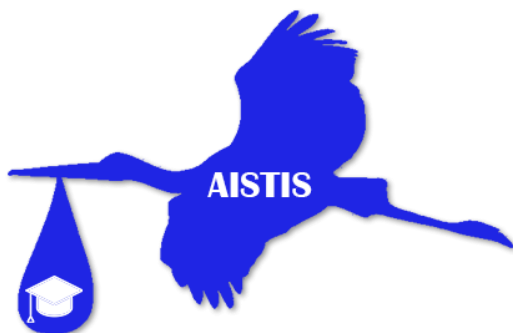


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА**



«ПРИКЛАДНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ»

**Збірник тез
IV Міжнародної науково-практичної конференції
30 вересня 2020 року**



м. Київ

УДК 004:378(082)

Адреса редакційної колегії:
Факультет інформаційних технологій
Київського національного університету імені Тараса Шевченка,
вул. Богдана Гаврилишина, 24, Київ, 04116, Україна

Тези друкуються мовою оригіналу,
відображають позицію автора,
який несе відповідальність за зміст

Прикладні системи та технології в інформаційному суспільстві: зб. тез доповідей і наук. повідомл. учасників IV Міжнародної науково-практичної конференції (Київ, 30 вересня 2020 р.) / за заг. ред. В.Л. Плескач, В.Л. Міронова. – К.: Київський нац. ун-т імені Тараса Шевченка, 2020. – 253 с.

Цей збірник містить тези учасників IV міжнародної науково-практичної конференції «Прикладні системи та технології в інформаційному суспільстві», яка проводилась 30 вересня 2020 року на базі факультету інформаційних технологій Київського національного університету імені Тараса Шевченка.

Робочі мови конференцій: українська, англійська, російська.

Основною метою конференції є вирішення актуальних проблем розвитку прикладних інформаційних систем у цифровій економіці, захисту даних зазначених систем, а також перспективних технологій в інфокомунікаційних системах, сучасній освіті та правових аспектів в інформаційно-комунікаційних технологіях.

Подані матеріали містять методологічні та методичні підходи, які можуть заслуговувати на увагу широкого кола фахівців.

УДК 004:378(082)

© Київський національний університет імені Тараса Шевченка
Факультет інформаційних технологій, 2020

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПРОГРАМНИЙ КОМІТЕТ

Андон Пилип Іларіонович – академік НАН України, доктор фізико-математичних наук, директор Інституту програмних систем НАН України, голова;
Баранов Георгій Леонідович – доктор технічних наук, професор, професор кафедри інформаційних систем і технологій Національного транспортного університету;

Бутнік-Сіверський Олександр Борисович – д.е.н., професор, академік УАН, АТН України, завідувач кафедри економіки, обліку та фінансів інституту післядипломної освіти НУХТ

Геєць Олександр Валерійович – директор Національного центру підготовки банківських працівників України;

Глушкова Віра Вікторівна – к.ф.-м.н., с.н.с., Інститут кібернетики імені В.М. Глушкова НАН України;

Дивак Микола Петрович – доктор технічних наук, професор, декан факультету комп'ютерних інформаційних технологій Тернопільського національного економічного університету;

Жадько Костянтин Степанович – д.е.н., професор, завідувач кафедри економіки підприємств Університету митної справи та фінансів, м.Дніпро;

Каптур Вадим Анатолійович – кандидат технічних наук, проректор з наукової роботи Одеської національної академії зв'язку ім. О.С. Попова;

Козленко Микола Іванович – кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій Прикарпатського національного університету імені Василя Стефаника;

Кузнєцова Анжела Ярославівна – доктор економічних наук, професор, ректор «Університет банківської справи»;

Лахно Валерій Анатолійович – доктор технічних наук, професор, завідувач кафедри комп'ютерних систем і мереж Національного університету біоресурсів і природокористування України;

Левашенко Віталій – кандидат технічних наук, професор, технічний університет, м.Жиліно;

Панасюк Ігор Васильович – доктор технічних наук, професор, академік Академії інженерних наук України та Української технологічної академії, директор Навчально-наукового інституту інженерії та інформаційних технологій, завідувач кафедри теплоенергетики, ресурсощадності та техногенної безпеки Київського національного університету технологій та дизайну;

Плескач Валентина Леонідівна – доктор економічних наук, професор, завідувач кафедри прикладних інформаційних систем факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Пурський Олег Іванович – доктор фізико-математичних наук, професор, завідувач кафедри комп'ютерних наук Київського національного торговельно-економічного університету;

Петухов Іван Михайлович – президент ІТ компанії «Адамант», віце-президент УСПП з питань науки та інформаційних технологій, голова Правління громадської спілки «Національна асамблея України»;

Сайко Володимир Григорович – доктор технічних наук, професор, професор кафедри прикладних інформаційних систем факультету інформаційних технологій Київського національного університету імені Тараса Шевченка;

Семенченко Андрій Іванович – доктор наук з державного управління, директор Інституту вищих керівних кадрів Національної академії державного управління при Президентові України;

Субач Ігор Юрійович – доктор технічних наук, професор, завідувач кафедри Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «КПІ імені Сікорського»;

Унковська Тетяна Євгенівна – доктор економічних наук, професор, директор Експертно-аналітичного центру «Оптима»;

Устименко Василь Олександрович – доктор фізико-математичних наук, професор, університет Марії Кюрі-Склодовської, Польща;

Чорноус Галина Олександрівна – доктор економічних наук, доцент, доцент кафедри економічної кібернетики економічного факультету Київського національного університету імені Тараса Шевченка;

Щербань Володимир Юрійович, доктор технічних наук, професор, академік Міжнародна Академії комп'ютерних наук і систем, завідувач кафедри комп'ютерних наук та технологій Київського національного університету технологій та дизайну, лауреат державної премії України в галузі науки і техніки;

Romanas Tumasonis – доктор технічних наук, професор, декан факультету електроніки та інформатики Вільнюського університету прикладних наук

ЗМІСТ

Бойко Ю.П., Баланюк Ю.В., Ліщиновська Н.О. Особливості синтезу резонаторів на нерегулярних лініях передачі для апаратури системи EGNOS	9
Бойко Ю.П., Зюбіна Р.В., Кулінський В.Д. Кібербезпека авіаційних підприємств.....	14
Большаков В.М., Лефтеров О.В. Погляд на модель архітектури корпоративної інформаційної системи	17
Браїловський М. М., Захарченко Є. О. Розподіл пам'яті зовнішніх носіїв для захисту інформації від несанкціонованого доступу та модифікації	24
Бучик С. С., Симониченко Я. А., Симониченко А. А. Стеганографічні методи для реалізації послуг захисту інформації	27
Бучик С.С., Швед А.В. Архітектура системи управління відносинами з клієнтами на прикладі CRM-системи Creatio	30
Ващіліна О.В. Аудит процесів розробки, впровадження та супроводу інформаційних систем на відповідність міжнародному стандарту якості ISO 9001:2015	35
Верес А.Ю. Дослідження механізму адаптації до завад в бездротових локальних обчислювальних мережах наступного покоління.....	40
Вишневський В.В., Круковський М.Ю. Управління життєвим циклом інформаційних систем спеціального призначення	43
Гарко І.І., Міронова В.Л. Використання сервісу online test pad для проведення тестування під час дистанційного навчання при викладанні програмування мовою java.....	45
Гладка О. М., Карпович І. М., Живий Я. В. Прикладна програма розпізнавання літер	48
Глушкова В.В., Карпец Э.П. Історія розвитку технологій інтерактивного управління в Україні.....	50
Гнатієнко Г.М., Гнатієнко В.Г. Технологія тестування з використанням закритих запитань при множинному виборі варіантів відповідей	55
Гончаренко Н. А. DARK WEB як частина всесвітньої павутини та його вплив на суспільство	65
Горіцький М.В. Організаційно - технологічні засади створення програмної системи електронного банкінгу.....	70

Давидько С.В. Перспективи і переваги впровадження електронного резидентства в Україні.....	72
Домрачев В.М., Семененко Т. О., Третиник В.В. Моделювання впливу динаміки облікової ставки на економічне зростання в Україні	75
Дудзінський Ю. М., Манічева Н. В., Найденко О. В. Застосування програмного забезпечення NI Multisim для дослідження та аналізу біомедичної апаратури.....	79
Зайцев Є.О., Кучанський В.В. Визначення оптимальних потужностей теплових електростанцій методом динамічного програмування.....	81
Карчева Г.Т., Карчева І.Я. Нові підходи до регулювання діяльності банків в умовах інформаційного суспільства.....	84
Кілієвич О.І. Вироблення доказової державної політики в умовах розвитку цифрової економіки	90
Kozlenko M., Lazarovych I., Kuz M. Deep learning approach to signal processing in infocommunications.....	92
Комісаренко О.С., Баранов Г.Л., Чака О.Г. Технології створення функціональних матеріалів за замовленнями в інформаційному суспільстві.....	94
Котенко Н.О., Жирова Т.О. Організація освітнього процесу в умовах смешанной работы учебного заведения.....	100
Краснощок В.М. Обробка великих неструктурованих даних в розподілених середовищах.....	104
Кобижча І.І. Сучасні технології і методи розробки веб-застосунків	108
Луценко В. В. Організація безпечної роботи при використанні електронної пошти	110
Мазютинець Г. В., Маляр М. М., Шаркаді М. М. Нечіткі моделі у системі фінансово-економічної безпеки.....	113
Макаренко О.С., Самородов Є.Л., Морева О.О., Патіоха А.А. Дослідження процесів міграції в науці та освіті з використанням моделей та ГІС	116
Малишев О. В. Життєвий цикл системи: погляд з висоти пташиного польоту	119
Малишев О. В., Калмиков В.Г. Концептуальна модель планування діяльності на основі спроможностей.....	123

Міронова В.Л., Гарко І.І., Богданець Є.І. Методика побудови інтелектуальних систем цифрового суспільства.....	126
Наконечний В.С., Толюпа С.В., Петренко А.І. Особливості побудови системи кібербезпеки в світі інтернет речей	128
Наконечний В.С., Кузьменко О.О. Клавіатурний почерк – механізм біометричної ідентифікації користувача в інформаційній системі	133
Ніколаєв М.О. Дослідження використання машинного навчання та алгоритмічного кодування при прогнозуванні цін та оцінці ризиків майбутніх періодів на світових фінансових ринках	138
Новіцька Т. В. Виклики та освітні технології у контексті підготовки фахівців математичних (фізичних) спеціальностей в умовах дистанційного навчання	141
Онуфрик О.І. Modern algorithms in natural language processing	143
Орехов О.А., Орехова Н.А. Застосування ансамблевих методів для прогнозування епідемічної ситуації (на базі класичної SIR-моделі).....	145
Павелко Т. М. Застосування мікроконтролерів у зв'язці з інформаційною системою електронного документообігу загальноосвітньої школи	149
Панасюк О. І. Програмні рішення для взаємодії між сервісами прикладних інформаційних систем.....	151
Передерій Н.О. Аналіз переваг і недоліків використання патерну event sourcing при побудові програмних систем е-комерції	154
Підлужний Д.О. Використання сучасних алгоритмів розпізнавання обличчя під час пандемії COVID-19	157
Пікуляк М.В., Корнута В.Р. Вдосконалення евристичного алгоритму пошуку оптимального маршруту до паркувальної зони.....	159
Пирог М.В., Дуля Д.В. Порівняння платформ .NET CORE та NODE.JS як технологій веб-розробки.....	164
Пирог М.В., Борсук О.С. Фреймворк Angularjs та бібліотека React.Js як інструменти розробки динамічних веб-застосунків	168
Плескач В.Л., Плескач М.В. Індекс розвитку електронного урядування та електронних публічних послуг в Україні: 2020	170
Поліщук Д.О. Веб-сервіс із підтримки діяльності кінотеатру.....	179

