному використанню потенціалу мікромереж для стабілізації та розвитку сучасної енергетичної інфраструктури.

Технічні рішення включають: 1) апаратно-програмний комплекс для інтеграції мікромереж, що складається з універсального шлюзу комунікації, який забезпечує підтримку основних протоколів керування таких як OpenADR, IEEE 2030.5, Modbus для інтеграції мікромереж з різними типами обладнання та платформами; 2) систему управління потоками енергії для автоматизації керування станом підключення мережі MicroGrid до загальних мереж та автоматичного обліку електроенергії; 3) інтерфейси інтеграції для операторaторів мережі. Економічні та аналітичні аспекти представляють собою тариф, який би підтримував динамічне ціноутворення, налаштування часу роботи, та стимулював нарощування потужностей генерації електроенергії господарствами.

Такий підхід сприятиме покращенню стабільності загальних електричних мереж, стимулюватиме подальший розвиток альтернативних джерел генерації електроенергії, та допоможе застосовувати децентралізовані рішення для динамічного реагування потреби електромережі, що покращить стабільність електропостачання в цілому.

Література

1. S. M. Hosseini, R. Carli and M. Dotoli, «Robust optimal energy management of a residential microgrid under uncertainties on demand and renewable power generation», IEEE Trans. Autom. Sci. Eng., vol. 18, no. 2, pp. 618-637, Apr. 2021.
2. Michael Stadler, Gonçalo Cardoso, Salman Mashayekh, Thibault Forget, Nicholas DeForest, «Value streams in microgrids: A literature review», Applied Energy, vol. 162, pp. 939–948, Jan. 2016.

УДК 004.3
Р. О. Жаровський, канд. техн. наук; В. А. Іваницький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

GSM-СИГНАЛІЗАЦІЇ ЯК СПОСІБ РОЗШИРЕННЯ ФУНКЦІОНАЛЬНОСТІ РОЗУМНИХ БУДИНКІВ ТА ПІДВИЩЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ НЕРУХОМОСТІ

UDC 004.3
R. O. Zharovskyi, PhD.; V. A. Ivanytskyi

GSM-ALARM AS A WAY OF SMART HOUSE FUNCTIONALITY EXTENDING AND PROPERTY'S SAFETY INCREASING

GSM-сигналізація відноситься до класу охоронних систем та базується на використанні мобільного зв'язку. У таких системах передбачається надсилання сигналу-сповіщення на смартфон з метою попередження власника фізичного стаціонарного об'єкту про виникненні небажаних подій. Передача даних від GSM-сигналізації відбувається на основі цифрового стандарту стільникового зв'язку.

Типова структура при організації GSM-сигналізації передбачає використання центрального блоку управління, який може бути реалізований за допомогою Raspberry PI, Arduino чи інших мікроконтролерів, GSM-модуля і сенсорів руху. Окрім цього, до пристрою керування GSM-сигналізацією можуть підключатися бездротові датчики газу та диму, сенсори розбиття скла чи відмикання дверей. Зазвичай, класичні системи безпеки подають сигнал тривоги у форматі SMS-повідомлення безпосередньо на мобільний телефон власника стаціонарного фізичного об'єкту.

Системи на базі GSM-технологій володіють і забезпечують гнучкість налаштування параметрів. Зокрема, можна реалізовувати режим оповіщення про пожежу у приміщенні, появу рухомих об'єктів, витік газу. Важливою також є функція одночасного надсилання повідомлень на мобільні телефони кількох адресатів, список яких налаштовується власником GSM-сигналізації. Інтеграція GSM-сигналізації у проєктах розумного будинку дає можливість значно підвищити функціональність, комфорт та безпеку таких рішень. Одна охоронна система на основі технології GSM може забезпечити контроль різних зон у квартирі чи будинку з ідентифікацією того, який конкретно компонент системи надіслав сигнал про порушення простору.

Для віддаленого керування систем, базованих на GSM-технології, використовуються додатки, які можна встановлювати на смартфон, а при реалізації охоронних систем важливо враховувати фактор розміру фізичного об'єкта, оскільки потрібно визначити кількість необхідних сенсорів.

Сучасні технології дозволяють GSM-системі функціонувати у наступних режимах:

– сповіщення власників – режим при якому передається повідомлення усім абонентам, які наявні у списку користувачів сигналізації

– локальне масове сповіщення – режим, який налаштовується у випадку виникнення пожежі або диму з додатковою комунікацією з системою сирен або підсвітки евакуаційних виходів;

– увімкнення захисних і додаткових систем – охоронна система на основі GSM-технології може паралельно працювати з системою вентиляції, пожежогасіння, газопостачання та водопостачання і керуватися GSM-сигналізацію.

Враховуючи високі функціональні можливості GSM базованих інструментів можна забезпечити повний захист будь-якої нерухомості.

УДК 004.3
Р. О. Жаровський, канд. техн. наук; В. А. Іваницький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОРГАНІЗАЦІЯ ЗАХИСТУ СТАЦІОНАРНОГО ОБ'ЄКТУ НЕРУХОМОСТІ НА ОСНОВІ GSM-СИГНАЛІЗАЦІЇ ТА МІКРОКОНТРОЛЕРА RASPBERRY PI

UDC 004.3
R. O. Zharovskyi, PhD.; V. A. Ivanytskyi

ORGANIZATION OF SAFETY OF A STATIONARY PROPERTY OBJECT BASED ON GSM-SIGNALIZATION AND RASPBERRY PI

Розвиток IT-технологій, окрім благородної мети, може вносити у суспільство багато нових загроз. У зв'язку з цим доцільно постійно вдосконалювати розумні комп'ютерні системи, орієнтовані на підвищення рівня безпеки кожної людини шляхом довіри і підтвердження надійності нових технологій.

Одним із таких способів є організація автоматизованих систем безпеки та охоронної сигналізації під керуванням GSM. Система блокування дверей з сервоприводом, що дозволяє блокувати входи/виходи всередині приміщення, є додатковою перевагою. Як тільки датчик розмикається, власник отримує дзвінок і через кілька хвилин всі двері в будинку будуть замкнені на окремий замок. Така система функціонує надійно, оскільки завжди наявний доступ до Інтернету.

Система розумного будинку на базі GSM і Bluetooth забезпечує визначену функціональність за низькою ціною і водночас не ставить під загрозу безпеку. Основним контролером управління у таких системах є Arduino. Проте точність передачі даних є не надто високою, а її складна інтеграція при підключенні аудіодинаміків споживає величезну енергію. Щоб уникнути цього, пропонується альтернативна система сповіщення на основі Raspberry Pi. На рис. 1 показано архітектуру пропонованого рішення.

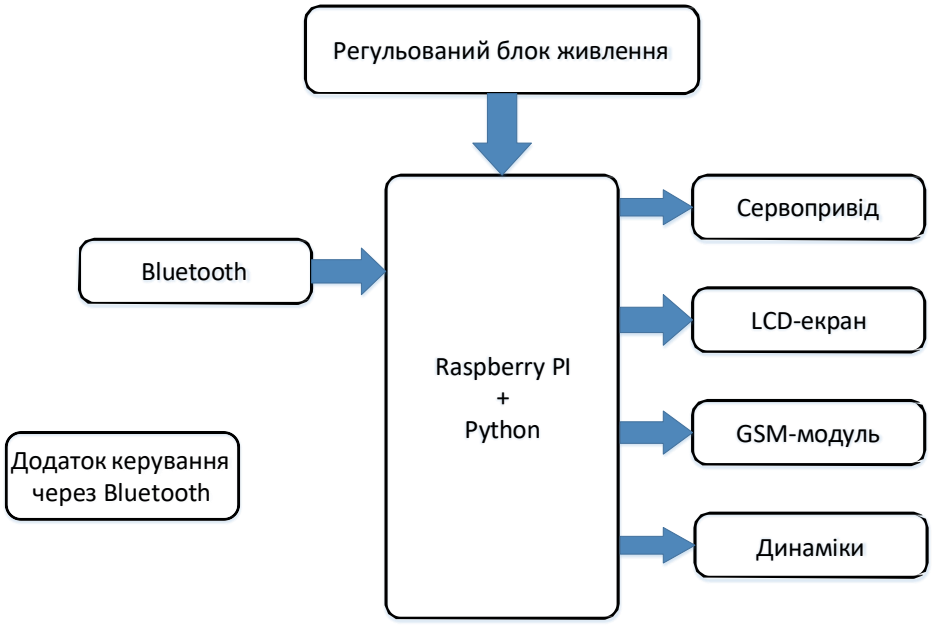


Рисунок 1. Архітектура системи захисту стаціонарних об'єктів на основі Raspberry PI

УДК 004.27
Р. О. Жаровський, канд. техн. наук; І. П. Цірка
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ ПРИ РЕАЛІЗАЦІЇ МЕРЕЖІ ЗБОРУ, ПЕРЕДАЧІ ТА АНАЛІЗУ ДАНИХ ВОДОСПОЖИВАННЯ

UDC 004.27
R. O. Zharovskyi, PhD.; I. P. Tsirka

DATA TRANSMISSION TECHNOLOGIES IN THE IMPLEMENTATION OF A NETWORK FOR COLLECTION, TRANSMISSION AND ANALYSIS OF WATER CONSUMPTION DATA

Реалізація розумних комп'ютерних систем зчитування показників з лічильників води передбачає наявність двох основних компонентів: модуля зчитування даних і комунікаційного модуля. Мережа передачі даних сьогодні, зазвичай, використовує технологію GSM, а сповіщення відправляються у вигляді SMS-повідомлень.

Технологія GSM забезпечує послугу SMS (служба коротких повідомлень) і GPRS (загальна служба пакетної передачі даних) для запиту та отримання даних. Мережа GSM широко використовується без будь-яких технічних проблем, що обумовлено ефективним, надійним і безпечним стандартом зв'язку.

Технологія ZigBee ефективна в протоколах зв'язку високого рівня при створенні персональних мереж, мереж з низьким енергоспоживання та практично нульовим трафіком. Дана технологія не потребує спеціальних дозволів і водночас може опрацьовувати кілька каналів. Даний протокол використовує діапазон частот ISM 2,4 ГГц.

ZigBee має радіус дії від 10 м до 2 км і добре працює з такими мережами, як Wi-Fi, Ethernet і GPRS, а також забезпечує масштабоване мережеве рішення, яке підходить для використання в програмах керування та моніторингу.

WPAN (бездротова персональна мережа) охоплює невелику географічну область і використовує стандарт IEEE 802.15. Це дозволяє пристроям забезпечувати зв'язок один з одним.

Технологія Bluetooth є стандартом для забезпечення бездротового зв'язку між мобільними комп'ютерами, мобільними телефонами, портативними пристроями та IoT. Бездротова локальна мережа (WLAN) дозволяє обмінюватися інформацією між різним обладнанням, розташованим на обмеженій відстані. Порівняльний аналіз технологій передачі даних при впровадженні мереж збору і трансферу даних з IoT пристроїв наведено у табл. 1.

Таблиця 1. Порівняльний аналіз технологій передачі даних у системі обліку води

Технологія	Вартість	Покриття	Надійність	Протокол зв'язку
GSM	Низька	Глобальне	Висока	Стабільний
ZigBee	Середня	Локальне	Низька	Не стабільний
WiMAX	Середня	Локальне	Середня	Стабільний
Wi-Fi	Низька	Локальне	Висока	Стабільний

УДК 681.518.3
Р. О. Жаровський, канд. техн. наук; І. В. Марценюк; А. М. Паламар, канд. техн. наук
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СТРУКТУРА АВТОМАТИЗОВАНОЇ ІОТ-СИСТЕМИ ДЛЯ МОНІТОРИНГУ КОНЦЕНТРАЦІЇ МЕТАНУ В ШАХТАХ

UDC 681.518.3
R. O. Zharovskyi, Ph.D; I. V. Martseniuk; A. M. Palamar, Ph.D

STRUCTURE OF AN AUTOMATED IOT SYSTEM FOR MONITORING METHANE CONCENTRATION IN MINES

Підвищення безпеки праці у вугільних шахтах є важливим завданням сучасної гірничої промисловості. Метан, що утворюється в середовищі шахт, є одним із найнебезпечніших газів через його високу вибухонебезпечність. Традиційні методи контролю концентрації метану часто не забезпечують належної швидкодії та точності, що створює ризики для працівників. Тому актуальною задачею є розробка автоматизованої системи моніторингу, яка б поєднувала сенсорні технології та можливості інтернету речей (IoT).

Метою цього дослідження є розробка структури автоматизованої IoT-системи для моніторингу концентрації метану, яка забезпечує безперервний контроль і своєчасне попередження про небезпеку. Запропонована система складається з сенсорного модуля, контролера, комунікаційного модуля та хмарної платформи. Структурна схема системи моніторингу концентрацій метану подана на рис. 1.

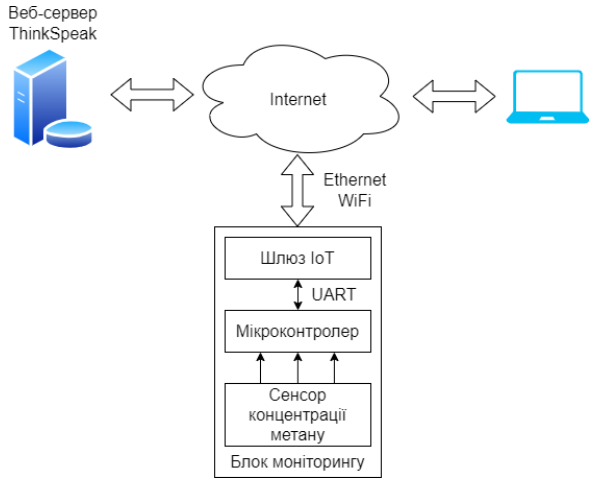


Рисунок 1. Структура системи моніторингу концентрацій метану

Сенсорний модуль виконує вимірювання рівня метану у виробках шахти. Зібрані дані передаються на мікроконтролер, який аналізує отриману інформацію, порівнюючи її з граничними значеннями. У разі перевищення безпечного рівня система активує сигналізацію та передає тривожне інформацію на хмарну платформу ThingSpeak. Через хмару дані стають доступними у вигляді графіків, що дозволяє оперативно реагувати на загрози.

Перевагами системи є її надійність, можливість віддаленого моніторингу та висока швидкодія. Використання IoT-технологій забезпечує інтеграцію з іншими системами безпеки та масштабованість для великих шахтних об’єктів. Впровадження таких систем значно знижує ризики аварійних ситуацій і сприяє підвищенню безпеки праці у вугільних шахтах.

УДК 004.9:550.34

Д. Клочко; Ю. Лещишин, к.т.н.; Р.Жаровський, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КОМП'ЮТЕРНА СИСТЕМА МОНІТОРИНГУ СЕЙСМІЧНОЇ АКТИВНОСТІ ЗЕМНОЇ КОРИ

UDC 004.9:550.34

D. Klochko; Y. Leshchyshyn, Ph.D.; R. Zharovskyi, Ph.D.

COMPUTER SYSTEM FOR MONITORING SEISMIC ACTIVITY OF THE EARTH'S CRUST

Моніторинг сейсмічної активності земної кори є надзвичайно актуальним оскільки є джерелом інформації для прогнозування природних катастроф, для розробки систем раннього попередження про землетруси, для наукового вивчення процесів у земній корі, для підвищення безпеки інфраструктури тобто будівництва стійких до землетрусів будівель і споруд, а також допомагає оцінити ризики для існуючих конструкцій. Також, що важливо сейсмічна активність часто пов'язана з іншими природними явищами, такими як цунамі, зсуви, та вулканічні виверження. Загалом покращення механізмів моніторингу сприяє зменшенню економічних збитків від землетрусів, які можуть спричинити руйнування інфраструктури, збої у виробництві та переселенню населення.

Оскільки землетруси трапляються раптово, тому комплексні системи моніторингу сейсмічної активності, повинні бути здатні надати попередження навіть за кілька секунд до події, що може зберегти життя та мінімізувати матеріальні збитки. Тому комп'ютеризовані системи моніторингу повинні забезпечувати отримання, передавання та автоматичну обробку сейсмічних сигналів у реальному часі. З наступним опрацюванням великих обсягів даних від сотень або тисяч сейсмічних станцій та використовувати алгоритми машинного навчання для прогнозування подій та ідентифікації аномалій. І як результатом роботи має бути миттєве оповіщення громадян через мобільні та інтернет-платформи.

Тому завданням комп'ютерної системи моніторингу сейсмічної активності земної кори, як частини комплексної системи, повинно бути відбір і передавання сейсмічних сигналів отриманих на значних віддалях і територіях у реальному масштабі часу із вказанням геолокації розміщення сенсора на сервери комплексної системи моніторингу. Також робота такої системи повинна забезпечувати тривалу автономну роботу без втручання людини на самодіагностику роботи.

Література

1. Жаровський Р.О., Щербак Л. М. Моделі геофізичних сигналів на основі лінійних випадкових процесів. Вісник ТДТУ. 2009. №1. С. 138–144**.**
2. Жаровський Р., Щербак Л. Задачі обробки геофізичних сигналів при дії завад дискретною кореляційною системою з вхідними ортогональними фільтрами. Вісник ТДТУ. 2010. Том 15. № 2. С. 172–181.
3. Жаровський Р.О. Кореляційні ортогональні системи у задачах оброблення геофізичних сигналів. Науковий вісник НЛТУ України: Збірник науково-технічних праць. Львів: РВВ НЛТУ України. 2010. № 20.7. С. 283–292.
4. Kozlovskyi V., Scherbak L., Martyniuk H., Zharovskyi R., Balanyuk Y., Boiko Y. Applying an adaptive method of the orthogonal laguerre filtration of noise interference to increase the signal/noise ratio. *Eastern-European Journal of Enterprise Technologies*. 2020. №2/9(104). Pp. 14–21.

УДК 621.391
Д. М. Козак; Н. Б. Стадник, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ СТАНДАРТІВ ФІЗИЧНОГО РІВНЯ WI-FI

UDC 621.391
D. M. Kozak; N. B. Stadnyk, PhD.

RESEARCH OF WI-FI PHYSICAL LAYER STANDARDS

Протокол IEEE 802.11, завершили розробляти який у 1997 р., є основним і він встановлює ті підстандарти, котрі потрібні для функціонування WLAN. З них є головними – протокол керування доступом до MAC і протокол передавання сигналів на фізичному рівні PHY [1]. Основним методом доступу протоколом 802.11 визначено протокол CSMA/CA. Остаточну редакцію стандарту 802.11b, відомого зараз як Wi-Fi, було успішно ратифіковано у 1999 році. Базовою радіотехнологією тут є метод DSSS із 8-розрядними рядами Волша. Для передавання сигналу застосовується DSSS, коли увесь діапазон поділяється на п’ять піддіапазонів, котрі перекриваються, дані передаються по кожному з них. Кожен біт закодовується набором додаткових кодів (CCK). Пропускна здатність каналу становить 11 Мбіт/сек. Варто відзначити, що DSSS і CCK включають пряму корекцію помилок (FEC) на бітовому рівні.

IEEE 802.11, що з'явилася в 2009 році, і отримала назву Wi-Fi 4, працює в діапазоні 2,4 і 5 ГГц, дозволяє досягати швидкостей до 150 Мбіт/с при ширині каналу 40 МГц на кожну незалежну антену [1]. Обладнання 802.11n здатне функціонувати у трьох режимах: успадкованому, змішаному та «чистому». При роботі в успадкованому (Legacy) режимі наявна підтримка обладнання 802.11b/g і 802.11a; за змішаного (Mixed) доповнюється режим 802.11n. «Чистий» режим дає перевагу підвищеній швидкості та збільшеній дальності передачі даних, що забезпечує стандарт 802.11n.

Основою стандарту 802.11n є технологія MIMO [1], за допомогою якої відбувається просторове мультиплексування, котре намічає одночасне передавання по одному каналу власне кількох інформаційних потоків і застосування для доставлення багатопроменевого сигналу поширення, це зводить до мінімуму вплив перешкод і втрат даних. Як раз і здатність одночасного передавання і приймання даних робить вищою пропускну здатність обладнання 802.11n. Але багатопроменеве поширення здатне негативно впливати на спільну продуктивність, а також на пропускну здатність і, властиво, збільшення затримок Wi-Fi мережі з огляду на потребу здійснення перенаправлення фреймів 2-го рівня, приводом котрих є міжсимвольна інтерференція. Пов’язано це з будь-якою мережею Wi-Fi. Стандарт IEEE 802. 11g здійснює передачу даних у тому частотному діапазоні, що і 802.11b і забезпечує швидкість з'єднання до 54 Мбіт/с. Він обернено сумісний зі стандартом 802.11b в режимі модуляції DSSS. В цьому випадку швидкість з'єднання буде обмежена 11 Мбіт/с. Але використовуючи режим модуляції OFDM швидкість може досягати 54 Мбіт/с. Розроблений стандарт бездротових локальних мереж Wi-Fi IEEE 802.11ac, який отримав назву Wi-Fi 5, функціонує у діапазоні 5 ГГц. Він дозволив значно розширити пропускну спроможність мережі до 6,77 Гбіт/с при 8х MU-MIMO - антенах (Multi User MIMO).

Наступним поколінням технології Wi-Fi стала розробка нового стандарту IEEE 802.1 1ax. Беручи до уваги особливості, новітній протокол 802.11ax може досягати фізичної швидкості близько 10 Гбіт/с, забезпечуючи повнофункціональну паралельну роботу множини клієнтських пристроїв та застосовуючи увесь наявний діапазон частот, що не ліцензується.

Література

1. Офіційний сайт IEEE 802.11. URL: https://ieeexplore.ieee.org /document/8360794 (дата звернення: 10.12.2024).

УДК 621.391
Д. М. Козак; Н. Б. Стадник, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ МАНІПУЛЯЦІЇ СИГНАЛОМ У БЕЗДРОТОВОМУ ЗВ'ЯЗКУ

UDC 621.391
D. M. Kozak; N. B. Stadnyk, PhD.

KEYING METHODS OF SYGNAL IN WIRELESS COMMUNICATION

При надсиланні даних сигнал передається з передавача. Щоб передавати дані необхідно керувати сигналом так, щоб сторона, що приймає, могла розрізнити нулі та одиниці. Метод маніпуляції або управління сигналом, при якому можна представляти множинні дані називається Методом кодування (Keying Method).

Існує три основні типи методів кодування [1]:

– ASK (Amplitude-Shift Keying) – кодування зі зміною амплітуди. ASK змінює амплітуду сигналу (висота) для подання двійкових даних Це техніка поточного стану, де один рівень амплітуди (висоти) представляє нуль, наприклад, велика амплітуда хвилі представляє одиницю, а менша - нуль. Це завдання вимагає почати з визначення періоду, в який сигнал може прийматися - символьний період. Потім приймач може використовувати це як спеціальний часовий інтервал-маску (семпл) для перевірки хвилі протягом саме символьного періоду для визначення амплітуди хвилі;

– FSK (Frequency-Shift Keying) – кодування зі зміною частоти. FSK змінює частоту сигналу подання двійкових даних. FSK – це техніка поточного стану, де одна частота є нуль, а інша частота становить одиницю. Зміна частоти визначає дані, що передаються. Коли приймач семплює сигнал протягом символьного періоду, він визначає значення частоти сигналу, і, залежно від цієї частоти, приймач може розпізнати відповідне двійкове значення.

FSK застосовується у деяких старих технологіях 802.11 (і у деяких існуючих старих мережах). Для підтримки більш високих швидкостей FSK вимагає більш дорогих компонентів і стає менш практичним для розробки.

– PSK (Phase-Shift Keying) – кодування зі зміною фази. PSK змінює фазу сигналу подання двійкових даних. PSK це техніка зміни стану, де зміна фази становить нуль, а статичний стан фази становить одиницю. Така зміна визначає двійкові дані, які передаються. Коли приймач семплює сигнал протягом символьного періоду він визначає фазу хвилі і відповідний стан біта даних.

PSK широко використовується для радіопередачі, що визначено у стандарті 802.11-2007. Звичайна реалізація передбачає, що приймач семплює сигнал протягом символьного періоду, порівнює фазу поточного семпла з попереднім семплом і визначає чи є відмінність. Кут такої відмінності або диференціал використовують для отримання значення біта.

Більш просунуті версії PSK можуть кодувати безліч бітів на символ. Можна використовувати, наприклад, не дві фази, а чотири та кожна така фаза може мати два двійкових значення нуль або одиниця (00, 01, 10, 11), а не просто (0, 1). Такий підхід дозволяє за однаковий час заняття ефіру передавати значно більший обсяг даних. Коли використовується більше двох фаз, це називається MPSK (Multiple PSK).

Література

1. Modulation in telecommunication. URL: https://www.britannica.com/technology/telecommunication/Modulation/ (дата звертання: 22.11.24).

УДК 004.72
М. В. Козачок; С. В. Марценко, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНКЛЮЗИВНОЇ ОСВІТИ

UDC 004.72
M. V. Kozachok; S. V. Martsenko, Ph.D., Assoc.

RESEARCH OF TELECOMMUNICATION TECHNOLOGIES FOR INCLUSIVE EDUCATION

У звіті ЮНІСЕФ за 2021 рік [1] подано інформацію, що у світі налічується 240 мільйонів дітей з інвалідністю. Використання нових сучасних методів та засобів забезпечення освітніх послуг є актуальною задачею, вирішення якої неможливе без надійних телекомунікаційних технологій, що будуть їх підтримувати.

Аналізуючи роль інформаційних технологій в інклюзивній освіті, можна виділити декілька напрямків їх застосування. Широкого розповсюдження отримало дистанційне навчання, яке разом з останніми подіями пов'язаними з пандемією COVID-19 та повномасштабною війною в Україні набуло нового значення поза межами інклюзії. Формування надійного середовища для надання освітніх послуг у дистанційному форматі є необхідною умовою забезпечення доступності освіти та безпеки у ситуації війни. Сучасні платформи дистанційного навчання надають доступ до відеоконференцій, віртуальних класів, роботі в групах та навчальних матеріалів розроблених провідними фахівцями різних університетів та шкіл. Навчання стало інтерактивним з використанням мобільних технологій і додатків, засобів тестування знань, інтерактивних дошок та програмного забезпечення, що враховує індивідуальну складову в інклюзивній освіті. Спілкування між учителем та учнем не обмежене в часі через використання комунікаційних інструментів таких як чати та тематичні форуми, обмін думками та враженнями можливий у закритих групах, що забезпечують потреби вузької спеціалізації певних груп учнів.

Сучасні засоби навчання враховують можливості перетворення тексту на мовлення для людей з вадами зору, розроблені програми навчання осіб з вадами слуху. Засоби віртуальної та доповненої реальності збагачують навчальний процес новими методиками та можливостями, що не були доступні раніше.

Узагальнюючи попередньо згадані потреби і можливості інклюзивної освіти, потрібно провести дослідження впровадження наступних телекомунікаційних технологій:

- розробка та впровадження телекомунікаційних платформ з можливістю інтеграції потреб інклюзивної освіти;
- використання рішень на базі мобільних телефонів та планшетів;
- персоналізація навчального процесу та його адаптація до особливих потреб через використання штучного інтелекту;
- застосування пристроїв Інтернету речей для формування шкільного та домашнього навчання.

Розробка сучасних та масштабованих телекомунікаційних рішень для потреб інклюзивної освіти дасть змогу зробити освіту доступнішою та гнучкішою.

Література

1. У світі живе близько 240 мільйонів дітей із інвалідністю – свідчать дані найповнішого статистичного аналізу ЮНІСЕФ [Електронний ресурс]. – Режим доступу: https://www.unicef.org/ukraine/press-releases/copy-nearly-240-million-children-disabilities-around-world-unicefs-most – Назва з екрану. – Дата звернення: 08.12.2024.

УДК 004.75
О. В. Крайник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИМОГИ ДО БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

UDC 004.75
O. V. Krainyk

REQUIREMENTS FOR WIRELESS SENSOR NETWORKS

Автономія. Ліквідація якогось вузла бездротової сенсорної мережі (БСМ) не має нести виплив на її функціонування. Так як мережа не має мати центрального вузла, який-небудь користувач здатен здійснювати функції віддаленої маршрутизації.

Енергетична ефективність. Протоколи маршрутизації мають максимально ефективно використовувати енергію.

Масштабованість. БСМ складаються із сотень мотів, саме тому протоколи маршрутизації повинні функціонувати з таким їх числом.

Стабільність. Давачі здатні раптово перестати працювати через поломку батареї живлення або із якихось зовнішніх причин. Маршрутизацйні протоколи мають опрацьовувати цю ймовірність так, щоб якщо струм у мотах пропаде, можна було використовувати альтернативний маршрут.

Неоднорідність приладів. Хоча більшість додатків БСМ залежить від однорідності вузлів, використання різних типів давачів може забезпечити значний привілей.

Мобільність. За певних подій моти здатні переміщуватися під час роботи.

Особливості та обмеження БСМ створюють спеціальні умови до маршрутизаційних протоколів.

Базується на параметрах. Для цих алгоритмів вузол надсилає запити до певних ділянок мережі та очікує відповіді від давачів, розташованих у цій частині. Вибирання параметрів перебуває у залежності залежить від визначеної програми. Головна особливість такої схеми – зміст меседжу даних піддається аналізу під час кожного етапу маршрутизації.

Енергетична ефективність. У цих алгоритмах можна вибрати шляхи, котрі, як сподівається, найбільше сприятимуть зберіганню енергії в мережі. З цією метою маршрут містить вузли із вищими енергетичними ресурсами.

Агрегування даних. Відносно близькі вузли можуть робити аналогічні дані, котрі здатні поєднуватися з деякою прийнятною втратою точності.

Застосування давачів істотно залежить від зв'язку між мотами, так як це потрібно для втілення визначених алгоритмів або процедур. На ділі є три головні типи алгоритмів маршрутизації для БСМ – централізовані, розподілені і локальні:

Алгоритми, що використовуються, є важливим фактором, який необхідно враховувати при вибиранні маршрутизаційного алгоритму. Коли застосовуються локальні алгоритми, тоді основною буде значна комунікаційна зв'язуваність вузлів, які знаходяться поруч. Для централізованих алгоритмів консолідація повідомлень буде значним привілеєм. Розподілені ж алгоритми мають надавати вірне з'єднання між двома мережевими мотами. Для локальних алгоритмів варто зважати на те, що застосування побічних механізмів позиціонування (як варіант GPS) здатне досить збільшити вартість такої мережі.

Класифікація за методом розрахунку шляхів: проактивні протоколи – всі шляхи розраховуються заздалегідь, як вони знадобляться; реактивні протоколи – шляхи розраховуються на вимогу; гібридні протоколи – це поєднання двох підходів.

УДК 004.056

О. В. Крайник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ZIGBEE GREEN POWER

UDC 004.056

O. V. Krainyk

ZIGBEE GREEN POWER

Альянс ZigBee, активний розробник стандартів і рішень для бездротових сенсорних мереж (БСМ), оголосив у 2009 році про своє рішення випустити стандарт Zigbee Green Power (GP) для пристроїв з власними альтернативними джерелами живлення, заснованими на технології запозичення енергії. Грунтуючись на стандарті ZigBee GP, у 2014 році році NXP Laboratories, випустила Посібник із використання стандарту GP під час роботи з мікроконтролерами серії NXP jn516x.

– використання більш короткого формату кадрів GP і, отже, меншого часу передачі, ніж у разі кадрів ZigBee стандартного формату IEEE 802.15.4, що дозволяє заощаджувати енерговитрати на передачу;

– вузли не обов'язково повинні бути повноцінними компонентами БСМ, можливо, що вузли передають дані лише у разі потреби.

Кадр GP відноситься до проксі-вузла, який є компонентом сенсорної мережі та оснащений «тунелем», який перетворює кадр GP на звичайний формат кадру ZigBee для повторної передачі в сенсорну мережу. Кластер GP не потребує вихідного вузла, але повинен взаємодіяти як з проксі-вузлом, так і з дренажем, щоб отримати кадри GP, що інтерпретуються. Базовий алгоритм стандарту GP ZigBee показано на рис. 1., де кадр 1 – це кадр GP, а кадр 2 – туннельований кадр GP.

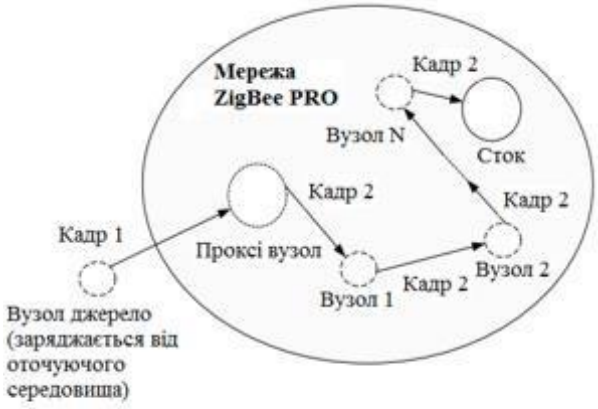


Рисунок 1 – Базовий механізм ZigBee GP

Переваги використання ZigBee GP полягають у наступному:

– підходить для вузлів, розташованих з можливістю підтримки роботи;

– можливість використання вузлів, основні джерела енергії при яких, батареї належним чином не захищені або недоступні, а також використання ізольованих вузлів або вузлів, розташованих небезпечно;

– використання відновлюваних джерел енергії вузлами;

– можливість усунення потреби в батареї у вузлах БСМ, колективне підтримання працездатності, споживання та відновлення енергії;

– дешева, швидка та проста установка вихідних вузлів.