Прокопенко Н.О. Інформаційні технології в системі середньострокового бюджетного планування України.....	182
Пяташова Е. С. Розумна мережа. Питання щодо кібербезпеки	187
Пурський О.І., Кузнецов О.Ф., Медяник В.В. Специфіка програмної реалізації web-системи оцінювання рівня регіонального розвитку.....	190
Рогущина Ю.В. Кількісні оцінки семантичної подібності між поняттями предметної області як засіб моделювання інтересів користувача	194
Saviak N. Improved deep learning algorithm for self-driving cars control	200
Сайко В.Г., Наритник Т.М., Диль Є.А., Кузьмінський Ю.В. Випромінюючий комплекс субтерагерцового діапазону для захисту об'єктів від несанкціонованого проникнення.....	202
Силантьєв С.О. Цифровізація ринків похідних фінансових інструментів України в умовах трансформації міжнародного регуляторного законодавства.....	208
Симонов Д.І., Симонов Є.Д. Планування та управління ланцюгами постачання.....	212
Тітова Н.В., Прокопович І.В. Застосування 3D друку в медицині	219
Толюпа С.В., Наконечний В.С., Браїловський М.М., Касьянов П. П. Застосування програмного продукту splunk machine learning toolkit в системі управління інформаційною безпекою.....	221
Толюпа С.В., Шестак Я.В., Кулько А.А., Чечуга А.М. Автоматизація процесу управління інцидентами інформаційної безпеки	227
Хижняк А.О., Толюпа С.В., Пархоменко І. Основні критерії готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу.....	234
Чаплінський Ю.П., Субботіна О.В. Контекст та його представлення при розв'язанні прикладних задач прийняття рішень	239
Шолохов О. В., Терентьєв О. М., Присянкін-Жарова Т. І. Підвищення ефективності соціальних комунікацій на основі аналізу інтернет-джерел засобами text mining	241
Шумейко О.А., Литвин І.С. Інформаційна технологія оптичного розпізнавання мови жестів	245
Ярмоленко Ю. А, Черноус Г. О. Мультиагентна інформаційна система підтримки транзакційного ціноутворення.....	247

Бойко Ю.П.

Київський національний університет імені Тараса Шевченка

julia_boyko2010@ukr.net

Баланюк Ю.В., Ліщиновська Н.О.

Національний авіаційний університет

natashalil858@ukr.net

ОСОБЛИВОСТІ СИНТЕЗУ РЕЗОНАТОРІВ НА НЕРЕГУЛЯРНИХ ЛІНІЯХ ПЕРЕДАЧІ ДЛЯ АПАРАТУРИ СИСТЕМИ EGNOS

One of the key criteria for choosing the location of the EGNOS system in Ukraine is the radio frequency (RF) environment, as it affects the performance of the system. Interference sources available in the system deployment area will adversely affect the performance of the EGNOS RIMS receiver, as their power exceeds the required level in the GPS frequency bands L1 and L2 used. In this paper, the peculiarities of resonator synthesis on closed and open segments of microstrip and symmetric strip transmission lines are considered, in order to eliminate interferences formed by satellite radio navigation systems.

Key words: *resonator, EGNOS, GPS.*

У 2017 році Державне космічне агентство України організувало проведення Європейськими експертами досліджень можливих місць для розміщення станції RIMS системи EGNOS. Місцем розміщення першої станції RIMS від EGNOS визначено Комунальне підприємство міжнародний аеропорт "Київ" (Жуляни), який за висновками експертів виявився найбільш для цього придатним.

Одним із ключових критеріїв вибору місця є радіочастотне середовище, оскільки умови навколишнього середовища мають безпосередній негативний вплив на продуктивність системи EGNOS. У той же час, в ході досліджень в районі аеропорту „Київ” (Жуляни) було виявлено джерела перешкод, потужність яких перевищує допустимий рівень, оскільки ці перешкоди негативно вплинуть на характеристики приймача станції RIMS у використовуваних діапазонах частот L1 та L2 (з центральними частотами 1575,42 МГц та 1227,6 МГц). Крім того, ці перешкоди є безперервними, що призводить до значного порушення вимог по розміщенню станції RIMS Україна взяла на себе зобов'язання усунути наявні перешкоди в прийомі радіосигналу, європейська - завезти в Україну і змонтувати обладнання станції.

При даних умовах актуальним завданням є розробка ефективних засобів усунення перешкод, які формуються супутниковим радіонавігаційним системами, що забезпечать можливість функціонування апаратури системи EGNOS в Україні.

У пристроях радіотехніки широко застосовуються коливальні системи на базі мікросмужкових і симетричних смужкових ліній [1]. В даній роботі розглянуті особливості синтезу резонаторів на замкнених і розімкнених відрізках вищевказаних конструкцій ліній передачі.

Оскільки лінія є замкненою, то в залежності від її довжини змінюється характер вхідного опору і частотні характеристики лінії стають аналогічними характеристиками відповідно послідовного або паралельного коливального контуру, а сама лінія стає еквівалентною послідовному або паралельному коливальному контуру поблизу резонансної частоти. Полюси вхідного опору короткозамкненою лінії слідує з періодом $\frac{\pi}{t_3}$, так як вхідний опір однорідної (регулярної) замкнутої лінії

$$Z_{кз} = jWtg\alpha t_3.$$

Закон зміни хвильового опору, що забезпечує максимальну добротність резонатора досягається за рахунок певного закону зміни ширини провідної смужки.

Ширину смужки $i - oї$ сходинки відрізка регулярної лінії W_i з хвильовим опором $W(\tau)$ визначається виразом:

$$W = \frac{8h}{e^d - 2e^{-a}}; \quad (1)$$

де h - товщина діелектричної підкладки в мм; ϵ_r - відносна діелектрична проникність підкладки; w - ширина провідної смужки в мм.

При цьому похибка обчислень за формулою (1) не перевищує 1%, що цілком задовольняє вимогам, що пред'являються до інженерних розрахунків.

Наведені формули були отримані в припущенні, що товщина провідної смужки нескінченно мала. Однак в тих випадках, коли $b/h > 0 < 006$ де b – товщина провідної смужки, необхідно враховувати товщину смужки. Для цього ширину смужки w , розраховану за умови, що її товщина дорівнює нулю, необхідно зменшити на величину, значення якої обчислюються наступним чином:

$$\text{при } w/h \leq 0,16 \quad \Delta w = b[1 + \ln(4\pi w/b)]/\pi, \quad (2)$$

$$\text{при } w/h > 0,16 \quad \Delta w = b[1 + \ln(2h/b)]/\pi.$$

(3)

Цей вираз справедливо, коли товщина смужки в кілька разів (але не більше) перевищує глибину скін-шару в металі. Довжина провідної смужки, відповідної i -ой сходинки $\Delta l_i = \Delta l_i' + \Delta l_i''$, де $\Delta l_i'$, $\Delta l_i''$ - довжини відрізків однорідних ліній передачі, відповідних i -ой сходинці.

Розглянуті вище вираження для розрахунку геометричних розмірів мікросмужкових ліній виведені за умови, що в лінії поширюється тільки TEM - хвиля, тобто відсутні поздовжні складові векторів напруженості електричного і магнітного поля. Фазова швидкість TEM - хвилі не залежить від частоти.

Насправді всі зазначені явища в різному ступені проявляються в реальній мікросмужковій лінії. Особливо в мікросмужковій лінії позначаються втрати на випромінювання в площині, перпендикулярній площині смужки, що знижує добротність резонатора.

Також, але в набагато меншому ступені випромінює замкнутий кінець резонатора через спотворення структури поля в кінці лінії в місці короткого замикання.

У мікросмужковій лінії не всі силові лінії поля між смужковим провідником і заземленої пластини проходять через підкладку. Тому хвиля, що розповсюджується вздовж мікросмужкового провідника, є не чисто Т - хвилею. Вона є квазі Т- хвилею. Її фазова швидкість в мікросмужковій лінії визначається формулою [1] :

$$V_{\phi} = \frac{C}{\varepsilon_{r\phi}} . \quad (4)$$

Відзначимо, що ефективна діелектрична постійна $\varepsilon_{r\phi}$ менше діелектричної постійної підкладки, так як ефективна діелектрична постійна враховує поле поза підкладки.

Втрати в мікросмужковій лінії складаються з втрат у провіднику і діелектрику. Зокрема, формула для обчислення загасання в провіднику провідної смужки α_{np} (дБ/м) може бути записана у вигляді:

$$\alpha_{np} = 1,38A \frac{R_s}{hW_0} \frac{32 - \left(\frac{w_{\text{э}}}{h}\right)^2}{32 + \left(\frac{w_{\text{э}}}{h}\right)^2}, \quad \left(\frac{w}{h}\right) < 1, \quad (5)$$

$$\alpha_{np} = 6,1 \cdot 10^{-5} A \frac{R_s w_{\text{э}} \varepsilon_{r\text{э}}}{h} \left(\frac{w_{\text{э}}}{h} + \frac{0,667 \frac{w_{\text{э}}}{h}}{\frac{w_{\text{э}}}{h} + 1,444} \right), \quad \left(\frac{W}{h}\right) > 1, \quad (6)$$

Резонатори у вигляді розімкнутих відрізків однорідних полоскових ліній застосовуються в якості прохідних, що практично виключає випромінювання з відкритого кінця відрізка. Так як лінія є розімкнутою, то чергування полюсів в ній відбувається з періодом $k\pi/2$, оскільки вхідний опір відрізка лінії $Z_{xx} = W \text{cth} \beta l$.

Залежно від характеру навантаження, підключеної до кінця лінії при паралельному включенні резонатора, довжина її буде зменшуватися або збільшуватися для створення режиму стоячих хвиль. При $W_0 > R_n$, $W_0 < R_n$, (R_n - опір навантаження) і, якщо лінія навантажена на комплексний опір, то в ній виникає режим змішаних хвиль.

Недоліком симетричної полоскової лінії є ускладнений доступ до внутрішнього провідника при монтажі схеми в корпус, а також ускладнена установка навісних елементів, які можуть застосовуватися для настройки, перебудови, регулювання характеристик резонатора.

При виконанні резонатора на діелектричній підкладці з високою діелектричною проникністю, загасанням за рахунок випромінювання можна знехтувати враховуючи його малість [2]. Підвищення добротності полоскової лінії можливо за рахунок збільшення відстані між пластинами і ширини смужки, однак існує межа, обумовлена появою хвилеводних типів коливань. Тому фізичними обмеженнями є полухвильовий розмір ширини токонесущої смужки і відстані між нею і заземлюючою пластиною. При невиконанні цієї вимоги уздовж резонатора починають поширюватися вищі типи коливань, що робить його практично марним. Що стосується розімкнутих резонаторів, то необхідно відзначити, що при малих електричних довжинах пристроїв з відкритим кінцем лінії, втрати на випромінювання можуть становити до 90% від загального числа втрат. У наявності невідповідність між вимогами до комплексної мікромініатюризації і втратами в резонаторах. Таким чином доцільно резонатор з відкритим кінцем використовувати як прохідний.

Зі збільшенням перепаду хвильового опору поліпшуються фільтруючі властивості резонатора і зменшується його довжина. Останнє означає, що зростають втрати на випромінювання з відкритого кінця лінії. Отже, при накладенні обмежень на мінімальне і максимальне значення хвильового опору, що задається з урахуванням фізичної можливості бути реалізованим, необхідно враховувати і фактор зростання втрат на випромінювання зі зменшенням довжини відрізка лінії.

Запропоновані в роботі фільтри були промодельовані для GPS L2 (рис.1).

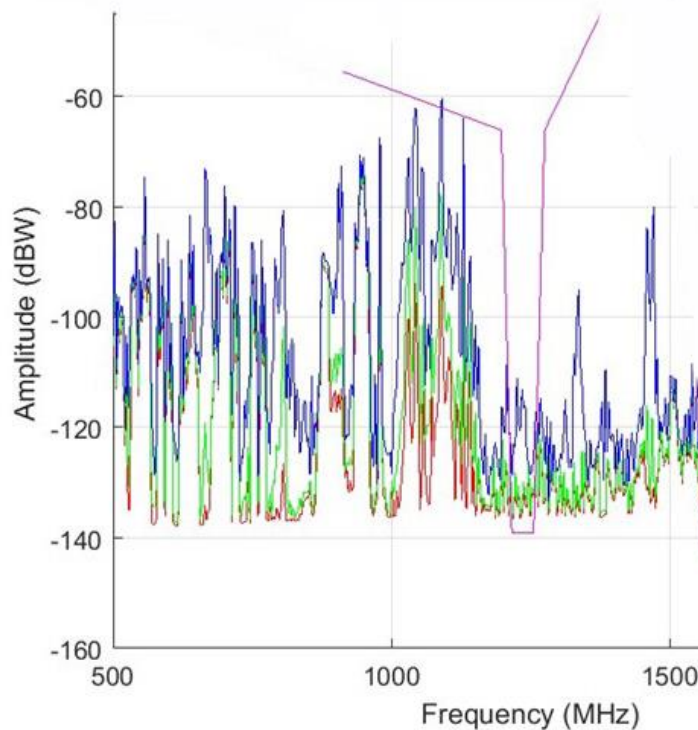


Рис.1 Фільтрація в діапазоні частот L2

З аналізу рисунку видно, що застосування запропонованих резонаторів є ефективним для усунення перешкод, які формуються супутниковим радіонавігаційним системами, що забезпечать можливість функціонування апаратури системи EGNOS в Україні.

ЛІТЕРАТУРА

1. Мищенко А.В., Приходько Т.Ю., Лициновская Н.А. Добротность резонатора на основе нерегулярной линии передачи. Вестник Инженерной академии Украины. №3, С. 97-102, 2017.

2. Барабаш О.В., Бойко Ю.П., Лициновская Н.А. Синтез конструкцій резонатора за критерієм забезпечення максимальної добротності. Телекомунікаційні та інформаційні технології. № 4(61), С. 5-13, 2018.

Бойко Ю.П., Зюбіна Р.В.

Київський національний університет імені Тараса Шевченка, Київ

julia_boyko2010@ukr.net

Кулінський В.Д.

Національний авіаційний університет, Київ

aa16vd@gmail.com

КІБЕРБЕЗПЕКА АВІАЦІЙНИХ ПІДПРИЄМСТВ

The paper examines the need to ensure cybersecurity of aviation enterprises, according to ICAO international recommendations and state regulations. It has been shown that it is effective to conduct cybersecurity audits of airlines and train staff on cybersecurity.

Key words: *cybersecurity, cyber threat, information system, civil aviation.*

Актуальною на сьогоднішній день є розробка узгодженої стратегії і порядку дій всіх зацікавлених сторін щодо захисту цивільної авіації від кіберзагроз, поряд із заходами щодо забезпечення захисту компонентів авіаційної галузі від зовнішніх впливів, відповідно до єдиного, комплексного і функціонального підходу в області безпеки авіакомпаній, аеропортів, повітряних суден, аеронавігації і управління повітряним рухом з урахуванням передового вітчизняного, міжнародного досвіду та Рекомендованої практики ІКАО.

Кількість кіберінцидентів зростає весь час, цілеспрямовані кібератаки можуть паралізувати не тільки роботу аеропортів та авіакомпаній, а й привести до серйозних інцидентів з великою кількістю жертв. Так, в червні 2017 році вірусом RetyaA було заблоковано роботу сервера аеропорту «Бориспіль», центральне табло не працювало, а оновлювалося в ручному режимі через кожні 15 хвилин. Інформаційні системи аеропорту «Одеса» зазнавали хакерської атаки двічі: в 2017 та в 2019 роках. А в листопаді 2019 року білий хакер через загальнодоступну мережу Wi-Fi отримав доступ до внутрішньої мережі аеропорту «Київ».

Кібербезпека в цивільній авіації становить серйозну проблему, актуальну для всіх учасників галузі, що вимагає узгоджених і скоординованих дій від усіх зацікавлених сторін. Захищеність від кіберзагроз в авіаційній галузі є питанням національної безпеки.

Визнавши актуальність і важливість захисту критично важливих систем інфраструктури цивільної авіації, її інформаційних систем і систем зв'язку, даних від кіберзагроз, на своїй тридцять дев'ятій сесії Асамблея ІКАО закликала до використання скоординованого підходу для забезпечення прийняттого і пропорційного рівня стійкості до кіберзагроз на глобальному рівні. У зв'язку з цим в резолюції ІКАО А39-19 «Рішення проблем кібербезпеки в цивільній авіації» викладені заходи, які слід вжити державам і зацікавленим сторонам для протидії кіберзагрозам в сфері цивільної авіації в рамках комплексного, єдиного і заснованого на співробітництві підходу.

У «Керівництві Європейської конференції цивільної авіації (ЄКЦА) щодо спрощення формальностей та безпеки» (Дос 30) сказано, що «Відповідний повноважний орган повинен забезпечити наявність процедур для виявлення і оцінки кіберризиків для цивільної авіації».

Також, Відповідний повноважний орган повинен забезпечити, щоб ці аспекти були включені в Національну програму безпеки цивільної авіації, Національну програму контролю якості та Національну програму навчання в області безпеки цивільної авіації.

Основними нормативно-правовими документами, якими керуються в Україні з питань кібербезпеки в авіаційній галузі є: Резолюція ІКАО А39-19 «Рішення проблем кібербезпеки в цивільній авіації», Конвенція про міжнародну цивільну авіацію 1944 року Додаток 17 «Безпека. Захист міжнародної цивільної авіації від актів незаконного втручання.» [1], Політика ЄКЦА у сфері авіаційної безпеки Дос 30 (Частина II) [2], Дос 8973 «Керівний документ з авіаційної безпеки» [3], Закон України «Про Державну програму авіаційної безпеки цивільної авіації» [4], Закон України «Про основні засади забезпечення кібербезпеки України» [5].

В Законі України "Про Державну програму авіаційної безпеки цивільної авіації" дано наступне визначення кіберзагроз: кіберзагрози цивільній авіації - наявні та потенційно можливі явища і чинники, що становлять загрозу кібербезпеці та можуть призвести до актів незаконного втручання в діяльність цивільної авіації.

Випадки і інциденти, пов'язані з авіаційною безпекою, можуть бути результатом випадкових або навмисних дій персоналу або навмисних атак

зловмисників. Вони також можуть виникати через недоліки в обладнанні, програмному забезпеченні, конфігураціях або процесах.

Найбільш уразливими місцями аеропортів та авіакомпаній є: система реєстрації, Wi-Fi мережі, сервери, локальні мережі, бази даних, web-сайт, персонал. В системі управління повітряним рухом вразливими місцями є канали передачі даних, ADS-B, персонал. На борту авіалайнерів: бортові комп'ютери, Wi-Fi мережі на борту авіалайнерів, персонал.

Згідно основних керівних документів ІКАО, держави повинні забезпечити наявність процедур для виявлення і оцінки кіберризиків для цивільної авіації, спрямовані на: зниження ймовірності виникнення кіберзагроз; своєчасне розпізнавання кібератак, коли вони мають місце; реалізацію плану протидії кібератакам; обмеження наслідків таких атак; створення і впровадження системи кібербезпеки.

Для забезпечення якісного захисту від кіберзагроз українським авіакомпаніям та аеропортам необхідно проводити аудит кібербезпеки та впроваджувати превентивні заходи з кібербезпеки. Аудит кібербезпеки виявить існуючі проблеми та вразливості, а також надасть рекомендації щодо впровадження комплексу організаційних заходів та програмно-апаратних засобів для підвищення захисту ресурсів інформаційних систем авіапідприємств.

Для зменшення кількості загроз з боку персонала, необхідно проводити його навчання теоретичним і практичним аспектам забезпечення кібербезпеки авіаційних підприємств і формування у них необхідних початкових знань і навичок щодо заходів протидії кібератакам, оцінці ризиків і своєчасному реагуванню на інциденти кібербезпеки відповідно до вимог ІКАО та з урахуванням національної нормативно-правової бази.

ЛІТЕРАТУРА

1. Безпека. Захист міжнародної цивільної авіації від актів незаконного втручання. Додаток 17 до Конвенції про міжнародну цивільну авіацію. 10-е видання, ІКАО, 2017, 64 с.

2. Дос 30. Безпека. Політика країн - членів Європейської конференції цивільної авіації в галузі авіаційної безпеки. ЄКЦА. Частина II. (13-е видання, травень 2010 року.

3. Дос 8973/10. Керівництво з авіаційної безпеки. ІКАО, 2017, С.18.1-18.17.

4. Закон України «Про Державну програму авіаційної безпеки цивільної авіації», від 21.03.2017 № 1965-VIII (Редакція станом на 13.02.2020. Електронний ресурс. Режим доступу: <https://zakon.rada.gov.ua/laws/show/1965-19#Text>.

5. Закон України «Про основні засади забезпечення кібербезпеки України», від 05.10.2017 № 2163-VIII (Редакція станом на 03.07.2020). Електронний ресурс. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> .

В.М.Большаков

*Інститут кібернетики ім.В.М.Глушкова НАНУ, Київ,
vnbicyb@gmail.com*

О.В.Лефтеров

*Інститут кібернетики ім.В.М.Глушкова НАНУ, Київ,
lifterov@nas.gov.ua*

ПОГЛЯД НА МОДЕЛЬ АРХІТЕКТУРИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

The need to develop new architectural models of the corporate segment of the market exists despite the growing popularity of the ready-made models of IT-solutions for the corporate information systems (CIS), advancing by the vendors of IT. The proposed architecture model integrates new and classic methodologies that allows it to be used by IT professionals as a generalization model of the full implementation cycle of corporate IT solutions. It combines standards and scientific information from various sources, reflects the organization and the information system as a whole, creating the basis for the effective integration of other approaches, standards and methods, serves as a coherent source of recommendations for the development of CIS. The architecture model helps to create a holistic and comprehensive view on IT, and implement corporate information technology based on the paradigm of cloud computing.

Keywords: *architectural model, corporate information system, cloud computing, stages of system creation.*

Зростання впливу соціально-економічних чинників [1], примушує корпорації об'єднувати можливості різних методологій у власну, використовуючи сучасні стандарти і технології для поєднання програмних продуктів і систем в IT-рішення.