Таким чином, можна сказати, що для оснащення БСМ можливістю запозичення енергії з навколишнього середовища пропонуються як готові рішення (наприклад, Silicon Lab), так і стандарти для створення модулів для запозичення енергії з навколишнього середовища.

Можна виділити Zigbee Alliance , яка розробила спеціалізований стандарт GP standard для доповнення стандартної мережі відновлюваними джерелами енергії. Ну, а як сфери застосування даної технології, щоб підвищити енергетичний потенціал сенсорної мережі можна розглянути розробку енергонезалежних модулів для БСМ.

УДК 004.451:656.025.2
І. О. Кухар
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕГРАЦІЯ СОНЯЧНИХ ЕЛЕКТРОСТАНЦІЙ У SMART GRID: СУЧАСНІ РІШЕННЯ ТА ГЛОБАЛЬНІ ТРЕНДИ

UDC 004.451:656.025.2
I. O. Kukhar

INTEGRATION OF SOLAR POWER PLANTS INTO SMART GRIDS: MODERN SOLUTIONS AND GLOBAL TRENDS

Сучасний розвиток енергетики обумовлює необхідність масштабного впровадження відновлюваних джерел енергії, зокрема сонячних електростанцій (СЕС). Їх інтеграція у розумні електромережі (Smart Grid) є критично важливою для досягнення енергетичної стійкості та декарбонізації.

Головними викликами інтеграції СЕС є нестабільність вироблення енергії, залежність від погодних умов та обмежена інфраструктурна сумісність із традиційними мережами. Для вирішення цих проблем сучасні дослідження пропонують використання систем прогнозування генерації, інтеграцію накопичувачів енергії та розвиток децентралізованих схем управління.

У рамках розумних мереж використовуються такі технології:

– машинне навчання для аналізу даних та прогнозування генерації енергії;
– системи накопичення енергії, що забезпечують баланс між попитом та генерацією;
– інтернет речей (IoT) для моніторингу та управління потоками енергії в реальному часі.

Використання інноваційних підходів у проектуванні розумних мереж дозволяє значно підвищити ефективність роботи СЕС. Впровадження таких рішень сприяє енергетичній незалежності, зниженню викидів парникових газів та підвищенню загальної стабільності енергосистеми.

Література

1. International Energy Agency. Global Energy Review 2023. URL: https://www.iea.org/reports/global-energy-review-2023.
2. International Energy Agency. World Energy Investment 2023. URL: https://www.iea.org/reports/world-energy-investment-2023.
3. International Energy Agency. World Energy Outlook 2024. URL: https://www.iea.org/reports/world-energy-outlook-2024.

УДК 004.451:656.025.2
І. О. Кухар
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕГРАЦІЯ ВІДНОВЛЮВАЛЬНИХ ДЖЕРЕЛ ЕНЕРГІЇ В РОЗУМНІ ЕЛЕКТРИЧНІ МЕРЕЖІ З ВИКОРИСТАННЯМ ПЕРЕДОВИХ ТЕХНОЛОГІЙ

UDC 004.451:656.025.2
I. O. Kukhar

INTEGRATION OF RENEWABLE ENERGY SOURCES INTO SMART GRIDS USING ADVANCED TECHNOLOGIES

Інтеграція відновлювальних джерел енергії в розумні електричні мережі є критично важливою для зниження залежності від традиційних джерел енергії та сприяє розвитку сталих енергетичних систем, що знижує викиди вуглецю та підвищує енергетичну незалежність. Цей процес є ключовим для забезпечення сталого розвитку енергетичних систем в умовах глобальних змін клімату.

Новітні моделі планування і прогнозування, що використовують стохастичні підходи, допомагають ефективно враховувати коливання попиту та пропозиції енергії. Це особливо важливо для стабільної роботи мереж з високою часткою відновлювальних джерел енергії, таких як сонячні та вітрові станції, що мають значні коливання в залежності від погодних умов. Смарт-мережі сприяють ефективному управлінню енергоспоживанням, знижуючи ризики перевантаження та оптимізуючи використання енергії. Це дозволяє підтримувати баланс між попитом і пропозицією енергії, що є особливо важливим при інтеграції змінних відновлювальних джерел, таких як сонячні та вітрові електростанції. Створення гнучкої інформаційної архітектури для управління розподілом енергії дозволяє зменшити втрати енергії та підвищити надійність енергетичних систем. Це дає можливість інтегрувати різні джерела енергії в єдину мережу, що є необхідним для сталого розвитку енергетичних систем в умовах високої частки відновлювальних джерел. Уряди багатьох країн активно підтримують модернізацію енергетичних систем, інвестуючи в інфраструктуру для інтеграції відновлювальних джерел. Наприклад, в Таїланді до 2037 року планується отримувати третину енергії з відновлювальних джерел, а в Нью-Йорку активно оновлюються енергомережі для переходу на чисту енергію до 2040 року.

Література

1. McKinsey & Company. Innovation at Work.URL: https://www.mckinsey.com/business-functions /operations/our-insights/innovation-at-work.
2. Innovation at Work. Integration of Renewable Energy in Smart Grids.URL: https://www. innovationatwork.com/articles/integrating-renewable-energy-in-smart-grids.

УДК 004.9:623.7
Ю. Лещишин, к.т.н.; А. Герасименко; О. Герасименко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

КОМП'ЮТЕРНА СИСТЕМА МОНІТОРИНГУ РАДІОЗВ'ЯЗКУ ВІД БПЛА

UDC 004.9:623.7
Yu. Leshchyshyn, Ph.D.; A. Herasymenko; O. Herasymenko

COMPUTER SYSTEM FOR MONITORING RADIO COMMUNICATIONS FROM UAVS

Стрімке зростання використання безпілотних літальних апаратів (БПЛА) у різних сферах діяльності викликає потребу забезпечити моніторинг та контроль за їх комунікаційними системами. БПЛА активно застосовуються в обороні, цивільній авіації, логістиці, сільському господарстві, екологічному моніторингу та інших сферах. Радіозв'язок є ключовим елементом управління БПЛА, тому моніторинг цих каналів стає критично важливим для забезпечення безпеки польотів та захисту від кіберзагроз і несанкціонованого використання БПЛА.

Основними загрозами для радіозв'язку БПЛА є [1, 2]: перехоплення керування за рахунок несанкціонованого доступу до каналів зв'язку та радіоелектронна боротьба (РЕБ), тобто глушіння сигналів або втручання у канали зв'язку, а також перевантаження смуги використовуваних частот, коли за великої кількості безпілотників може виникати конкуренція за частоти.

Комп'ютерна система моніторингу може бути реалізована за допомогою апаратної частини у вигляді багатоканальних радіочастотних сканерів або модулів для виявлення сигналів. А також із застосуванням програмно-керованих радіостанцій (SDR) для аналізу спектра. Їх поєднання дасть можливість, як широкого сканування радіоефіру, так і зосередженого супроводу вибраних БПЛА. Причому для ефективної роботи такої системи має бути розгорнута мережа сканерів із роботою в реальному масштабі часу для покриття заданої зони спостереження. А отримані дані можуть бути використані для роботи алгоритмів штучного інтелекту із використанням хмарних обчислень для зберігання та аналізу великих обсягів даних, з метою виявлення порушників та аномалій у зв'язку для подальшого аналізу та модифікації алгоритмів виявлення.

Практична реалізація такої системи дозволить вирішити вразливі завдання в цивільній і військовій сферах. Зокрема для цивільної сфери це контроль використання БПЛА у заборонених зонах (поблизу аеропортів атомних електростанцій і т.п.) та захист об'єктів критичної інфраструктури, а також організацію руху БПЛА по маршрутах і використання дозволеного частотного діапазону. Для військової сфери це виявлення та відстеження ворожих БПЛА, а також аналіз можливих атак через перехоплення сигналів.

Література

1. Теорія і практика застосування безпілотних літальних апаратів (дронів). URL: https: //jurkniga.ua/contents/teoriya- i-praktika-zastosuvannya-bezpilotnikh-litalnikh-aparativ-droniv.pdf (дата звернення:10.12.2024).
2. Кучеренко Ю. Ф., Науменко М. В., Кузнєцова М. Ю. Аналіз досвіду застосування безпілотних літальних апаратів та визначення напрямку їх подальшого розвитку при веденні мережецентричних операцій. Системи озброєння і військова техніка. 2018. № 1 (53). С. 25–30. URL: http://surl.li/nfnrc.

УДК 004.9
А. Луцків; А. Люлька
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ АЛГОРИТМІВ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ В ПРОЦЕСАХ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ

UDC 004.9
A. Lutskiv; A. Liulka

APPLICATION OF LOAD BALANCING ALGORITHMS IN THE PROCESSES OF MODERN OPERATING SYSTEMS

Забезпечення ефективного використання ресурсів є критично важливим завданням для сучасних операційних систем (ОС). Алгоритми балансування навантаження виступають ключовим інструментом у розподілі доступних ресурсів між процесами та потоками виконання. Ключовими ресурсами виступають пам’ять, обчислювальні процесори та процесорні ядра, а іноді й сервери. Ці алгоритми дозволяють мінімізувати затримки, запобігати перевантаженню окремих ресурсів та забезпечувати справедливий розподіл обчислювальної потужності.

Для правильного розподілу навантаження між обчислювальними одиницями, в комп’ютерних системах використовуються певні алгоритми. А саме:

– Round Robin – алгоритм послідовного розподілу навантаження;
– Least connections – алгоритм розподілу навантаження до обчислювальних одиниць з найменшою кількістю активних підключень;
– Least Response Time – алгоритм переадресування запитів до обчислювальної одиниці з найкоротшим часом відповіді;
– IP Hash – алгоритм розподілу на основі хешу IP адреси;
– Weighted Round Robin – варіація Round Robin алгоритму з можливістю призначення ваги обчислювальної одиниці для подальшого визначення можливого навантаження цієї обчислювальної одиниці;
– Random – алгоритм випадкового розподілу;
– Dynamic Load Balancing – алгоритм визначення навантаження для кожної обчислювальної одиниці базуючись на метриках, навантаженні центрального процесора та використанні пам’яті.

Дуже важливу роль також відіграють алгоритми планування виконання процесів всередині одної обчислювальної одиниці. Існують основні алгоритми планування процесів всередині кожної обчислювальної одиниці, а саме:

– Round Robin;
– Shortest Job Next;
– First-Come, First-Served;
– Multilevel Queue Scheduling;

У сучасних операційних системах планувальники необхідні для розподілення навантаження процесів між ядрами центрального процесора. Такий принцип дозволить іншим ядрам обробити чергу процесів у випадку:

– Збою сусіднього ядра;
– Негайним переключенням ядра не невідкладну та довготривалу задачу.

Ключовою задачею дослідження є обґрунтування вибору алгоритму та створення власного планувальника обчислювальних завдань для власної системи виконання ресурсоємних обчислювальних задач.

УДК 004.93
Я. О. Мишаківський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ РОЗПІЗНАВАННЯ СТАТІ ТА ВІКУ ЗА ЗОБРАЖЕННЯМ ОСОБИ

UDC 004.93
Ia. O. Myshakivskyi

METHODS OF GENDER AND AGE RECOGNITION FROM THE IMAGE OF A PERSON

Розпізнавання по обличчю є популярним і точним підходом до завдання визначення статі та віку по фото або відео. Причиною цього є присутність на обличчі всіх візуальних особливостей, які дозволяють визначати стать, вік, расу, настрій та багато інших рис людини, візуально видимі в основному (або виключно) на вигляд і подання особи. На відео розпізнавання по особі переважно для визначення статі та віку у випадках, коли на кадрах особа людини видно чітко. У послідовності дій для вирішення описаної задачі можна виділити три етапи: визначення людей на кадрах відеопотоку та побудова детекцій; детектування осіб; розпізнавання статі та віку по особі.

Виявлення особи (face detection) є досить відомим завданням, у якого є множина різних підходів. Для роботи системі необхідно обмежувати область пошуку особи. Це необхідно для можливості однозначного зіставлення виявленої особи з людиною Так само це рішення дозволить прискорити розробку та загальну швидкість роботи системи, оскільки відсутня необхідність у написанні та тестуванні додаткового модуля в порівнянні обмежуючих вікон детектованих осіб та обмежуючих вікон пішоходів. Нижче розписані підходи до задачі детектування особи на кадрі.

Класичні методи визначення осіб. Підходи, які широко використовувалися на початку 2000х років. Використовувалися, тому числі, класичні статистичні методи, аналіз головних компонентів, лінійні та нелінійні класифікатори. Також використовувалися методи зображення, що відображають на площину і за допомогою знаходження відстані Махаланобіса [1], знаходили ступінь близькості поточного виявленого об'єкта з референс вектор обличчя. Незважаючи на хорошу теоретичну базу для відповідних методів, вони майже не застосовувалися в реальних промислових застосунках. Проблемою була вкрай низька здатність подібних підходів адаптуватись до інваріантності середовища.

Методи, засновані на застосуванні нейронних мереж. Deep CNN добре себе зарекомендували в завданні детектування об'єктів на зображеннях. Вони здатні визначати характерні риси об'єкта безпосередньо з пікселів зображення [2]. До найвідоміших архітектур CNN можна віднести AlexNet, GoogLeNet, VGGNet, ResNet. Для навчання CNN потрібен величезний обсяг даних, тому для застосування їх до вузькоспрямованих завдань, зазвичай, використовують передбачені на відомих датасетах моделі, а потім, застосовуючи метод переносу навчання (transfer learning), розраховують ваги на останніх шарах мережі. Підходи на основі CNN є найбільш точними і в той же час найвибагливішими до обчислювальних потужностей.

Методи, засновані на вейвлетах Хаара та Габора. За допомогою вейвлетів із зображення отримували найбільш сильні сигнали, фактично виділяючи найважливіші ознаки на зображенні, відкидаючи інше. Вейвлети Габора були представлені в дослідженнях алгоритмів розпізнавання осіб. Різні вейвлети застосовувалися з ідеєю виділення візуальних ознак незалежно від завдання. Надалі дані візуальні ознаки використовувалися в авторських алгоритмах, у тому числі і для знаходження особи, як, наприклад, в алгоритмі Віоли-Джонса. Використання ознак, отриманих вейвлетом Габора, є складним та часо затратним. Існуючі спрощені вейвлети та алгоритми на їх основі працюють швидше, проте сильно залежать від освітлення та інших зовнішніх факторів.

Методи, що ґрунтуються на знаходженні дескрипторів особи. Замість використання всього зображення алгоритми розбивають його на підобласті, у кожній з яких розраховують гістограми і знаходять найбільш яскраві та важливі ознаки для вирішуваної на даний момент завдання.

Надалі отримані ознаки можуть бути використані для завдання визначення особи, так і в задачі ідентифікації, якщо є приклад, для якого також можна отримати ознаки подібним способом. Наприклад, автори застосовували підхід на основі локальних дескрипторів, включаючи різні локальні бінарні шаблони, для завдання ідентифікації по обличчю. При цьому знаходилися такі дескриптори, які були стійкі до вікових змін особи. Дані методи компактні та швидко працюють, добре справляються із змінами у висвітленні та різними емоціями на обличчі. Однак ці підходи дуже чутливі до шуму на зображенні.

Методи, що базуються на тривимірних зображеннях та картах глибини. Багато сучасних камер, і навіть смартфонів, оснащені лідарами і мають можливість швидко та точно отримувати карту глибини зображення. Цей метод зйомки дозволяє значно знизити чутливість алгоритмів до освітлення та зовнішніх факторів зйомки. Моделі, що працюють із тривимірними зображеннями, набагато більш точні та інваріантні до змін ніж працюючі з двовимірними. Методи використовують текстури зображення, компенсують варіативне освітлення, а також компенсують різні пози людини за допомогою прагнення до симетричного обличчя особи під час аналізу. Такі системи, що вимагають особливого обладнання, ретельного калібрування та синхронізації даних, що робить їх складно застосовними в системах загального призначення.

Визначення статі та віку. Якщо визначення статі є завданням бінарної класифікації, то завдання визначення віку можна вирішувати як мультикласову класифікацію за віковими кластерам, так і як завдання регресійного передбачення кількості років. Наприклад удля визначення віку автори донавчили модель VGG-face методом перенесення навчання на наборі даних із зображеннями людей, для кожного з яких була мітка про вік. На вихідному шарі нейронної мережі було 8 виходів, відповідних до вікових груп. У для завдання визначення віку також використовувалися CNN (Ranking -CNN), але з бінарним виходом, а проставлення мітки про вік людини відбувалося агрегацією виходів «базових» нейромереж. Кожна з базових згорткових мереж була навчена на мітках приналежності людини до групи «старші» або «молодші» певного віку.

Якщо для завдання визначення особи на кадрі методи не на основі нейромереж мають досить хорошу точність і можуть скласти конкуренцію CNN, то для завдання визначення віку по особі згорткові мережі є неперевершеними лідерами. Так, у 2015 році було представлено мережу AgeNet, що демонструє високу точність у завданнях визначення віку по особі та посіла призове місце у змаганні «ChaLearn 2015 apparent age competition». Підхід є глибокою згортковою нейронною мережею, в якій як функція втрат використовуються як Евклідова норма, так і крос-ентропія. Більшість сучасних методів для визначення статі та віку використовують відомі архітектури глибоких згорткових нейромереж, таких як VGG-16 або ImageNet.

Література

1. Perlibakas V. Distance measures for PCA-based face recognition / V. Perlibakas // Pattern Recognition Letters. 2004. Vol. 25(6). Pp. 711–724.
2. Liu W. A survey of deep neural network architectures and their applications / W. Liu, Z. Wang, X. Liu [at al.] // Neurocomputing. 2017. Vol. 234. Pp. 11–26.

УДК 004.93
Я. О. Мишаківський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ДЛЯ РЕАЛІЗАЦІЇ АЛГОРИТМУ РОЗПІЗНАВАННЯ СТАТІ ТА ВІКУ ЛЮДИНИ У ВІДЕОПОТОЦІ ДАНИХ

UDC 004.93
Ia. O. Myshakivskyi

METHODS FOR IMPLEMENTING AN ALGORITHM FOR RECOGNITION OF A PERSON'S GENDER AND AGE IN A VIDEO DATA STREAM

Провівши аналіз існуючих на сьогоднішній день методів розпізнавання статі та віку людини, які не використовують зображення особи, вилучення ознак з треклету об'єкта було обрано алгоритм побудови GEI (Gait Energy Image – енергетичне зображення ходи), який вимагає проведення етапу сегментації та безпосередньо створення самого зображення (мапи ознак). Вибір на користь саме цього підходу було зроблено завдяки ефективності, показаній у кількох успішних роботах та відповідність підходу до особливостей даних, що завантажуються на платформу – відеодані переміщень людей у певному напрямку (людина протягом свого треклету рухається в одну сторону). Додатковою перевагою використання GEI-ознак є можливість побудови зображення навіть на основі кадрів, де видно лише силует людини (немає інформації про кольори, важко виділити ключові точки або текстурні ознаки) – такі дані у тому числі відносяться до загальних умов зйомки

Для здійснення етапу сегментації обмежуючого вікна людини, необхідного для побудови GEI-зображення, було обрано рішення PaddleSeg. Дані та інструменти сегментації, що містять у своєму складі, включають зображення людей на повний зріст, на відміну від більшості інших, де зйомки здійснювалися під менш відповідним під дані платформи гострим кутом до горизонту. Завдяки цьому, моделі сегментації не потрібно навчати з нуля, для побудови моделі може використовуватись підхід перенесення навчання [1].

Завдання розпізнавання віку було вирішено не як завдання регресії та розрахунку точного числового значення, а як завдання класифікації та визначення однієї з трьох вікових категорій. Вибір на користь такого рішення було зроблено на підставі практично повної відсутності відкритих даних, умови зйомки яких наближені до даних, властивих платформі детектування та трекінгу об'єктів, і великий трудомісткості створення власного набору, що відповідає всім вимогам розробки алгоритму розпізнавання статі. Рішення підзадачі класифікації статі та віку було прийнято здійснювати за допомогою згорткової нейронної мережі, яка використовує для отримання ознак попередньо навчені ваги нейронної мережі esNet, що показує хороші результати у різних завданнях класифікації на зображення реального світу.

Розроблена версія алгоритму розпізнавання статі та віку буде враховувати особливості його впровадження в роботу ядра платформи детектування та трекінгу об'єктів (враховує доступність даних, їх структуру та формат, а також інтерфейси наявних програмних компонентів), а також можливості щодо подальшої оптимізації продуктивності для досягнення необхідних показників часу обробки відеопотоків.

Література

1. Liu, Yi & Chu, Lutao & Chen, Guowei & Wu, Zewu & Chen, Zeyu & Lai, Baohua & Hao, Yuying. (2021). PaddleSeg: A High-Efficient Development Toolkit for Image Segmentation. 10.48550/arXiv.2101.06175.

УДК 004.9
М. Є. Олійник; І. В. Мудрий; Н. С. Луцик, докт. філософ. наук, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ТА ЗАСОБИ ОПТИМАЛЬНОГО РОЗПОДІЛУ ЗАВДАНЬ В КОМП'ЮТЕРИЗОВАНІЙ СИСТЕМІ БЕЗПІЛОТНОЇ ДОСТАВКИ

UDC 004.9
M. Y. Oliinyk; I. V. Mudryi; N. S. Lutsyk, Ph.D., Assoc. Prof.

METHODS AND TOOLS FOR OPTIMAL TASK ALLOCATION IN A COMPUTERIZED UNMANNED DELIVERY SYSTEM

Забезпечення оптимального розподілу завдань є одним з основних етапів в роботі комп'ютеризованої системи безпілотної доставки. Особливо це актуально в умовах обмежених ресурсів, де необхідно зважати на заряд батареї пристрою та його фізичні характеристики. В комп'ютеризованій системі з різними типами пристроїв така необхідність тільки зростає. Одним із перспективних підходів для вирішення таких задач є використання генетичних алгоритмів (GA).

Генетичні алгоритми є ефективним підходом для розв'язання NP-складних задач завдяки їхній здатності досліджувати великі й складні простори рішень. NP-складні задачі характеризуються неможливістю їх розв'язання за поліноміальний час, і традиційні методи, такі як повний перебір або градієнтний підхід, стають непридатними через високі обчислювальні витрати при збільшенні розміру задачі [1].

Пропонований метод передбачає алгоритм на основі протилежних хромосом з подвійним кодування та множинних операторів мутації (OGA-DEMMO). В даному алгоритмі одна частина хромосоми описує розподіл завдань між безпілотниками, а інша – оптимальні маршрути виконання цих завдань.

Такий підхід дозволяє інтегрувати два рівні оптимізації в єдиний алгоритм, що підвищує точність та ефективність рішень [2]. Застосування операцій кросоверу, мутації та відбору сприяє дослідженню великих просторів рішень і запобігає передчасному застряганню на локальних оптимумах [3].

Таким чином, OGA-DEMMO алгоритм є універсальним і надійним інструментом оптимізації, який ефективно працює в задачах високої складності. Застосування генетичного алгоритму для динамічного розподілу завдань показує хороший результат в контексті енергетичних витрат, але він не враховує різні типи пристроїв та зони їхньої дії. Це обмежує сферу застосування, може призвести до некоректних результатів або збоїв у роботі даного алгоритму. Для ефективного розподілу завдань в комп'ютеризованій системі безпілотної доставки, зменшення витрат енергії та підвищення ефективності запропоновано враховувати тип і характеристики пристроїв та їхню робочу зону у цьому процесі.

Література

1. Bicchieri, C. 2023. A genetic algorithm for a task allocation problem in an urban air mobility. https://webthesis.biblio.polito.it/26956/1/tesi.pdf.
2. Zhu Wang, Li Liu, Teng Long, Yonglu Wen. Multi-UAV reconnaissance task allocation for heterogeneous targets using an opposition-based genetic algorithm with double-chromosome encoding. https://doi.org/10.1016/j.cja.2017.09.005.
3. Younas, I., Kamrani, F., Bashir, M., Schubert J., 2018. Efficient genetic algorithms for optimal assignment of tasks to teams of agents. https://doi.org/10.1016/j.neucom.2018.07.008.

УДК 004.8-9: 656.07
Н. Сороківська; В. Яцишин, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВИКОРИСТАННЯ АДАПТОВАНИХ МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ІДЕНТИФІКАЦІЇ ПТАХІВ У ПРИРОДНИХ УМОВАХ

UDC 004.8-9: 656.07
N. Sorokivska; V. Yatsyshyn, Ph.D. Assoc. Prof.

APPLICATION OF ADAPTED ARTIFICIAL INTELLIGENCE MODELS FOR BIRD IDENTIFICATION IN NATURAL ENVIRONMENTS

Розробка та впровадження комп'ютеризованих систем з вбудованими інтелектуальними сервісами на основі алгоритмів штучного інтелекту забезпечує автоматизацію процесів збору та аналізу даних, а також сприяє ефективності прийняття рішень щодо збереження екосистем. Це обумовлено актуальністю методів спостереження на які накладають обмеження стаціонарність пунктів, що охоплюють лише невеликі території, або вимагають значних людських ресурсів. Інші обмеження включають складність роботи в умовах фонових шумів, недостатню точність моделей і труднощі у зборі якісних даних. Апаратні пристрої з вбудованими, попередньо навченими моделями машинного навчання, здатні автоматично виконувати ідентифікацію видів птахів, оцінювати кількість особин і збирати інші дані. Це дає змогу оптимізувати часові затрати і людський ресурс при проведенні процедур аналізу. Як наслідок, впровадження технологій машинного навчання дозволяє масштабувати процес спостереження за птахами. Основною проблемою при створенні інтелектуальної системи є побудова моделі, яка б дозволила точно визначати усі наявні у наборі даних види птахів. Це , в першу чергу, пов'язано із незбалансованістю даних, оскільки певні види досліджуваних об'єктів представлені недостатньо і також наявні фонові шуми, які складно усувати. Для боротьби з дисбалансом даних застосовуються техніки resampling, зокрема oversampling, для рідкісних класів птахів. Також може використовуватися метод ковзного вікна для створення додаткових зразків із частковим перекриттям. Паралельно проводиться аугментація даних, додаються штучні варіації аудіофайлів, фонових шумів у вигляді окремих файлів, що підвищує стійкість моделі до реальних умов. Щоб надати даним зручний для аналізу формат, аудіозаписи перетворюються на спектрограми за допомогою різних методів. Важливим етапом є коректний розподіл набору даних на навчальну, валідаційну й тестову вибірки, що забезпечить об'єктивність оцінки роботи моделі і буде враховувати критичність кількості екземплярів рідкісних класів при навчанні моделі. Описані вище процедури спрямовані на забезпечення якісного представлення аудіосигналів у моделі і створення умов для її ефективного навчання.

Попередньо навчені моделі, такі як ResNet, що були адаптовані для аудіозадач, виявляються конкурентними завдяки їхній здатності працювати з великими наборами ознак. У деяких експериментах ResNet перевершує моделі CNN за точністю, особливо коли дані спектрограм є складними або містять шум. Водночас BirdNet, спеціалізована система для ідентифікації птахів, демонструє хороші результати для конкретних завдань класифікації. Однак існують обмеження її застосування для загальних задач, оскільки вона сильно орієнтована на типові для своєї архітектури сценарії.

Література

1. He, K., Zhang, X., Ren, S., & Sun, J. Deep Residual Learning for Image Recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR*)*, 2016.
2. Knight, E. C., et al. Acoustic monitoring reveals long-term population trends of threatened bats. Biological Conservation, 2019.

УДК 004.65
[1]А. А. Станько, Ph.D; [2]А. В. Гончаренко$ [1]І. В. Журик
([1]Тернопільський національний технічний університет імені Івана Пулюя, Україна)
([2]Київський національний університет будівництва і архітектури, Україна)

РОЗУМНІ МІСТА: ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ, ДАНИХ І СТРАТЕГІЙ СТАЛОГО РОЗВИТКУ МІСЬКОЇ ЕКОСИСТЕМИ

UDC 004.65
A. A. Stanko, Ph.D; A. V. Honcharenko; I. V. Zhuryk

SMART CITIES: INTEGRATING TECHNOLOGIES, DATA AND STRATEGIES FOR SUSTAINABLE URBAN ECOSYSTEM DEVELOPMENT

Розумні міста намагатимуться використовувати технології, інформацію та дані для покращення інфраструктури та послуг. «Розумне місто» – це хвиля трансформації, коли люди конкретного міста отримують всі види основних послуг, таких як питна вода, санітарія, транспорт, дороги, вуличне освітлення, заклади освіти, інформаційні технології, лікарні, садочки, паркування та готелі, залізниці, сполучення з аеропортами, протипожежна безпека, включаючи ліквідацію наслідків стихійних лих та кращий план поводження з твердими побутовими відходами, щоб громадські організації могли підтримувати бездоганну чистоту у відповідних містах. Орієнтованість на громадян лежить в основі перетворення розумних міст на реальність. Міські органи влади повинні розробляти план «розумного міста» на основі ретельного аналізу проблем і пріоритетів громадян. Важко дати визначення «розумного міста», оскільки його концепція варіюється від країни до країни, а в Індії його значення змінюється від міста до міста. Воно спрямоване на розвиток всієї міської екосистеми, яка представлена чотирма стовпами комплексного розвитку: інституційною, фізичною, соціальною та економічною інфраструктурою [1].

Місія «розумних міст» полягає в тому, щоб сприяти розвитку міст, які забезпечують основну інфраструктуру та гідну якість життя своїх громадян, чисте та стійке довкілля, а також застосування розумних рішень. Основна увага приділяється сталому та інклюзивному розвитку, а ідея полягає в тому, щоб розглянути компактні райони, створити відтворювану модель, яка буде діяти як світлий дім для інших міст, що прагнуть до цього [2].

«Розумне місто» – це концепція, яка вважається рішенням проблем сьогодення та сталого майбутнього. З розвитком сільської місцевості люди мігрують до міст в пошуках роботи, засобів до існування, освіти та інших зручностей, в результаті чого місто збільшується в розмірах і багато будинків будуються на сільськогосподарських угіддях. Нагальною потребою є перетворення міста на «розумне місто», щоб уникнути проблем безробіття, забруднення, транспорту тощо [4]. Розумні міста можуть привести до сталого розвитку суспільства. Для створення «розумного» міста необхідна участь уряду та людей. Держави та міські органи місцевого самоврядування відіграватимуть ключову допоміжну роль у розвитку «розумних» міст. «Розумне» лідерство і бачення на цьому рівні, а також здатність до рішучих дій будуть важливими факторами. Розуміння концепцій модернізації, редевелопменту та розвитку з нуля політиками, виконавцями та іншими зацікавленими сторонами на різних рівнях потребують допомоги в розвитку потенціалу.

Література

1. Grossi, G., & Welinder, O. (2024). Smart cities at the intersection of public governance paradigms for sustainability. Urban Studies, 00420980241227807.
2. Gracias, J. S., Parnell, G. S., Specking, E., Pohl, E. A., & Buchanan, R. (2023). Smart cities—a structured literature review. Smart Cities, 6(4), 1719-1743.
3. McKenna, H. P. (2024). An exploration of theory for smart spaces in everyday life: enriching ambient theory for smart cities. In Smart Spaces (pp. 17-46). Academic Press.
4. Fan, X. M., Li, X. H., Ding, Y. M., He, J., & Zhao, M. (2023). Demand response scheduling algorithm for smart residential communities considering heterogeneous energy consumption. Energy and Buildings, 279, 112691.

УДК 004.65
А. А. Станько, Ph.D; С. З. Кульчицький; Ю. В. Срібний
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ФОРМУВАННЯ КЕРОВАНИХ ОЗЕР ДАНИХ: МЕТОДОЛОГІЇ, ІНСТРУМЕНТИ ТА ПРАКТИЧНІ АСПЕКТИ

UDC 004.65
A. A. Stanko, Ph.D; S. Z. Kulchytskyi; Y. V. Sribnyi

FORMATION OF MANAGED DATA LAKES: METHODOLOGIES, TOOLS AND PRACTICAL ASPECTS

Конвеєри даних широко використовуються для збору даних з гетерогенних джерел, для виконання низки перетворень над ними та для передачі перетворених даних до системи призначення для аналізу даних. Такий конвеєр даних також можна назвати процесом ETL (вилучення, перетворення, завантаження), який часто використовується для надходження чистих і трансформованих даних до сховища даних [1]. Конвеєри даних все ще вважаються найсучаснішою технологією, хоча деякі недоліки добре відомі [2]. Однією з таких проблем є втрата інформації під час процесу ETL, що може статися, наприклад, коли найбільш релевантні атрибути агрегуються для того, щоб зробити формат придатним для сховища даних. Як наслідок, для подальшого аналізу доступна лише заздалегідь визначена підмножина атрибутів. Таким чином, семантика «схема-на-запис» цього підходу обмежує повторне використання даних, що зберігаються в традиційних системах управління даними, для аналітики за межами початкового обсягу. Для того, щоб запобігти цій втраті інформації, у 2010 році Діксоном було введено концепцію озер даних. Озеро даних, на відміну від сховища даних, зазвичай розробляється як центральне сховище для всіх наборів даних з усіх джерел даних у їхньому первинному форматі [4]. Оскільки для надходження даних в озеро даних не потрібно ніяких перетворень і не робиться ніяких припущень щодо подальшого аналізу, використовується підхід, заснований на зчитуванні схем, що забезпечує високу гнучкість і можливість багаторазового використання.