Архітектура, як інструмент інтеграції, лежить в основі розробки і експлуатації будь-яких складних корпоративних систем та ІТ-рішень. Вона допомагає здійснити цілісний і всебічний погляд на ІТ та дозволяє долати проблеми складності за рахунок пошарово представлення багатоаспектних явищ. За допомогою архітектури вже на ранніх етапах розробки ІТ можна отримати уявлення про основні функції та особливості інтеграції компонентів, що проектуються. Вибір і затвердження архітектури ІТ-рішення для корпорації є одним із найважливіших заходів її управління. Від обраної архітектури і створеного згідно з цією архітектурою ІТ-рішення залежить успішність функціонування всієї інформаційної інфраструктури підприємства. Використовуючи архітектурний підхід в роботі [2] було запропоновано розглядати КІС як багатовимірну багаторівневу структуру, одночасно виділяючи рівні для трьох типів ієрархій: "страти"- рівні опису, "шари"- рівні складності рішення, що приймається, "ешелони"- рівні організаційної ієрархії.

Кожне з цих понять має свою сферу застосування. Далі наведено опис вказаних трьох типів ієрархій, згідно [3].

Загальні характеристики стратифікованого опису систем:

- вибір страт, в термінах яких описується ця система, залежить від спостерігача, його знання і зацікавленості в діяльності системи, хоча для багатьох систем деякі страти здаються природними, внутрішньо їм властивими; аспекти опису функціонування системи на різних стратах в загальному випадку не пов'язані між собою, тому принципи і закони, що використовуються для характеристики системи на будь-якій страті, в загальному випадку не можуть бути виведені з принципів, що використовувалися на інших стратах;
- існує асиметрична залежність між умовами функціонування системи на різних стратах;
- на кожній страті є свій власний набір термінів, концепцій, і принципів;
- розуміння системи зростає при послідовному переході від однієї страти до іншої: чим нижче ми спускаємося за ієрархією, тим детальнішим стає розкриття системи, чим вище ми піднімаємося, тим ясніше стає сенс і значення усієї системи.

Інше поняття ієрархії відноситься до процесів ухвалення складних рішень. Приклад шарів функціональної ієрархії ухвалення рішень або управління:

- шар вибору (шар вибору стратегії, яка має бути використана);
- шар навчання, або адаптації (конкретизація невизначеності, з якими має справу шар вибору);

- шар самоорганізації (вибір структури, функцій і стратегій, використовуваних на шарах, що пролягають нижче, так, щоб по можливості наблизитися до глобальної мети).

Поняття ешелонів ієрархії має на увазі, що:

- система складається з сімейства чітко виділених взаємодіючих підсистем;
- деякі з підсистем є елементами, що приймають рішення;
- елементи, що приймають рішення, розташовуються ієрархічно в тому сенсі, що деякі з них перебувають під впливом або управляються іншими вирішальними елементами.

Приведений опис трьох типів ієрархії слід конкретизувати стосовно корпоративних інформаційних систем. Для кожного типу ієрархії пропонується використати три рівні: концептуальний, логічний і фізичний. Вперше трирівнева модель була представлена Комітетом з планування стандартів і вимог ANSI/X3/SPARC, очолюваним Чарльзом Бахманом в 1975 році для СУБД [4]. Потім вона стала широко використовуватися, як основа проектування інформаційних систем, зокрема при використанні ERD і у методології інформаційної інженерії [5].

Для здійснення стратифікації сучасну інформаційну систему слід розглядати з концептуальної, логічної, та фізичної точок зору зацікавлених сторін - тобто, з точки зору замовника, розробника та постачальників ІТ послуг. У свою чергу, у замовника концептуальне бачення формують інвестори, власники і вище керівництво організації, погляд на логіку і бізнес-процеси формують менеджери, бізнес аналітики, комерційні директори, а фізично реалізують співробітники, постачальники, партнери, клієнти та інші користувачі. У розробника концепції створюють конструктори, архітектори і системні інженери, логіку - аналітики і дизайнери, фізичну реалізацію - програмісти та тестувальники. Концепції для постачальників ІТ послуг формують керівництво і фахівці ІТ підрозділу, функціональні компоненти поставляють провайдери хмарних сервісів, апаратні забезпечення забезпечують системні інтегратори і інтернет - провайдери. Перспективи цих учасників процесу складають стратифікований опис ІС, тобто перший вимір узагальненої архітектури Корпоративної ІС (див. рис.1).

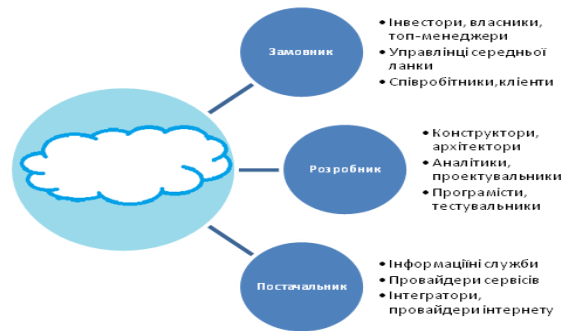


Рисунок 1. Зацікавлені сторони

Другий вимір (шари інформаційної системи) визначається підходами до управління (менеджменту) організацією (див. рис. 2).

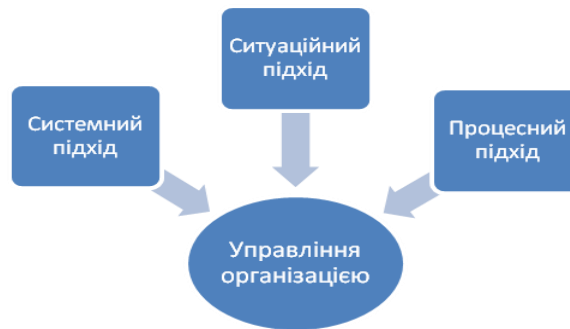


Рисунок 2. Підходи до управління організацією

Тут також присутня тріада (процесний – ситуаційний – системний підходи), які знаходять своє відображення в трьох парадигмах розробки програмного забезпечення: хмарної – об'єктної – структурної (див. рис. 3).



Рисунок 3. Парадигми розробки програмного забезпечення

Третій вимір архітектури - ешелони, визначається типами описів власне програмного продукту (див. рис. 4). Концептуальні описи формуються в термінах цілей, намірів, інтерфейсів, описи логіки - в робочих практиках і описах процесів, фізичні описи – в структурах даних і схемах їх зберігання.



Рисунок 4. Типи описів системи.

Знаходять своє відображення в архітектурі і різні етапи створення ІС у відповідності до поступової конкретизації страт:

- формування цілей, стандартів, специфікації;
- вибір системних рішень, аналіз і проектування, реалізація і тестування;
- впровадження і навчання, налагодження та підтримка сервісів, експлуатація.

Для кожної страти є порівняльний етап створення КІС, в якому доля відповідної групи зацікавлених учасників досягає максимального значення в порівнянні з участю цієї групи на інших етапах створення системи.

Таким чином сукупний вплив інтересів зацікавлених сторін, соціально - економічних чинників, технологій, різних підходів до управління підприємством, методологій створення інформаційних систем і різних способів описів системи визначає загальний архітектурний опис системи. На рис. 5 відображені головні зовнішні суб'єкти і сутності, що впливають на систему і напрями їх дії на різні рівні системи.

Функціональність хмарних рішень, що надають послуги і отже, будівельні блоки, що реалізують цю функціональність визначені двома стандартами ISO/IEC 17789: 2014[6] і ISO/IEC 18384-2:2016[7]. Запропонований архітектурний опис розділяє усі компоненти на 9 взаємозв'язаних рівнів:

- рівень споживацьких функцій («Споживання»);
- рівень послуг («Послуги»);
- рівень ресурсів («Ресурси»);
- рівень керівництва і комерційного управління хмарою («Керівництво»);
- рівень оперативного управління («Управління»);
- рівень контролю і безпеки («Контроль і безпека»);
- рівень розробки («Розробка»);
- рівень інтеграції («Інтеграція»);

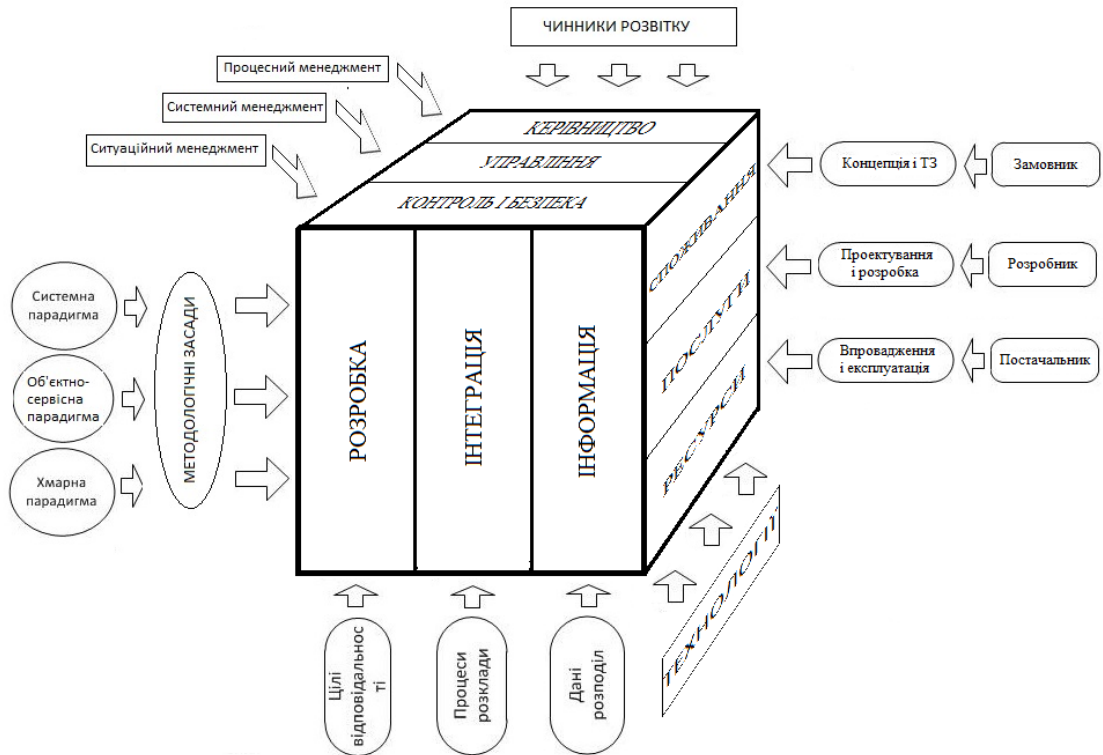


Рисунок 5. Зовнішні впливи на систему.

- рівень обробки інформації («Інформація»).

Рис. 6 містить загальний погляд на архітектуру корпоративної розподіленої інформаційної системи з умовним відображенням рівнів і компонентів системи, що складають ці рівні.

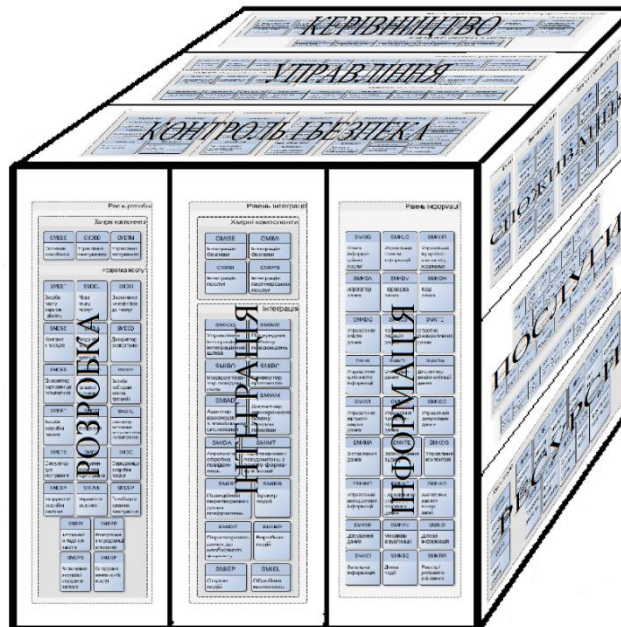


Рисунок 6. Загальний погляд на архітектуру КІС.

Ринкова потреба [8] в розробці подібних архітектурних моделей існує, незважаючи на те, що зростає популярність ІТ-рішень для КІС на базі прикладних платформ, які пропонують провідні вендори ІТ. Запропонована модель архітектури:

- відповідає новітнім та класичним принципам і методам, і тому за наявності різних підходів до керівництва та управління в галузі інформаційних технологій організації та підприємства можуть використовувати її в якості узагальнюючої моделі;
- поєднує стандарти та наукову інформацію, розташовану в різних джерелах, з урахуванням того, що вона створена в результаті проведених досліджень, об'єднує всі ці напрацювання, моделі та підходи;
- вона відображує організацію та інформаційну систему в цілому, створюючи основу для ефективної інтеграції інших підходів, стандартів та методів, служить цілісним джерелом рекомендацій;
- містить ряд рекомендацій, які можуть стати основою для розвитку корпоративних інформаційних систем;
- являє собою просту модель архітектури, що полегшує структурування рекомендацій стандартів та пов'язаних з ними методів у узгоджену сукупність проектних рішень.

Таким чином, запропонована модель архітектури реалізує єдиний і цілісний підхід, необхідний для розробки та впровадження корпоративних інформаційних технологій на основі парадигми хмарних обчислень.

ЛІТЕРАТУРА

1. Biro M., Business Drivers and Challenges of Cloud Computing and Social Networking Application Development. In Proceedings of the IFIP TC8 WG8.9 International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS 2009) (ed. by M. Raffai)
2. Управление в иерархических производственных структурах/ Подчасова Т.П., Лагода А.П., Рудницкий В.Ф.; Отв.ред.Шкурба В.В.; АН УССР.Ин-т киберн.-Киев:Наук.думка, 1989.-184с.- ISBN 5-12-000538-1.
3. Месарович М., Мако Д., Такахара И. Теория иерархических многоуровневых систем.-М:Мир, 1973.-344с. (Mesarovic M., Macko D., Takahara Y.,1970. Theory of Multi-level Hierarchical Systems. Academic Press, 1970.)
4. ANSI Study Group on Database Management Systems. Interim Report, FDT, vol. 7, no. 2, ACM, 1975.] .

5. C. Finkelstein, Information Engineering Methodology, pp. 459-483 in Handbook on Architectures of Information Systems, Editors P. Bernus K. Mertins, G. J. Schmidt, Springer-Verlag Berlin Heidelberg, 2006, ISBN 978-3-540-25472-0]

6. ДСТУ ISO/IEC 17789:2015 : (ISO/IEC 17789:2014 IDT) : Інформаційні технології. Хмарні обчислення. Еталонна архітектура (Information technology - Cloud Computing - Reference Architecture), — Чинний від 01.01.2016. — ISO. — 2014. — 53 p.

7. ISO/IEC 18384-2:2016 Information technology -- Reference Architecture for Service Oriented Architecture (SOA RA) -- Part 2: Reference Architecture for SOA Solutions

8. Кривонос Ю.Г., Івлічев В.П., Гавриленко С.О., Щетинін І.Є. Базові теоретичні принципи та архітектурні основи створення корпоративних розподілених інформаційних технологій на засадах моделі хмарних обчислень // Збірник матеріалів міжнародної наукової конференції "Сучасна інформатика: проблеми, досягнення та перспективи розвитку", (13-15 грудня 2017р.) – Київ: Інститут кібернетики імені В.М.Глушкова НАН України – 2017. – С. 276 – 278.

Браїловський М. М., Захарченко Є. О.

Київський національний університет

імені Тараса Шевченка, м. Київ.

⁽¹⁾ *bk1972@ukr.net*

⁽²⁾ *jenua.zahar4enko@gmail.com*

РОЗПОДІЛ ПАМ'ЯТІ ЗОВНІШНІХ НОСІЇВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ТА МОДИФІКАЦІЇ

Today, Internet technologies are evolving faster and faster. We use social networks to communicate and transfer files. More and more data is transmitted via the Internet. There are more and more hacking methods, there is a high probability of unauthorized use of personal data, information for the benefit of the attacker. There are also more and more viruses and spyware that can be secretly installed on computers, collect and modify data, and use your device's resources.

Thus, the issue of transmission and storage of information is one of the most important issues of human security and personal data.

Keywords: *external storage media, virtual disk, confidential information, access distribution, invisibility.*

Через ресурси мережі інтернет, соціальні мережі зловмисники можуть підключитися до мобільного пристрою та викрасти персональні дані. Один телефон, залишений без паролю надає зловмиснику можливості здійснити придбання на значну суму, форматувати всі дані, включно з хмарного сховища і навіть знищити соціальне життя людини. Передача та зберігання інформації потребує детального розгляду та знаходження надійного способу його здійснення.

Для передачі закритої інформації краще використовувати зовнішні носії інформації ніж інтернет чи хмарні сховища. Так як, доступ до останніх не передбачає прямого доступу до системи. Це можливо здійснити з будь-якого місця, де працює Wi-fi, мобільна чи будь яка інша безпроводова мережа.

Наразі існують багато типів зовнішніх носіїв інформації. Серед яких найбільш відомі дискети, компакт диски, жорсткі диски, карти пам'яті та флеш-носії. Деякі з них застарілі, мають на сьогоднішній день відносно малу пам'яті або просто не актуальні.

На сьогодні для зберігання та передачі даних використовуються USB-флеш-накопичувачі, жорсткі диски та карти пам'яті. Але всі вони мають як свої переваги, так і недоліки.

Карти пам'яті мають занадто маленькі розміри. Для їх використання на комп'ютері слід використовувати спеціальні пристрої для читання карток – картридери. Крім того їх легко загубити.

Зовнішні жорсткі диски маючи великі об'єми пам'яті інформації, що зберігається, є не зручними у фізичному перенесенні. Їх габарити та вага занадто великі для постійного переміщення з одного місця на інший.

Флеш-носій є, напевно, найдоцільнішим варіантом для повсякденного використання. На ньому можна зберігати безліч документів. У наш час USB-накопичувачі можуть містити терабайти інформації. Більшість персональних комп'ютерів підтримують цей формат.

Існують різні інструменти захисту даних на USB-накопичувачах. Один з основних кроків для захисту інформації використовують шифрування [1]. Для забезпечення доступності встановлюються паролі. Часто використовують прив'язку до інформації про користувача / серійного номера компонентів його комп'ютера. Для захисту від копіювання найчастіше використовують наступні

методи: запис інформації в невикористовуваних секторах та перевірка розташування і вмісту «збійних» секторів. Ці методи практично не приносять користі завдяки можливості зняття повного образу з носія з використанням відповідного прикладного програмного забезпечення[2].

Основна ідея захищеності зовнішнього носія в роботі авторів, полягає в розподіленні пам'яті на дві частини. Одна з них буде прихована для користувача та для системи.

Для отримання доступу до прихованого сховища буде використовуватися порівняння ключових файлів на обох частинах пам'яті. Тобто у закритій області існує ключ-зразок, який повинен бути ідентичний певному файлу на відкритому диску. Наприклад, ми можемо мати папку - RIZNE. Для відкриття закритої частини повинна бути створена аналогічна тека з таким же самим змістом. Великою перевагою цього надзвичайна велика варіативність ключа. Це може бути файл будь-якого формату з різноманітним змістом. Це може бути як текстовий документ, так і зображення чи файл програми [3].

При використанні на сторонніх пристроях це буде звичайна флешка, без атрибутів захищеної флешки. Тобто у звичайного користувача навіть не буде гадки про приховану інформацію. Навіть при її втраті та повному форматуванні закрита область залишається цілою та недоступною.

У разі втрати пароля можна використовувати перевірки прив'язку до інформації серійного номера компонентів комп'ютера.

Таким чином, використання запропонованого методу захисту даних на зовнішньому мобільному носії буде забезпечувати основні властивості інформації: конфіденційність, цілісність та доступність.

ЛІТЕРАТУРА

1. Задірака В.К., Кудін А.М., Людвиченко В.О., Олексюк О.С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: Навчальний посібник. – Київ; Тернопіль: Підручники і посібники, 2007. – 272 с.

2. Петренко А. Б. Протидія витоку інформації через з'ємні носії в автоматизованих системах / А. Б. Петренко, Е. В. Бетанов // Інформатика і комп'ютерні технології: VII міжнародна наук.-техн. конф.: зб. праць. — Донецьк: ДонНТУ, 2011. — С. 259—260.

3. Браіловський М.М., Ткаченко А.С. Захист та приховування інформації в графічних та мультимедійних об'єктах на базі стеганотехнологій. // Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів

доповідей та тез; м. Київ, 05-06 квітня 2018 року; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. К.: ВПЦ «Київський університет», 2018. – 510 с. С.444-447.

Бучик С. С.

Київський Національний університет імені Тараса Шевченка, м. Київ

e-mail: buchuk@knu.ua

Симониченко Я. А.

Національний авіаційний університет, м. Київ

e-mail: yaroslavsim@ukr.net

Симониченко А. А.

Київський Національний університет імені Тараса Шевченка, м. Київ

e-mail: annasim98@ukr.net

СТЕГАНОГРАФІЧНІ МЕТОДИ ДЛЯ РЕАЛІЗАЦІЇ ПОСЛУГ ЗАХИСТУ ІНФОРМАЦІЇ

The abstracts of the report identify the possibility of using steganographic methods of protection in order to implement information protection services of state information resources. The authors believe that such security services may include the services "Sender Authentication" and "Exchange Confidentiality". This indicates the direction of research into the possibility of using steganographic methods to protect government information resources and consider their protection as meeting the requirements of relevant services in the information and telecommunications system.

Keywords: *information protection; steganographic methods; the steganographic system; government information resources; services information security.*

Для державних установ важливим питанням є забезпечення інформаційної безпеки (ІБ) та захист інформації (ЗІ) під час її обробки в інформаційно-телекомунікаційних системах (ІТС).

Захист державних інформаційних ресурсів (ДІР) виконується безпосередньо через реалізацію комплексної системи захисту інформації (КСЗІ). В статті [1] авторами було запропоновано визначення комплексної системи захисту державних інформаційних ресурсів як сукупності організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист державних

інформаційних ресурсів, що підлягають захисту згідно визначеної політики безпеки й чинного законодавства в інформаційно-телекомунікаційних системах (інформаційних, телекомунікаційних, інтегрованих системах) держави, суспільства або громадян. Таким чином одним із важливих заходів ЗІ ІТС – це впровадження та використання різних засобів захисту.

Оцінки механізмів захисту програмних/технічних засобів ЗІ та оцінка функцій ЗІ, що використовується при побудові КСЗІ виконується згідно встановлених функціональних критеріїв (ФК). ФК мають чотири групи, що описують вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів: цілісність, конфіденційність, доступність та спостереженість.

З аналізу літератури [2,3], можна зробити висновок з приводу використання стеганографічних методів приховування інформації, щоб вирішити основні завдання в задачах ЗІ: захист авторського права на інтелектуальну власність із використанням цифрових водяних знаків; захист конфіденційної інформації від несанкціонованого доступу; організація прихованих каналів витоку інформації; проходження механізмів захисту технічних засобів захисту при реалізації загроз.