Хоча не існує загальноприйнятої концепції озера даних, узгоджена схема за Діксоном вимагає масштабованої системи зберігання гетерогенних даних, де вчені можуть досліджувати та аналізувати ці набори даних. Ці вимоги йдуть пліч-о-пліч з потребою в недорогих технологіях і спочатку призвели до сильної асоціації реалізацій озер даних з Apache Hadoop. Потім їх витіснили пропрієтарні хмарні рішення на базі Azure або AWS [4], які привнесли в концепцію озер даних перевагу розділення ресурсів зберігання і обчислювальних ресурсів.

Оскільки необроблені дані в озері даних, швидше за все, піддаються багатьом послідовним перетворенням, що призводить до появи декількох артефактів, які будуть поглинуті назад в озеро даних, збереження стислої інформації про походження є дуже складним завданням, але має вирішальне значення для збереження керованості озером даних. Оброблені дані, які щойно зберігаються у сховищі даних, згодом буде важко знайти і, ймовірно, неможливо зрозуміти та відтворити, що потенційно зробить їх марними.

Література

1. Dinesh, Lina, and K. Gayathri Devi. «An efficient hybrid optimization of ETL process in data warehouse of cloud architecture.» Journal of Cloud Computing 13.1 (2024): 12.
2. Munappy, A.R., Bosch, J., Olsson, H.H.: Data pipeline management in practice: Challenges and opportunities. In: Morisio, M., Torchiano, M., Jedlitschka, A. (eds). Product-Focused Software Process Improvement, pp. 168–184. Springer, Cham (2020)
3. Zhao, Xiaoyan, Conghui Zhang, and Shaopeng Guan. «A data lake-based security transmission and storage scheme for streaming big data.» Cluster Computing 27.4 (2024): 4741-4755.
4. Errami, S. A., Hajji, H., El Kadi, K. A., & Badir, H. (2023). Spatial big data architecture: from data warehouses and data lakes to the Lakehouse. Journal of Parallel and Distributed Computing, 176, 70-79.

УДК 658.8
О. Чорновол
(Тернопільський національний університет імені Івана Пулюя, Україна)

ХМАРНІ ТЕХНОЛОГІЇ ЯК ОСНОВА ДЛЯ МАСШТАБУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ У РИТЕЙЛІ

UDC 658.8
O. Chornovol

CLOUD TECHNOLOGIES AS A BASIS FOR SCALING INTELLIGENT SYSTEMS IN RETAIL

У сучасному ритейлі автоматизація та впровадження інтелектуальних систем є ключовими факторами для підвищення ефективності бізнес-процесів і забезпечення конкурентних переваг. Особливу роль у цьому відіграють хмарні технології, які забезпечують необхідну інфраструктуру для обробки великих обсягів даних, масштабування систем та інтеграції нових рішень.

Інтелектуальні системи, такі як системи комп'ютерного зору, штучного інтелекту (ШІ) та машинного навчання, активно використовуються у ритейлі для таких задач, як автоматизація обліку товарів, моніторинг заповненості полиць, аналіз поведінки покупців та прогнозування попиту. Проте реалізація цих систем вимагає значних обчислювальних ресурсів, що часто перевищує можливості локальної інфраструктури. Хмарні платформи, такі як AWS, Google Cloud та Microsoft Azure, пропонують оптимальне рішення для цих викликів [1].

Хмарні технології забезпечують масштабованість інтелектуальних систем, дозволяючи легко збільшувати обчислювальну потужність у пікові періоди або при обробці великих обсягів даних. Наприклад, використання AWS Lambda дає можливість запускати функції на вимогу без необхідності постійного утримання серверів. Це значно знижує витрати на інфраструктуру та підвищує гнучкість системи [2].

Однією з важливих переваг хмарних технологій є можливість інтеграції з інструментами штучного інтелекту. Такі сервіси, як Google Cloud Vision або Amazon Rekognition, дозволяють швидко впроваджувати моделі комп'ютерного зору для аналізу зображень без необхідності самостійної розробки складних алгоритмів. Це особливо важливо для ритейлу, де точність і швидкість розпізнавання об'єктів, таких як товари на полицях, відіграють ключову роль.

Таким чином, хмарні технології є невід'ємною складовою сучасних інтелектуальних систем у ритейлі. Вони забезпечують високу продуктивність, гнучкість і масштабованість, необхідні для обробки великих обсягів даних та швидкої адаптації до змін ринку. Впровадження цих технологій відкриває нові можливості для автоматизації бізнес-процесів, підвищення ефективності та забезпечення кращого досвіду для клієнтів.

Література

1. Марін Г. "Архітектура хмарних обчислень: основи та практика" 2020 – 256 с
2. Szeliski, R. "Computer Vision: Algorithms and Applications" 2019 – 101 с.

УДК 004.7:621.39
А. Чуба; В. Тимощук; А. Микитишин; В. Шиманська
(Тернопільський національний технічний університет імені Івана Пулюя)

СУЧАСНІ ПІДХОДИ ДО МОНІТОРИНГУ ТА УПРАВЛІННЯ В DOCSIS-МЕРЕЖАХ

UDC 004.7:621.39
A. Chuba; V. Tymoshchuk; A. Mykytyshyn; V. Shymanska

MODERN APPROACHES TO MONITORING AND MANAGEMENT IN DOCSIS NETWORKS

Швидкий розвиток інформаційних технологій та збільшення кількості інтернет-користувачів вимагають високошвидкісних і надійних систем передачі даних. Мережі кабельного телебачення (КТБ), первісно розроблені для трансляції відеоконтенту, перетворилися на потужну інфраструктуру, яка підтримує передачу даних та автоматизоване управління мережами. Кабельні модеми, використовуючи існуючі мережі КТБ, забезпечують високошвидкісний доступ до Інтернету та є складовою для інтегрованих систем моніторингу.

Кабельні модеми використовують протокол DOCSIS (Data Over Cable Service Interface Specification) для забезпечення високошвидкісної передачі даних. DOCSIS підтримує двосторонню передачу інформації через інфраструктуру КТБ [1]. Його еволюція від версії 1.0 до 3.1 дозволила значно покращити швидкість, надійність і масштабованість. Застосування сучасних методів модуляції, таких як QAM, підвищує ефективність передачі даних, забезпечуючи швидкість до 1 Гбіт/с у сучасних мережах. Мережі КТБ зазвичай використовують деревоподібну топологію, що дозволяє ефективно розподіляти сигнали від центральних вузлів до кінцевих користувачів. Сучасні кабельні модеми використовують методи корекції помилок і адаптивної модуляції для мінімізації впливу електромагнітних перешкод. Широкомовний характер передачі даних у КТБ-мережах створює ризики перехоплення інформації. Посилення шифрування в протоколах DOCSIS за допомогою алгоритмів AES і RSA забезпечує високий рівень захисту даних.

Висока щільність користувачів у години пікового навантаження часто призводить до перевантаження мережі, що знижує якість обслуговування. Для вирішення цієї проблеми запропоновано впровадження динамічних алгоритмів розподілу пропускної здатності та балансування навантаження. Автоматизовані системи є важливим компонентом для ефективного управління мережами DOCSIS, оскільки вони дозволяють інтегрувати моніторинг, діагностику та оптимізацію в єдину платформу. Моніторинг забезпечує збирання та аналіз даних у реальному часі, що дає змогу виявляти потенційні проблеми та швидко реагувати на них. Діагностика дозволяє автоматично визначати причини несправностей або зниження продуктивності, що мінімізує час простоїв і витрати на усунення проблем. Оптимізація спрямована на автоматичне налаштування параметрів мережі, що забезпечує максимальну пропускну здатність, ефективність використання ресурсів і високу якість обслуговування. Дослідження, проведене в DOCSIS мережі показало суттєве підвищення пропускної здатності та зниження простоїв завдяки впровадженню автоматизованих систем управління.

Література

1. RFC 8034: active queue management (AQM) based on proportional integral controller enhanced (PIE) for data-over-cable service interface specifications (DOCSIS) cable modems. IETF Datatracker. URL: https://datatracker.ietf.org/doc/rfc8034/ (date of access: 03.12.2024).

УДК 004.93:616.12:618.3
Г. Франчевська; Є. Яворська, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя)

УДОСКОНАЛЕНИЙ АЛГОРИТМІЧНИЙ ПІДХІД ДО ВИДІЛЕННЯ ЕЛЕКТРОКАРДІОСИГНАЛУ ПЛОДА

UDC 004.93:616.12:618.3
H. Franchevska; E. Yavorska, Ph.D., Assoc. Prof

ADVANCED ALGORITHMIC APPROACH FOR FETAL ELECTROCARDIOGRAM SIGNAL EXTRACTION

Безперервний моніторинг серцевої діяльності плода є життєво важливим для покращення пренатального догляду та зниження рівня мертвонароджуваності. За даними Всесвітньої організації охорони здоров'я (ВООЗ), щорічно відбувається приблизно 2,6 мільйона мертвонароджень, багато з яких можна було б запобігти завдяки ефективному і безперервному моніторингу плода. Незважаючи на розвиток медичних технологій, в умовах обмежених ресурсів все ще існують проблеми із забезпеченням точного моніторингу плода в режимі реального часу. Традиційні методи, такі як доплерівське ультразвукове дослідження, пропонують лише періодичні оцінки, що обмежує їхню здатність виявляти тонкі, але критичні ознаки дистресу плода. У цьому дослідженні представлено математичну модель і надійний алгоритм для виділення електрокардіосигналів плода (фЕКС) зі змішаних записів матері і плода.

Сигнал, що спостерігається, є комбінацією ЕКС матері, ЕКС плода та шуму:

$$s_{obs}(t) = A_m s_m(t) + A_f s_f(t) + B_m S_m(t) s_f(t) + n(t),$$

Сигнали суміші ЕКС матері та плода є квазіперіодичними і можуть бути представлені за допомогою рядів Фур'є.

Алгоритм, зображений на рисунку 1 включає кілька ключових кроків:

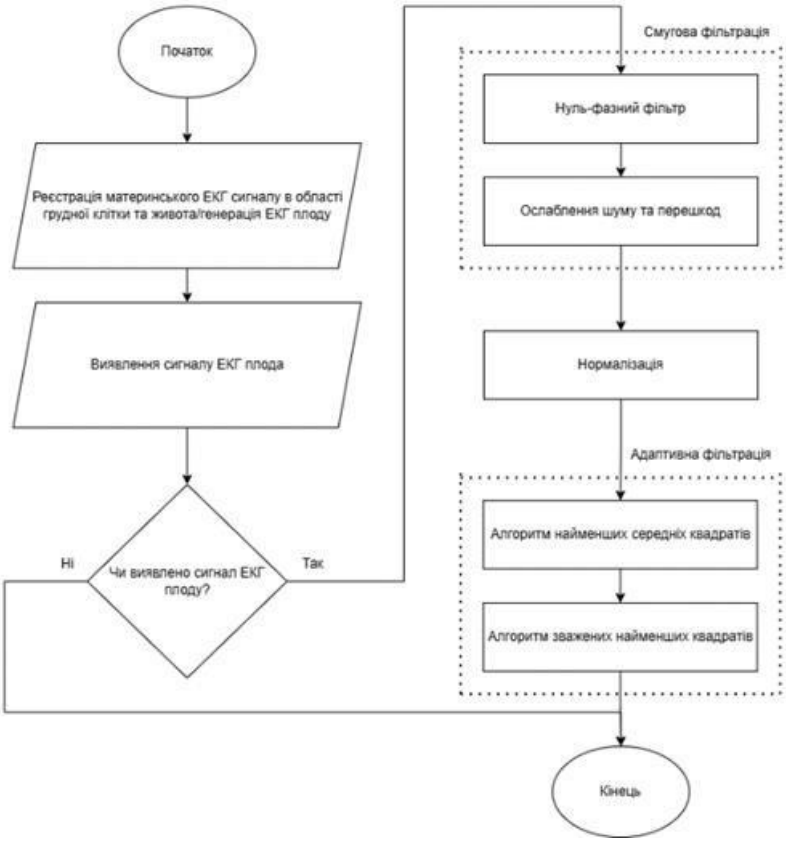


Рисунок 1. Алгоритм виділення ЕКС плода

Спочатку неінвазивні електроди фіксують абдомінальні сигнали, що містять як материнські, так і плодові компоненти. Попередня обробка зменшує високочастотний шум і підвищує чіткість материнського сигналу. Виявлення R-піків ідентифікує материнські сигнали для відокремлення. Потім частотно-специфічні фільтри низьких і високих частот ізолюють ЕКС плода в межах його характерного діапазону. Нарешті, нормалізація стандартизує амплітуди, а адаптивна фільтрація ще більше покращує виділений сигнал для точності та чіткості.

Результати, що показані на рисунку 2, демонструють, що запропонований алгоритм досягає високого співвідношення сигнал/шум (SNR), зберігаючи ключові характеристики, такі як P-хвиля, комплекс QRS і T-хвиля, важливі для внутрішньоутробної діагностики.

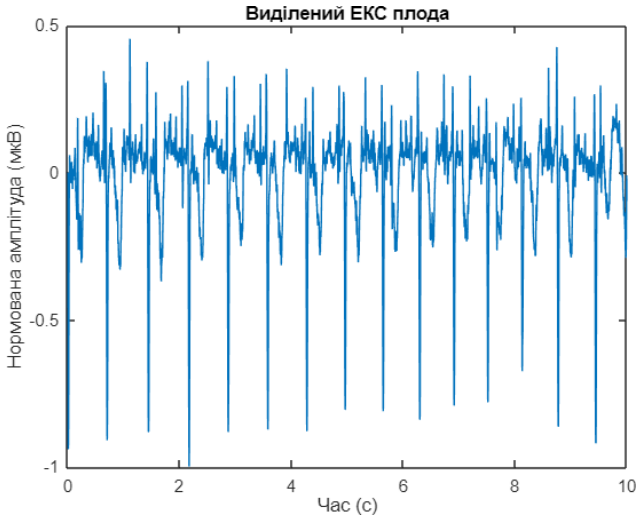


Рисунок 2. Виділений ЕКС плода

Кількісний аналіз вказує на значні покращення порівняно з традиційними методами, особливо в шумному середовищі. Представлення на основі Фур'є та адаптивна фільтрація виявилися ефективними для розділення ЕКГ плода без порушення цілісності материнського сигналу. Ці результати підтверджують потенціал алгоритму для неінвазивного моніторингу в реальному часі в клінічних умовах.

Таким чином, це дослідження представляє надійний та адаптивний алгоритм для вилучення фЕКС, який вирішує проблеми накладання сигналів та шуму навколишнього середовища. Завдяки збереженню критично важливих характеристик форми сигналу та досягненню високого SNR, метод підтримує точний моніторинг плода. Масштабованість і економічна ефективність роблять його придатним для різних медичних установ, в тому числі в умовах обмежених ресурсів. Подальша робота буде зосереджена на інтеграції та оптимізації в режимі реального часу для ширшого клінічного застосування.

Література

1. World Health Organization. Stillbirth. – 2019. URL: https://www.who.int/health-topics/stillbirth.
2. H. Franchevska, M. Khvostivskyi, V. Dozorskyi, E. Yavorska, and O. Zastavnyy, «The Method and Algorithm for Detecting the Fetal ECG Signal in the Presence of Interference,» in Proc. 1st Int. Workshop on Computer Information Technologies in Industry 4.0 (CITI 2023), Ternopil, Ukraine, 2023, pp. 263–272.
3. Patel, J. H., & Zheng, Y. An additive-multiplicative approach for improved fetal ECG extraction. Journal of Biomedical and Health Informatics.

УДК 004.6
Т. Щур; Г. Осухівська, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЕФЕКТИВНЕ УПРАВЛІННЯ ІНВЕНТАРЕМ ЗА ДОПОМОГОЮ ДРОНІВ І ШТУЧНОГО ІНТЕЛЕКТУ

UDC 004.6
T. Shchur; H. Osukhivska, Ph.D., Assoc. Prof.

EFFECTIVE INVENTORY MANAGEMENT USING DRONES AND ARTIFICIAL INTELLIGENCE

Поєднання технології дронів та штучного інтелекту, а саме систем розпізнавання, відкриває нові можливості для автоматизації систем інвентаризації, які раніше було виконати складніше. Системи з використанням штучного інтелекту дозволяють збирати, обробляти та аналізувати дані у режимі реального часу, що покращує системи управління процесом інвентаризації, що є важливим фактором для ефективного управління. Дрони забезпечуватимуть швидке та точне відстеження товарів на складах та їх ідентифікацію при використанні технологій розпізнавання для виявлення штрих-кодів і QR-кодів та їх читання. Ці системи використовують комп'ютерне бачення та алгоритми машинного навчання для ідентифікації, декодування та обліку товарів [1]. Завдяки цьому дрони можуть вільно переміщатися складським приміщенням для моніторингу товарів. Це зменшує потребу в безпосередній участі людини в процесах інвентаризації та мінімізує помилки.

Системи комп’ютерного бачення для виявлення об’єктів працюють шляхом розпізнавання шаблонів в сирих даних (значенях пікселів для зображень). Такі системи використовують згорткові нейронні мережі (CNN), які здатні аналізувати зображення в режимі реального часу. При цьому в системах інвентаризації можуть бути використані для розпізнавання та класифікації кодів чи самих товарів на складі.

Окрім автоматизації пошуку товару для його ідентифікації та інвентаризації у системі, для ефективного управління інвентарем також можна автоматизувати чи оптимізувати процес формування маршрутів для дронів [2]. Представлення схеми топографії приміщень складу у вигляді графу, дозволить використовувати такі алгоритми як метод Дейкстри чи Беллмана-Форда у виборі найшвидшого (відповідно найменш енергозатратного) шляху переміщення. Це дозволяє дронам швидко охоплювати великі ділянки складу, точно оновлювати інформацію про наявний товар, що вагомо зменшує час на інвентаризацію та підвищує її точність.

Отже, системи управління інвентарем, що використовують дрони з технологіями розпізнавання та моделі штучного інтелекту, є великим кроком вперед у автоматизації процесів. Використання сучасних алгоритмів дозволяють розпізнавати об’єкти в режимі реального часу, будувати шлях переміщення дрону та керувати ним.

Література

1. Cho Hyeon, et al. 2D barcode detection using images for drone-assisted inventory management. In: 2018 15th International Conference on Ubiquitous Robots (UR). IEEE, 2018. p. 461-465.
3. Maweni, Thabisa; Setati, Tiro; Botha, Natasha. Optimized path planning of a UAV for inventory management applications. In: MATEC Web of Conferences 388, 04021, 2023.

УДК 004.89
В. Яцишин, канд. техн. наук, доцент; А. Демиденко; В. Яцишин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЛОГІСТИЧНА РЕГРЕСІЯ В ЗАДАЧАХ ВИЯВЛЕННЯ АНОМАЛІЙ ТРАФІКУ КОМП'ЮТЕРНИХ МЕРЕЖ

UDC 004.89
V. Yatsyshyn, PhD., Assoc. Prof., A. Demydenko; V. Yatsyshyn

LOGISTIC REGRESSION IN COMPUTER NETWORK TRAFFIC ANOMALIES DETECTION PROBLEMS

Логістична регресія відноситься до класу керованих алгоритмів машинного навчання, які використовується для задач класифікації. Основна ціль такого алгоритму полягає в тому, щоб спрогнозувати ймовірність приналежності екземпляра даних до одного чи іншого класу.

Логістична регресія доволі ефективно застосовується при бінарній класифікації з використанням сигмоїдної функції, яка приймає вхідні дані як незалежні змінні та генерує значення ймовірності в діапазоні від 0 до 1.

Наприклад, існує два класи (у даному випадку аномальний і нормальний трафік): клас 0 і клас 1. Якщо значення логістичної функції для вхідних даних перевищує 0,5 (порогове значення), тоді воно належить до класу 1, інакше воно належить до класу 0.

Логістична регресія прогнозує вихід категоріальної залежної змінної. Отже, результат повинен мати категоріальне або дискретне значення. Це може бути «Так» або «Ні», «0» або «1», «Істинно» або «Хибно» тощо, але замість того, щоб давати точні значення 0 або 1, алгоритм формує ймовірності, які знаходяться між 0 і 1.

У логістичній регресії замість «підгонки» лінії регресії підбирають логістичну функцію S-подібної формі, яка прогнозує два максимальні значення (0 або 1).

Логістична функція є сигмоїдною функцією, тобто математичною функцією, яка використовується для відображення прогнозованих значень у ймовірності. Сигмоїд перетворює будь-яке реальне значення на інше в діапазоні від 0 до 1. Значення логістичної регресії повинно бути між 0 і 1 і не може виходити за межі цього інтервалу, тому воно утворює криву, подібну до форми «S».

Крива S-подібної форми називається сигмоподібною функцією або логістичною функцією. У логістичній регресії використовується поняття порогового значення, яке визначає ймовірність 0 або 1. Наприклад, значення вище порогового значення прямує до 1, а значення нижче порогових значень прямують до 0.

На основі категорій логістичну регресію можна класифікувати на три типи:

– біноміальна або бінарна: у біноміальній логістичній регресії може бути лише два можливих типи залежних змінних, наприклад 0 або 1, «Пройшов» або «Не пройшов» тощо;

– мультиноміальна: у мультиноміальній логістичній регресії може бути 3 або більше можливих невпорядкованих типів залежної змінної, наприклад «кіт», «собаки» або «вівця»;

– порядкова: у порядковій логістичній регресії може бути 3 або більше можливих упорядкованих типів залежних змінних, таких як «низький», «середній» або «високий».

Модель логістичної регресії перетворює неперервні вихідні дані функції лінійної регресії у категоріальні вихідні значення за допомогою сигмоїдної функції, яка відображає будь-який дійсний набір вхідних незалежних змінних у значення від 0 до 1.

СЕКЦІЯ 4. ПРОГРАМНА ІНЖЕНЕРІЯ ТА МОДЕЛЮВАННЯ СКЛАДНИХ РОЗПОДІЛЕНИХ СИСТЕМ

УДК 004.41

А. Бачинський; А. Бачинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ЗАСОБІВ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ КОНВЕРТАЦІЇ МЕДІА ФАЙЛІВ У ТЕКСТОВИЙ ФОРМАТ

UDC 004.41

A. Bachynskiy; A. Bachynskyi

RESEARCH OF SOFTWARE DEVELOPMENT TOOLS FOR CONVERTING MEDIA FILES INTO TEXT FORMAT

Сучасне суспільство стикається з постійно зростаючим обсягом мультимедійних даних, які потребують ефективної обробки та збереження. Конвертація аудіо та відео в текстовий формат має велике значення для підвищення доступності інформації, створення баз даних, аналізу тексту та автоматизації рутинних процесів. Важливість цього напряму підтверджується широким використанням у журналістиці, освіті, судовій практиці, медицині та інших сферах [1].

В даній доповіді пропонується фреймворк для дослідження проєктів з розробки програмних продуктів з метою оцінювання ефективності процесів розробки з впровадженням CI/CD. Для досягнення цієї мети пропонується оцінювати процеси за такими характеристиками [2].

1. Проаналізувати сучасні алгоритми розпізнавання мовлення.
2. Розробити програмне забезпечення, яке інтегрує найкращі методи розпізнавання.
3. Забезпечити підтримку різних форматів файлів(mp3,wav,mp4 тощо).
4. Тестувати систему на різних типах даних для оцінки ефективності.

У роботі реалізовано систему конвертації медіа-файлів та аудіозаписів у текстовий формат із застосуванням сучасних веб-технологій. Використання JavaScript як основної мови розробки забезпечує високу продуктивність та гнучкість коду. Фреймворк Vue дозволив створити інтерактивний інтерфейс для взаємодії з користувачем, зокрема завантаження файлів, налаштування параметрів обробки та виводу результатів. Основна перевага такого підходу – кросплатформнність і можливість використання системи у веб-браузері без додаткових програм [3].

Для обробки аудіо- та відеофайлів інтегровано сторонні API та бібліотеки розпізнавання мовлення, які підтримують багатомовність та обробку у реальному часі. У роботі використано підхід клієнт-серверної архітектури: клієнтська частина на Vue відповідає за взаємодію з користувачем, а серверна обробляє файли за допомогою API, таких як Google Speech-to-Text чи Whisper[4]. Це дозволило мінімізувати затримки та досягти високої точності розпізнавання (WER – до 10% для чистого аудіо). Стек технологій для розробки наведено у таблиці 1.

Розроблене програмне забезпечення може використовуватися як основа для створення комерційних сервісів, покращення доступності інформації для людей з інвалідністю, автоматизації аналітики в бізнесі[5]. Окрім користі для людей з інвалідністю та автоматизації бізнес-процесів, цей проект може бути корисним у таких сферах:

1. Освіта. Автоматична трансформація записів лекцій у текстовий формат допомагає студентам створювати конспекти, особливо коли немає можливості записувати вручну.

2. Журналістика та медіа. Журналісти можуть використовувати ваш інструмент для автоматизації процесу транскрипції аудіо- та відеоінтерв'ю, що значно економить час. Розпізнавання тексту у відео та подкастах допомагає створювати архіви для подальшого пошуку та аналізу [6].

Таблиця 1. Огляд ключових технологій

Компонент	Технологія	Функція	Переваги
Фронтенд	JavaScript, Vue.js	Створення інтерактивного користувацького інтерфейсу	Кросплатформність, швидка розробка
Серверна частина	SQL	Обробка запитів, управління медіа-файлами	Легкість інтеграції з API
Розпізнавання мовлення	Google Speech-to-Text API	Конвертація аудіо у текст	Висока точність, багатомовність
Обробка файлів	FFmpeg	Конвертація форматів файлів (mp3, wav, mp4)	Підтримка різноманітних форматів

3. Судова система. Автоматичне створення протоколів із записів судових засідань зменшує навантаження на працівників канцелярій та покращує точність записів.

4. Здоров'я та медицина. Записи лікарів, зроблені у вигляді аудіо, можуть автоматично перетворюватися в текст для використання в електронних медичних картках. Інструмент дозволяє перетворювати аудіозаписи консультацій у текстовий вигляд, спрощуючи створення звітів.

5. Розробка програмного забезпечення. Інструмент може бути корисним для IT-команд для створення протоколів із записів онлайн-зустрічей, наприклад, у Zoom чи Google Meet.

6. Особисте використання. Люди можуть використовувати систему для конвертації голосових нотаток у текст, полегшуючи особисту організацію. Транскрипція допомагає блогерам і подкастерам створювати текстові версії своїх матеріалів, що позитивно впливає на SEO.

Розробка систем для конвертації аудіо та відео в текстовий формат є важливим напрямом в сучасній інформатиці. Створений прототип підтверджує доцільність використання новітніх алгоритмів розпізнавання мовлення для забезпечення високої точності результатів.

Література

1. Digital Media Literacy Education Framework - An overview of concepts and techniques involving digital media management and file handling (ERIC, 2022)
2. Modern Patterns for Developing Modern Applications by Alex Banks and Eve Porcello – A book to dive into React.js.
4. "JavaScript: The Definitive Guide" by David Flanagan – A comprehensive guide to JS, including modern features(2023-2024).
5. RESTful API Design with Node.js 10 practical book for creating APIs using Node.js. "Designing Web APIs: Building APIs That Developers Love" by Brenda Jin, Saurabh Sahni, and Amir Shevat - API Design Guide.
6. "Technology and Its Impact on Modern Communication: Case Studies on Video Conferencing" – Analysis of video platforms and their impact on society (Cambridge Core, 2023)
7. "Speech and Language Processing" by Daniel Jurafsky and James H. Martin – A primer on speech recognition and natural language processing.
1. Deep Learning for Speech Recognition Review of Machine Learning Algorithms Applied to Speech (Springer).

УДК 004.4; 004.738.5; 004.056
А. Бачинський; А. Бачинський
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІЖЕННЯ ЗАСОБІВ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБМІНУ ПОВІДОМЛЕННЯМИ В РЕАЛЬНОМУ ЧАСІ З АУТЕНТИФІКАЦІЄЮ КОРИСТУВАЧІВ

UDC 004.4; 004.738.5; 004.056
A. Bachynskiy; A. Bachynskyi

SOFTWARE DEVELOPMENT TOOLS RESEARCH FOR REAL-TIME MESSAGING WITH USERS AUTHENTICATION

В ході вивчення підходів до створення програмного забезпечення для обміну повідомленнями в реальному часі було досліджено ряд технологій розробки та програмних фреймворків. В процесі розробки програмного забезпечення для обміну повідомленнями в реальному часі для реалізації функціоналу на клієнтській стороні можна використати бібліотеку **React JS**, що забезпечує ефективне керування станом інтерфейсу користувача [1].

Серверна частина реалізована з використанням **Node.js** та **Express.js**, що дозволяє здійснювати обробку HTTP-запитів та забезпечувати взаємодію з клієнтами через API [2]. Для реалізації реального часу комунікації між сервером і клієнтом застосовано **WebSocket** за допомогою бібліотеки **Socket.io**, що забезпечує двосторонній зв'язок і дозволяє передавати повідомлення без перезавантаження сторінки.

Під час взаємодії клієнта з сервером клієнт ініціює з'єднання через **Socket.io**. Після встановлення з’єднання клієнт може надсилати повідомлення серверу, а сервер, у свою чергу, миттєво передає це повідомлення всім підключеним клієнтам або певному користувачеві, залежно від вимог бізнес-логіки [3].

Це забезпечує високий рівень інтерактивності та дозволяє зберігати зв'язок між користувачами в реальному часі.

Коли клієнт надсилає повідомлення, воно передається через відкритий канал WebSocket на сервер, де воно обробляється та зберігається в базі даних (у даному випадку, використовується **MongoDB**) [4]. Після обробки повідомлення сервер надсилає його назад всім підключеним користувачам через **Socket.io**. Завдяки цьому користувачі можуть отримувати нові повідомлення без необхідності перезавантаження сторінки або повторних запитів.

Ключовою перевагою цього підходу є забезпечення низької затримки при передачі даних і можливість постійного збереження з'єднання між клієнтом і сервером. Використання **Socket.io** дозволяє також обробляти різні події в реальному часі, наприклад, повідомлення про нові вхідні дані або розрив з'єднання, що робить систему більш стабільною і зручнішою для користувачів. Така реалізація дозволяє забезпечити швидку доставку повідомлень у реальному часі з мінімальними затримками.

Одним з основних аспектів системи є забезпечення безпеки користувачів, яке реалізовано через механізм аутентифікації за допомогою **JWT (JSON Web Token)**.

У процесі аутентифікації користувачі проходять етап реєстрації та входу, після чого отримують унікальний токен, який використовується для доступу до захищених ресурсів системи [5].

Токен зберігається на клієнтському боці і передається разом з кожним запитом до серверу для перевірки авторизації користувача. Така система дозволяє забезпечити безпечний доступ до функцій, що вимагають ідентифікації користувача, без необхідності зберігання сесійної інформації на сервері [6].

Таблиця 1. Характеристика використаних технологій

Технологія	Опис	Переваги	Недоліки
React JS	Бібліотека для створення інтерфейсу користувача на основі компонентів	Підтримка компонентного підходу, висока продуктивність при рендерингу, гнучкість у використанні	Необхідність додаткових інструментів для повноцінної розробки складних додатків
Node.js	Платформа для виконання JavaScript на сервері	Підтримка асинхронної обробки запитів, висока ефективність обробки I/O операцій, масштабованість	Можливе низьке виконання в CPU-інтенсивних задачах
Express.js	Мінімалістичний веб-фреймворк для Node.js	Спрощує створення серверних API, підтримка middleware для обробки запитів	Необхідність додаткових налаштувань для великих проектів
MongoDB	Документо-орієнтована база даних	Масштабованість, швидкість виконання запитів до неструктурованих даних, зручність для зберігання JSON-даних	Обмежена підтримка транзакцій у порівнянні з реляційними базами даних
Socket.io	Бібліотека для двостороннього зв'язку між клієнтом і сервером	Забезпечення реального часу комунікації, підтримка WebSocket, проста інтеграція	Погіршення роботи за умов нестабільного з'єднання

Це дозволяє знизити навантаження на сервер та підвищити рівень безпеки через використання криптографічних алгоритмів для генерації та перевірки токенів.

Література

1. Behrendt, K. & Lumsden, A. (2022). Real-Time Messaging Systems: Architectures and Techniques. Springer. Available at https://reactjs.org/.
2. Möller, J. & Neumann, P. (2021). Mastering Node.js: Building Scalable and Fast Web Applications. Packt Publishing.
1. 3 Abrams, P. (2023). Real-Time Web Application Development with Node.js and Socket.io. O'Reilly Media. Available at https://socket.io/docs/.
3. Garvin, S. (2020). Learning MongoDB: A Guide to NoSQL Data Storage for Modern Web Apps. O'Reilly Media.
4. Schmidt, A. (2023). Building Real-Time Applications with Node.js, MongoDB, and JWT Authentication. Packt Publishing.
5. Hamedani, M. (2021). MERN Stack React, Node, Express, MongoDB - Web Development. Udemy Course

УДК 004.4’2
О. Бойко; Г. Цуприк, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОЄКТУВАННЯ ТА РОЗРОБКА САЙТУ ІНТЕРНЕТ-МАГАЗИНУ ДЕКОРУ З ВИКОРИСТАННЯМ ФРЕЙМВОРКУ DJANGO

UDC 004.4’2
O. Boiko; H. Tsupryk, Ph.D., Assoc. Prof

DESIGN AND DEVELOPMENT OF AN ONLINE DECOR STORE WEBSITE USING THE DJANGO FRAMEWORK

Актуальність теми роботи полягає у зростанні значення електронної комерції, особливо у сфері продажу товарів для дому та декору. У зв’язку з пандемією та поширенням дистанційних моделей споживання, необхідність у зручних та функціональних інтернет-магазинах стає дедалі важливішою. Сучасні умови ринку вимагають створення інноваційних рішень, які забезпечують високу якість обслуговування клієнтів та зручність користування. Django, як інструмент веброзробки, дозволяє швидко та ефективно реалізовувати функціональні та масштабовані інтернет-магазини, що відповідають вимогам часу.