Втілення стеганографічних методів приводить до створення спеціальних стеганографічних систем. Стеганографічна система – це об'єднання методів і засобів, які використовуються для створення прихованого каналу передачі інформації. Стеганосистема вбудовує приховане повідомлення в певний інформаційний об'єкт, передає його стеганографічним каналом та декодує приховане повідомлення [2].

Щоб узгодити дії користувачів при використанні стеганосистеми використовують стеганографічні протоколи таких типів: безключові системи; системи із секретним ключем; системи із відкритим ключем та змішані системи [4].

Здебільшого у стеганосистемах вбудовування та декодування прихованого повідомлення відбувається через ключ, який зумовлює алгоритм, що визначає порядок внесення повідомлення в інформаційний об'єкт. Існує два типи стеганосистем: з секретним ключем – використовується один ключ для вбудовування та декодування прихованого повідомлення; з відкритим ключем – для вбудовування та декодування прихованого повідомлення використовуються різні ключі [5].

З огляду на вище описані сфери використання стеганографічних методів та їх реалізацію, є можливість визначити послуги захисту, при реалізації яких можуть використовуватися ці методи. До таких послуг безпеки можна віднести: «Автентифікація відправника» та «Конфіденційність при обміні».

Послуга безпеки «Автентифікація відправника» дає можливість забезпечити захист від відмови від авторства і встановити належність певного об'єкта певному

користувачу, тобто те, що об'єкт був створений або відправлений певним користувачем. При реалізації цієї послуги можуть висуватися вимоги щодо: процедури, які дозволяють встановити, що об'єкт був відправлений (створений) певним користувачем та автентифікація належності об'єкта незалежною третьою стороною; використання протоколу, що дає можливість однозначного підтвердження належності об'єкта незалежною третьою стороною та ін.

Таким чином, використання вище описаної стеганографічної системи та відповідних протоколів, а також, використання стеганографічних методів для приховування невидимої для людини, мітки, що зберігається в інформаційному об'єкті та виявляється спеціальним програмним забезпеченням, дозволяє виконувати вимоги даної послуги.

Послуга безпеки «Конфіденційність при обміні» дає можливість забезпечення захисту об'єктів під час їх експорту/імпорту через незахищене середовище, від несанкціонованого ознайомлення з інформацією, що міститься в них. При реалізації цієї послуги можуть висуватися вимоги відносно політики конфіденційності: визначання рівня захищеності інформації; визначення множини об'єктів, до яких вона належить; забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в об'єкті та ін.

Таким чином, використання стеганографічних методів для реалізації документованих прихованих каналів з метою забезпечення конфіденційності інформації від несанкціонованого доступу під час її обробки в ІТС, дає можливість виконувати вимоги даної послуги із реалізацією вище описаної стеганографічної системи та відповідних протоколів.

Висновок. З метою реалізації послуг захисту інформації ДІР було визначено можливість використання стеганографічних методів захисту. Таким чином, стеганографічні методи дають можливість виконати основні вимоги послуг ЗІ в ІТС, де обробляється інформація, яка містить ДІР. До таких послуг безпеки відносять: «Автентифікацію відправника» та «Конфіденційність при обміні» на різних рівнях. Реалізація вище описаних вимог досягається при використанні механізмів стеганосистеми, відповідних протоколів та її основних показників.

ЛІТЕРАТУРА

1. Юдін О. К. Принципи побудови комплексної системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. – 2015. – № 1 (25). – С. 15 – 20.

2. Юдін О. К. Дослідження сучасних стеганографічних методів та засобів обробки цифрових зображень / О. К. Юдін, Я. А. Симониченко, А. А. Симониченко // Наукоємні технології. – 2017. – №2 (34). – С. 126-133.

3. Конахович Г. Ф. Оцінка ефективності систем захисту інформації в телекомунікаційних системах / Г. Ф. Конахович, О. Г. Голубничий, О. Ю. Пузиренко // Проблеми інформатизації та управління. – 2007. – №3 (21). – С. 75-83.

4. Єлізаров А. Б. Дослідження сучасних програмних стеганографічних засобів приховування інформації / А. Б. Єлізаров, Я. А. Симониченко, А. А. Симониченко // Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації». – 2018. – С. 108-110.

5. Конахович Г. Ф. Захист інформації від витоку по технічних каналах / Г. Ф. Конахович, Є. Л. Назаренко, В. М. Свириденко // Наукоємні технології. – 2009. – №2 (2). – С. 90-93.

Бучик С.С., Швед А.В.

Київський Національний університет імені Тараса Шевченка

м. Київ

e-mail: buchyk@knu.ua

e-mail: w.a.shved@gmail.com

АРХІТЕКТУРА СИСТЕМИ УПРАВЛІННЯ ВІДНОСИНАМИ З КЛІЄНТАМИ НА ПРИКЛАДІ CRM-СИСТЕМИ CREATIO

The abstracts of the report describe the main functions of modern CRM-systems (Customer Relationship Management). On the example of the Creatio system the typical scheme of the CRM-system architecture is considered and the analysis of its key components is carried out

Key words: *Customer Relationship Management system Creatio; architecture of CRM-system Creatio; horizontal scaling.*

Сьогоднішнє збільшення кількості товарів та послуг призводить до зростання конкуренції серед підприємств та виникнення нових способів утримання конкурентної переваги і збільшення прибутку. Саме тому організації намагаються залучати нових клієнтів та утримувати вже існуючих. Звичайно, зі збільшенням кількості споживачів повинна зростати і кількість менеджерів по роботі з клієнтами, але не всі компанії можуть собі дозволити збільшувати штат відповідно до зростання кількості клієнтів. Це призводить або до зменшення швидкості

обслуговування клієнтів, або до зниження якості роботи менеджерів. Обидва варіанти дуже негативно впливають на репутацію підприємства, що зрештою призводить до ще більшого зменшення кількості споживачів товару або послуг та зниження прибутків організації.

Системи управління відносинами з клієнтами призначені для збору, зберігання й аналізу інформації про споживачів, а також для автоматизації споживчих бізнес-процесів, що допомагає персоналу з роботи з клієнтами виконувати свої функції швидше та ефективніше [1].

Базові можливості CRM-системи Creatio дозволяють збирати всю інформацію про клієнтів та контрагентів в єдиній системі, актуалізувати її з відкритих джерел, за допомогою інтеграцій зі сторонніми системами; гнучко налаштовувати весь цикл продажів та створювати каталог всіх продуктів чи сервісів з повним набором їх характеристик та особливостей; використовувати єдине вікно операторів контакт-центру, яке дозволяє користувачам виконувати всі свої робочі функції, не переключаючись між розділами системи [2].

Незважаючи на великий список можливостей CRM-системи (як Creatio, так і будь-якої іншої представленої на ринку), підприємства частіше за все вдаються до розширення існуючих функцій системи та підлаштовують її до власних потреб. CRM-система Creatio дозволяє користувачам на своїй платформі здійснювати користувацьку розробку, що зобов'язує її власників розуміти не лише інтерфейсну частину додатку, а й всю її архітектуру для того, щоб не призвести своїми діями до відмови в роботі системи.

На прикладі CRM-системи Creatio розглянемо два можливі способи побудови такої системи – схему архітектури для задоволення потреб малого бізнесу та схему архітектури з використанням горизонтального масштабування для великих організацій з великою кількістю користувачів.

Розглянемо типову схему архітектури CRM-системи Creatio, що представлена на рис.1.

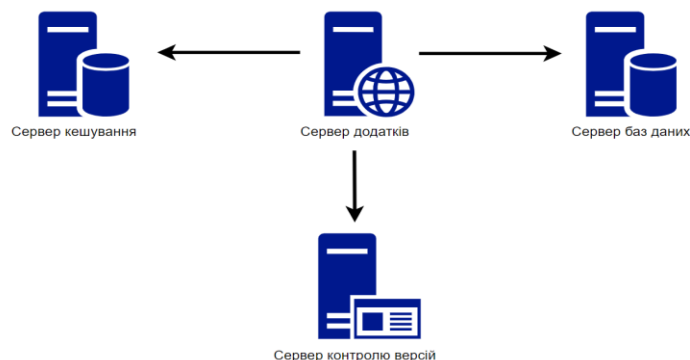


Рис. 1. Схема архітектури основного додатку Creatio

Така типова схема може бути використана на підприємствах з невеликою кількістю користувачів (близько 20 – 100) та не потребує значних витрат на потужні сервери – достатньо використання лише трьох обов’язкових виділених серверів: серверу додатків, серверу баз даних та серверу кешування. Сервер контролю версій в даному випадку є опціональним компонентом схеми та використовується лише у випадку, коли існує багатокористувацька розробка додаткового функціоналу системи.

Сервер додатків виконує основну обчислювальну роботу системи. Додаток на платформі .NET Framework працює під управлінням Internet Information Services (IIS) та складається з завантажувача (WebAppLoader) і конфігураційної частини (WebApp).

Основне призначення завантажувача – виконання службових функцій системи, і подальше перенаправлення користувачів в основну програму Creatio. Після обробки в завантажувачі запиту на авторизацію, користувачі можуть працювати в конфігураційній частині – програмі, яка відповідає за роботу бізнес-логіки системи.

Сервер баз даних. В базі даних додатку зберігаються користувацькі дані, дані, необхідні для роботи системи та конфігураційні налаштування. Найбільш використовуваними системами управління баз даних Creatio є MS SQL Server або Oracle. Також система підтримує PostgreSQL [3].

Сервер кешування Redis відповідає за зберігання даних користувача і додатку (профіль користувача, сесійні дані тощо), зберігання кешованих даних, обмін даними між вузлами веб-ферми.

Redis підтримує такі стратегії зберігання даних [4]:

- зберігання даних лише в пам’яті;
- періодичне збереження даних на диск (за замовчуванням);
- лог транзакцій;
- реплікація.

В Creatio зберігання даних здійснюється в пам’яті з періодичним збереженням дампу на диск [3].

Як вже було зазначено раніше, великим підприємствам недостатньо базової функціональності системи Creatio, тому компанії намагаються власними силами або через посередників розширювати функціонал системи. **Сервер системи контролю версій** є опціональним компонентом додатку та використовується саме у тому випадку, коли паралельно з експлуатацією системи необхідно на платформі організувати розробку користувальницької конфігурації.

Відповідно до того, які завдання ставить підприємство перед CRM-системою, зростають і її масштаби; відповідно до величини підприємства визначається й кількість співробітників, які будуть використовувати систему.

Для CRM-системи організації, що складається з великих бізнес-процесів, які виконують складні, ресурсномісткі функції, та кількість користувачів якої сягає понад 100, 200 або навіть 1000 користувачів, використання одного серверу додатків, одного серверу баз даних та серверу кешування вже не буде достатнім для забезпечення безперервної та стабільної роботи системи.