Розроблений інтернет-магазин декору призначений для забезпечення користувачів можливістю зручного перегляду, пошуку та замовлення товарів для прикрашення житлових і комерційних приміщень. Сайт надає широкий вибір категорій товарів, систему фільтрації для швидкого пошуку, а також інтеграцію з платіжними системами для забезпечення безпечних транзакцій.

Об'єктом дослідження є процеси розробки вебдодатків для електронної комерції з використанням сучасних технологій. Зокрема, акцент зроблено на архітектурі вебдодатків, побудованих на фреймворку Django.

Для реалізації проєкту було обрано такі технології:

- Фреймворк Django – для створення серверної частини та управління базами даних.
- СУБД PostgreSQL – для зберігання інформації про товари, користувачів і замовлення.
- HTML, CSS, JavaScript – для розробки інтерфейсу користувача.
- Bootstrap – для адаптивного дизайну.
- Visual Studio Code – як основне середовище розробки.

Розроблений вебсайт ілюструє можливості Django як фреймворку для створення зручних, безпечних і конкурентоздатних платформ. Використання Django сприяє зниженню витрат на розробку, а також забезпечує можливість легкої адаптації до змін ринкових умов. Інтеграція зручного інтерфейсу, функціоналу замовлень і аналітичних інструментів сприяє автоматизації процесів продажу, що в свою чергу підвищує ефективність бізнесу та забезпечує кращий досвід для кінцевого споживача.

Література

1. Michael Dinder. Becoming an Enterprise Django Developer 1st Edition/ Michael Dinder. – Packt Publishing, 2022. – 526 с.
2. М.Р. Петрик, Д.М. Михалик, О.Ю. Петрик, Г.Б. Цуприк. Методичні вказівки до виконання атестаційної роботи магістра за спеціальністю 121 – «Інженерія програмного забезпечення» для усіх форм навчання [Текст] – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2020 – 27 с.

УДК 004.94; 681.3
А. П. Бортняк; О. А. Пастух, д.т.н., проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АВТОМАТИЗАЦІЯ КАДРОВОЇ РОБОТИ ПІДПРИЄМСТВ

UDC 004.94; 681.3
A. P. Bortnyak; O. A. Pastukh, Dr. Prof

AUTOMATION OF ENTERPRISE HR WORK

У сучасному світі, де технології стрімко розвиваються, автоматизація процесів стає важливою складовою успіху для компаній різного масштабу. Одним із ключових напрямів автоматизації є облік працівників, який є не лише частиною кадрової роботи, а й важливим елементом в управлінні ресурсами підприємства.

Автоматизація обліку працівників – це процес впровадження програмного забезпечення та інформаційних систем для обробки та зберігання даних про працівників організації, включаючи їх персональні дані, трудову діяльність, заробітну плату, відпустки, лікарняні та інші аспекти, що стосуються кадрового обліку.

Основною метою автоматизації є забезпечення ефективного, точного та швидкого збору, обробки та аналізу інформації про працівників, що дозволяє зменшити витрати часу та знизити ймовірність помилок, пов’язаних із ручним введенням даних.

Основні етапи автоматизації обліку працівників:

– Вибір програмного забезпечення. Першим кроком є вибір відповідного програмного забезпечення для автоматизації обліку кадрів. На ринку існують різні рішення, як для великих корпорацій, так і для малих і середніх підприємств. Вибір залежить від потреб компанії, її бюджету та специфіки роботи.

– Введення та інтеграція даних. Наступний етап — це введення початкових даних про працівників в систему, включаючи їх персональні дані, трудові договори, відпустки, історію роботи. Важливо також інтегрувати нову систему з іншими корпоративними програмами, такими як бухгалтерія та фінансові системи.

– Навчання співробітників. Оскільки автоматизація часто змінює звичні процеси, співробітники повинні пройти навчання щодо роботи з новими програмами. Це дозволить їм швидко освоїти інтерфейс та максимально ефективно використовувати можливості автоматизованої системи.

– Тестування та налаштування. Після запуску системи потрібно провести тестування її функцій, перевірити, чи коректно працюють всі процеси і чи немає помилок. При необхідності здійснюються налаштування для поліпшення ефективності роботи системи.

Автоматизація обліку працівників — це потужний інструмент, який значно підвищує ефективність роботи компанії, знижує ризики помилок і полегшує роботу кадрових відділів. Впровадження такої системи дозволяє зекономити час, оптимізувати процеси та поліпшити прийняття управлінських рішень на основі точних та актуальних даних. Тим не менш, для успішної автоматизації необхідно враховувати всі аспекти, включаючи вибір програмного забезпечення, інтеграцію з іншими системами та навчання співробітників.

Література

1. Облік персоналу й кадрове діловодство. [Електронний ресурс] – Режим доступу до ресурсу: https://zkg.ua/oblik-personalu-j-kadrove-dilovodstvo.

УДК 004.415
В. Герасим; Д. Михалик, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СОРТУВАЛЬНИХ ТА ОЧИЩУВАЛЬНИХ МАШИН

UDC 004.415
V. Herasym; D. Mykhalyk, PhD, Assoc. Prof.

SOFTWARE DEVELOPMENT FOR SORTING AND CLEANING MACHINES

Сортувальні машини для зернової продукції відіграють ключову роль у забезпеченні якості сільськогосподарських продуктів і підвищенні економічної ефективності галузі. Наявність сторонніх домішок у зібраному врожаї значно знижує його ринкову вартість. За оцінками, близько 65% малих фермерських господарств змушені продавати своє зерно за зниженими цінами через високий вміст сміття після збору врожаю. Це знижує їхню прибутковість і економічну стабільність [1].

Метою цього дослідження є вивчення існуючих рішень і розробка власного програмного забезпечення для автоматизації процесу сортування. Ефективна система дозволить підвищити продуктивність і забезпечити високу якість кінцевої продукції. Впровадження такого програмного забезпечення сприяє мінімізації людського втручання, забезпеченню стабільності роботи та максимізації прибутку підприємства.

Розробка програмного забезпечення для сортувальних машин є складним завданням, яке потребує детального аналізу ринку, ретельного тестування і вдосконалення. Для досягнення конкурентоспроможності в цьому секторі необхідно забезпечити високу точність роботи алгоритмів, адаптивність системи під різні типи зернових культур і зручність у користуванні. Враховуючи швидкі темпи впровадження автоматизованих технологій, така розробка є стратегічно важливою як для малих фермерів, так і для великих агрохолдингів [2].

Для розробки програмного забезпечення сортувальної машини було обрано мову програмування Java через її стабільність , що забезпечує ефективну роботу. Використано фреймворки JavaFX для створення користувацького інтерфейсу, що дозволяє реалізувати зручне та інтуїтивне управління системою.

Таким чином, впровадження сучасних програмно-апаратних рішень у сортувальні машини відкриває нові можливості для розвитку аграрного сектору, дозволяючи забезпечити високу якість готової продукції та економічну стабільність підприємств.

Література

1. Steponavičius D., Špokas L., Petkevičius S., The influence of sorting machines in the present time. Agronomy Research, 2011. С. 377-385.
2. Технологічне обладнання зернопереробних та олійних виробництв / За редакцією О. В. Дацишина. Навчальний посібник. – Вінниця: Нова Книга, 2008. – 488 с.

УДК 621.396.67
Н. Б. Войцеховський; Ю. Б. Паляниця, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОБҐРУНТУВАННЯ МЕТОДУ ПЕРЕДАЧІ ІНФОРМАЦІЙНОГО СИГНАЛУ ДЛЯ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ СУПУТНИКОВИХ СИСТЕМ ЗВ'ЯЗКУ.

UDC 621.396.67
N. B. Voytsekhovskyi; Y. B. Palyanytsia, PhD

JUSTIFICATION OF THE METHOD OF INFORMATION SIGNAL TRANSMISSION TO INCREASE THE BANDWIDTH OF SATELLITE COMMUNICATION SYSTEMS

Супутникові телекомунікаційні системи класифікуються за типом орбіт, на яких розташовані супутники, що визначає такі параметри, як покриття, затримка сигналу, енергетичні витрати та кількість супутників для глобального покриття. Основними типами орбіт є низька (LEO), середня (MEO) та геостаціонарна (GEO), кожна з яких має унікальні характеристики та сферу застосування (Таблиця 1).

Параметр	Тип орбіти	Геостаціонарна орбіта (GEO)	Низька орбіта (LEO)	Середня орбіта (MEO)
Висота орбіти (км)	Геостаціонарна	35,786	500-2,000	2,000-35,786
Період обертання (годин)	Геостаціонарна	24	1-2	2-12
Швидкість орбітального руху (км/с)	Геостаціонарна	3.07	7.9-8.5	3.5-6
Кут нахилу орбіти	Геостаціонарна	0°	0-90°	0-90°
Розподіл смуг частот	Супутникові канали	C, Ku, Ka, L	L, S, Ku	C, Ku, Ka
Пропускна здатність каналу (Гбіт/с)	Супутникові канали	10-50	0.1-2	1-10
Максимальна затримка сигналу (мс)	Супутникові канали	240-300	10-50	100-250
Мобільність (переміщення супутників)	Геостаціонарна	Немає	Має	Має

Пропускна здатність супутникових систем зв’язку визначається низкою параметрів, серед яких частота сигналу, ширина смуги пропускання, тип модуляції, співвідношення сигнал/шум (SNR) та коефіцієнт помилок на біт (BER). Частотний спектр, наприклад, у Ka- та Ku-діапазонах, забезпечує високу швидкість передачі даних завдяки широкій смузі пропускання, хоча й залежить від погодних умов. Різні види цифрової модуляції, такі як QPSK та 16-QAM, дозволяють оптимізувати ефективність передачі, підвищуючи кількість бітів на символ, але вимагають вищого SNR.

Застосування сучасних технологій, таких як адаптивна модуляція і кодування (ACM) та мультиплексування з ортогональним частотним поділом (OFDM), є ключем до підвищення ефективності використання частотного спектра. ACM автоматично змінює параметри залежно від умов каналу, забезпечуючи надійність передачі навіть у складних умовах. OFDM, у свою чергу, дозволяє зменшити вплив інтерференції і більш ефективно використовувати спектр.

У випадку квадратурної амплітудно-фазової модуляції (QAM), кількість бітів, переданих за символ, визначається так:

$$R_{b/s} = \log_2(M) \quad (1)$$

Для оцінки впливу ширини смуги пропускання, типу модуляції та інших параметрів було проведено порівняльний аналіз з використанням теоретичних моделей. Наприклад, збільшення ширини смуги пропускання вдвічі дозволяє подвоїти пропускну здатність, а використання модуляції 64-QAM – значно підвищити швидкість передачі даних порівняно з QPSK за умови високого співвідношення сигнал/шум (Рис. 1).

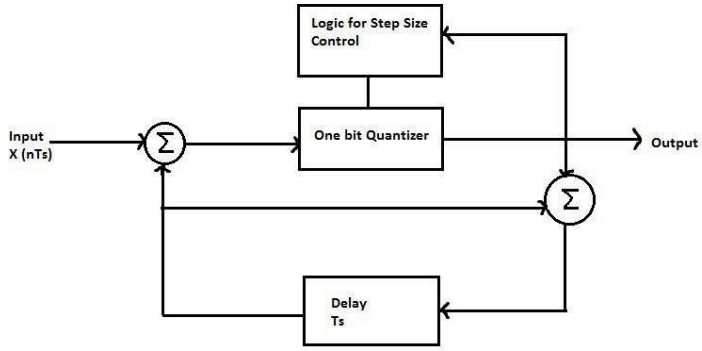


Рисунок 1. Схема технології адаптивної модуляції і кодування

Таким чином, оптимізація пропускної здатності супутникових систем зв'язку є комплексним завданням, що включає вдосконалення методів модуляції, кодування і використання частотного ресурсу. Формула пропускної здатності каналу, яка враховує ширину смуги частот і співвідношення сигнал/шум, є ключовою для проєктування ефективних супутникових систем.

Формула для пропускної здатності каналу в разі використання модуляції виглядає так:

$$C = B \cdot \log_2(1 + \frac{S}{N}) \quad (2)$$

Ця формула добре ілюструє залежність пропускної здатності від ширини смуги пропускання і якості сигналу.

Література

1. Methods of Processing Cyclic Signals in Automated Cardiodiagnostic Complexes. IV Lytvynenko, A Horkunenko, O Kuchvara, Y Palaniza ICTES, 116-127
2. Artificial Intelligence Based Emergency Identification Computer System D Velychko, H Osukhivska, Y Palaniza, N Lutsyk, Ł Sobaszek Advances in Science and Technology. Research Journal.
3. Method, Algorithm and Computer Tool for Synphase Detection of Radio Signals in Telecommunication Networks with Noises L Khvostivska, M Khvostivskyi, I Dediv, V Yatskiv, Y Palaniza.

УДК 004.4
І. Гаврилюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ТА МОДЕЛЮВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ АВТОМАТИЗАЦІЇ ФІНАНСОВОГО АУДИТУ ТА ОПТИМІЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ КОМЕРЦІЙНИХ ПІДПРИЄМСТВ

UDC 004.4
I. Havryliuk

DEVELOPMENT AND MODELING OF INFORMATION SYSTEM FOR AUTOMATION OF FINANCE AUDIT AND OPTIMIZATION OF BUSINESS-PROCESSES OF COMMERCIAL ORGANIZATIONS

На сьогодні існує багато комерційних підприємств всередині яких панує хаос та незорганізованість. Це проявляється в несистемному підході до фінансового обліку та аудиту, невизначеності та невпорядкованості бізнес-процесів та в результаті неприбутковості самого підприємства. Статистика говорить що 80% бізнесу не виживає навіть 1 рік, а 10% з тих, які проіснували хоча б 1.5 року не приносять прибутку 1].

Прийнято вважати, що область фінансів є відокремленою від організаційної складової будь-якого комерційного підприємства, проте я вважаю це невірним твердженням, оскільки область фінансів напряму залежить від того, як побудовані бізнес-процеси. Бізнес-процес являє собою певну одиницю яка в свою чергу репрезентує певну низку подій які є послідовними, упорядкованими, узгодженими та успадкованими для правильної та прибуткової роботи бізнесу.

Метою наукового дослідження є розробка та моделювання інформаційної системи для автоматизації фінансового аудиту та оптимізації бізнес-процесів комерційних підприємств.

Проєктування та розробка такого роду системи є не із простих. Потрібно бути уважним до кожних дрібниць, бо від результатів у майбутньому залежитиме становище комерційних підприємтсв. Велика кількість процесів обробки та аналізу даних, отриманих від пристроїв діагностування, додавали свої перешкоди для коректної розробки застосунку [2].

Література

1. Я.В. Янушевич. Інституційний механізм забезпечення сфери оподаткування в Україні: теорія та практика 358, 220-235(2020).
2. International Institute of Business Analysis, Toronto, Ontario, Canada . BUSINESS ANALYSIS BODY OF KNOWLEDGE. 459, 350-356, (2008).

УДК 004.63
А. В. Гарасівка; А. М. Лупенко, д. т. н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАЛЕЖНІСТЬ ШВИДКОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ ВІД ГЕОГРАФІЧНОГО РОЗТАШУВАННЯ СЕРВЕРІВ ХМАРНИХ СХОВИЩ

UDC 004.63
A. V. Harasivka; A. M. Lupenko, Dr.

DEPENDENCE OF INFORMATION TRANSFER SPEED ON THE GEOGRAPHICAL LOCATION OF REMOTE CLOUD STORAGE SERVERS

Сервери хмарних сховищ, таких як Dropbox, Google Drive і iCloud, розташовані по всьому світу, що дозволяє забезпечувати максимально можливу доступність 99.5%-99.9% згідно угоди про рівень послуг - Service-level agreement (SLA) [1] 24 години на добу, 7 днів на тиждень і високу продуктивність для користувачів.

Проте швидкість передачі інформації у хмарних сервісах суттєво залежить від фізичної відстані між користувачем і сервером. Хмарні сервіси використовують багато технологій і географічно розподілені сервери, зокрема мережу доправлення контенту - Content Delivery Networks (CDN), що дозволяє мінімізувати затримки.

Google Drive використовує власну інфраструктуру Google Cloud, яка має центри обробки даних у багатьох країнах по всьому світу [2], забезпечуючи низьку затримку для завантаження та завантаження даних, найближчий датацентр розташований в Гаміна, Фінляндія (~1200км від Тернополя). Dropbox орендує місця в хмарних сервісах Amazon Web Services (AWS) і зберігає дані в різних регіонах, а також сервер метаданих в США [3] для підвищення надійності, найближчий датацентр розташований в Німеччині (~920 км від Тернополя). Водночас iCloud працює на серверах Apple в Каліфорнія, США (~9800 км від Тернополя), але також використовує сервери Google Cloud для глобальної доступності [4]. Порівняльна схема залежності затримки до сервера через команду пінг (ping) до відстані до сервера хмарного сховища (Рисунок 1).

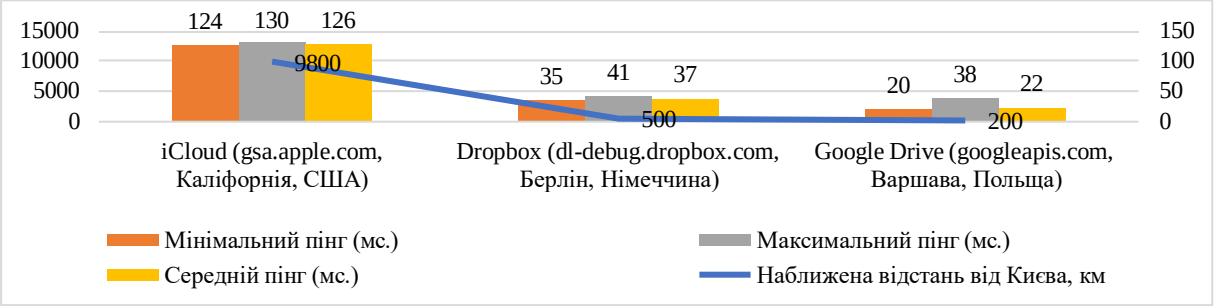


Рисунок 1. Затримка доступу до серверів хмарного сховища

Отже, вибір провайдера хмарного сховища суттєво впливатиме на швидкість обміну інформацією з віддаленим сервером, наприклад затримка обміну з серверами iCloud (126 мс.) в 3 рази більша від серверів Google Drive (22 мс).

Література

1. Google Workspace Service Level Agreement, https://workspace.google.com/terms/sla/
2. Discover our data center locations, https://www.google.com/about/datacenters/locations/
3. Dropbox Security Whitepaper, https://assets.dropbox.com/www/en-us/business/solutions/solutions/dfb_security_whitepaper.pdf
4. iCloud – Wikipedia, https://en.wikipedia.org/wiki/ICloud

УДК 004.9, 004.45
В. Глива, Ph.D.; І. Мудрик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЕНТЕРПРАЙЗ ПАТЕРНИ ДЛЯ КРОСПЛАТФОРМНОЇ РОЗРОБКИ

UDC 004.9, 004.45
V. Hlyva, Ph.D.; I. Mudryk

ENTERPRISE PATTERNS FOR CROSS-PLATFORM DEVELOPMENT

У сучасній кросплатформній розробці програмних продуктів дедалі більшої популярності набувають ентерпрайз патерни, які забезпечують масштабованість, підтримку та ефективну інтеграцію. Основними викликами в цьому процесі є забезпечення продуктивності, спрощення підтримки та гарантування коректної роботи програмного забезпечення на різних платформах.

Дослідження демонструє ефективність використання таких патернів, як Repository, Unit of Work, Dependency Injection та Event Aggregator. Repository забезпечує ізоляцію бізнес-логіки від джерел даних, тоді як Unit of Work допомагає ефективно управляти транзакціями. Dependency Injection спрощує управління залежностями, що є критичним для великих кросплатформних проєктів. Event Aggregator сприяє зменшенню зв’язності між компонентами в багатоплатформних системах. Всі згадані патерни можуть використовуватись імплементації архітектурного стилю MVVM (Model-View-ViewModel). Суть MVVM полягає в максимально можливому розділенні обов'язків між сутностями системи, що приводить до можливості легко маштабувати та підтримувати кросплатформний застосунок.

Практичне впровадження цих патернів було протестоване у розробці додатків за допомогою .NET MAUI. Результати показали значне скорочення часу розробки та спрощення процесу масштабування системи.

Отримані результати підтверджують ефективність ентерпрайз патернів для побудови сучасних кросплатформних рішень і можуть бути використані як рекомендації для розробників програмного забезпечення.

Ключові слова: ентерпрайз патерни, кросплатформна розробка, .NET MAUI, Repository, Dependency Injection, масштабованість.

Література

1. Fowler M. Patterns of Enterprise Application Architecture. Addison-Wesley Professional, 2002.
2. Gamma E., Helm R., Johnson R., Vlissides J. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley Professional, 1994.
3. Troelsen A., Japikse P. Pro C# 9 with .NET 5: Foundational Principles and Practices in Programming. Apress, 2021.
4. Esposito D. Modern Web Development with ASP.NET Core 3: An end to end guide covering the latest features of Visual Studio 2019, .NET Core 3, and C# 8. Packt Publishing, 2019.
5. O Bryk, I Mudryk, M Holubovskyi, Y Stoianov. Machine learning models and methods aspects of processing unstructured data. Proceedings of the 1st International Workshop on Bioinformatics and Applied Information Technologies (BAIT 2024) Zboriv, Ukraine, 2024. pp. 64-74,
6. Riccomini C., Ryaboy D. The Enterprise Big Data Lake: Delivering the Promise of Big Data and Data Science. O'Reilly Media, 2019.

УДК 004.41
В. В. Деркач; Г. Б. Цуприк, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА УНІВЕРСАЛЬНОЇ МОБІЛЬНОЇ WEB-СИСТЕМИ АВТОМАТИЗАЦІЇ ОБЛІКУ РЕСУРСІВ БІЗНЕС-СТРУКТУРИ

UDC 004.41
V.V. Derkach; H. B. Tsupryk, PhD, Assoc.Prof.

DEVELOPMENT OF A UNIVERSAL MOBILE WEB-SYSTEM FOR AUTOMATION OF BUSINESS-STRUCTURE RESOURCES

Автоматизована інформаційна система (системи) є одним із невід'ємних атрибутів бізнес-структур всіх цивілізованих країн, в тому числі і країн Західної Європи вже впродовж. без перебільшення, кількох останніх десятиліть. Саме їх використання підвищує ефективність, а заразом із цим і прибутковість бізнесу, тим самим збільшуючи і його конкурентоспроможність. Якщо ж розглядати світовий ринок розробок програмного забезпечення в цілому то, на сьогоднішній день, з відкритих джерел можна констатувати, що успішно працюють цілий ряд компаній, рівня корпорації, які спеціалізуються на розробці такого типу програмних систем, для реалізації якої розвивається специфічний цілий комплекс технологій, який і отримав всім вже відому назву «об'єктно-орієнтовний аналіз та проєктування». Не дивлячись на складний, в плані ведення будь-якої успішно діяльності час, віримо, що вже дуже скоро війна переможно завершиться і будемо опиратись на той факт, що сучасна динаміка розвитку бізнес-структур в саме нашій країні вимагатиме, і в найкоротший час, впровадження інформаційних систем для автоматизації їх діяльності. Саме це і було базовим при виборі теми, яка є актуальною адже пов'язана саме із розробкою програмної системи подібного класу та призначення.

Важливою характеристикою сучасних автоматизованих корпоративних систем призначених для застосування саме бізнес-структурами можна назвати їхню мобільність та загальну доступність. Для забезпечення цих таких вимог досить добре підходить середовище типу Web, оскільки, зазвичай, системи такого класу володіють Web-інтерфейсом, що робить їх мобільними та дає змогу використовувати в буд-якій точці світу де є доступ до світової мережі.

Враховуючи потреби військового часу та поствоєнного національного ринку такого продукту як програмне забезпечення та визначаючи Web як всеохоплююче інформаційне середовище, актуальною є розробка програмного забезпечення саме із підтримкою Web-інтерфейсу і конкретно для вдосконалення і пришвидшення, без будь-яких втрат, через автоматизацію, діяльності бізнес-структур.

Microsoft. NET Framework є тією платформою запропоновано використати для розробки та яка вважається базовою та такою що можна об'єднати потрібні для процесу розробки технології та інструментальні засоби.

В якості основної мови програмування при реалізації представленого програмного проєкту обрано мову C# в якості простої, сучасної, об'єктно-орієнтованої і безпечної щодо типів мови програмування, наслідувану від мов C/C++.

Серйозним аргументом на користь .NET технології є можливість керувати пам'яттю, котра базується на принципі «без сміття». Головною ідеєю цього під ходу є те, що якщо об'єкт не використовується (тобто кількість посилань на нього рівна нулю), то його слід знищити. Такий підхід знімає з розробника відповідальність за звільнення зарезервованої динамічної пам'яті і, як наслідок, значно спростити безпосередньо сам процес розробки.

Варто зауважити, що хоча й C# призначена для розробки коду, що виконується середовищем .NET, сама вона не є частиною .NET. Існують деякі можливості, які підтримуються .NET, але не підтримуються C#. І, як не дивно, існують можливості C#, які не підтримуються .NET.

В представленому програмному проєкті в якості механізму обробки даних та доступом до бази данних обрано LINQ (зокрема, LINQ to SQL). Такий вибір зумовлено тим, що ця, порівняно молода технологія, надає ряд гнучких та зрозумілих механізмів роботи з даними.

В процесі розвитку платформи .NET і підтримуваних нею мов C# та VB, стало зрозуміло, що однією із найбільше проблемних областей для розробників залишається доступ до даних із різноманітних джерел. Маніпуляція з XML та безпосередній доступ до бази данних часто, в кращому випадку, заплутані, а в гіршому взагалі проблемні.

Література

1. Плескач В.Л. Інформаційні системи і технології на підприємствах: підручник /В.Л. Плескач, Т.Г. Затонацька. —К. :Знання, 2011. —718с
3. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Інформаційні технології видобутку даних (Data mining, високопродуктивні обчислення у складних системах): навчальний посібник. Тернопіль: : ТНТУ 2020 – 62 с.
4. Петрик М.Р., Михалик Д.М., Петрик О.Ю., Цуприк Г.Б. Методичні вказівки до виконання атестаційної роботи магістра за спеціальністю 121 – «Інженерія програмного забезпечення» для усіх форм навчання – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2020 – 27 с.
5. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Моделювання та видобуток даних (високопродуктивні обчислення у великих та числових системах, комбінаторному аналізі): навчальний посібник. Тернопіль : ТНТУ 2019 – 62 с.

УДК 004.41
М. Дмитраш
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗГОРТАННЯ РЕСУРС, ЯКИЙ БУЛО РОЗРОБЛЕНО З ВИКОРИСТАННЯМ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ

UDC 004.41
M. Dmytrash

DEPLOYMENT OF RESOURCE THAT WAS DEVELOPED USING MICROSERVICE ARCHITECTURE

Мікросервіси розгортаються як окремі самодостатні сервіси, кожен з яких виконує певну бізнес-функцію. Цей підхід дозволяє розробникам самостійно масштабувати, оновлювати та керувати службами, забезпечуючи гнучку та стійку архітектуру. Під час розгортання сервіси контейнеризуються за допомогою програм, таких як Docker, для упаковки їхніми залежностями, забезпечуючи узгодженість у різних середовищах. Потім цими контейнерами можна керувати та оркеструвати їх за допомогою таких інструментів, як Kubernetes, який автоматизує розгортання, масштабування та роботу контейнерних програм.

Kubernetes спрощує розгортання мікросервісів, пропонуючи такі функції, як балансування навантаження, виявлення сервісів та їх відмовостійкість. Це дозволяє розробникам визначати, як служби мають бути розгорнуті, масштабовані та підключені за допомогою файлів конфігурації. Kubernetes забезпечує роботу потрібної кількості екземплярів (або реплік) для кожної служби, автоматично замінюючи несправні екземпляри та розподіляючи трафік між ними [1]. Це робить його ідеальним вибором для керування складними продуктам, які базуються на мікросервісній архітектурі.

Мікросервіси, розгорнуті через Kubernetes, можуть працювати на різноманітних платформах, що дає організаціям гнучкість у виборі місця для розміщення своїх програм. Локальне розгортання є варіантом для організацій, які потребують більшого контролю або обробки конфіденційних даних. Крім того, такі хмарні платформи, як Amazon Web Services, Microsoft Azure та Google Cloud Platform, пропонують керовані сервіси Kubernetes, зменшуючи накладні витрати на підтримку власної інфраструктури [2].

Гібридні хмарні середовища також набувають популярності, дозволяючи організаціям запускати одні служби локально, одночасно залучаючи хмарні ресурси для інших. Це забезпечує переваги обох світів — контроль і масштабованість. Крім того, периферійні обчислювальні платформи дозволяють розгортати мікросервіси ближче до користувачів або пристроїв, зменшуючи затримку для чутливих до часу програм.

Гнучкість і автоматизація, які забезпечує Kubernetes, у поєднанні з широким спектром варіантів розгортання роблять його потужним рішенням для розгортання мікросервісів.

Література

1. Kubernates conepts [електронний ресурс]. – 2024 – Режим доступу до ресурсу: https: //kubernetes.io/docs/concepts/.
2. Sujatha R. Managed Kubernetes Services [електронний ресурс]. – 2024 – Режим доступу до ресурсу: https://www.digitalocean.com/resources/articles/managed-kubernetes-services.

УДК 004.414.3
О. А. Заяць
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

С4-ДІАГРАМИ ЯК ГРАФІЧНИЙ МЕТОД ОПИСУ ВИМОГ І АРХІТЕКТУРИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

UDC 004.414.3
O. A. Zaiats

C4-DIAGRAMS AS A GRAPHICAL METHOD FOR DESCRIBING SOFTWARE REQUIREMENTS AND ARCHITECTURE

При описі вимог до програмного забезпечення важливою є чіткість їхнього формулювання зі сторони замовника, а також доступність для розуміння з точки зору виконавця. Для задоволення цих критеріїв використовуються різні підходи: текстові, графічні, комбіновані, а також неформальні – особисті розмови, анкетування тощо. Важливе місце в цьому ряді посідають саме графічні методи опису вимог, оскільки вони дають можливість замовнику візуально представити свої вимоги, а виконавцю – однозначно їх зрозуміти та реалізувати.

Серед графічних підходів залишаються популярними такі нотації як: UML-діаграми; Data Flow Diagrams; Entity-Relationship Diagrami; Workflow Diagrams. Деякі графічні методи мають низку обмежень.

UML може бути занадто складним у використанні для нефахівців через часто високу деталізацію, що не завжди забезпечує чітке узгодження вимог між замовником і виконавцем.

Data Flow Diagrams зосереджуються лише на потоках даних, залишаючи поза увагою архітектуру системи, тоді як ERD охоплюють тільки структуру даних, не відображаючи їх функціонального контексту.

Workflow-діаграми добре ілюструють бізнес-процеси, але не враховують технічні вимоги або інтеграцію з іншими компонентами. Через це попередні підходи часто не здатні забезпечити повноцінне уявлення про вимоги до ПЗ, яке було б зрозумілим для всіх учасників проекту.

С4-діаграми (Context, Container, Component, Code) дозволяють описувати вимоги до ПЗ на різних рівнях абстракції, забезпечуючи єдність між високорівневим контекстом і технічними деталями. Вони дозволяють чітко представити функціональні вимоги через моделювання компонентів та їх взаємозв’язків, а також враховувати деякі нефункціональні вимоги, такі як масштабованість або інтеграція з іншими системами.

С4-діаграма включає наступні рівні:

1. Рівень контексту (Context): допомагає замовникам і стейкхолдерам зрозуміти, як система взаємодіє з користувачами та зовнішніми системами.

2. Рівень контейнерів (Container): надає загальний огляд архітектури, що корисно для розробників та архітекторів, а для стейкхолдерів дає розуміння технологій та основних модулів, які використовуватимуться при розробці системи.

3. Рівень компонентів (Component): деталізує внутрішню структуру контейнерів, що полегшує реалізацію.

4. Рівень коду (Code): дозволяє документувати за необхідності окремі модулі.

Використання С4-діаграм дозволяє забезпечити високу якість і однозначність трактування вимог, багаторівневе і чітке їх моделювання. Перевагою підходу С4-діаграм є прозорість взаємодії між сутностями і однозначність трактування вимог стейкхолдерами.

УДК 004.41
В. В. Коваль; Г. Б. Цуприк, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ВЕБ-ІНТЕРФЕЙСУ ДЛЯ ІНТЕРАКТИВНОЇ ВІЗУАЛІЗАЦІЇ API-ДАННИХ НА ОСНОВІ JAVASCRIPT

UDC 004.41
V. V. Koval; H. B. Tsupryk, PhD, Assoc.Prof

DEVELOPMENT OF A WEB INTERFACE FOR INTERACTIVE VISUALIZATION OF API DATA BASED ON JAVASCRIPT

У сучасному світі веб-інтерфейси відіграють ключову роль у створенні зручних та інтуїтивно зрозумілих інструментів для обробки та аналізу даних. Їх використання дозволяє ефективно інтегрувати візуалізацію великого обсягу інформації в різноманітних галузях – від бізнесу до наукових досліджень. Здатність адаптуватися до швидких змін і забезпечувати інтерактивність робить такі інструменти надзвичайно затребуваними.

Проблема обробки та візуалізації даних, отриманих через API, набула особливого значення через стрімке зростання обсягів інформації. Інтерфейси, які можуть відображати ці дані в графічному вигляді, сприяють кращому розумінню складної інформації і допомагають у прийнятті рішень. Саме це визначає актуальність створення інструментів, здатних забезпечити динамічну та гнучку візуалізацію.

JavaScript було обрано як основний інструмент для розробки через його універсальність та потужний набір інструментів для створення інтерактивних графічних елементів. Бібліотеки, такі як D3.js і Apache ECharts, дозволяють швидко реалізовувати складні механізми візуалізації, а також створювати адаптивні рішення, що підходять для різних типів даних.

Головні особливості розробленого інтерфейсу:

- Доступність – можливість використовувати систему через веб-браузер на будь-якому пристрої.
- Гнучкість – підтримка різних типів графіків та інтерактивних елементів, що дозволяють користувачу легко налаштовувати відображення даних.
- Ефективність – оптимізація запитів до API та обробки великих обсягів даних, що забезпечує швидкість роботи.

Для розробки було використано такі технології:

- JavaScript як мова для інтерактивної логіки.
- ECharts.js для побудови динамічних графіків.
- RESTful API для отримання та оновлення даних.
- Next.js для створення інтерфейсу, що адаптується до різних пристроїв.

Результатом роботи стала система, яка забезпечує інтерактивну візуалізацію даних у режимі реального часу. Реалізовано можливість масштабування, фільтрації та сортування інформації, що робить інструмент зручним для широкого кола користувачів.

Практична значущість цієї роботи полягає у створенні платформи, яка може застосовуватись у фінансовому аналізі, дослідженні ринкових трендів, наукових обчисленнях та інших галузях, де потрібна наочна візуалізація даних.

Таким чином, розроблений веб-інтерфейс не лише відповідає сучасним вимогам до інтерактивних інформаційних систем, але й демонструє великий потенціал для подальшого розвитку у сфері обробки та візуалізації даних.

Література

1. Петрик М.Р., Михалик Д.М., Петрик О.Ю., Цуприк Г.Б. Методичні вказівки до виконання атестаційної роботи магістра за спеціальністю 121 – «Інженерія програмного забезпечення» для усіх форм навчання – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2020 – 27 с.

2. «Data Visualization with JavaScript» від Stephen A. Thomas. https://blog.tomsawyer.com/exploring-javascript-libraries-for-data-visualization
3. Vadim Ogievetsky, Joseph Lowery. «JavaScript and jQuery for Data Analysis and Visualization»
4. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Моделювання та видобуток даних (високопродуктивні обчислення у великих та числових системах, комбінаторному аналізі): навчальний посібник. Тернопіль : ТНТУ 2019 – 62 с.
5. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Інформаційні технології видобутку даних (Data mining, високопродуктивні обчислення у складних системах): навчальний посібник. Тернопіль: : ТНТУ 2020 – 62 с.

УДК 004.4’2
Т. Колєватих; Г. Цуприк, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОЗРОБКИ СИСТЕМИ СПОЖИВЧОГО КРЕДИТУВАННЯ

UDC 004.4’2
T. Kolievatykh; H. Tsupryk, Ph.D. Assoc. Prof

ANALISIS OF SOFTWARE FOR THE DEVELOPMENT OF A CONSUMER LENDING SYSTEM

Актуальність теми роботи полягає у значній ролі споживчого кредитування, що стає все вагомішою на фоні розвитку економіки в цілому протягом останнього двадцятиріччя: від різких змін економічних тенденцій до фінансової глобалізації, цифровізації банківських послуг з кредитування. Існує потреба розробки новітніх кредитних продуктів, їх вивчення з метою з’ясування їх особливостей використання, з’ясування важелів ризиковості, що дасть змогу розробляти ефективніші механізми контролю і управління ними.

Така економічна категорія, як споживчий кредит, на сучасному етапі розвитку економічної науки досі не сформувала/не має спільної єдиної класифікованої системи характеристик та ознак, а отже, існує необхідність у проведені подальшого вивчення цієї економічної категорії - наявний глибокий науковий потенціал обраної теми.

Для комерційних банків України, які є одним з найважливіших елементів інфраструктури економіки України та які забезпечують взаємозв’язок між державою, товаровиробником і населенням шляхом здійснення між ними розрахунків, надання споживчих кредитів/позик є пріоритетним джерелом комісійного та процентного доходу банку. Для отримання доходу потрібно управління кредитним ризиком для зменшення супутніх проблеми кредитування, ризиків неповернення тощо, задля чого потрібно створити оптимальний кредитний механізм відбору позичальників, підбору відповідних для них умов кредитування.

В сьогоденні управління кредитним ризиком – є більш освітленим та вивченим важелем провадження фінансово-кредитної діяльності, головним інструментом для досягнення визначеної мети є андеррайтинг позичальника, обмеження позичальника в об’ємі позики та ідентифікація/верифікація його даних, в тому числі – застосування скорингу (так званих статистичних моделей оцінки кредитоздатності позичальника на основі наданих ним відомостей про себе). Розроблення скорингових аналітичних моделей споживчого кредитування для практичного застосування в приватних банках Україні вимагає постійного оновлення, доопрацювання та вивчення.

Задля ефективного аналізу розробки системи споживчого кредитування необхідний комплексний підхід з розглядом всіх зазначених умов, проведенням досліджень та розробок за напрямом, з урахуванням особливостей предметної галузі та вимог комплексної постановки завдання.

Таким чином, обрана тема має глибокий науковий потенціал з урахуванням соціальної та економічної значущості споживчого кредиту, та потребує проведення подальшого вивчення такої фінансової послуги.

Для реалізації проєкту було обрано технології MS SQL для керування базами даних, що виконує головний функціонал зі збереження та надання даних з інших застосунків на запити, як на локальному сервері, так і у мережі.

Література

1. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Інформаційні технології видобутку даних (Data mining, високопродуктивні обчислення у складних системах): навчальний посібник. Тернопіль: : ТНТУ 2020 – 62 с.

2. Камінський А. Б. Характеристичні особливості ризик-менеджменту в сегменті мікрокредитування / А. Б. Камінський // Наукові записки НаУКМА. Економічні науки. - 2016. - Т. 1, вип. 1. - С. 80-85.
3. Петрик М.Р., Михалик Д.М., Петрик О.Ю., Цуприк Г.Б. Методичні вказівки до виконання атестаційної роботи магістра за спеціальністю 121 – «Інженерія програмного забезпечення» для усіх форм навчання – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя – 2020 – 27 с.
4. Бойко І.В., Петрик М.Р., Цуприк Г.Б. Моделювання та видобуток даних (високопродуктивні обчислення у великих та числових системах, комбінаторному аналізі): навчальний посібник. Тернопіль: : ТНТУ 2019 – 62 с.

УДК 004.4
О. Колодій; Ю. Стоянов, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕГРАЦІЯ OPENAI API ДЛЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПРОДУКТИВНОСТІ В СИСТЕМАХ УПРАВЛІННЯ ЗАВДАННЯМИ

UDC 004.4
O. Kolodii; Y. Stoyanov, Ph.D.

INTEGRATION OF OPENAI API FOR INTELLIGENT PERFORMANCE ANALYSIS IN TASK MANAGEMENT SYSTEMS

Першими системами управління завданнями можна вважати записники та ручки, які використовувалися для створення списків справ. Сьогодні багато людей перейшли до сучасніших методів – використання мобільних або настільних додатків для нотаток. Зі впровадженням хмарних технологій ці нотатки синхронізуються між пристроями, що забезпечує доступ до них у будь-який час.

Попри зручність, такі підходи мають певні недоліки: завдання можуть бути забутими без відповідних нагадувань. Тому все більшої популярності набувають календарі та додатки для управління завданнями, які дозволяють встановлювати дедлайни та отримувати сповіщення.

З розвитком штучного інтелекту, зокрема великих мовних моделей (LLM), таких як ChatGPT, функціонал систем управління завданнями може бути значно розширений. Наприклад, за допомогою OpenAI API додатки можуть:

- Автоматично генерувати корисні підказки при створенні завдань.
- Аналізувати виконання завдань за певний період (наприклад, за тиждень) та надавати звіт про продуктивність.
- Ідентифікувати слабкі місця у підході користувача до планування [1].

OpenAI API забезпечує зручний інструментарій для інтеграції таких функцій завдяки JavaScript-бібліотеці. Робота з API організована через створення запитів (prompt) та передачу контексту моделі. Наприклад, модель можна налаштувати як персонального асистента для управління завданнями, який надає рекомендації на основі аналізу списку справ [1].

Подібні можливості можуть бути корисними для спеціалістів різних галузей, допомагаючи підвищити ефективність і точність виконання робочих завдань. Впровадження таких технологій сприяє оптимізації робочих процесів та дозволяє зробити системи управління завданнями ще більш адаптивними [2].

Література

1. OpenAI API Reference [Електронний ресурс] – Режим доступу до ресурсу: https://platform.openai.com/docs/api-reference/introduction.
2. GPT-4 Technical Report [Електронний ресурс] – Режим доступу до ресурсу: https://openai.com/research/gpt-4.

УДК 004.7
К. Кулішова; С. Дячук, канд. техн. наук, доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА РІШЕНЬ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ КОНТЕНТУ В СУЧАСНИХ CRM-СИСТЕМАХ

UDC 004.7
K. Kulishova; S. Dyachuk, Ph.D.; Assoc. Prof.

DEVELOPMENT OF ARTIFICIAL INTELLIGENCE-BASED SOLUTIONS FOR CONTENT AUTOMATION IN MODERN CRM SYSTEMS

Сучасні CRM-системи стали важливими інструментами для управління взаємодією з клієнтами, однак традиційні методи створення і персоналізації контенту все ще мають ряд обмежень. Зростання обсягів даних та необхідність швидкої адаптації контенту вимагають нових підходів, і використання штучного інтелекту для автоматизації процесів контенту є перспективним рішенням [1].

Штучний інтелект здатен оптимізувати маркетингові процеси, автоматично створюючи персоналізовані матеріали для різних сегментів клієнтів. Алгоритми не лише генерують контент, а й прогнозують поведінку клієнтів, що покращує точність маркетингових стратегій. Важливою перевагою є зниження потреби в людських ресурсах, що значно скорочує витрати та час на виконання завдань.

Для успішного впровадження таких рішень у CRM-системи необхідно враховувати кілька ключових аспектів. По-перше, система повинна бути здатна до інтеграції з існуючими платформами, щоб забезпечити безперебійну передачу даних та синхронізацію контенту. По-друге, необхідно забезпечити високий рівень безпеки даних, оскільки обробка персональної інформації є важливою складовою роботи CRM. Останнім, але не менш важливим аспектом є масштабованість рішення, адже з ростом обсягів даних система повинна зберігати свою ефективність [2].

Таким чином, автоматизація контенту в CRM-системах за допомогою штучного інтелекту за допомогою штучного інтелекту підвищує ефективність взаємодії з клієнтами, знижує витрати та покращує досвід користувачів. Інтеграція таких рішень не тільки покращить маркетингові кампанії, а й оптимізує внутрішні процеси компаній, дозволяючи їм швидше адаптуватися до змін на ринку.

Література

1. Artificial Intelligence for Customer Relationship Management: Personalization and Automation. [Електронний ресурс]. URL: https://ieeexplore.ieee.org/document/10434568 Дата доступу: 09.12.2024.
2. AI-Driven Customer Relationship Management (CRM). [Електронний ресурс]. URL: https: //www.researchgate.net/publication/376618237 Дата доступу: 09.12.2024.

УДК 004.92
А. О. Кривко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВІЗУАЛІЗАЦІЯ ЯК ВИБІР ДИЗАЙНУ

UDC 004.92
A. O. Kryvko

VISUALIZATION AS A DESIGN CHOICE

Сформулювати базову візуалізацію набору даних d можна як набір взаємопов'язаних варіантів дизайну C = {c}, кожен з яких вибирається з можливого простору c ~ ℂ. Однак не всі варіанти дизайну призводять до правильних візуалізацій - деякі варіанти несумісні один з одним. Наприклад, кодування категоріального стовпця з віссю Y лінійної графіки неприпустимо. Отже, множина варіантів, що призводять до правильних візуалізацій, є підмножиною простору всіх можливих варіантів $\mathbb{C}1 \times \mathbb{C}2 \times \ldots \times \mathbb{C}_{|C|}$.

Ефективність візуалізації може бути визначена інформаційними показниками, такими як ефективність, точність і запам'ятовуваність, або емоційними показниками, такими, як залучення. Дослідження також показують, що ефективність визначається низькорівневими принципами сприйняття та властивостями набору даних, на додаток до контекстуальних факторів, таких як завдання, естетика, домен, аудиторія та середовище. Інакше кажучи, аналітик вибирає дизайн для візуалізації C_{max}, який максимізує ефективність візуалізації E ff з урахуванням набору даних d і контекстуальних факторів T:

$$C_{max} = arg\max_{C} \text{Eff}(C|d,T)$$

Але вибір дизайну може бути коштовним. Мета рекомендацій візуалізації – знизити вартість створення візуалізацій за рахунок автоматичної пропозиції підмножини варіантів дизайну $Crec \subseteq C$ (рис. 1).

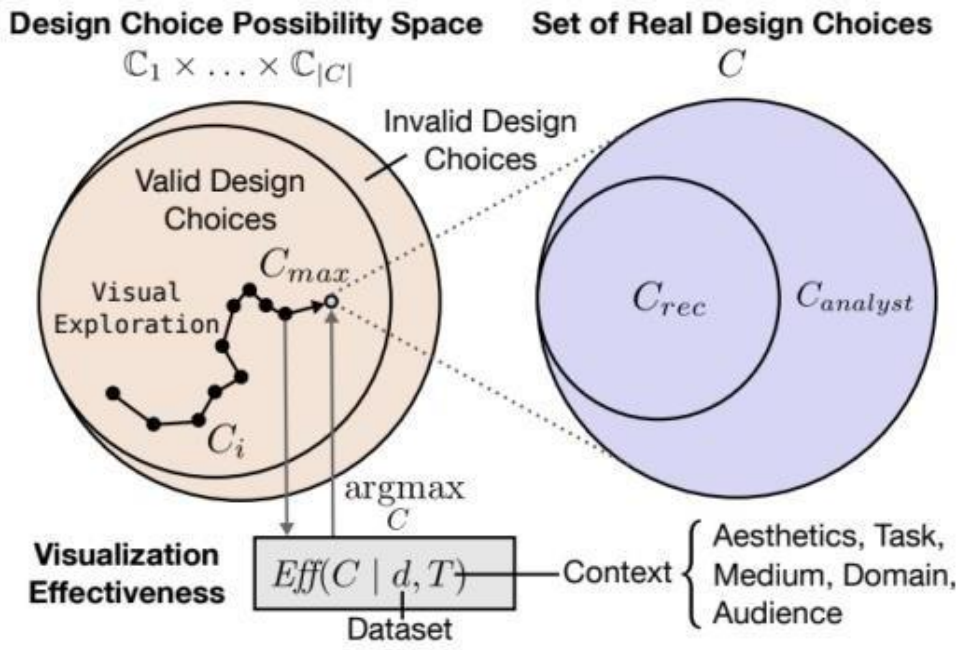


Рисунок 1. Створення візуалізацій – це процес вибору дизайну, який може бути рекомендований системою або вказаний аналітиком

УДК 004.41
Т. Ланевич
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ РЕФАКТОРИНГУ В ГНУЧКІЙ РОЗРОБЦІ

UDC 004.41
T. Lanevych

REFACTORING METHODS IN AGILE DEVELOPMENT

Рефакторинг в Agile – це процес реструктуризації існуючого коду без зміни його зовнішньої поведінки. Це передбачає виявлення та усунення технічної заборгованості, а також покращення якості коду та забезпечення того, щоб кодова база залишалася добре організованою та легкою для розуміння в міру розвитку проєкту. Рефакторинг – це проактивний підхід до розробки програмного забезпечення, що дозволяє командам постійно оптимізувати свій код і адаптуватися до мінливих вимог.

Команди гнучкої розробки мають у своєму розпорядженні широкий спектр методів рефакторингу, зокрема:

1. Перейменування – покращення ясності та виразності назв змінних, методів і класів.
2. Вилучення методів – розбиття великих, складних методів на менші, більш сфокусовані.
3. Виділення класів – розділення завдань шляхом створення нових класів для інкапсуляції конкретних обов'язків.
4. Вбудовані функції – усунення непотрібних непрямих посилань шляхом вбудовування невеликих простих методів.
5. Видалення дубльованого коду – виявлення та усунення надлишкових фрагментів коду за допомогою таких методів, як вилучення та абстракція.
6. Спрощення умовних виразів – зменшення складності операторів if-else та switch.
7. Покращення організації коду – реорганізація структури кодової бази для покращення читабельності та обслуговування.

Гнучкий рефакторинг – це потужний інструмент у процесі розробки програмного забезпечення, який підвищує якість коду, покращує продуктивність, оптимізує процеси розробки і, зрештою, призводить до створення кращих продуктів. Регулярно рефакторингуючи свій код, Agile-команди можуть гарантувати, що їхні додатки залишатимуться масштабованими, ефективними та відповідатимуть потребам бізнесу, що постійно змінюються. Зрештою, ця практика підтримує основні принципи гнучкої розробки, сприяючи створенню надійного та гнучкого середовища для розробки програмного забезпечення.

Література

1. Agile Code Refactoring Explained: Why You Need It and How to Do It [Електронний ресурс] – Режим доступу до ресурсу: https://www.nan-labs.com/blog/refactoring-in-agile/.
2. Agile Refactoring: Techniques, Best Practices & Challenges [Електронний ресурс] – Режим доступу до ресурсу: https://brainhub.eu/library/refactoring-in-agile-techniques-best-practices.
3. Refactoring in Agile: Streamlining Code for Optimal Efficiency [Електронний ресурс] – Режим доступу до ресурсу: https://www.metridev.com/metrics/refactoring-in-agile-streamlining-code-for-optimal-efficiency/.

УДК 004.41
Т. Ланевич
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ TEST-DRIVEN DEVELOPMENT НА ЯКІСТЬ РОЗРОБКИ

UDC 004.41
T. Lanevych

INFLUENCE OF TEST-DRIVEN DEVELOPMENT ON DEVELOPMENT QUALITY

Test Driven Development (TDD) – це методологія розробки програмного забезпечення, яка акцентує на написанні тестів перед написанням фактичного коду. Це гарантує, що код завжди протестований і функціональний, зменшує кількість помилок і покращує якість коду. У TDD розробники пишуть невеликі, сфокусовані тести, які визначають бажану функціональність, потім пишуть мінімальний код, необхідний для проходження цих тестів, і, нарешті, рефакторингують код для покращення структури та продуктивності. TDD – це безперервний ітеративний процес (цикл), який складається з трьох основних фаз: Червона, Зелена та Рефакторинг (рис. 1).

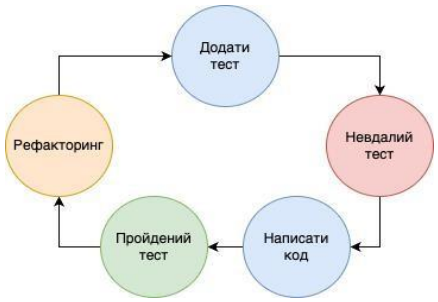


Рисунок 1. Цикл Test-Driven Development

Переваги тестової розробки (TDD):

1. Сприяє створенню оптимізованого коду.
2. Допомагає розробникам краще аналізувати та розуміти вимоги клієнта та вимагати чіткості, якщо вони не визначені належним чином.
3. Додавання та тестування нових функцій стає набагато легшим на останніх етапах розробки.
4. Тестове покриття у TDD значно вище, оскільки цей підхід зосереджується на створенні тестів для кожної функції від початку.
5. Підвищує продуктивність розробника та сприяє розробці кодової бази, яка є гнучкою та легкою в обслуговуванні.

TDD використовується в різних мовах програмування та середовищах, таких як Java, Python, C#, JavaScript та зазвичай інтегрується у CI/CD процеси для забезпечення якості.

Література

1. A Guide To Test Driven Development (TDD) [Електронний ресурс] – Режим доступу до ресурсу: https://www.qatouch.com/blog/test-driven-development/.
2. What is Test-driven Development? A Complete Guide To TDD [Електронний ресурс] – Режим доступу до ресурсу: https://katalon.com/resources-center/blog/what-is-tdd.
3. What is Test-Driven Development? [Електронний ресурс] – Режим доступу до ресурсу: https://testdriven.io/test-driven-development/.

УДК 691.544
А. С. Луговий; Є. В. Тиш, к.т.н.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОДИ ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ ETL-СИСТЕМ У БАГАТОРІВНЕВИХ АНАЛІТИЧНИХ ПЛАТФОРМАХ

UDC 691.544
A. S. Lugovyi; I. V. Tysh, Ph.D.

METHODS FOR OPTIMIZING ETL SYSTEM PERFORMANCE IN MULTI-TIER ANALYTICAL PLATFORMS

ETL (Extract, Transform, Load) є ключовим процесом для забезпечення інтеграції та аналізу великих даних у сучасних інформаційних системах. У контексті зростання обсягів даних і вимог до їх обробки, критично важливим є розробка методів оптимізації ETL-процесів, що дозволяють ефективно працювати в умовах високих навантажень та забезпечувати масштабованість системи.

Одним із ключових напрямків розвитку ETL-процесів є використання розподілених обчислювальних платформ, таких як Apache Spark або AWS Glue, що дозволяють паралельно обробляти великі обсяги даних. Це досягається шляхом поділу даних на партиції та виконання операцій одночасно на кількох вузлах кластеру.

Оптимізація також охоплює автоматизацію етапів трансформації даних. Використання метаданих для динамічного визначення схем і структури даних значно скорочує час налаштування процесів. Крім того, застосування алгоритмів для зменшення обсягів проміжних даних (наприклад, агрегування на етапі завантаження) дозволяє знизити затримки при передачі інформації.

Важливою складовою є інтеграція інструментів моніторингу та управління процесами ETL. Вони забезпечують своєчасне виявлення вузьких місць у системі та дозволяють адаптуватися до змін у робочих навантаженнях. Наприклад, адаптивне масштабування ресурсів у хмарних платформах дозволяє автоматично виділяти додаткові ресурси у пікові періоди.

З огляду на стрімке зростання обсягів даних і складність сучасних систем, однією з перспективних тенденцій є інтеграція штучного інтелекту (ШІ) для автоматизації оптимізації ETL-процесів. Використання ШІ дозволяє прогнозувати пікові навантаження, адаптувати конфігурацію процесів у реальному часі та забезпечувати виявлення аномалій. Іншою важливою тенденцією є перехід до потокових ETL-систем, які дозволяють обробляти дані в режимі реального часу, що особливо актуально для IoT і фінансових систем. Удосконалення інструментів інтеграції хмарних сервісів також відіграє важливу роль, забезпечуючи гнучкість і доступність ресурсів для ETL-процесів

Реалізація сучасних методів оптимізації ETL-процесів у масштабованих системах обробки великих даних забезпечує підвищення продуктивності, зниження витрат на обробку даних і забезпечення їхньої доступності для бізнес-аналітики та інших потреб організації.

Література

1. Pavlo A., Aslett M. Big Data Analytics for Data Engineers. Springer, 2019. 82 с
2. Netezza, Big Data Integration: Efficient ETL Processes in a Distributed Environment. IBM Press, 2021. 382 с.

УДК 004.6
М. А. Лукасевич
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОДЕЛЬ ДАНИХ ДЛЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ ДЛЯ ПРОГНОЗУВАННЯ КОТИРУВАНЬ КРИПТОВАЛЮТНИХ АКТИВІВ

UDC 004.6
M. Lukasevych

DATA MODEL FOR INFORMATION AND ANALYTIC SYSTEM FOR FORECASTING QUOTATIONS OF CRYPTOCURRENCY ASSETS

Модель даних (МД) є комплексною структурою, яка охоплює різні аспекти системи. Вона включає моделі, такі як Account, AccountPortfolio, Order, Signal та Prediction, які взаємодіють один з одним для забезпечення функціональності системи.

МД містить інформацію про трейдерів та їх акаунти (Account), їх портфелі (AccountPortfolio) з балансами і прибутком/збитком, ордери на купівлю та продаж (Order), сигнали (Signal), які рекомендують певні дії з торгівлі, та передбачення (Prediction), із інформацією про прогнозовані значення і пов'язані з певними сигналами.

Кожен користувач (Account) має свій акаунтний портфель (AccountPortfolio), в якому зберігається інформація про баланс та прибуток. Користувачі можуть створювати замовлення на купівлю або продаж крипто валютних активів. Кожне замовлення містить інформацію про символ активу, кількість та напрямок операції.

Діаграма класів UML для МД у системі зображено на рис. 1, де:

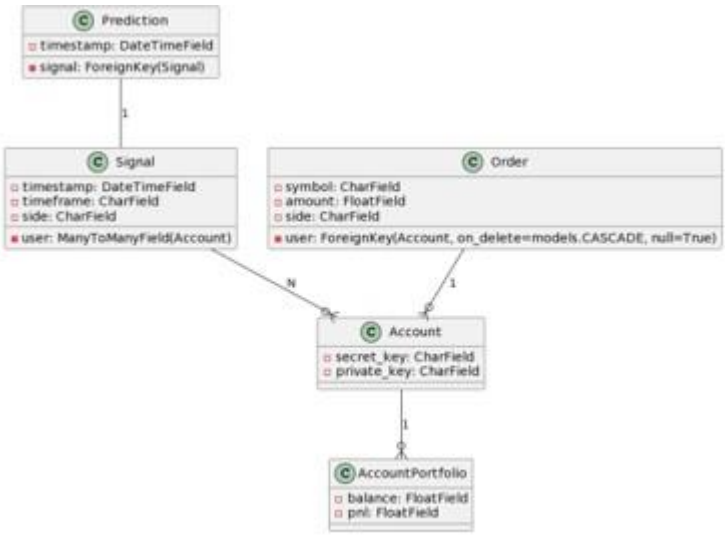


Рисунок 1 – Діаграма класів UML для моделі даних

- відношення між класами Account та AccountPortfolio: 1 вказує на зв'язок «один до одного» (One-to-One) між Account та AccountPortfolio. Один обліковий запис може бути пов'язаний лише з одним портфелем облікового запису;
- відношення між класами Signal та Account: N вказує на зв'язок "багато до багатьох" (Many-to-Many) між Signal і Account. Один сигнал може бути пов'язаний з декількома обліковими записами, і один обліковий запис може бути пов'язаний з кількома сигналами;
- відношення між класами Order та Account: 1 вказує на зв'язок «один до багатьох» (One-to-Many) між Order та Account. Одне замовлення може бути пов'язане лише з одним обліковим записом, але один обліковий запис може мати кілька замовлень.
- відношення між класами Prediction та Signal: 1 вказує на зв'язок «один до одного» (One-to-One) між Prediction та Signal. Один прогноз може бути пов'язаний лише з одним сигналом.

Отже, МД підтримує зберігання інформації про користувачів, портфелі, сигнали, прогнози та замовлення, що дозволяє системі ефективно прогнозувати і управляти торговими операціями з криптовалютами.

УДК 004.45+004.62
Н. Мельник; А. М. Луцків, канд. техн. наук, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗГОРТАННЯ ВЛАСНИХ АРТЕФАКТІВ ЕКОСИСТЕМИ HADOOP

UDC 004.45+004.62
N. Melnyk; A. Lutskiv, Ph.D., Associate Professor

DEPLOYMENT OF OWN ARTIFACTS OF THE HADOOP ECOSYSTEM

Ключові слова: Великі Дані, Hadoop, артефакт, Bigtop, Ambari.
Key words: Big Data, Hadoop, artifact, Bigtop, Ambari.

Зростання обсягу даних у світі робить критично важливим використання програмного забезпечення для їх ефективної обробки та управління [1]. Однією з найпоширеніших платформ для роботи з Big Data є екосистема Apache Hadoop, яка забезпечує можливості для обробки великих обсягів структурованих і неструктурованих даних [2]. Одним із важливих аспектів у цьому контексті є розгортання власних артефактів Hadoop, що дозволяє адаптувати платформу під конкретні потреби організацій. Артефакти Hadoop – це сформовані пакети програмних компонентів екосистеми Hadoop.

Актуальність дослідження методу розгортання власних артефактів екосистеми опрацювання великих даних Hadoop обумовлена необхідністю забезпечення ефективної та надійної роботи з даними. Системи, побудовані на основі Hadoop, використовуються в різних сферах, таких як аналітика структурованих і неструктурованих даних, машинне навчання та управління ресурсами.

Основною метою використання методу розгортання власних артефактів Hadoop виступає забезпечення більшої незалежності від зовнішніх корпорацій та розробників, що надають свої рішення, а також забезпечення можливості повного налаштування екосистеми під власні потреби компанії методом перетворення і переконфігурування наявних рішень для власних потреб або створення власних сервісів і інтегрування їх у інфраструктуру.

Використання таких інструментів, як Apache Bigtop для побудови та тестування артефактів, та Apache Ambari для управління кластерами, дає змогу значно підвищити продуктивність шляхом переконфігурування сервісів платформи з урахуванням власних вимог та забезпечити високу якість розгорнутих систем.

Apache Bigtop виступає важливим інструментом для побудови й тестування артефактів екосистеми Hadoop. Він забезпечує можливість пакування та перевірки сумісності компонентів, що гарантує стабільність і ефективність роботи розгорнутих систем [3].

Для формування артефактів Apache Bigtop спочатку клонує необхідний GitHub репозиторій сервісу і застосовує спеціальні git-патчі для внесення необхідних змін у локальний репозиторій, не змінюючи при цьому оригінальні origin-гілки на GitHub. Після цього він запускає необхідну команду для формування проєкту і пакує двійкові файли у інсталяційні пакети (deb або rpm).

Існує три основних варіанти переналаштування екосистеми Hadoop з використанням Apache Bigtop:

- створення власних відгалужень або використання відгалужень інших організацій GitHub репозиторіїв оригінальних сервісів та внесення змін безпосередньо в код програм, після чого необхідно змінити посилання на репозиторій у файлі налаштування “bigtop.bom”;
- створення власних git-патчів для внесення змін у локальний репозиторій, клонований з оригінального GitHub репозиторію;
- реалізація та інтеграція власних сервісів у стек. Даний метод передбачає повну розробку власного сервісу (створення нового проєкту, його структури, написання програмних скриптів, цифрове підписування файлів тощо), а також написання тестів та реалізацію механізму пакування двійкових файлів.

Одним із ключових завдань при роботі з екосистемою Hadoop є розгортання та управління кластером. Apache Ambari спрощує цей процес, надаючи інструменти для налаштування, моніторингу та повного управління кластером Hadoop. Ambari забезпечує зручний інтерфейс для встановлення, конфігурації та оновлення сервісів Hadoop.

Для розгортання артефактів Ambari використовує попередньо визначені стеки. Стек Ambari – це сукупність компонентів та технологій, які використовуються самим програмним рішенням Ambari для спрощення та автоматизації розгортання, налаштування, управління та моніторингу окремих сервісів Hadoop та у загальному кластері Hadoop [4]. Кожен компонент стеку виконує певну роль при розгортанні та взаємодіє з іншими компонентами для досягнення спільної мети. Стеки можуть мати власні версії, а також вони забезпечують власні інструменти для керування версіями сервісів. Кожна версія стеку пропонує попередньо визначений перелік сервісів певних версій для забезпечення сумісності. Варто окремо відзначити, що для забезпечення сумісності необхідно використовувати вже наявні API та протоколи, реалізовувати обробку даних у форматах, визначених та підтримуваних сервісами із якими ведеться взаємодія, забезпечувати безпеку тощо. Для перевірки сумісності необхідно проводити тестування та перевіряти роботу як кожного з сервісів, так і взаємодію між ними перед використанням у кінцевому робочому середовищі (Production).

Використання таких інструментів, як Apache Bigtop та Apache Ambari, є критично важливим для побудови і розгортання артефактів екосистеми Hadoop. Завдяки цим інструментам можна досягти високого рівня продуктивності та стабільності роботи систем, що опрацьовують великі обсяги даних. Власні артефакти дають змогу адаптувати Hadoop до конкретних завдань організації, забезпечуючи при цьому ефективну обробку і зберігання даних.

Література

1. Джавад А. Ш., Мухаммад А. Х. Big Data Systems. A 360-degree Approach. Лондон: Taylor & Francis, 2023. 340 с.
3. Apache Hadoop. Apache Software Foundation. URL: https://hadoop.apache.org/, (дата звернення: 20.11.2024).
4. Apache Bigtop. Apache Software Foundation. URL: https://bigtop.apache.org/, (дата звернення: 22.11.2024).
5. Defining a Custom Stack and Services. Confluence Apache Ambari. URL: https://cwiki.apache.org/confluence/display/AMBARI/Defining+a+Custom+Stack+and+Services , (дата звернення: 04.12.2024).