В такому випадку, підвищити продуктивність великих проектів дозволяє горизонтальне масштабування системи. При цьому схема архітектури системи Creatio (рис. 2) приймає наступний вигляд:

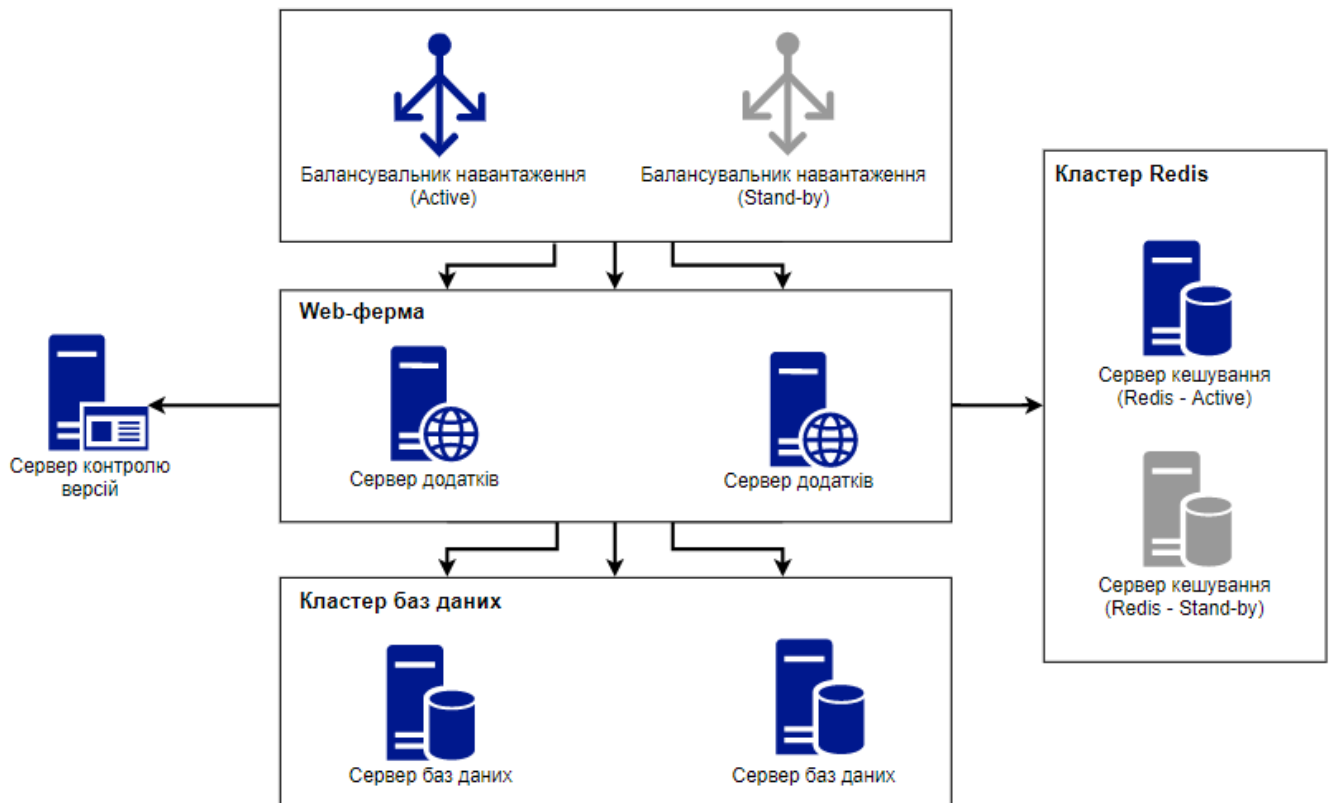


Рис. 2. Схема архітектури основного додатку Creatio при використанні горизонтального масштабування

При використанні горизонтального масштабування обов'язковим компонентом системи є балансувальник навантаження, який може бути як програмним, так і апаратним. У системі Creatio для роботи у відмовостійкому режимі використовується балансувальник HTTP / HTTPS-трафіку з підтримкою протоколу WebSocket – HAProxy. Балансувальник HAProxy підтримує такі операційні системи як Linux, FreeBSD, OpenBSD, Solaris, AIX та являється

програмою з відкритим кодом, що дозволяє переконатися у відсутності вразливостей додатку [3].

Для більшої надійності системи балансувальник навантаження працює в режимі Active / Stand-by, тобто один з балансувальників знаходиться в активному режимі, інший – в режимі очікування; у разі виникнення проблем в активній системі, її роботу замінює резервна система, поки проблема не буде вирішена.

Крім цього, якщо кількість користувачів системи налічує декілька тисяч, звичайні сервери додатків, сервер баз даних та сервер кешування Redis замінюються серверною Web-фермою, кластером баз даних та кластером Redis, відповідно. Такий підхід до реалізації дозволяє мінімізувати відмови в роботі системи.

Розглянувши схему архітектури CRM-системи на прикладі Creatio можна прийти до висновку, що сучасні системи управління відносинами з клієнтами забезпечують гнучкий підхід до вирішення і автоматизації завдань конкретної організації. А використання горизонтального масштабування дозволяє великим підприємствам налагоджувати свої бізнес-процеси без страху втратити при цьому продуктивність системи.

ЛІТЕРАТУРА

1. Шовкопляс С. Как повысить конкурентоспособность при помощи CRM // Office. – 2005. – № 3-4. – с. 12-18
2. Опис CRM-системи Creatio [Електронний ресурс] – Режим доступу: <https://www.terrasoft.ru/page/crm-products>.
3. Документація Creatio Terrasoft [Електронний ресурс] – Режим доступу: <https://academy.terrasoft.ru/documentation>.
4. Документація Redis [Електронний ресурс] – Режим доступу: <https://redis.io/documentation>.

Ващіліна О.В.

Київський Національний університет

імені Тараса Шевченка

vashchilina@ukr.net

АУДИТ ПРОЦЕСІВ РОЗРОБКИ, ВПРОВАДЖЕННЯ ТА СУПРОВОДУ ІНФОРМАЦІЙНИХ СИСТЕМ НА ВІДПОВІДНІСТЬ МІЖНАРОДНОМУ СТАНДАРТУ ЯКОСТІ ISO 9001:2015

The purpose of this Report is to share the practical experience of conducting an internal audit of IT project, obtained by the author as a result of an internship at the IQusion IT Company. This company is a market leader in Ukraine for the development and implementation of high-tech software products and IT solutions for the Public Sector of Ukraine. The Company has implemented a quality management system, which has received a certificate of compliance with the requirements of the international quality standard ISO 9001:2015. There is a checklist according to which the Company conducts an internal quality audit of the IT project (planning and implementation phase) and describes a method of measuring the audit result.

Keywords: *quality standard ISO 9001: 2015, IT project, an internal quality audit, checklist, measuring*

Мета даної доповіді – поділитися практичним досвідом проведення внутрішнього аудиту ІТ-проекту, отриманого автором в результаті проходження стажування в компанії Айкюжн ІТ (IQusion), яке проходило з листопада 2019 по березень 2020 року.

Компанія IQusion націлена на завоювання провідних позицій на ринку високотехнологічних програмних продуктів і ІТ-рішень для Державного сектору України. IQusion впроваджує, супроводжує та модернізує програмне забезпечення, розроблене фахівцями Компанії за час її роботи на ринку ІТ-послуг. Для забезпечення якості розроблюваних інформаційних систем в Компанії впроваджено систему менеджменту якості, яка отримала сертифікат відповідності вимогам міжнародного стандарту якості ISO 9001:2015 в сфері «Розробка, постачання, інтеграція, впровадження та супровід корпоративних інформаційних систем, програмних продуктів, а також послуги у сфері інформатизації і захисту інформації» [1, 2].

Для своєчасного виявлення невідповідностей до вимог Стандарту та своєчасного їх оперативного виправлення в компанії проводиться моніторинг всіх

охоплених системою менеджменту якості процесів у формі проведення внутрішніх аудитів. Зокрема, якість процесів розробки, впровадження та супроводу інформаційних систем перевіряється під час проведення внутрішнього аудиту відповідного проекту. Такий аудит проводиться на всіх стадіях життєвого циклу існування проекту: планування, розробка та завершення. Кожен з видів аудиту проводиться згідно із пунктами спеціально розробленого чек-листа. У таблиці нижче наведені пункти чек-листа для проведення внутрішнього аудиту процесу управління проектом (фаза планування та виконання, стандартний виробничий процес).

№	Предмет проверки
1	Информация по созданному паспорту проекта заполнена в полном объеме и в соответствии с требованиями по заполнению полей
2	Бизнес план прошел утверждение до списания затрат
3	Наличие календарного плана договора/рабочего КП?
4	Наличие плана проекта.
5	Определено ли лицо, ответственное за управление договором?
6	Зафиксированы ли данные по субподряду?
7	Зафиксированы ли риски проекта?
Управление требованиями	
Фаза планирования	
8	Наличие плана управления требованиями
9	Наличие документа с высокоуровневыми требованиями (техническое задание, требования к системе или другой)?
10	Определена ли модель вариантов использования ?
План управления требованиями	
11	Содержит ли план перечень артефактов требований, которые должны быть созданы в ходе выполнения проекта?
12	Содержит ли план описание механизма прослеживаемости, который будет использоваться на проекте?
13	Описаны ли в плане правила обработки и согласования изменений требований?
Фаза выполнения проекта	
14	Разработаны ли все запланированные артефакты требований (если на дату должны уже быть разработаны) в виде запланированных артефактов?
15	Запланированные для требований атрибуты фиксируются для каждого типа требований?

16	Запланированные уровни прослеживаемости (матрица трассирования) по требованиям фиксируются и находятся в актуальном состоянии?
17	Выполняется ли обработка и согласование изменений требований согласно правилам определенным в Плане управления требованиями?
Проектирование и разработка информационной системы (ИС)	
18	Разработан документ «Архитектура ИС»
19	Документ «Архитектура ИС» подвергался технической ревизии (в соответствии с требованиями процесса технической ревизии)
20	В процессе реализации подсистемы/компоненты выполняются мероприятия по улучшению создаваемого кода - Кросс-проверка кода - Рефакторинг кода - Отладка кода - Unit testing
21	В процессе реализации создана необходимая документация
Тестирование	
22	Осуществляется ли планирование работ по тестированию?
23	Ведется ли работа с требованиями?
24	Ведется ли тестовая документация?
25	Настроено ли отдельное тестовое окружение?
26	Активен ли процесс тестирования? Из каких работ состоит?
27	Проводится ли анализ результатов тестирования и корректировка работ по тестированию и разработке?
28	Определены ли условия приемочного тестирования?
Поставка и приемка	
29	В контракте определены требования к приемке, комплектность и способ поставки
30	Результаты приемки ИС регистрируются и анализируются
31	Выявленные заказчиком ошибки ИС устраняются командой проекта
32	Пожелания заказчика по доработкам, усовершенствованию регистрируются и обрабатываются в соответствии с процессом управления требованиями
33	По результатам приемки составлен акт приемки, подписанный заказчиком
Внедрение	
34	Разработан план внедрения
35	План внедрения содержит всю необходимую информацию согласно шаблону
36	Разработана ли программа/план обучения и материалы для обучения

	пользователей
Сопровождение	
37	Определена ли система регистрации сообщений и запросов
38	Все поступившие сообщения зарегистрированы в определенной системе регистрации.
39	По каждому запросу принято решение, либо есть комментарий об аргументированном отказе
40	В системе регистрации в запросах от пользователей указаны сроки реализации и версия ИС, в которой будет реализован запрос.
41	Патчи, которые передаются заказчику, хранятся в репозитории проекта по сопровождению. Новая версия ППК или патч сопровождаются документом «Описание релиза».
Управление конфигурацией	
42	Определено ли на проекте лицо, выполняющее роль менеджера конфигурации?
43	Наличие Плана управления конфигурацией
44	Заполнены все основные разделы Плана УК (или информация указана в полном объеме в Плане проекта)
45	Есть ли в репозитории проекта последняя версия, поставленная заказчику (согласно данным в сетевого графика работ или календарноо плана или протокола о выполненных работах)?
46	Готовит ли менеджер конфигурации при выпуске публичного релиза описание релиза, где описываются основные его функциональные характеристики ?
Технические ревизии	
47	Соблюдены критерии для определения необходимости проведения технических ревизий
48	В плане проекта запланированы технические ревизии, определены эксперты для их проведения. Запланированные ревизии проведены в соответствии с графиком, результаты зафиксированы (протокол с общим заключением)
49	Все обнаруженные дефекты и замечания зафиксированы
50	Автор объекта ревизии исправил дефекты в установленный срок
Управление субподрядом	
51	Прошли ли привлекаемые на проект субподрядчики внутреннюю процедуру сертификации?
52	Запланировано ли в бизнес плане выполнение субподрядных работ?