УДК 004.8
Б. Б. Млинко, к.т.н., доц.; І. М. Климко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ОБРОБКИ ПРИРОДНЬОЇ МОВИ ЗАСОБАМИ ГЛИБИННОГО НАВЧАННЯ

UDC 004.8
B. B. Mlynko, Ph.D., Assoc. Prof., I. M. Klymko

APPLICATION OF ARTIFICIAL INTELLIGENCE METHODS FOR NATURAL LANGUAGE PROCESSING USING DEEP LEARNING TECHNIQUES

Генерація тексту на основі методів глибинного навчання є одним із ключових напрямів у сучасній обробці природної мови. Враховуючи зростаючі вимоги до автоматизованого створення текстового контенту, актуальним стає завдання розробки моделей, здатних створювати послідовності символів із врахуванням синтаксичних, семантичних і структурних особливостей тексту. LSTM мережі показують високу ефективність у задачах моделювання послідовностей завдяки здатності запам’ятовувати довгострокові залежності. Однак основними викликами при їх застосуванні залишаються оптимізація навчання, подолання ефекту "забування" контексту та забезпечення балансу між узгодженістю і різноманітністю згенерованого тексту.

Метою дослідження було вдосконалити процес генерації тексту за допомогою LSTM-мереж шляхом впровадження методів оптимізації параметрів, поліпшення обробки навчальних даних та адаптації підходів до семплювання, що забезпечує генерування тексту із реалістичною структурою і змістом.

Для досягнення поставленої мети було розроблено експериментальну LSTM-модель, що працює на рівні символів. На етапі підготовки даних виконано токенізацію тексту на символи та побудову словника, що дозволяє перетворювати текст у послідовності числових індексів. Модель включає шар вбудовування, який знижує розмірність входу, а також LSTM-комірки, що обробляють дані послідовно. Навчання здійснювалося за допомогою алгоритму зворотного поширення похибки через час, при цьому дані поділено на батчі фіксованої довжини для ефективного опрацювання.

У процесі оптимізації параметрів моделі використано стохастичний градієнтний спуск із поступовим зменшенням швидкості навчання, що забезпечує стабільне сходження. Для запобігання перенавчанню та зниження ризику переваги локальних мінімумів застосовано методи регуляризації, такі як обмеження норми ваг та масштабування градієнтів. Генерація тексту здійснювалася на основі семплювання із використанням softmax-розподілу. Цей підхід дозволив регулювати баланс між детермінованістю вибору символу та різноманітністю вихідного тексту.

Результати експериментів продемонстрували, що оптимізація параметрів моделі та впровадження регуляризації дозволили покращити якість згенерованого тексту. Модель виявила здатність підтримувати базові патерни англійської мови, відтворювати структуру речень та зберігати контекст на рівні декількох символів. Під час навчання спостерігалося поступове зниження перплексії, що свідчить про ефективне опрацювання довгострокових залежностей.

Література

1. I. Goodfellow. Deep Learning (Adaptive Computation and Machine Learning series) / I. Goodfellow, Y. Bengio, A. Courville., 2016.

УДК 004.89
Є. В. Огінський; Д. С. Антонюк, канд. пед. наук, доцент
(Державний університет «Житомирська політехніка», Україна)

ВИКОРИСТАННЯ ЙМОВІРНІСНОЇ ПРИРОДИ ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ В СФЕРІ ПЕРСОНАЛЬНИХ ФІНАНСІВ

UDC 004.89
Y. V. Ohinskyi; D. S. Antoniuk, PhD, Assoc. Prof.

UTILIZING THE PROBABILISTIC NATURE OF LARGE LANGUAGE MODELS IN THE FIELD OF PERSONAL FINANCE

Останнім часом можна спостерігати ріст застосування великих мовних моделей (LLM) у різних сферах завдяки здатності обробляти природну мову, автоматизувати складні завдання, створювати і готувати інформаційні матеріали. Персональні фінанси – одна зі сфер, у якій LLM також можуть ефективно застосовуватися. Моделі можуть бути використані для допомоги у створенні бюджету, аналізу витрат і плануванні заощаджень, допомоги у покращенні фінансової грамотності, роз'яснення понять і термінів, або для підтримки у отриманні навичок, наприклад, складання пенсійного плану чи вибір вигідного фінансового інструменту. Існують приклади застосування LLM у фінсовому секторі. BloomergGPT – модель, навчена на широкому спектрі фінансових даних і даних загального характеру для виконання різноманітних завдань у фінансовій галузі [1]. FinGPT – модель з відкритим кодом, яка потенційно може бути застосована у якості автоматизованого радника (robo-adviser), у сфері алгоритмічного трейдингу, тощо [2].

У сфері персональних фінансів існує елемент невизначеності і часто неможливо однозначно обрати оптимальне рішення. Результати використання того чи іншого фінансового інструменту має ймовірнісний характер і може залежати від багатьох факторів, таких як інфляція, курсова різниця, невизначена дохідність самого інструменту. У кожної людини є власні уподобання, що є додатковим фактором у визначенні більш зручного і комфортного інструменту або рішення. Крім того, часто постає проблема у виборі між ризикованим, потенційно більш прибутковим інструментом і безпечним, але менш прибутковим. LLM у свою чергу працюють на основі ймовірнісного підходу. Один й той самий запит до моделі може привести до різних результатів. Ступінь невизначеності або випадковості у процесі генерації відповідей моделями зазвичай регулюється окремим параметром, який називається температурою. Деякий ступінь випадковості у відповідях при одних і тих же умовах дає додаткову перевагу використання LLM для відповідей у персональних фінансах, тому що можуть бути знайдені нові, потенційно більш вигідні (або більш комфортні) рішення для конкретної людини при визначених умовах. Різноманітність у відповідях моделей може допомогти у вирішенні дилеми дослідження та використання (exploration-exploitation dilemma) у сфері персональних фінансів.

Література

1. Wu S. та ін. BloombergGPT: A large language model for finance. arXiv preprint arXiv:2303.17564. 2023. DOI: https://doi.org/10.48550/arXiv.2303.17564.
2. Yang, H., Liu, X. Y., & Wang, C. D. FinGPT: Open-source financial large language models. FinLLM at IJCAI 2023. 2023. DOI: http://dx.doi.org/10.2139/ssrn.4489826.

УДК 528.8.044
П. С. Панчишин; М. І. Паламар, д.т.н., професор.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПІДВИЩЕННЯ ЯКОСТІ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ У ВІДЕОПОТОЦІ В РЕАЛЬНОМУ ЧАСІ

UDC 528.8.044
P. Panchyshyn; M. I. Palamar Dr., Prof.

IMPROVING THE QUALITY OF OBJECT RECOGNITION IN A REAL-TIME VIDEO STREAM

Розпізнавання об'єктів у реальному часі є важливим завданням у багатьох галузях, включаючи автономні системи, безпілотні літальні апарати, системи відеоспостереження та роботи. Технології, такі як нейромережа **YOLO (You Only Look Once)**, вже демонструють високу швидкість і точність, але складні умови, такі як погане освітлення, шуми або мала роздільна здатність відео, вимагають додаткових підходів для підвищення якості розпізнавання.

Розглянемо методи та алгоритми, які покращують точність та стабільність розпізнавання об'єктів у відеопотоці, для моделі YOLO, зокрема використання механізмів уваги, такі як **SE-блоки (Squeeze-and-Excitation)**, що дозволить моделі зосередитися на важливих частинах зображення, ігноруючи другорядні деталі. Це важливо для поліпшення точності в умовах складних сцен, де на зображенні можуть бути як значні, так і незначні об'єкти.

SE-блоки (Squeeze-and-Excitation):

Блоки працюють шляхом зменшення просторової інформації через глобальне середнє зменшення (**squeeze**) та потім виділяють важливі канали в мережі (**excitation**).

В результаті модель фокусується на найбільш інформативних ознаках, покращуючи детекцію об'єктів, що важливі для поставленої задачі.

Як працюють механізм уваги SE?

1. Після надходження зображення до нейронної мережі.
2. **Крок 1 — Squeeze (скорочення):**

Використовує глобальне середнє згортання по простору, щоб отримати згорнуті ознаки для кожного каналу.

Для кожного каналу *c* підраховуємо середнє значення по всіх просторових координатах:

$$z_c = \sigma\left(\frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W} x_{ijc}\right)$$

де x_{ijc} – значення пікселя на координатах *i*,
j для каналу *c*,
H та *W* – висота та ширина карти ознак,
а σ – сигмоїдальна функція активації для отримання вихідного значення в межах [0,1].

3. **Крок 2 – Excitation (збудження):**

Після отримання згорнутого вектора для кожного каналу, механізм генерації коефіцієнтів важливості кожного каналу через два повнозв'язкові шари:

$$s_c = \sigma(W_2\delta(W_1 z_c))$$

де W_1, W_2 – це ваги для двох лінійних шарів,
δ – *ReLU* активація для ненегативних значень,
S_c – вихідний коефіцієнт важливості для каналу c, що визначає, на скільки цей канал повинен бути посилений чи ослаблений.

4. **Крок 3 – Оновлення ознак:**

Множимо оригінальну карту ознак на відповідні коефіцієнти важливості S_c для кожного каналу:

$$\hat{x}_{ijc} = s_c x_{ijc}$$

Таким чином, канали з високими значеннями S_c будуть посилені, а канали з низькими значеннями – ослаблені.

5. **Вихід:**

Модифікована карта ознак, готова для подальшої обробки.

Переваги:

Покращена точність завдяки зосередженню уваги на важливих частинах зображення, модель може більш точно визначати об'єкти навіть у складних ситуаціях.

Зниження помилок зменшення ймовірності пропуску або неправильної детекції об'єктів, особливо при великій кількості фону або маленьких об'єктах.

Таким чином застосування механізму уваги **SE** у моделі **YOLO** є потужним інструментом для покращення ефективності глибоких нейронних мереж. Він дозволяє зосередити увагу на найбільш важливих каналах і забезпечує значне підвищення точності розпізнавання об'єктів, сегментації та інших задач. Впровадження SE-блоків дозволяє значно покращити загальну ефективність моделі без значного збільшення обчислювальних витрат.

Література

1. Xuan-Phung Huynh and Yong-Guk Kim. Discrimination between genuine versus fake emotion using long-short term memory with parametric bias and facial landmarks. In Proceedings of the IEEE International Conference on Computer Vision Workshops, 2017.
2. David Daniel Cox and Thomas Dean. Neural networks and neuroscience-inspired computer vision. Current Biology, 2014.
3. Bin Yang, Junjie Yan, Zhen Lei, and Stan Z Li. Convolutional channel features. In Proceedings of the IEEE international conference on computer vision, 2015.
4. Athanasios Voulodimos, Nikolaos Doulamis, Anastasios Doulamis, and Eftychios Protopapadakis. Deep learning for computer vision: A brief review. Computational intelligence and neuroscience, 2018
5. Behzad Hasani and Mohammad H Mahoor. Facial expression recognition using enhanced deep 3d convolutional neural networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2017

УДК 004.9, 004.45
Д. Романюк, Ph.D.; І. Мудрик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ СУЧАСНИХ ТЕХНОЛОГІЙ НА БУХГАЛТЕРСЬКИЙ ОБЛІК

UDC 004.9, 004.45
D. Romaniuk, Ph.D.; I. Mudryk

IMPACT OF MODERN TECHNOLOGIES ON ACCOUNTING

Цифрова трансформація кардинально змінює методи ведення бухгалтерського обліку, впливаючи на його ефективність, прозорість і адаптивність до потреб сучасного бізнесу. Інноваційні технології, такі як хмарні обчислення, штучний інтелект, машинне навчання та аналіз великих даних, пропонують нові можливості для обробки, аналізу та представлення фінансової інформації. Їхнє впровадження створює нову парадигму в обліковій сфері, яка орієнтована на автоматизацію, зменшення помилок і підвищення продуктивності.

Одним із ключових чинників цифрової трансформації є впровадження хмарних обчислень [1]. Хмарні платформи дозволяють компаніям забезпечувати безперервний доступ до фінансових даних з будь-якої точки світу, що особливо важливо в умовах віддаленої роботи та глобалізації бізнесу. Інтеграція хмарних технологій не лише оптимізує витрати на обслуговування серверів і програмного забезпечення, а й забезпечує швидке оновлення інформації, спрощуючи управлінські процеси. Завдяки цьому облікові системи перетворюються на динамічні інструменти для підтримки прийняття рішень.

Технології штучного інтелекту та машинного навчання суттєво змінюють характер виконання рутинних облікових завдань. Автоматизація таких процесів, як обробка рахунків-фактур, класифікація транзакцій та підготовка звітності, дозволяє бухгалтерам зосередитися на стратегічному аналізі, управлінні ризиками та консультуванні керівництва. Наприклад, алгоритми машинного навчання можуть виявляти аномалії у фінансових даних, що сприяє зниженню ризиків шахрайства та помилок. Крім того, використання прогнозної аналітики допомагає компаніям краще оцінювати майбутні фінансові результати, що є важливим для довгострокового планування.

Аналіз великих даних (Big Data) відкриває нові можливості для фінансового моделювання та управління. Завдяки можливості обробляти величезні обсяги інформації в режимі реального часу, компанії отримують змогу виявляти приховані тенденції, оцінювати вплив зовнішніх факторів на фінансову стабільність і оперативно реагувати на зміни ринку. Такий підхід значно підвищує точність управлінських рішень, що є критично важливим в умовах конкурентного середовища.

За даними дослідження [2], компанії, які впровадили хмарні облікові системи, скоротили витрати на IT-інфраструктуру на 20-30%. Наприклад, у 2022 році корпорація "ABC" зекономила 2 млн доларів на обслуговуванні серверів після переходу на хмарну платформу. Штучний інтелект: Алгоритми, які використовуються для аналізу транзакцій, можуть обробляти понад 100 000 операцій за годину, що в 10 разів перевищує продуктивність традиційних методів. Компанія "XYZ" у своїх звітах за 2023 рік зазначила, що застосування AI дозволило зменшити помилки у фінансовій звітності на 85%. У 2023 році HSBC повідомив, що використання блокчейн-рішень дозволило зменшити час на обробку міжнародних переказів з 3-5 робочих днів до кількох годин. Зокрема, це відбувалося через платформу we.trade, яка забезпечує швидке виконання транзакцій і підвищує прозорість завдяки смарт-контрактам. Крім того, банк скоротив операційні витрати на 10-15% у цій сфері.

Цифрова трансформація також змінює роль бухгалтера, перетворюючи його на стратегічного партнера бізнесу. Замість виконання ручних операцій бухгалтери все більше займаються інтерпретацією даних, розробкою прогнозів та участю в розробці бізнес-стратегій. Це вимагає нових компетенцій, таких як знання аналітичних інструментів, розуміння принципів роботи сучасних інформаційних систем та здатність адаптуватися до швидких змін технологій.

Попри значні переваги, цифрова трансформація бухгалтерського обліку супроводжується певними викликами. Основними з них є високі витрати на впровадження нових технологій, необхідність перекваліфікації персоналу та ризики, пов'язані з кібербезпекою. Для ефективного впровадження цифрових технологій компаніям потрібно розробляти довгострокові стратегії, які враховують технічні, організаційні та юридичні аспекти. Крім того, регуляторні органи повинні забезпечити адаптацію нормативно-правової бази до нових реалій цифрової економіки.

Інтеграція блокчейн-технологій [2] у бухгалтерський облік є ще одним перспективним напрямом. Використання розподілених реєстрів забезпечує високий рівень прозорості та достовірності даних, що знижує ризик маніпуляцій та помилок. Завдяки автоматизації процесів перевірки та підтвердження транзакцій, блокчейн може значно спростити аудит і скоротити час, необхідний для підготовки фінансових звітів. Крім того, впровадження смарт-контрактів може замінити ручне управління окремими операціями, виконуючи їх заздалегідь визначеними умовами.

Загалом цифрова трансформація бухгалтерського обліку є не лише технологічним, а й стратегічним процесом, який вимагає комплексного підходу [3]. Компаніям важливо зважувати переваги впровадження нових технологій із можливими ризиками, такими як кібербезпека чи складнощі інтеграції із застарілими системами. Лише за умови належного управління цим процесом цифрові інновації зможуть забезпечити значний приріст продуктивності, конкурентоспроможності та якості управлінських рішень, перетворивши бухгалтерський облік на ключовий елемент бізнес-екосистеми майбутнього.

Література

1. Busulwa, R., & Evans, N. Digital Transformation in Accounting. Routledge, 2020.
2. Kanaparthi, V. (2024). Exploring the Impact of Blockchain, AI, and ML on Financial Accounting Efficiency and Transformation. DOI:10.48550/arXiv.2401.15715.
3. Савка, Н., Васильків, Н., Дубчак, Л., & Мудрик, І. (2023). РАДІАЛЬНО-БАЗИСНІ НЕЙРОННІ МЕРЕЖІ ДЛЯ ПРОГНОЗУВАНЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВ. European Science, 3(sge17-03), 42–48. https://doi.org/10.30890/2709-2313.2023-17-03-012

УДК 004.55
О. А. Саган; К. Б. Швирло
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІННОВАЦІЙНІ СТРАТЕГІЇ АДАПТИВНОЇ МОБІЛЬНОЇ ВЕРСТКИ: ЗАБЕЗПЕЧЕННЯ ШВИДКОСТІ, ЗРУЧНОСТІ ТА ФУНКЦІОНАЛЬНОСТІ

UDC 004.55
O. A. Sahan; K. B. Shvyrlo

INNOVATIVE STRATEGIES OF ADAPTIVE MOBILE WEBSITE: PROVIDING SPEED, CONVENIENCE AND FUNCTIONALITY

У сучасному світі дизайн веб-сайтів є критично важливим для забезпечення зручності користувачів і ефективності їх взаємодії з цифровими продуктами. Зростаюча популярність мобільних пристроїв підкреслює необхідність створення ефективного дизайну, який сприяє досягненню високої продуктивності та позитивного користувацького досвіду.

Адаптивний підхід до розробки веб-сайтів є базовою стратегією, яка забезпечує коректне відображення сторінок на пристроях із різними розмірами екрану. Використання таких методів дозволяє створювати універсальний інтерфейс, зручний як для мобільних телефонів, так і для планшетів чи великих моніторів, що сприяє поліпшенню візуального сприйняття та взаємодії [1].

Зменшення часу очікування користувачів є важливим чинником зручності. Застосування технологій оптимізації, таких як зменшення розміру зображень, використання кешування та мінімізація обсягу контенту, забезпечує швидке завантаження сторінок, що позитивно впливає на користувацький досвід і ранжування в пошукових системах.

Інтуїтивно зрозуміла структура сайту сприяє швидкому доступу до інформації. Простота навігації, мінімізація кроків для виконання ключових дій користувача та чітка структура контенту забезпечують зручність використання та скорочують час виконання завдань.

Розробка інтерфейсів, адаптованих для використання на мобільних пристроях, включає спрощення форм, уникнення перевантаження елементами дизайну та врахування особливостей сенсорного введення. Це значно полегшує процес взаємодії з сайтом.

Інтеграція сучасних мобільних функціональностей, таких як геолокація, доступ до камери чи сенсорів пристрою, дозволяє розширити можливості веб-сайтів. Це сприяє їх інтерактивності та додає нові сценарії використання, підвищуючи загальну функціональність.

Таким чином, впровадження цих принципів у процес створення мобільних веб-сайтів забезпечує підвищення зручності, доступності та продуктивності, що є критично важливим у сучасних умовах зростаючого використання мобільних пристроїв.

Застосування цих стратегій значно покращує користувацький досвід і продуктивність мобільних сайтів. Ураховуючи велику частку мобільного трафіку в глобальному інтернеті, впровадження адаптивного і швидкого дизайну є важливим для забезпечення ефективної взаємодії з користувачами [2].

Література

1. Responsive Layout Grid. Material Design. URL: https://m2.material.io/design/ layout/responsive-layout-grid.html.
2. 25 Top Web Design Trends 2025. TheeDigital. URL: https://www.theedigital.com/ blog/web-design-trends.

УДК 004.4
В. Сарновський; Ю. Стоянов, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПРОЄКТУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ЗАЯВКАМИ ГРОМАДЯН З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ .NET

UDC 004.4
V. Sarnovskyi; Y. Stoyanov, Ph.D., Assoc. Prof.

DESIGNING AN AUTOMATED SYSTEM FOR MANAGING CITIZENS' APPLICATIONS USING .NET TECHNOLOGIES

Державні установи щодня отримують значний обсяг звернень громадян, які потребують своєчасної та ефективної обробки. Традиційні методи роботи зі зверненнями мають низку недоліків, зокрема ручну обробку даних і відсутність сучасних інструментів для їх аналізу. Дослідження присвячене розробці автоматизованої системи для управління заявками громадян, яка базується на технологіях .NET і забезпечує підвищення продуктивності роботи відповідних служб.

Створення системи, що автоматизує процеси реєстрації, обробки та зберігання звернень громадян, з можливістю аналізу інформації та інтеграції з іншими державними платформами. Така система повинна бути зручною для користувачів та забезпечувати ефективну взаємодію.

Для реалізації проєкту використовується платформа .NET, яка забезпечує розробку масштабованих і надійних рішень. База даних на основі Microsoft SQL Server надає можливість зберігати великі обсяги даних та швидко їх обробляти. Інтерфейс користувача створений за допомогою ASP.NET MVC, що забезпечує зручність роботи з системою. Для взаємодії з базою даних використовується Entity Framework, що полегшує управління дани.

Система надає можливість громадянам подавати заявки онлайн і контролювати їх статус. Автоматизація процесів дозволяє знизити навантаження на персонал державних установ, прискорити реагування на запити та покращити якість надання послугів.

Література

1. Troelsen, A., Japikse, P. Pro C# 8.0 and the .NET Core 3.0 Framework. Apress, 2020.
2. Soni, M., Thakkar, P., Patel, H. ASP.NET MVC with Entity Framework and CSS. BPB Publications, 2021.

УДК 519.711.3:004.7
М. Стрілецький
(Західноукраїнський Національний Університет, Україна)

МЕТАМОДЕЛЬ ФОРМУВАННЯ ПАРНИКОВИХ ГАЗІВ МАЛИМИ ПІДПРИЄМСТВАМИ МАШИНОБУДІВНОГО СПРЯМУВАННЯ

UDC 519.711.3:004.7
M. Striletskyi

METAMODEL OF GREENHOUSE GAS FORMATION BY SMALL MACHINE-BUILDING ENTERPRISES

Протягом десятиліть дослідження парникових газів, таких як водяна пара, озон (стратосферний і тропосферний), метан та діоксид вуглецю, проводяться в різних аспектах: їх утворення, процес викидів та методи ліквідації. Попри значну інтенсивність цих досліджень, їхні практичні результати поки залишаються менш помітними, ніж очікувалося. За аналогічний період викиди парникових газів, спричинені діяльністю людини, не лише не скоротилися, а навіть зросли. Більшість зусиль теоретиків і практиків, спрямованих на протидію утворенню та викидам парникових газів в атмосферу, зосереджені переважно на великих підприємствах, що є цілком виправданим. Малі підприємства здебільшого залишаються осторонь від вирішення екологічних проблем, пов'язаних із парниковими газами. Водночас кількість невеликих виробництв, цехів, майстерень, особливо машинобудівного спрямування, постійно зростає, що призводить до накопичення і збільшення обсягу забруднень у навколишньому середовищі. Тому доцільно розробити раціональні моделі утворення парникових газів та їх ліквідації на різних платформах (Модель / МетаМодель / Мета-МетаМодель), з врахуванням особливостей виробничої діяльності, що є метою представлених досліджень, а також базою для розробки практичних рекомендацій.

Безумовно, пріоритет на початковій стадії потрібно надавати розробці моделей утворення парникових газів окремими агрегатами (обладнаннями) малих підприємств. Тут вже утворюється широкий спектр Моделей, побудований на різних підходах, кожен з яких має право на існування: в основу закладені тільки паспортні дані агрегатів; для вихідних даних здійснюється вибірка (ручна або автоматизована) показників датчиків використаних об’ємів енергоносіїв; застосування у системі контролю за викидами парникових газів контролерів, а відповідно їх врахування у Моделі. Моделі стають динамічними, оскільки враховують поточні зміни. І це лише на рівні накопичення вихідних даних. З урахуванням численних нюансів, кількість моделей зростає лавиноподібно. Необхідно встановити раціональну модель для кожного конкретного випадку, і тільки тоді приймати практичні дії. У таких умовах доцільним є повне або часткове об'єднання окремих моделей, що, зрештою, призводить до створення МетаМоделі (або декілька МетаМоделей).

Під час моделювання створюється модель, яка може бути різних типів залежно від мети та застосованих методів. Зокрема, моделювання може бути математичним, геометричним, тривимірним, емпіричним, механістичним (наприклад, моделювання трофічної мережі в екосистемі) або кінематичним. У цьому контексті МетаМодель – це модель, компоненти якої є самостійними моделями. Якщо існує кілька подібних моделей, необхідно створити модель, що їх об'єднує, – новостворена метамодель. Такий підхід отримав назву принципу метамодельного переходу, який є основним принципом метамоделювання. МетаМодель ("мета" означає "поза", "за межами", "понад") – це модель, яка описує структуру та принципи функціонування іншої моделі. Фактично, МетаМодель є абстракцією, що використовується для опису моделей. У широкому сенсі розробка МетаМоделі належить до процесу дизайну (конструювання). Процес моделювання утворює безперервний ланцюжок: Оригінал / Модель / МетаМодель. Це означає, що існує взаємозв'язок (instance) від оригіналу до МетаМоделі та відображення (represente) від МетаМоделі до оригіналу. Метамоделювання – це складний процес, що охоплює перехід від реального світу до МетаМоделі і навіть до Мета-МетаМоделі. Реальний світ складається з предметів і явищ, уявний світ – з об'єктів, МетаМодель – з класів, а модель – з елементів. Ця лінійка і характер переходу становлять сутність моделювання. Алгоритми побудови моделів

включають: предмети і явища / об'єкти / класи / елементи. МетаМоделі набувають різних форм і знаходять застосування в різних галузях, зокрема у вивченні викидів парникових газів, спричинених роботою агрегатів підприємств машинобудівного спрямування.

Метамоделювання – це спосіб об’єднання рішень та розширення можливостей в застосуванні. Вирішення проблеми краще здійснити на основі загального підходу, ніж обмежуватися окремими випадками. Хоча на початкових стадіях це вимагає більших трудовитрат і фінансових вкладень, але в перспективі це окупиться. При включенні в модель додаткових функцій необхідно узагальнити і включити в систему не спеціальну одиничну фічу (окремі специфічні можливості), а принципово змінити архітектуру, розширити клас її можливостей. У перспективі такий підхід доводить свою ефективність.

Однак, у процесі створення МетаМоделі важливо уникати її перевантаження, яке може призвести до надмірного ускладнення формалізації. Доцільніше розробити кілька окремих МетаМоделей і перейти на вищий рівень моделювання – створення Мета-МетаМоделі, яка об'єднує ці моделі в єдину систему.

Не варто надмірно захоплюватися універсальними рішеннями, важливо зберігати розумний баланс між складними універсальними підходами та простими специфічними розв’язками.

Потреба в багаторівневій системі існувала давно і поступово формувалася з часом. Так, моделі різних рівнів потрібні, але раніше програмного забезпечення, яке б працювало на рівні Метамоделей, а тим більше Мета-МетаМоделей, не існувало. Теорія, технології та софт для метамоделювання були недостатньо розвинені. Як відомо, слово "софт" походить від англійського software (програмне забезпечення), що протиставляється апаратному забезпеченню (hardware), а слово soft означає "м'який, програмно-реалізований". Згодом ситуація змінилася: тепер доступне не лише програмне забезпечення, але й ретельно розроблена парадигма.

Сучасне програмне забезпечення характеризується продуманою архітектурою та метамоделлю організації даних. У результаті всі завдання, що виникають, ефективно вирішуються в межах цього софту, а створені в ньому дані й моделі є прозорими для системи й легко піддаються інтерпретації.

Метамоделювання є фундаментальним принципом, давно відомим і описаним у філософії, математиці та природничих науках. Тепер воно отримало нову назву, а разом із нею – нове життя. Метамоделювання завжди було основою для інтеграції та узагальнення, навіть якщо в явній формі цей термін не використовувався.

Метамоделювання є ключовим і надзвичайно важливим етапом у тріаді Модель – Алгоритм – Програма, що забезпечує вирішення глобальних завдань інтеграції бізнесу та даних, а також створення довготривалих, складних і масштабованих систем, до яких відносяться і екосистеми.

УДК 004.5
С. Сучков
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СЕРВІСИ ДЛЯ МАШИННОГО ПЕРЕКЛАДУ КЛЮЧОВИХ СЛІВ ТА АНОТАЦІЇ НАУКОВИХ ТЕКСТІВ

UDC 004.5
S. Suchkov

SERVICES FOR MACHINE TRANSLATION OF KEYWORDS AND ANNOTATION OF SCIENTIFIC TEXTS

Існує кілька найбільш популярних сервісів для перекладу текстів:

– DeepL Translator (https://www.deepl.com/translator) – використовує нейронні мережі глибокого навчання для обробки природної мови та перекладу текстів між різними мовами. Сервіс спирається на великі мовні дані та алгоритми для моделювання мовних структур та контексту, що дозволяє досягати високої точності та природності перекладу;

– Google Translate (https://translate.google.com/) – використовує статистичні та нейронні методи обробки природної мови для перекладу слів, фраз та веб-сторінок між різними мовами. Сервіс інтегрує технології машинного навчання та великі обсяги даних для покращення якості перекладу;

– Microsoft Translator (https://translator.microsoft.com/) – надає функції перекладу тексту та мовлення в реальному часі. Також використовує нейронні мережі та методи машинного навчання для забезпечення перекладу з підтримкою багатьох мов, а також пропонує інтеграцію з іншими продуктами та сервісами Microsoft;

– Baidu Translate (https://fanyi.baidu.com) – розроблений китайським гігантом Baidu. Застосовує комбінацію статистичних методів та нейронних мереж для перекладу текстів та веб-сторінок різними мовами, прагнучи забезпечити високу точність та розуміння контексту перекладених матеріалів.

Для порівняльного аналізу чотирьох сервісів перекладу, які можна інтегрувати в систему, було розглянуто такі ключові аспекти: підтримка мов, функціональність і доступність. Результати порівняльного аналізу представлені у табл. 1.

Таблиця 1. Порівняння сервісів машинного перекладу тексту з метою інтеграції в систему, що розробляється

Критерій	DeepL Translator	Google Translate	Microsoft Translator	Baidu Translate
Підтримка мов	близько 30	понад 100	понад 70	понад 100
Наявність API	DeepL API	Google Cloud Translation API	Microsoft Translator Text API	Baidu Translate API
Вартість	Є версія безкоштовна	Є версія безкоштовна	Є версія безкоштовна	Є версія безкоштовна
Доступність API	Сервіс доступний	Сервіс доступний	Сервіс доступний	Сервіс доступний обмежено

Важливим критерієм є доступність сервісів, тому серед розглянутих найкращим вибором є Google Translate API. У випадку системи, що розробляється, було вирішено, що сервіс Google Translate якнайкраще підходить для реалізації прототипу системи.

УДК 004.4
В. Сухарський; М. Петрик, докт. фіз.-мат. наук; проф.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА ANDROID-ЗАСТОСУНКУ ДЛЯ УПРАВЛІННЯ СКЛАДОМ З ВИКОРИСТАННЯМ JAVA ТА SQL SERVER

UDC 004.4
V. Sukharskyi; M. Petryk, Dr; Prof.

DEVELOPMENT OF AN ANDROID APPLICATION FOR WAREHOUSE MANAGEMENT USING JAVA AND SQL SERVER

Сучасні інформаційні технології активно інтегруються у бізнес-процеси, автоматизуючи й оптимізуючи їх. Управління складом є однією з важливих сфер, яка вимагає надійних рішень для обліку товарів, моніторингу запасів та оптимізації логістики [1].

Метою наукового дослідження є розробка Android-застосунку для управління складом з використанням мови програмування Java та бази даних SQL Server. Такий застосунок забезпечить автоматизацію обліку, скорочення ручної праці та зменшення ризику помилок, пов’язаних з людським фактором.

Основними завданнями проєкту є:

1. Проєктування архітектури Android-застосунку.
3. Розробка інтерфейсу користувача з урахуванням принципів зручності (UI/UX).
4. Інтеграція бази даних SQL Server для забезпечення збереження та швидкого доступу до даних.
1. Тестування функціоналу додатка для забезпечення його стабільної роботи.
2. Розроблений застосунок має використовувати можливості мобільних пристроїв для доступу до даних у реальному часі, надаючи зручний інструмент для керування товарними запасами.
3. Розробка такого застосунку має велике практичне значення, оскільки дозволяє покращити якість управління складом, знизити витрати часу на облік і підвищити ефективність роботи підприємств [2].

Література

1. Курсова робота: «Розробка застосунків під ОС Андроїд». URL: https://ekmair.ukma.edu.ua.
2. Стаття: "Мобільні застосунки для сфери виробництва". URL: https://freshtech.global/ua/blog/mobile-apps-for-the-manufacturing-sector.

УДК 004.41
М. Франчевський; М. Петрик, д.ф.-м.н., професор
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА МОБІЛЬНОГО ДОДАТКУ ДЛЯ ПЕРСОНАЛІЗОВАНОЇ АНАЛІТИКИ ПРОГРЕСУ ЧИТАННЯ

UDC 004.41
M. Franchevskyy; M. Petryk, Dr., Prof.

DEVELOPMENT OF A MOBILE APPLICATION FOR PERSONALIZED ANALYTICS OF READING PROGRESS

Мобільні додатки стали важливими інструментами для підвищення продуктивності та особистого розвитку, а програми-трекери для читання дають користувачам можливість відстежувати свої звички, ставити цілі та аналізувати прогрес. Мобільний додаток, призначений для персоналізованої аналітики прогресу читання, є комплексним рішенням для відстеження читацьких сесій. Він дозволяє користувачам реєструвати активність, вимірювати такі показники, як швидкість та середня швидкість читання, витрачений час, а також аналізувати шляху до завершення книг. Інтегруючи внутрішні сервіси Firebase, додаток забезпечує безпечне зберігання та синхронізацію даних, дозволяючи користувачам мати доступ до своїх даних на різних пристроях. Використання архітектурного шаблону модель-вид-контролер (MVC) забезпечує модульність, зручність у супроводі і масштабованість, що робить його ефективною основою для реалізації даного додатку [1].

Шаблон MVC є фундаментальною основою архітектури додатку. Модель інкапсулює основну бізнес-логіку, керує зберіганням даних і взаємодією з Firebase. Вид відповідає за інтерфейс користувача, забезпечуючи інтуїтивно зрозумілий і візуально привабливий досвід, а контролер виступає в ролі посередника, з'єднуючи модель і вид.

Ключовою особливістю програми є її персоналізована аналітика, така як середня швидкість читання, приблизний час, необхідний для завершення книги, а також візуальні підсумки читацьких звичок. Завдяки оновленню даних у режимі реального часу через Firebase, користувачі отримують динамічну інформацію, яка адаптується до їхньої читацької поведінки [2]. Така персоналізація спрямована на посилення залученості користувачів і сприяння формуванню стійких читацьких звичок.

Використання шаблону MVC надає низку переваг, серед яких легше тестування та обслуговування, більша гнучкість у розширенні додатку без впливу на існуючий функціонал. Процес розробки також передбачає подолання таких викликів, як забезпечення безперебійної синхронізації даних та розробка модульної структури, яка підтримує масштабованість та адаптивність.

Таким чином, даний проєкт демонструє практичне застосування архітектури MVC для розробки надійного та зручного мобільного додатку. Поєднуючи інтуїтивно зрозумілий дизайн з детальною аналітикою, додаток надає користувачам змістовну інформацію про їхній прогрес у читанні, що робить його цінним інструментом для читачів.

Література

1. Freeman E., Robson E. Head First Design Patterns: Building Extensible and Maintainable Object-Oriented Software. 2nd ed. O'Reilly Media, 2021. 669 p.
2. Android Programming: The Big Nerd Ranch Guide / B. Sills et al. 5th ed. Addison-Wesley, 2022. 688 p.

УДК 004.41
А. Харлан; М. Петрик, д.ф.-м.н., професор
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЗРОБКА МОДУЛЬНИХ СИСТЕМ ЗВІТНОСТІ У ФІНАНСОВИХ ДОДАТКАХ З КОМПОНЕНТНОЮ АРХІТЕКТУРОЮ

UDC 004.41
A. Kharlan; M. Petryk, Dr., Prof.

DEVELOPMENT OF MODULAR REPORTING SYSTEMS IN FINANCIAL APPLICATIONS WITH COMPONENT ARCHITECTURE

Системи звітності є ключовим елементом фінансових додатків, оскільки вони забезпечують користувачів аналітичними даними для прийняття рішень, прогнозування та моніторингу. Впровадження компонентно-орієнтованої архітектури відкриває нові можливості для створення гнучких, масштабованих і налаштовуваних систем звітності, які відповідають індивідуальним потребам користувачів. Модульність стає основою для адаптації систем до нових вимог без необхідності перепроєктування базової інфраструктури.

Система звітності в рамках компонентної архітектури складається з окремих незалежних елементів, кожен з яких відповідає за певний функціонал: побудову діаграм, формування таблиць, реалізацію фільтрів даних, візуалізацію ключових показників тощо [1]. Всі ці елементи можуть бути організовані у вигляді бібліотеки готових модулів, що забезпечує їх багаторазове використання у різних частинах додатку. Такий підхід спрощує оновлення функціональності, оскільки заміна або вдосконалення одного модуля не потребує значних змін у роботі інших компонентів.

Динамічна побудова звітів є одним із ключових завдань. Користувачі повинні мати можливість самостійно налаштовувати структуру звітів, вибираючи потрібні компоненти з доступної бібліотеки. Наприклад, фінансовий аналітик може створити власний звіт із діаграмою грошового потоку, таблицею витрат за категоріями та графіком прогнозування доходів. Реалізація таких функцій можлива завдяки використанню React, що забезпечує високу швидкість візуалізації компонентів.

Захист даних у фінансових системах є одним із найважливіших аспектів, адже робота з конфіденційною інформацією вимагає високого рівня надійності. Використання компонентно-орієнтованої архітектури [2] створює умови для впровадження передових механізмів безпеки, таких як шифрування, контроль доступу та багаторівнева аутентифікація, безпосередньо на рівні окремих модулів. Цей підхід дозволяє ефективно ізолювати потенційні вразливості та забезпечувати баланс між гнучкістю системи й захистом даних.

Розробка модульних систем звітності відкриває нові горизонти для фінансових додатків, що поєднують високу продуктивність, інтуїтивно зрозумілий інтерфейс і адаптивність до зростаючих потреб користувачів. Такі рішення сприяють оптимізації операційних процесів для бізнесу та приватних осіб, стаючи інструментом для аналізу й прогнозування фінансової діяльності. Використання сучасних технологічних підходів у розробці подібних систем формує основу для фінансових додатків майбутнього, здатних відповідати викликам цифрової трансформації та запитам нової ери економіки.

Література

1. Healy Kieran. Data Visualization: A Practical Introduction. Princeton University Press, 2018. 296 p.
2. George T. Heineman, Ivica Crnkovic, Heinz G. Schmidt. Component-Based Software Engineering. Springer, 2008. 304 p.

УДК 004.45
В. З. Шеремета; Р. О. Жаровський, к.т.н
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ТЕСТУВАННЯ ВЕБ-ДОДАТКІВ РОЗРОБЛЕНИМИ НА ОСНОВІ SPRING BOOT ЗА ДОПОМОГОЮ TESTNG

UDC 004.45
V. Z. Sheremeta; R. O. Zharovskyi, Ph.D

TESTING WEB APPLICATIONS DEVELOPED ON SPRING BOOT WITH TESTNG

Тестування веб-додатків суттєво відрізняється від тестування класичних програмних продуктів. Однією з ключових відмінностей є технологічна основа. Класичні додатки зазвичай базуються на одній або спорідненій групі технологій, тоді як веб-додатки інтегрують різноманітні інструменти, такі як сервери баз даних, веб-сервери та сервери додатків. Веб-додатки працюють за принципом "запит-відповідь", де обробка дій користувача відбувається лише після запиту до сервера.

TestNG є потужним фреймворком для тестування, який добре інтегрується з веб-додатками, розробленими на основі Spring Boot. Spring Boot пропонує вбудовані інструменти для конфігурації та тестування, а TestNG дозволяє ефективно розширити ці можливості. Наприклад, за допомогою анотацій TestNG, таких як @BeforeSuite, @AfterTest, можна гнучко управляти життєвим циклом тестів, інтегруючи їх з контекстом Spring. Це забезпечує автоматичну ініціалізацію компонентів і перевірку залежностей під час тестування. Інтеграція TestNG з Spring Boot дозволяє створювати параметризовані тести, що корисно для перевірки поведінки додатка за різних умов. Наприклад, можна перевіряти роботу API-методів із різними наборами вхідних даних. Використання параметризації спрощує виконання таких тестів у кілька потоків, що значно прискорює процес. TestNG використовує анотації - спеціальні мітки у коді, що дозволяють розробникам вказувати конфігурацію тестів, установлювати порядок виконання, групувати тести, робити параметризовані тести та використовувати багато інших функціональних можливостей.

Написання тесту зазвичай складається з трьох етапів:

1. Написання бізнес-логіки свого тесту та вставка анотацій TestNG у свій код.
3. Додавання інформації про свій тест (наприклад, назва класу, групи, які ви хочете запустити тощо) у файл testng.xml або build.xml.
4. Запуск TestNG.

Для інтеграції TestNG із Spring Boot необхідно додати відповідні залежності до файлу *pom.xml* (у випадку використання Maven) або *build.gradle* (якщо використовується Gradle). Зазвичай це включає бібліотеки TestNG та Spring Boot Starter Test. Крім того, потрібно вказати спеціальні анотації Spring, такі як @SpringBootTest, що забезпечують завантаження контексту додатка перед запуском тестів.

Конфігурація тестового середовища у файлі *testng.xml* дозволяє чітко визначити класи або групи тестів, які будуть виконуватись. Завдяки цьому тестувальники можуть організовувати тести за різними критеріями, наприклад, для окремих REST API-методів або сервісів додатка.

Використання TestNG у поєднанні зі Spring Boot дозволяє створювати потужні й ефективні сценарії тестування для веб-додатків. Завдяки гнучким можливостям анотацій, підтримці залежностей між тестами, параметризації й паралельному виконанню, TestNG чудово підходить для перевірки складних багатокомпонентних систем, які характерні для сучасних веб-додатків.

УДК 004.41
В. Ямко; М. Петрик, д.ф.-м.н., професор
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПРОВАДЖЕННЯ ВЕКТОРНОГО ПОШУКУ У СИСТЕМІ ДОКУМЕНТООБІГУ

UDC 004.41
V. Yamko; M. Petryk, Doctor of Physical and Mathematical Sciences, Professor

IMPLEMENTATION OF VECTOR SEARCH IN A DOCUMENT MANAGEMENT SYSTEM

Системи управління документами пройшли довгий шлях від фізичних архівів до складних цифрових рішень. Сьогодні вони активно використовуються у багатьох сферах для зберігання, пошуку та аналізу даних. Однією з важливих сучасних тенденцій у цій галузі є інтеграція штучного інтелекту, зокрема методів роботи з векторними просторами та контекстного аналізу тексту.

Звичайний пошук за ключовими словами у текстових полях, таких як назва документа чи ім'я клієнта, має суттєві обмеження. Він часто не враховує семантичну близькість слів. Наприклад, запити «договір оренди» та «контракт на оренду» можуть бути релевантними, але традиційні методи пошуку цього не розуміють.

Для розв'язання цієї проблеми використовуються текстові ембедінги – числові векторні представлення тексту, які зберігають його семантичний зміст. Завдяки алгоритмам, як-от Word2Vec, GloVe, або сучасним моделям типу BERT і GPT, кожен текстовий фрагмент можна представити у вигляді багатовимірного вектора [1]. Векторні пошуки дозволяють знаходити документи за їх схожістю у векторному просторі, навіть якщо слова у запиті не повністю збігаються зі словами у документі.

Наприклад, запит може бути перетворений на вектор, який порівнюється із векторами, що представляють документи у базі. Це відкриває нові можливості для гнучкого пошуку:

- Розуміння синонімів та контексту.
- Пошук релевантних документів, навіть якщо формулювання у запиті відрізняється.
- Аналіз зв’язків між документами для рекомендації пов’язаних матеріалів.

У випадках, коли документ містить великий обсяг тексту, наприклад, десятки сторінок, пряме використання ембедінгів для всього тексту може бути неефективним. Виникає ризик втрати важливої інформації або збільшення обчислювальної складності.

Контекстне чанкування є підходом, який дозволяє розбивати великий текст на менші логічні частини (чанки), кожна з яких аналізується окремо [2]. Наприклад, документ можна поділити за абзацами, розділами або навіть реченнями, залежно від поставленої задачі.

Чанки обробляються за допомогою моделей, які створюють ембедінги для кожного фрагмента тексту. Це дозволяє:

- Проводити більш точний пошук, фокусуючись лише на релевантних частинах документа.
- Підвищувати ефективність обчислень за рахунок паралельної обробки фрагментів.
- Зберігати контекстні зв’язки між частинами документа, що важливо для відновлення повної картини під час пошуку.

Для зберігання та пошуку векторів у реальному часі використовуються спеціалізовані рішення, такі як Pinecone, Weaviate або MongoDB Atlas Search [3]. Вони підтримують:

- Зберігання багатовимірних векторів у базах даних.
- Пошук найближчих сусідів (nearest neighbor search) для швидкого знаходження релевантних записів.
- Інтеграцію з традиційними SQL або NoSQL системами для гібридного підходу до пошуку.

Такі системи можуть стати незамінними у великих організаціях, де пошук і аналіз документів є ключовою задачею. Завдяки ембедінгам і контекстному чанкуванню досягається новий рівень точності та швидкості обробки інформації.

Література

1. Hugging Face Transformers [Електронний ресурс] – Режим доступу до ресурсу: https://huggingface.co/docs/transformers/index
2. LangChain Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://python.langchain.com/docs/introduction/
3. MongoDB Atlas Search Documentation [Електронний ресурс] – Режим доступу: https://www.mongodb.com/docs/atlas/search/.

УДК 631.348.45: 534.13

Т. Семчишин; Я. Гурник; М. Сташків, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МОДАЛЬНИЙ АНАЛІЗ WAVE-ДИСКА ГРУНТООБРОБНОГО АГРЕГАТУ

UDC 631.348.45: 534.13

T. Semchyshyn; Ya. Hurnyk; M. Stashkiv, Ph.D, Assoc. Prof.

MODAL ANALYSIS OF THE WAVE-DISK OF A SOIL TILLING MACHINE

У сучасній практиці проектування різного роду конструкцій широко застосовується дослідження їх експлуатаційних характеристик на основі попередньо створених моделей.

У даній роботі подано результати модального аналізу цифрової моделі сучасного робочого органу ґрунтообробного агрегату - wave-диска, виконаного методом скінчених елементів з використанням програмного комплексу SOLIDWORKS.

Основні етапи підготовки цифрової моделі та деякі результати модального аналізу wave-диска показано на рис. 1.

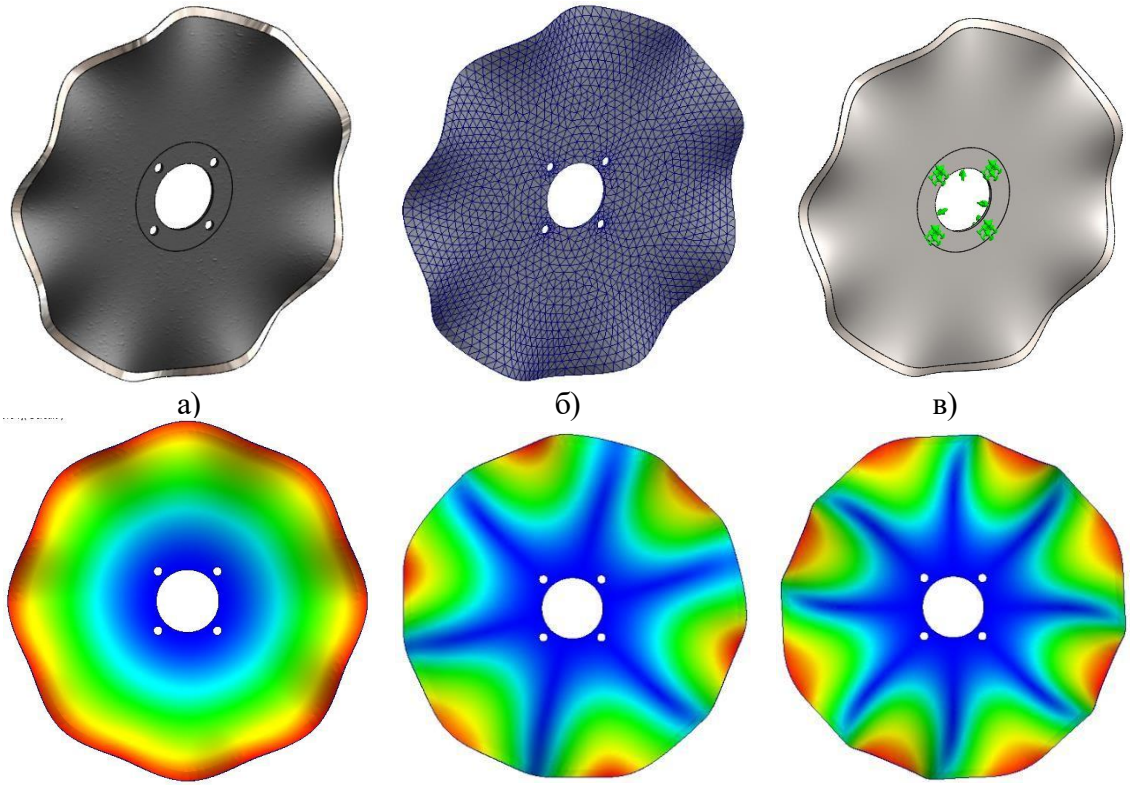


Рисунок 1. Етапи модального аналізу wave-диска:
а – твердотільна модель диска; б – сітка скінчених елементів; в – умови закріплення диска;
г – мода 75 Гц; д – мода 250 Гц; е – мода 456 Гц.

Твердотільна модель диска (рис. 1, а) створена на основі 3D-ескізів. Сітка скінчених елементів (рис. 1. б) побудована на основі змішаної кривизни з максимальним розміром елемента 14 мм. Тип закріплення диска по отворах – шарнір та защемлення (рис. 1, в).

За результатами модального аналізу встановлено, що найбільш критичною для досліджуваного wave-диска є мода з частотою 75 Гц (рис. 1, г), масова участь якої складає 78%. Цікавими є також моди з частотою 250 Гц (рис. 1, д) та 456 Гц (рис. 1, е), які хоч і не мають такої вагомої масової участі, але мають найбільші результуючі амплітуди.

УДК 631.348.45: 534.13
І. Борис; Р. Булаєнко; М. Сташків, к.т.н., доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

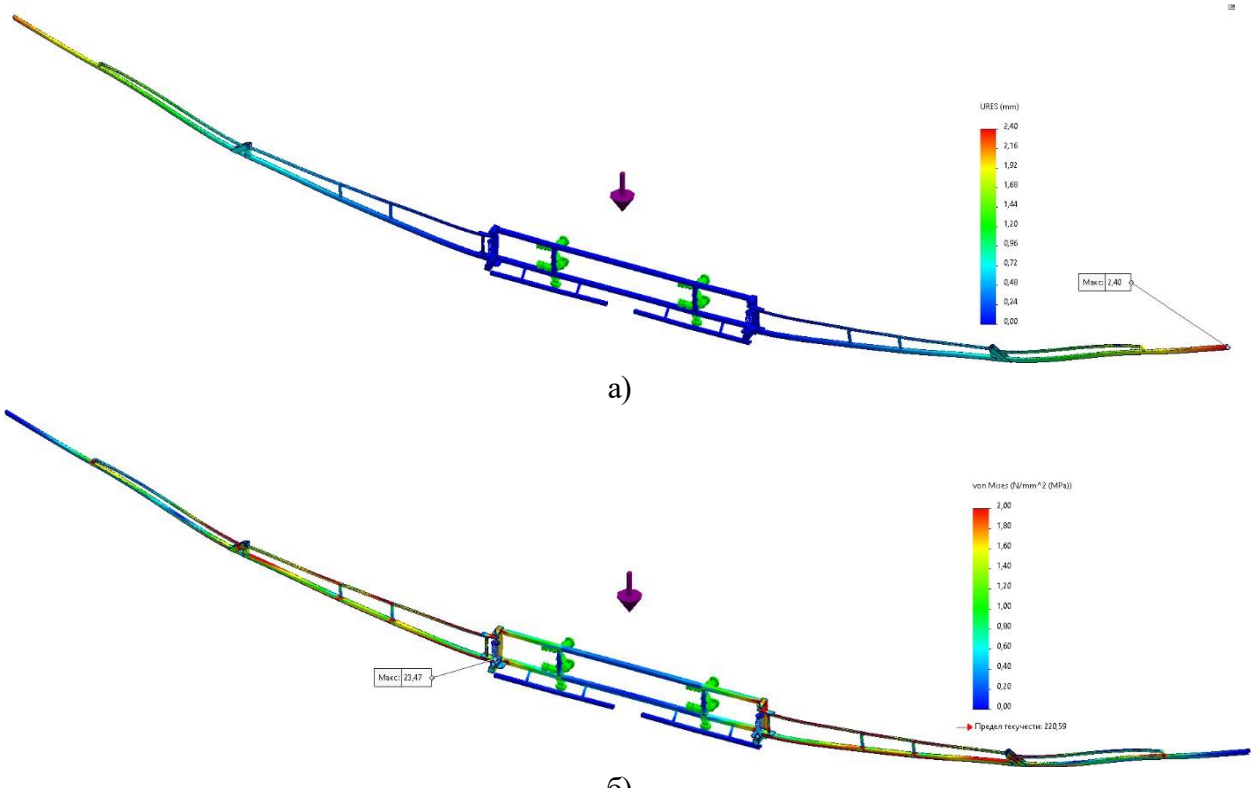
МОДЕЛЮВАННЯ ДИНАМІКИ ШТАНГИ НАЧІПНОГО ОБПРИСКУВАЧА

UDC 631.348.45: 534.13
I. Borys; R. Bulaienko; M. Stashkiv, Ph.D, Assoc. Prof.

SIMULATION OF THE MOUNTED SPRAYER BOOM DINAMICS

Створення комп'ютерних моделей механічних систем є основою комплексного аналізу складних несучих конструкцій при дослідження їхньої міцності, довговічності та надійності в експлуатаційних умовах. Основною проблемою такого підходу є якнайповніше відтворення у моделях властивостей реальної конструкції, параметрів її статичної поведінки, врахування особливостей зміни напружено-деформованого стану (НДС) у динамічній постановці задачі [1].

У даній роботі подано результати дослідження динаміки штанги начіпного обприскувача з шириною захвату 12 м на основі побудованої твердотільної моделі та попередньо проведеного у [2] модального аналізу штанги методом скінчених елементів за допомогою програмного комплексу SOLIDWORKS. За результатами модального аналізу штанги обприскувача отримано найбільш небезпечні частоти за основними осями штанги обприскувача: у напрямку повздовжньої осі (вісь X) ≈ 144,4 Гц; вздовж вертикальної поперечної осі (вісь Y) ≈ 7 Гц та вздовж горизонтальної поперечної осі ≈ 1,4 Гц. Динамічне навантаження задавали у вигляді збурення основи штанги з прискоренням 1 м/с^2 окремо по кожній з поперечних осей. Результати моделювання НДС штанги обприскувача при дії збурень у вертикальній площині показано на рис. 1.



а)

б)

Рисунок 1. НДС штанги оприскувача при дії збурень у вертикальній площині:
а – ізограма переміщень (мм); б – ізограма напружень (МПа)

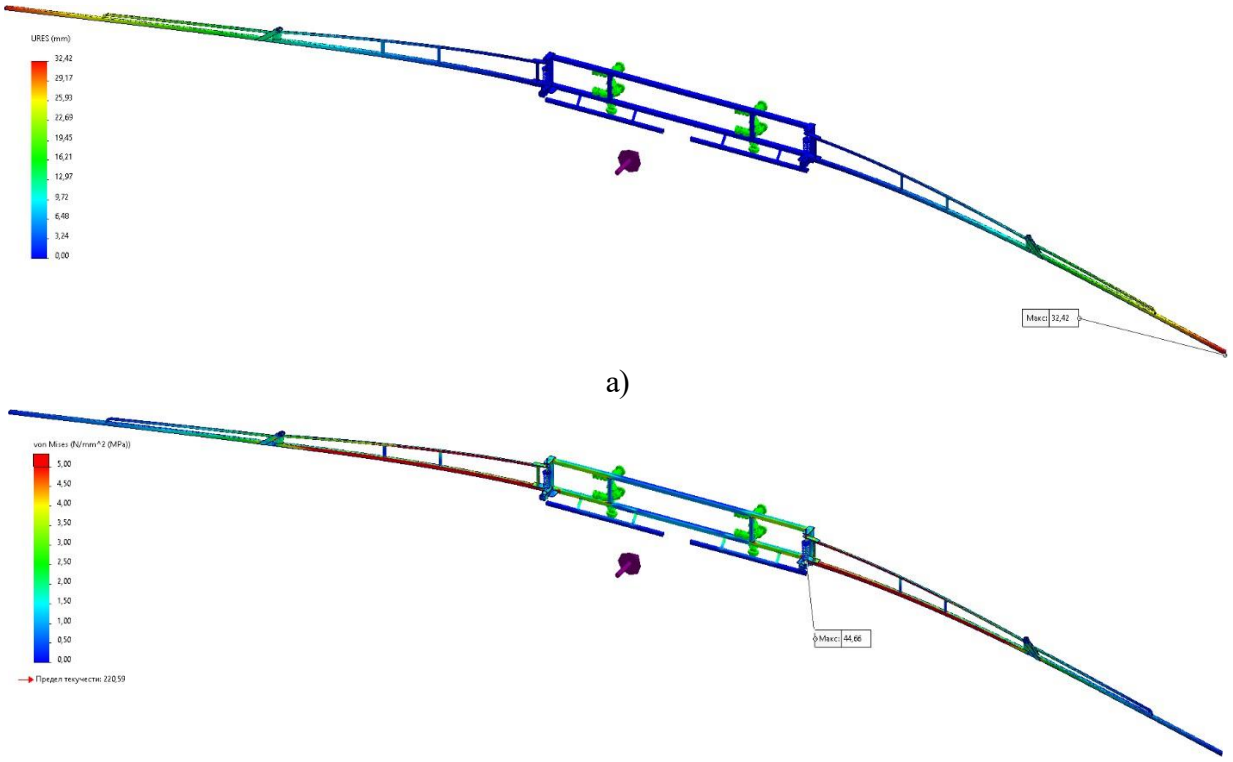


Рисунок 2. НДС штанги оприскувача при дії збурень у горизонтальній площині:
а – ізограма переміщень (мм); б – ізограма напружень (МПа).

Результати моделювання НДС штанги обприскувача при дії збурень у горизонтальній площині показано на рис. 2.

За отриманими результатами бачимо, що для обидвох досліджуваних випадків максимальні переміщення спостерігаються на вільних кінцях консольних частин штанги, а максимальні напруження виникають у місцях їх кріплення до центральної секції.

При побудові моделі штанги сітку скінчених елементів задано за замовчуванням з наступними параметрами: тип – сітка на основі змішаної кривизни з мінімальним та максимальним розміром елементів 4,65 мм та 93 мм відповідно; мінімальна кількість елементів в околі – 8, співвідношення збільшення розміру елемента – 1.4.

Література

1. Сташків М. Модальний аналіз штанги широкозахватного польового обприскувача / М. Сташків, М. Підгурський, І. Підгурський, І. Борис // Процеси, машини та обладнання агропромислового виробництва: проблеми теорії та практики: зб. тез доповідей міжнар. наук.-практ. конф. присвяченої 90-річчю від дня народження професора Рибака Тимофія Івановича та 60-річчю кафедри технічної механіки та сільськогосподарських машин / М-во освіти і науки України, Терн. націон. техн. ун-т ім. І. Пулюя [та ін]. – Тернопіль: ФОП Паляниця В. А., 2022. –с 145 - 146.
2. Борис І.М. Модальний аналіз штанги начіпного обприскувача / І.М. Борис, Р.О. Булаєнко, М.Я. Сташків // Матеріали V Міжнародної науково-практичної конференції "Підвищення надійності і ефективності машин, процесів і систем. Improving the reliability and efficiency of machines, processes and systems", Кропивницький: ЦНТУ, 2023. – С. 135- 137.

УДК 621.867.2
А. Д. Бобков
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

УДОСКОНАЛЕННЯ ШНЕКОВИХ ПОДАЮЧИХ МЕХАНІЗМІВ У ПРОЦЕСАХ РОЗЛИВУ НА ГЕРМЕТИЗАЦІЇ

UDC 621.867.2
A. D. Bobkov

IMPROVEMENT OF SCREW FEEDING MECHANISMS IN SEALING FILLING PROCESSES

У харчовій промисловості шнеки знайшли широке застосування [1]. Проте загалом ми найбільше зустрічаємо їх у якості елементів транспортуючих та змішуючих механізмів. Одним з елементів використання шнекових елементів є їх застосування в процесах наповнення та герметизації тари в харчовій промисловості. Розглянемо деякі машин, дамо їх коротку характеристику та опишемо основні способи уніфікації даних машин шляхом використання шнеків зі змінним кроком.

Автоматичні закаточні машини - це машини для герметизації металевої і скляної тари з готовими харчовими продуктами [2]. В їх конструкції, пластинчастий транспортер і шнек входять до складу механізму прийому банок, він виставляє їх на рівну відстань і передає на механізм подачі кришок. Однією з таких машин є Б4-КЗК-75. Дане обладнання виконує роботу до якої постають підвищені вимоги щодо контролю виробництва. До герметичності закатаних банок потрібно ставитись відповідально, оскільки потрапляння кисню під не щільну кришку спричинить розвиток мікроорганізмів, псування продукту і як наслідок – серйозні харчові отруєння. Проте у даній машині шнек виготовлений з суцільного куска пластмаси і не його використання призводить до частого бою скляної тари.

Наповнювачі, наприклад, ДН1 [2]. Влаштовано цей наповнювач таким чином: механізм прийому подає банки на наповнення з цехового транспортера. Порожні банки надходять на транспортер приймального пристрою і подаються по шнеку, який розділяє їх за кроком і передає на приймальну зірку, а з неї банки потрапляють на столики каруселі. Далі вона обертається і підіймаються до дозатора.

В даному випадку шнек виконує подачу склотари на своє місце, а саме, барабанну (карусельну) підставку, де і відбувається її подальше наповнення сиропом, маринадом, томатом, олією і т. д. Пропоную зупинитись та більш детально розглянути саме ці дві вищезазначені машини. На мою думку, вони мають найбільший потенціал для вдосконалення. Звичайно, згадані машини і механізми експлуатуються вже не один десяток років і дуже добре себе зарекомендували. Проте, технічний прогрес ніколи не повинен стояти на місці. Шнеки вище перерахованих машин об’єднує те, що виготовлені вони або зі сталі, або з жорсткої пластмаси. Саме через жорсткість і виникають певні недоліки під час роботи, такі як, наприклад, пошкодження і подрібнення сировини, яка контактує зі шнеком (небажане явище для всіх типів машин, окрім пресів і дробарок), або ж у випадку з машиною для герметизації тари Б4-КЗК-75 та наповнювачем ДН1, це биття склотари.

Чітко визначеної цифри, який саме відсоток биття тари, немає. Проте, проаналізувавши інші машини, їх умови роботи, особливості конструкції і продуктивність, можна з’ясувати, що це приблизно 5% від загального обсягу виробництва продукції. Тому, доцільно було би внести в конструкцію певні зміни, а саме, замість жорсткого шнека використати гнучкий полімерний зі змінним кроком, тим самим це дозволить наявні недоліки якщо не усунути повністю, то хоча б знизити приблизно до 2 відсотків биття тари. Варто одразу зазначити, що сама концепція виготовлення шнека з полімерного матеріалу не нова, і вже існує, проте, саме машини для герметизації тари та наповнювачі типу ДН1 ще досі експлуатуються із жорсткими шнеками. Якщо замінити їх на гнучкі полімерні, це не вплине негативно на роботу і розставлення банок по місцях буде виконуватися як і

раніше, тому що крок витків шнека не зміниться, а відсоток биття тари знизиться, через те що банки контактуватимуть з набагато м’якшим матеріалом.

Література

1. Заплетніков І.М., Мирончук В.Г., Кудрявцев В.М. Експлуатація і обслуговування технологічного обладнання харчових виробництв [Текст] / Заплетніков І.М., Мирончук В.Г., Кудрявцев В.М.- Київ: Центр навчальної літератури, 2019. – 344 с.
2. Механізація переробки і зберігання плодоовочевої продукції: Навч. посібник/ О. В. Дацишин, О. В. Гвоздєв, Ф. Ю. Ялпачик, Ю. П. Рогач. - К.: Мета, 2003. - 288 с.10. - 736 с.

УДК 621.396.67
Н. Б. Войцеховський; Ю. Б. Паляниця, к.т.н, доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОБҐРУНТУВАННЯ МЕТОДУ ПЕРЕДАЧІ ІНФОРМАЦІЙНОГО СИГНАЛУ ДЛЯ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ СУПУТНИКОВИХ СИСТЕМ ЗВ'ЯЗКУ

UDC 621.396.67
N. B. Voytsekhovskyi; Y. B. Palyanytsia, PhD

JUSTIFICATION OF THE METHOD OF INFORMATION SIGNAL TRANSMISSION TO INCREASE THE BANDWIDTH OF SATELLITE COMMUNICATION SYSTEMS

Супутникові телекомунікаційні системи класифікуються за типом орбіт, на яких розташовані супутники, що визначає такі параметри, як покриття, затримка сигналу, енергетичні витрати та кількість супутників для глобального покриття. Основними типами орбіт є низька (LEO), середня (MEO) та геостаціонарна (GEO), кожна з яких має унікальні характеристики та сферу застосування.

Таблиця 1

Параметр	Тип орбіти	Геостаціонарна орбіта (GEO)	Низька орбіта (LEO)	Середня орбіта (MEO)
Висота орбіти (км)	Геостаціонарна	35,786	500-2,000	2,000-35,786
Період обертання (годин)	Геостаціонарна	24	1-2	2-12
Швидкість орбітального руху (км/с)	Геостаціонарна	3.07	7.9-8.5	3.5-6
Кут нахилу орбіти	Геостаціонарна	0°	0-90°	0-90°
Розподіл смуг частот	Супутникові канали	C, Ku, Ka, L	L, S, Ku	C, Ku, Ka
Пропускна здатність каналу (Гбіт/с)	Супутникові канали	10-50	0.1-2	1-10
Максимальна затримка сигналу (мс)	Супутникові канали	240-300	10-50	100-250
Мобільність (переміщення супутників)	Геостаціонарна	Немає	Має	Має

Пропускна здатність супутникових систем зв’язку визначається низкою параметрів, серед яких частота сигналу, ширина смуги пропускання, тип модуляції, співвідношення сигнал/шум (SNR) та коефіцієнт помилок на біт (BER). Частотний спектр, наприклад, у Ka- та Ku-діапазонах, забезпечує високу швидкість передачі даних завдяки широкій смузі пропускання, хоча й залежить від погодних умов. Різні види цифрової модуляції, такі як QPSK та 16-QAM, дозволяють оптимізувати ефективність передачі, підвищуючи кількість бітів на символ, але вимагають вищого SNR.

Застосування сучасних технологій, таких як адаптивна модуляція і кодування (ACM) та мультиплексування з ортогональним частотним поділом (OFDM), є ключем до підвищення ефективності використання частотного спектра. ACM автоматично змінює параметри залежно від умов каналу, забезпечуючи надійність передачі навіть у складних умовах. OFDM, у свою чергу, дозволяє зменшити вплив інтерференції і більш ефективно використовувати спектр.

У випадку квадратурної амплітудно-фазової модуляції (QAM), кількість бітів, переданих за символ, визначається так:

$$R_{b/s} = \log_2(M) \quad (1)$$

Для оцінки впливу ширини смуги пропускання, типу модуляції та інших параметрів було проведено порівняльний аналіз з використанням теоретичних моделей. Наприклад, збільшення ширини смуги пропускання вдвічі дозволяє подвоїти пропускну здатність, а використання модуляції 64-QAM – значно підвищити швидкість передачі даних порівняно з QPSK за умови високого співвідношення сигнал/шум (Рис. 1).

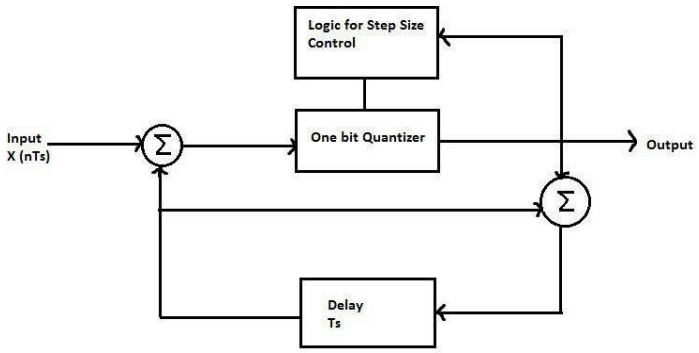


Рисунок 1. Схема технології адаптивної модуляції і кодування

Таким чином, оптимізація пропускної здатності супутникових систем зв'язку є комплексним завданням, що включає вдосконалення методів модуляції, кодування і використання частотного ресурсу. Формула пропускної здатності каналу, яка враховує ширину смуги частот і співвідношення сигнал/шум, є ключовою для проєктування ефективних супутникових систем.

Формула для пропускної здатності каналу в разі використання модуляції виглядає так:

$$C = B \cdot \log_2(1 + \frac{S}{N}) \quad (2)$$

Ця формула добре ілюструє залежність пропускної здатності від ширини смуги пропускання і якості сигналу.

Література

1. Methods of Processing Cyclic Signals in Automated Cardiodiagnostic Complexes. IV Lytvynenko, A Horkunenko, O Kuchvara, Y Palaniza ICTES, 116-127
2. Artificial Intelligence Based Emergency Identification Computer System D Velychko, H Osukhivska, Y Palaniza, N Lutsyk, Ł Sobaszek Advances in Science and Technology. Research Journal.
3. Method, Algorithm and Computer Tool for Synphase Detection of Radio Signals in Telecommunication Networks with Noises L Khvostivska, M Khvostivskyi, I Dediv, V Yatskiv, Y Palaniza.

УДК 612.741.1:519.218
Л. Дедів, канд. техн. наук, доц.; В. Варварчук; С. Ковалик
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПОВЕРХНЕВИХ ЕЛЕКТРОМІОГРАФІЧНИХ СИГНАЛІВ ДЛЯ ЗАДАЧІ БІОПРОТЕЗУВАННЯ

UDC 612.741.1:519.218
L. Dediv, Ph.D, Assoc. Prof.; V. Varvarchuk; S. Kovalyk

MATHEMATICAL MODELING OF SURFACE ELECTROMYOGRAPHIC SIGNALS FOR THE PROBLEM OF BIOPROSTHESIS

Сьогодні біонічний протез кисті руки з технічної точки зору є витвором мистецтва, однак залишається інструментом, призначеним для максимально можливої компенсації функцій втраченої кінцівки. Для керування цим інструментом потрібна інформація, при чому в достатній кількості, оскільки за її недостатності пацієнт не зможе використовувати в необхідній мірі функціонал доступних можливостей протеза. Сьогодні особлива увага приділяється вивченню біоелектричних процесів, що відбуваються під час скорочення м'язових волокон. Виявлені закономірності дозволяють використовувати ці сигнали для керування електричними двигунами протезів. Власне вибір джерела інформації безпосередньо впливає те, якими засобами цю інформацію буде отримано. На даний момент з метою керування протезами верхніх кінцівок розглядають використання біоелектричних сигналів скелетної мускулатури, периферичних нервів та структур головного мозку.

На основі аналізу конструкцій найпоширеніших біонічних протезів та особливостей реєстрації біосигналів для їхнього керування встановлено, що більшість з них працюють на основі відбору та опрацювання поверхневих електроміографічних сигналів, що пояснюється простотою самих електродів, методів реєстрації, неінвазивністю та низькою вартістю. Однак, для забезпечення надійного контролю протезом та можливості виконання великої кількості захватів і рухів необхідним є розроблення чи обґрунтування вибору адекватної математичної моделі таких сигналів і методу їхнього опрацювання для формування відповідних сигналів керування елементами протеза. Власне на основі моделі та методу опрацювання можливим стає розроблення алгоритмів керування виконавчими елементами протеза і, за можливості, розширення його функціональних можливостей. Таким чином, задача обґрунтування вибору математичної моделі та методу опрацювання поверхневих електроміографічних сигналів для задачі біопротезування є актуальною.

Проаналізовано відомі математичні моделі та методи опрацювання електроміографічних сигналів, зокрема розглянуто подання такого типу сигналів як стаціонарного випадкового процесу а також методів спектрального та кореляційного аналізу. Встановлено, що така модель має обмеження стосовно аналізу часової структури сигналів та присутньої повторюваності.

Для цього можливим є застосування окремого класу стаціонарних процесів, а саме кусково стаціонарних випадкових процесів. При цьому ділянки електроміографічного сигналу, на яких присутні ознаки виконання окремих рухів пальців, вважатимуться стаціонарними з відмінними параметрами та характеристиками для таких же ділянок при виконанні інших типів рухів. В такий спосіб виправдано застосування до опрацювання електроміографічних сигналів методів теорії стаціонарних випадкових процесів.

УДК 661.831-073.97-71
В. Дозорський, канд. техн. наук, доц.; О. Дозорська, канд. техн. наук; Г. Франчевська; М. Гункевич
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

МЕТОД ТА ЗАСІБ РЕЄСТРАЦІЇ БІОПОТЕНЦІАЛІВ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НЕЙРОФУНКЦІОНАЛЬНИХ ДОСЛІДЖЕНЬ

UDC 661.831-073.97-71
V. Dozorskyi, Ph.D, Assoc. Prof.; O. Dozorska, Ph.D; H. Franchevska; M. Hunkevych

METHOD AND MEANS OF BIOPOTENTIALS REGISTRATION TO INCREASE THE EFFICIENCY OF NEUROFUNCTIONAL RESEARCH

Серед методів нейрофункціональних досліджень та діагностики метод електроенцефалографії (ЕЕГ) є найбільш складним в плані проведення та забезпечення однорідності статистичного матеріалу.

Застосування методу ЕЕГ дає можливість виявляти осередки патологічної активності, оцінювати функціональну роботу та навантаження на мозок, а також досліджувати та виявляти нейродегенеративні розлади головного мозку. Крім цього, ЕЕГ широко застосовується для реалізації технології інтерфейсу мозок-комп'ютер, а також дослідження нейрофідбека, який є окремим прикладом біологічного зворотного зв'язку. Крім того, на сьогоднішній день активний розвиток отримали такі напрямки як нейрогеймінг, нейромаркетинг та інтегративне використання нейрогарнітур разом із технологіями віртуальної та доповненої реальності.

В ході проведених досліджень встановлено, що якість відібраних сигналів ЕЕГ а в кінцевому випадку і результат експериментального дослідження залежить від умов відбору, зокрема якості накладання електродів, контакту їх із шкірою поверхні голови, дотримання місць накладання електродів тощо. При цьому встановлено, що відомі поширені сьогодні на ринку медичного обладнання шоломи та електроди для реєстрації ЕЕГ мають багато недоліків. Зокрема у випадку використання шоломів із силіконових чи гумових трубок, до яких вручну кріпляться електроди, потребує дуже багато часу для правильного одягання шолома та розміщення на ньому електродів (кожен електрод встановлюється вручну, а таких електродів може бути більше 16; також потрібно окремо контролювали лікарю якість накладання кожного окремого електрода, якість контакту із поверхнею голови, наносити контактний гель тощо). У випадку ж використання силіконових чи гумових шапочок із наперед встановленими електродами є некомфортним для пацієнтів при довготривалому ЕЕГ дослідженні. Також в останньому випадку може виникати потіння шкіри голови та зменшення міжелектродного опору і подавлення корисних сигналів, чи перетискання кровоносних судин шкіри, потертості. Основним же недоліком електродів для відбору сигналів ЕЕГ є або необхідність використання спеціальних контактних гелів, або змочування спеціальними розчинами контактної поверхні електродів або видалення волосяного покриву голови. Все це створює значний дискомфорт для пацієнтів.

Таким чином, актуальність роботи визначається необхідністю удосконалення існуючих або розроблення нових методів та засобів реєстрації ЕЕГ сигналів через наявність у існуючих і поширених на ринку медичної техніки систем значних недоліків, пов'язаних із недосконалістю електродів для реєстрації електроенцефалографічних сигналів, недосконалістю конструкцій шоломів для фіксації електродів і складністю точного їхнього позиціонування на поверхні голови пацієнтів, схемотехнічних рішень виконання блоків підсилення біопотенціалів.

УДК 612.741.1
В. Дозорський, канд. техн. наук, доц.; Р. Лупой; О. Плавуцький; Р. Кохан
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОСТІ ТА НАДІЙНОСТІ БІОНІЧНИХ ПРОТЕЗІВ КИСТІ РУКИ

UDC 612.741.1
V. Dozorskyi, Ph.D, Assoc. Prof.; R. Lupoi; O. Plavutskyi; R. Kohan

INCREASING THE FUNCTIONALITY AND RELIABILITY OF BIONIC HAND PROSTHESES

Протези рук використовуються людьми, які перенесли певний рівень ампутації руки. Серед них є значна частка людей з трансрадіальною ампутацією, тобто втраченою кінцівкою нижче ліктя. Існує ряд типів протезів рук, зокрема протези, що керуються рухами тіла, і міоелектричні протези. При цьому такі протези різняться між собою за функціональними можливостями і складністю їх керування. Під функціональністю виробу розуміють в загальному випадку можливість забезпечення виконання ним необхідних функцій. Коли мова йде про протез кисті руки, то функціональний протез мав би забезпечувати виконання усіх функцій здорової руки людини. Сюди можна віднести виконання усіх природних рухів пальців при виконанні жестів та захватів, контролю швидкості цих рухів тощо. І в цьому плані сучасні протези мають значні обмеження, оскільки дуже складно (чи практично неможливо) технічно реалізувати таку біомехатронну систему використовуючи сучасні досягнення науки і техніки та наявну матеріальну та компонентну базу. Так, важко забезпечити необхідну вагу конструкції, в якій для забезпечення потрібної кількості виконуваних рухів та захватів потрібно помістити значну кількість елементів приводу та відповідних контролерів. Також особливо складною є задача забезпечення надійного керування таким протезом на основі біосигналів. Останнє обмеження якраз і є основною причиною зниження функціональності існуючих біонічних протезів кисті руки.

З біомеханічної точки зору людська рука має 27 ступенів свободи, але комерційно доступні протези рук зазвичай мають лише 2–6 ступенів. Крім того, було доведено, що більшість рухів руками можуть бути реалізовані лише двома основними компонентами синергії. Крім того, вища кількість ступенів свободи накладає на користувача значне навантаження. Таким чином, стратегії контролю повинні віддавати пріоритет зменшенню кількості ступенів свободи відносно ідеальної конфігурації руки людини. Тому важливим стає питання підвищення функціональності біонічних протезів за рахунок розроблення оптимальної їхньої конструкції за можливості із зниженням кількості ступенів свободи та спрощенням способів керування таким протезом. Також за рахунок використання меншої кількості складових елементів зросте й надійність такого протеза.

На противагу відомим конструкціям біонічних протезів запропоновано використати конструкцію ендоскелета. В цьому випадку на його елементах можна розмістити силіконові вставки, які були б м’якими та надавали б естетичного і природного вигляду протезу, а також в середині цих вставок можна було б розмістити давачі тактильних відчуттів. Такий протез буде легшим, матиме меншу кількість елементів та з’єднань, тобто буде більш надійним. Також можливим стає зменшення кількості ступенів свободи при виконанні тих самих захватів, що і прототипи, що спростило б керування таким протезом. Тобто, при такому підході пропонована конструкція протеза була б більш функціональною та надійною.

УДК 615.823
Л. Дедів, канд. техн. наук, доц.; В. Куц; Д. Підлужний
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСОБИ АПАРАТУРНОГО МАСАЖУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАБІЛІТАЦІЇ ХВОРИХ З ВАДАМИ ОПОРНО-РУХОВОГО АПАРАТУ

UDC 615.823
L. Dediv, Ph.D, Assoc. Prof.; V. Kuts; D. Pidluzhny

MASSAGE EQUIPMENT TO INCREASE THE EFFICIENCY OF REHABILITATION OF PATIENTS WITH MUSCULOSKELETAL DISORDERS

Лікувальний масаж є ефективним лікувальним та реабілітаційним методом, що застосовується з метою нормалізації функцій організму при різних захворюваннях та ушкодженнях. Популярність лікувального масажу постійно зростає. Його використовують у хірургії, травматології, терапії, гінекології, невропатології, кардіології, ендокринології, спортивній медицині та реабілітації. Найбільш поширеним є класичний масаж, оскільки має різноманітні прийоми, дозволяє широко варіювати дозування, візуально і відчутно контролювати точність виконання прийомів і оцінювати їх результати тощо. Ручний масаж має перевагу перед апаратним і комбінованим, так як він може бути використаний не тільки в палаті, масажному кабінеті, а й удома, у ванній тощо, а також у вигляді самомасажу. Апаратний метод масажу використається як додатковий. Залежно від різновидів може виконуватись як шляхом безпосереднього контакту зі шкірою, так і через повітряне або водне середовище. Серед різновидів апаратного методу масажу найбільшого поширення набули вібраційний, гідро- та пневматичний масаж. У лікувальній практиці застосовується і електростимуляційний, ультразвуковий масаж та ін. Апаратні види масажу, як і ручний масаж, можуть використовуватися в процесі сегментарного, точкового, періостального та інших видів масажу.

Також, на відміну від ручного масажу, в технічних засобах для апаратурного масажу зачасту реалізуються лише обмежені прийоми, наприклад вібрації в комплексі із прогріванням. Також технічні засоби мають обмеження щодо областей впливу. Поширеними сьогодні на ринку медичної техніки є два типи масажерів. Перший тип виконано у вигляді пояса з елементами створення ефекту масажу. Другий тип включає масажери у вигляді накидок змінної форми, що можуть розміщуватись горизонтально поверх матраца для проведення масажу лежачи, або на кріслі у вигляді накидки, або у вигляді матраців, всередині яких розміщуються масажні елементи. Можуть бути передбачені функції підігріву, регулювання сили впливу, частоти вібрацій тощо.

В роботі проводиться обгрунтування методу та розроблення засобу проведення апаратурного масажу для підвищення ефективності реабілітації хворих з вадами опорно-рухового апарату.

Література

1. В.М. Мухін. Фізична реабілітація в травматології : монографія. Л., ЛДУФК, 2015. 428 с.
2. Гевко О.В., Дозорський В.Г., Дедів Л.Є., Дедів І.Ю., Дозорська О.Ф. Структурний синтез вібромасажної апаратури. ПЕРСПЕКТИВНІ ТЕХНОЛОГІЇ ТА ПРИЛАДИ. Луцьк, 2022. Випуск 20. С. 23-31.
4. .В. Вакуленко, Л.О. Вакуленко, О.В. Кутакова, Г.В. Прилуцька. Лікувально-реабілітаційний масаж : навч. посіб. К., ВСВ «Медицина», 2020. 568 с.

УДК 621.395.625.6
І. Дедів, канд. техн. наук, доц.; М. Пліс; В. Степанов; С. Брегін; В. Лотоцький
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАДАЧА ОЦІНЮВАННЯ РОЗБІРЛИВОСТІ МОВИ ДЛЯ ПОКРАЩЕННЯ ЯКОСТІ СИСТЕМ ГРОМАДСЬКОГО ОПОВІЩЕННЯ

UDC 621.395.625.6
I. Dediv, Ph.D, Assoc. Prof.; M. Plis; V. Stepanov; S. Bregin; V. Lototskyi

THE TASK OF SPEECH INTELLIGIBILITY ASSESSMENT FOR IMPROVING THE QUALITY OF PUBLIC ANNOUNCEMENT SYSTEMS

Сьогодні в Україні, в умовах війни, особливо гостро стоїть питання своєчасного оповіщення громадян про ймовірні небезпечні непередбачувані ситуації, зокрема повітряні ракетні атаки, обмеження руху та пересування через ймовірності вибухів зокрема, виникнення пожеж чи значні викиди шкідливих речовин в повітря, воду тощо. З цією метою використовуються системи громадського оповіщення, що є організованими спеціалізованими системами, які призначені для своєчасної передачі певних сигналів та інформаційних повідомлень стосовно цивільного захисту до відповідних органів влади, підприємств, організацій, установ та населення. Ці системи включають в себе технологічні підходи та способи оповіщення, спеціалізоване обладнання, прилади та канали зв'язку. Метою роботи систем оповіщення є забезпечення максимально швидкого інформування якомога більшої кількості людей про безпосередню небезпеку. Громадські (публічні) оповіщення здійснюються дистанційно шляхом використання електромеханічних сирен (зовні), мереж мовлення всіх частотних типів, систем телевізійного та мобільного зв'язку. Основна функція, яку виконує система оповіщення в аварійній ситуації, – це трансляція мовних повідомлень, спрямованих на запобігання паніці людей, та передача інформації про напрям руху для евакуації.

В поширених сьогодні варіантах побудови систем оповіщення як основний інформаційний сигнал про виникнення надзвичайної ситуації використовується мовний чи голосовий сигнал, що являє собою голосове повідомлення, яке повинне бути однозначно донесене та сприйняте людьми чи персоналом, що перебуває в зоні дії цієї системи. При цьому, часто для підвищення ефективності технічних засобів оповіщення, зокрема підвищення випромінюваної гучномовцями потужності, проводиться попередня обробка таких сигналів, зокрема фільтрація, що передбачає подавлення високочастотних та низькочастотних складових сигналу-повідомлення та підсилення середньочастотних складових. Відповідно, часто системи оповіщення транслюють готосові повідомлення в ділянці саме середніх частот голосового сигналу. Але це в свою чергу разом із впливом зовнішніх факторів значно впливатиме на якість того голосового повідомлення, яке будуть чути люди, для яких воно транслюється. Ці і додаткові фактори значно спотворюватимуть сигнали повідомлення та вливатимуть на степінь сприйняття оточуючими людьми таких повідомлень від системи оповіщення.

В цьому плані важливим є контроль якості роботи системи з можливістю коригування параметрів чи характеристик голосових повідомлень для забезпечення надійного та однозначного їхнього сприйняття оточуючими людьми. Власне для цього і потрібно розробити новий чи обґрунтувати вибір відомого методу оцінювання розбірливості мови.

УДК 621.395.625.6
І. Дедів, канд. техн. наук, доц.; В. Шмир; М. Олійник
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ВПЛИВ ЕКЗОГЕННИХ ФАКТОРІВ НА ЕФЕКТИВНІСТЬ ОПТОВОЛОКОННИХ ЛІНІЙ ЗВ'ЯЗКУ

UDC 621.395.625.6
I. Dediv, Ph.D, Assoc. Prof.; V. Shmyr; M. Oliynyk

INFLUENCE OF EXOGENIC FACTORS ON THE EFFICIENCY OF FIBER OPTIC COMMUNICATION LINES

Сьогодні відбувається стрімкий перехід на використання цифрових оптоволоконних ліній зв’язку. Однак, специфічність оптоволоконного кабелю зв'язку полягає не тільки в особливостях поширення інформаційного сигналу, а й у конструкції самого волокна, критичності його до різноманітних впливів і навантажень. Оптичне волокно чутливе до впливів екзогенних факторів, зокрема вологи, температури, радіації, зовнішніх електромагнітних впливів, електротермічної деградації, механічних впливів. Всі ці фактори призводять до збільшення згасання, а також на поверхні волокна з'являються мікротріщини і відбувається його руйнування.

Вивчення питань впливу екзогенних факторів на передавальні параметри оптичного волокна є актуальним при проектуванні високоефективних оптоволоконних ліній зв’язку. Так, сьогодні в Україні починають стрімко розвиватися технології застосування оптоволокон для організації керування БПЛА, зокрема FPV дронами. При цьому в конструкції такого БПЛА розміщується котушка з оптоволоконним кабелем, який в процесі руху дрона розмотується. Однак, мало дослідженим є питання втрат в оптоволокні, яке є змотане в бухті. Так, зазвичай оптоволоконний кабель є розмотаний та спеціальним чином прокладений і має мінімальну кількість згинів, а самі згини є зачасту незначними. Однак, коли такий кабель знаходиться змотаним в бухні, то радіус згину для використання для керування FPV дроном є досить малим і відповідно вплив на передачу даних може бути відчутним. Також, враховуючи те, що оптоволокно буде розмотуватись від дрона у відкритому просторі, на нього будуть діяти такі додакові зовнішні фактори, як навколишня температура, вологість, тиск повітря, радіаційні впливи тощо.

Все це може вносити додаткові обмеження на використання цієї технології для керування FPV дроном, або потребувати внесення певних коректив чи змін у способи модуляції і перетворення сигналів.

Література

1. Senior, John M.; Jamro, M. Yousif (2009). Optical fiber communications: principles and practice. Pearson Education. pp. 7–9. ISBN 978-0130326812.
2. Lee, Byoungho (2003). «Review of the present status of optical fiber sensors». Optical Fiber Technology. 9 (2): 57–79. Bibcode:2003OptFT...9...57L. doi:10.1016/s1068-5200(02)00527-8
3. Posinna, Mariddetta (April 1, 2014). »different types of fiber optic cables». HFCL. Archived from the original on April 20, 2016. Retrieved April 11, 2016.
5. Large, David; Farmer, James (January 13, 2004). Modern Cable Television Technology. Elsevier. ISBN 978-0-08-051193-1.

УДК 622.691.4
І. Ярема, к.т.н., доц.; І. Зелінський, к.т.н., доц.; Ю. Наконечний; А. Закамарко
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ДОСЛІДЖЕННЯ ЗНОШУВАННЯ ПОЛІМЕРНИХ КОНСТРУКТИВНИХ МАТЕРІАЛІВ

UDC 622.691.4
I. Yarema, Ph.D., Assoc.Prof; I. Zelinsky, Assoc.Prof; Y. Nakonechnyi; A. Zakamarko

RESEARCH ON WEAR OF POLYMER CONSTRUCTIVE MATERIALS

В сучасному машинобудуванні широко застосовуються полімерні конструктивні матеріали, які працюють в умовах ударно-абразивного навантаження. Тому актуальною є задача вивчення та дослідження впливу ударних навантажень на зносостійкість пластмас, наприклад, деяких термопластів групи «поліамідів».

Дослідження проводилися на зразках, виготовлених методом литва під тиском на термопластавтоматах. Зразки попередньо піддавались ударним циклічним деформаціям з частотою та енергією удару, наближеним до реальних умов експлуатації, а потім проводились дослідження їх ударно-абразивного зношування в середовищі з абразивом.

На рис. 1 представлена залежність ударно-абразивного зношування термопластів від кількості циклів навантаження.

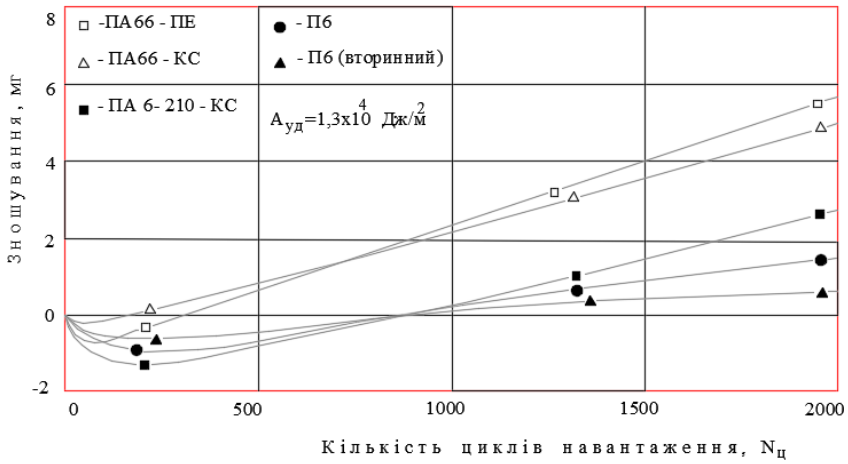


Рисунок 1. Залежність зношування термопластів від кількості циклів навантаження

В початковий момент часу на поверхні зразка відбувається інтенсивне вдавлювання абразивних частин, що приводить до насичення ними поверхневого шару зразків (шаржування), про що свідчить збільшення маси зразків і утворення від'ємного участку на графіку. При цьому процес шаржування переважає над процесом зношування матеріалу. Після максимального накопичення абразиву, починається зменшення маси зразка і зношування стає пропорційним кількості ударів – період усталеного зношування. Швидкість зношування склонаповнених термопластів вища (визначається кутом нахилу графіка) швидкості зношування ненаповнених термопластів. Причиною цього є те, що ненаповненим термопластам з лінійною будовою молекул властива досить розвинута вимушена еластичність. Вони здатні протягом довшого часу багатократно деформуватись, а значить менше піддаватись дарно-абразивному зношуванню, ніж склонаповнені, які є більш жорсткими і крихкими матеріалами.

УДК 623.17.38
Б. Оробчук, канд. техн. наук, доц.; М. Ярошевський; Я. Котелянець
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ КІБЕРБЕЗПЕКИ ЦИФРОВИХ ПІДСТАНЦІЙ

UDC 623.17.38
B. Orobchuk, Ph.D., Assoc.; M. Yaroshevsky; Y. Kotelyanets

CYBERSECURITY ANALYSIS OF DIGITAL SUBSTATIONS

Цифрова підстанція є важливою ланкою технологічного керування електроенер-гетичною системою. У зв'язку з «цифровізацією» енергетики та розвитком електро-енергетичних систем на основі інноваційних засобів та технологій сучасні об'єкти електроенергетики, у тому числі цифрові підстанції, необхідно розглядати як складні комплексні кіберфізичні системи.

Для забезпечення інформаційно-технологічної захищеності цифрової підстанції має мати властивості стійкості, адаптивності, відновлюваності, які можуть бути розвинені на основі глибокого аналізу проблем безвідмовної роботи цифрової підстанції [1]. Відмінною особливістю цифрової підстанції є передача інформації через мережу з комутацією пакетів Ethernet, налаштовану спеціальним чином. У зв'язку з цим закритість об'єкта більше не є бар'єром для зловмисника, і, якщо не вжити спеціальних захисних заходів, усі дані на верхньому рівні автомати-зації підстанції можуть стати доступними для кібератак. Крім того, до загроз безпеки звичайної підстанції додаються загрози втручання у роботу шини процесу та систему синхронізації часу. Кіберстійкість енергосистеми є відносно новим терміном, що характеризує її здатність відновлю-ватися після реалізації явно спрямованих чи прихованих кібератак. Відмова елемента фізичної підсистеми може призвести до аварійного стану електричної частини та сприяти виходу з ладу системи управління інформаційно-комунікаційної підсистеми

Процес «цифровізації» енергетичних систем, використання інтелектуальних тех-нологій, складного технічного, інформаційного та комунікаційного обладнання підви-щили ризики в галузі кібербезпеки енергетичних підприємств, у тому числі цифрової підстанції. Серед основних напрямів цифровізації електроенергетики є важливим місце відводиться розвитку цифрових технологічних систем виробництва, транспорту, дис-петчеризації та споживання електроенергії [2]. Цифрова підстанція є одним із пілотних проектів розвитку цифровізації електроенергетики.

Втрата та недостовірність інформації внаслідок кібератак на інформаційно-комунікаційну підсистему можуть призвести до вироблення та реалізації неправильних керуючих впливів та розвитку аварійних ситуацій у фізичній підсистемі як самої цифрової підстанції, так і в електроенергетичній системі загалом, тож проблема кіберстійкості об'єктів енергетики є критично важливою і має вирішуватися як технічними засобами, так і організаційними, включаючи підвищення кваліфікації оперативного персоналу.

Література

1. Розвиток технологій будівництва цифрових підстанцій / Друбецька Т.І., Земський Д. Р., Шмельова В. С., Артемчук В. В. // Енергетика: економіка, технології, екологія : науковий журнал. – 2024. – № 1. – С. 106-113. – Бібліогр.: 3 назви.
2. Orobchuk, B., Buniak, O., Babiuk, S., Sysak, I. Design of an intelligent system to control educational laboratory equipment based on a hybrid mini-power plant. Eastern-European Journal of Enterprise Technologies, 2023, 2(9-122), pp. 59–72. (Scopus ISSN 1729-3774).

УДК 004.41
В. Москалик; Ю. Стоянов, к.т.н. доц., старший викладач
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

РОЛЬ МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ У ЗАБЕЗПЕЧЕННІ МАСШТАБОВАНОСТІ ВЕБ-ДОДАТКІВ

UDC 004.41
V. Moskalyk; Y. Stoyanov, Ph.D.

THE ROLE OF MICROSRVICES ARCHITECTURE IN ENSURING SCALABILITY OF WEB APPLICATIONS

Сучасні веб-додатки повинні швидко обробляти великі обсяги даних, забезпечувати високу продуктивність та надійність навіть за умови пікових навантажень. Мікросервісна архітектура часто стає ключовим варіантом для проектування великих та складних додатків.

Однією з ключових переваг мікросервісної архітектури є її здатність забезпечувати масштабованість окремих компонентів системи. На відміну від монолітних додатків, де масштабування можливе лише для всієї програми, у мікросервісах можна масштабувати лише ті сервіси, які цього потребують. Наприклад у веб-додатку із сервісами авторизації, публікації контенту та аналітики під час пікових навантажень можна збільшити потужності лише для сервісу аналітики [1].

Оскільки мікросервіси є автономними, відмова одного компонента не впливає на роботу інших. Це забезпечує високу надійність системи, бо ключові функції, такі як авторизація чи перегляд контенту, продовжують працювати навіть під час збоїв в інших мікросервісах додатку.

Ще важливою перевагою даної архітектури є можливість використовувати різні технології для реалізації окремих сервісів. Для сервісу аналітики можна використати мову програмування Python через її зручність у роботі з даними, тоді як для реалізації мікросервісів, які потребують високої продуктивності та стабільності, можуть використовуватись C# або Java. Така технологічна незалежність дозволяє оптимізувати кожен компонент системи під конкретні завдання. Також, завдяки автономності в системі можуть впроваджуватися інструменти, які набирають популярності з швидким розвитком інформаційних технологій.

Попри суттєві переваги мікросервісна архітектура має недоліки. Одним з яких є складність тестування та налагодження. При великій кількості сервісів, коли виникає помилка в системі, то пошук причини вимагає велику кількість часу та потребує досвідчених спеціалістів [2].

Хоча цей підхід має свої виклики, його переваги, включно зі зменшенням ризику збоїв та економією ресурсів при масштабуванні, роблять мікросервіси перспективним вибором для веб-додатків.

Література

1. Andersen G. The Role of Microservices Architecture in Web Development [Електронний ресурс] / Grady Andersen. – 2024. – Режим доступу до ресурсу: https://moldstud.com/articles/p-the-role-of-microservices-architecture-in-web-development.
2. Архітектура мікросервісів: Особливості, переваги, реальні приклади [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://www.hostzealot.com.ua/blog/about-solutions/arxitektura-mikroservisiv-osoblivosti-perevagi-realni-prikladi.

ЗМІСТ

ДЛЯ НОТАТОК

ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ

Матеріали

тез доповідей

XII науково-технічної конференції

18–19 грудня 2024 року

Формат 60х90, папір ксероксний.
Обл. вид. арк. 16,61
Тираж 300 прим.

Видавництво Тернопільського національного технічного унверситету імені Івана Пулюя
вул. Руська, 56, м. Тернопіль, 46001
Тел. 52-21-99, 42-79-65

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції ДК № 4226 від 08.12.2011 р.