53	Заключен ли договор с субподрядчиком?
54	Зафиксированы ли в плане проекта особенности организации работы с субподрядчиком?
55	Идентифицированы ли риски, связанные с субподрядом?

Внутрішній аудитор проводить оцінку кожного пункту чек-листа за наступних алгоритмом: у разі відсутності зауважень виставляється 5 балів, у разі виявлення незначних зауважень виставляється 3 бали і у разі виявлення грубих порушень (невідповідностей) виставляється 1 бал. Якщо ж деякі пункти є незастосовними до тих чи інших проектів, то виставляється 0 балів і такі пункти не беруть участі у формуванні загальної оцінки якості виконання проекту. Загальна підсумкова метрика аудиту обчислюється у відсотках за формулою:

$$Q = (1 - (N + M/2) / (P - L)) * 100\%$$

де М-кількість зауважень, N – кількість невідповідностей, L – кількість незастосовних пунктів чек-листа, P – загальна кількість пунктів чек-листа.

Проект відповідає вимогам системи менеджменту якості якщо його метрика $Q \geq 80\%$. У разі недосягнення даного показника проводиться корекція виявлених зауважень та невідповідностей, проводиться аналіз причин їх виникнення.

Таким чином, внутрішній аудит ІТ-проекту є ефективним способом досягнення належної якості інформаційної системи, яка розробляється в результаті роботи цього проекту, дозволяє вчасно виявити та усунути проблемні моменти з метою запобігання повторення подібних ситуацій у майбутньому, а також напрямлений на виявлення корисних практик з метою їх подальшого впровадження в діючу систему менеджменту якості.

ЛІТЕРАТУРА

1. ISO 9001 системы менеджмента качества [Електронний ресурс] // Международная организация по стандартизации : [офіційний веб портал]. – Режим доступу: <https://www.iso.org/ru/iso-9001-quality-management.html>, вільний. – Назва з екрана.

2. Система менеджменту якості [Електронний ресурс] // IQusion: [офіційний веб портал]. – Режим доступу: <https://iqusion.com/main/%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-%D0%BC%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82%D1%83D1%8F%D0%BA%D0%BE%D1%81%D1%82%D1%96/>, вільний. – Назва з екрана.

Верес А.Ю.

Одеська національна академія зв'язку імені О.С. Попова

Київ, Україна

andriy@veres.im

ДОСЛІДЖЕННЯ МЕХАНІЗМУ АДАПТАЦІЇ ДО ЗАВАД В БЕЗДРОТОВИХ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ НАСТУПНОГО ПОКОЛІННЯ

Investigating the possibility of improving the mechanism of adaptation to interference in local area networks of the next generation 802.11ax standard, taking into account the further combination of orthogonal frequency division multiple access (OFDMA) technique and preamble puncturing mechanism, in interference scenarios with non-multiples of 20 MHz signal band in order to further improve the 802.11ax standard in terms of the changes optimal ratio, that need to be made in the signaling exchange.

Key words: *OFDMA, preamble puncturing, 802.11ax, 802.11ac, 802.11n.*

Телекомунікаційне обладнання стандартів 802.11n та 802.11ac набуло неабияку популярність в останні роки, для побудови як корпоративних, так і домашніх ЛОМ. У стандарті 802.11ac абонентський пристрій (STA) та точка доступу (AP) можуть узгоджувати передачу даних адаптивно обираючи смугу передачі для кожного окремого прийнятого та відправленого пакету (PPDU). Надаючи базовий гарантований доступ до каналів зі смугою 20 МГц AP та STA можуть адаптивно змінювати смугу передачі задля збільшення пропускної здатності каналу, шляхом об'єднання декількох каналів зі смугами 20 МГц (в подальшому будемо називати їх "20 МГц субканали") в канали зі смугами 40, 80 та 160 МГц.

В діапазоні 5 ГГц в деяких країнах Світу працюють радарні установки, що використовуються за метеорологічним та військовим призначенням. З урахуванням цього в стандарті 802.11ac окрім історично успадкованого з 802.11n механізму доступу до каналу CSMA/CA, а також механізму автоматичної зміни каналу (ACS), які покликані узгодити роботу декількох пристроїв, сертифікованих згідно з стандартом 802.11, для забезпечення електромагнітної сумісності, був введений механізм DFS – механізм обрання та зміни каналу в залежності від присутності в каналі працюючого радара. При цьому аналізуються так звані

шаблони (patterns) радарних імпульсів з метою виявлення типу радару та прийняття рішення про зміну каналу в залежності від типу радару.

Однак враховуючи неліцензований характер використання радіочастотного ресурсу в діапазоні ISM, при збільшенні смуги передачі збільшується ймовірність впливу завад як з сусідніх каналів зі смугами 20 МГц, так й інших завад, джерела яких – не відомі. Шалена популярність бездротових ЛОМ призвела до появи пристроїв, які не є стандартизовані згідно з 802.11n чи 802.11ac, особливо, які використовуються в сценаріях розгортання систем типу "розумний дім". Через відносно малу потужність випромінювання їх практично не можливо виявити та локалізувати методами радіочастотного моніторингу. Ці пристрої можуть мати смугу передачі відмінну та не кратну 20 МГц, так що механізм ACS не завжди зможе забезпечити 100% їх виявлення. З іншого боку завади, створені такими пристроями, можуть мати поведінку, що не зовсім схожа і на радар – це призводить до того що й механізм DFS не завжди може їх виявити.

В новітньому стандарті 802.11ax, (так званий Wi-Fi 6 покоління), серед наявних поліпшень є два [1], що мають підвищений науковий інтерес:

1) Запроваджена техніка так званого “подавлення преамбули” (preamble puncturing) – коли під час передачі в каналі з достатньо широкою смугою пропускання, наприклад 160 МГц, у випадку коли завада розташовується в межах одного 20 МГц субканалу, для її уникнення раніше можливо було лише зменшити смугу пропускання з 160 МГц до 80 МГц, 40 МГц чи 20 МГц, за рахунок цього сильно знижувалась пропускна здатність каналу. У порівняння з цим в 802.11ax можна узгодити передачу з відключенням будь-якого 20 МГц субканалу, таким чином можливо більш гнучкіше відпрацьовувати вплив завад, також не застосовуючи ACS, щоб не змушувати AP та STA змінювати канал, витрачаючи при цьому дорогоцінний час для передачі даних задля переналаштування на інший канал та проходження процедури з’єднання.

2) На рівні з CSMA/CA запроваджений множинний доступ з ортогональним частотним розподілом каналів, OFDMA, з метою подолання суттєвих недоліків CSMA/CA з точки зору ефективності спільного доступу до каналу, під впливом успіху впровадження та опрацювання в системах LTE. AP та STA можуть узгоджувати який метод множинного доступу вони будуть використовувати.

Це відкриває нові можливості поліпшення роботи зокрема при:

1) Одночасній передачі декільком STA або прийому від декількох STA PPDU [3].

2) Адаптації смуги пропускання за рахунок активації при передачі не всіх піднесучих OFDMA сигналу.

Сучасні техніки цифрової обробки сигналів [2] дозволяють достатньо гнучко керувати піднесучими OFDMA, тому подальша еволюція preamble puncturing з огляду на поступову заміну CSMA/CA на OFDMA є логічною. Відчутною буде різниця між пропускними здатностями в сценаріях, коли смуга завади менша за 20 МГц або коли вона розташована між двома 20 МГц субканалами. При правильному угодженню передачі між AP та STA в присутності таких завад можна буде значно підвищити пропускну здатність каналу порівняно з наявними зараз в 802.11ax методами.

Висновки. Подальше впровадження мереж наступного покоління стандарту 802.11ax за рахунок наявності OFDMA та механізму preamble puncturing відкриває широкі можливості для дослідження алгоритмів адаптації до завад з метою їх покращення та пристосування до завад різного типу, які не можуть бути визначеними наявними на сьогоднішній день механізмами ACS та DFS. Зокрема є необхідність в дослідженнях декількох аспектів:

1) Ефективні алгоритми визначення та локалізації OFDMA піднесучих які піддалися впливу завади.

2) Ефективний обмін службовою інформацією між AP та STA з метою узгодження передачі з подавленням піднесучих, які піддалися впливу завади.

3) Критерії оцінки ефективності роботи механізму з точки зору забезпечення максимально досяжної пропускну здатності.

4) Дослідження продуктивності роботи механізму в умовах великої кількості STA, що обслуговуються AP, так званий BSS (Basic Service Set) та завад які впливають як на весь BSS одразу, так і на окремі STA.

ЛІТЕРАТУРА

1. E. Khorov, I. Levitsky and I. F. Akyildiz, "Current Status and Directions of IEEE 802.11be, the Future Wi-Fi 7," in IEEE Access, vol. 8, pp. 88664-88688, 2020, doi: 10.1109/ACCESS.2020.2993448.

2. United States Patent Application Publication 2004, Subcarrier puncturing in communication systems, US 2004/0264362 A1

3. S. Bhattarai, G. Naik and J. J. Park, "Uplink Resource Allocation in IEEE 802.11ax," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761594.

Вишневецький В.В., Круковський М.Ю.

Інститут проблем математичних машин і систем НАН України,

Київ, Україна

e-mail: vit@immsp.kiev.ua

УПРАВЛІННЯ ЖИТТЄВИМ ЦИКЛОМ ІНФОРМАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

The report discusses modern approaches to managing the life cycle of information systems in accordance with NATO recommendations.

Key words: *information system, life cycle, systems engineering*

Як відомо, до цього часу складні інформаційні системи розробляються в Україні у відповідності до вимог групи стандартів 90-х років 20-го сторіччя ГОСТ 34 (інформаційні технології). Зрозуміло, що документо-орієнтовані вимоги стандартів ГОСТ 34 зазвичай важко виконувати в сучасному швидкоплинному світі. Більш сучасним, на цей час, вважається процесно-орієнтований підхід, який вивчається інженерною дисципліною «інженерія систем».

Цікаво зазначити, що при більш глибокому вивченню процесно-орієнтованих підходів проектування у порівнянні з документо-орієнтованими підходами ГОСТ34 з'ясувалося, що останнім взагалі не передбачено терміну «управління життєвим циклом», хоча поняття «життєвий цикл автоматизованої системи» має визначення і в ГОСТ34. Пояснюється це дуже просто. Для того, щоб управляти, треба детермінувати діяльність по створенню системи до типових процесів, які мають свої входи та виходи. Тоді, обираючи комплекти тих чи інших процесів для конкретного проекту, буде можливим бачити весь життєвий цикл інформаційної системи в динаміці та управляти ним. Самі процеси на цей час вивчаються дисципліною з назвою «інженерія систем» або «системна інженерія» та рекомендовані в стандарті ISO15288, який вже має українську локалізацію та статус ДСТУ [1].

Як можна побачити з рис.1 всього таких процесів на цей час виділено 31 і вони розділені на 4 групи, а саме – процеси угоди, процеси організаційного забезпечення проекту, проектні процеси та технічні процеси.

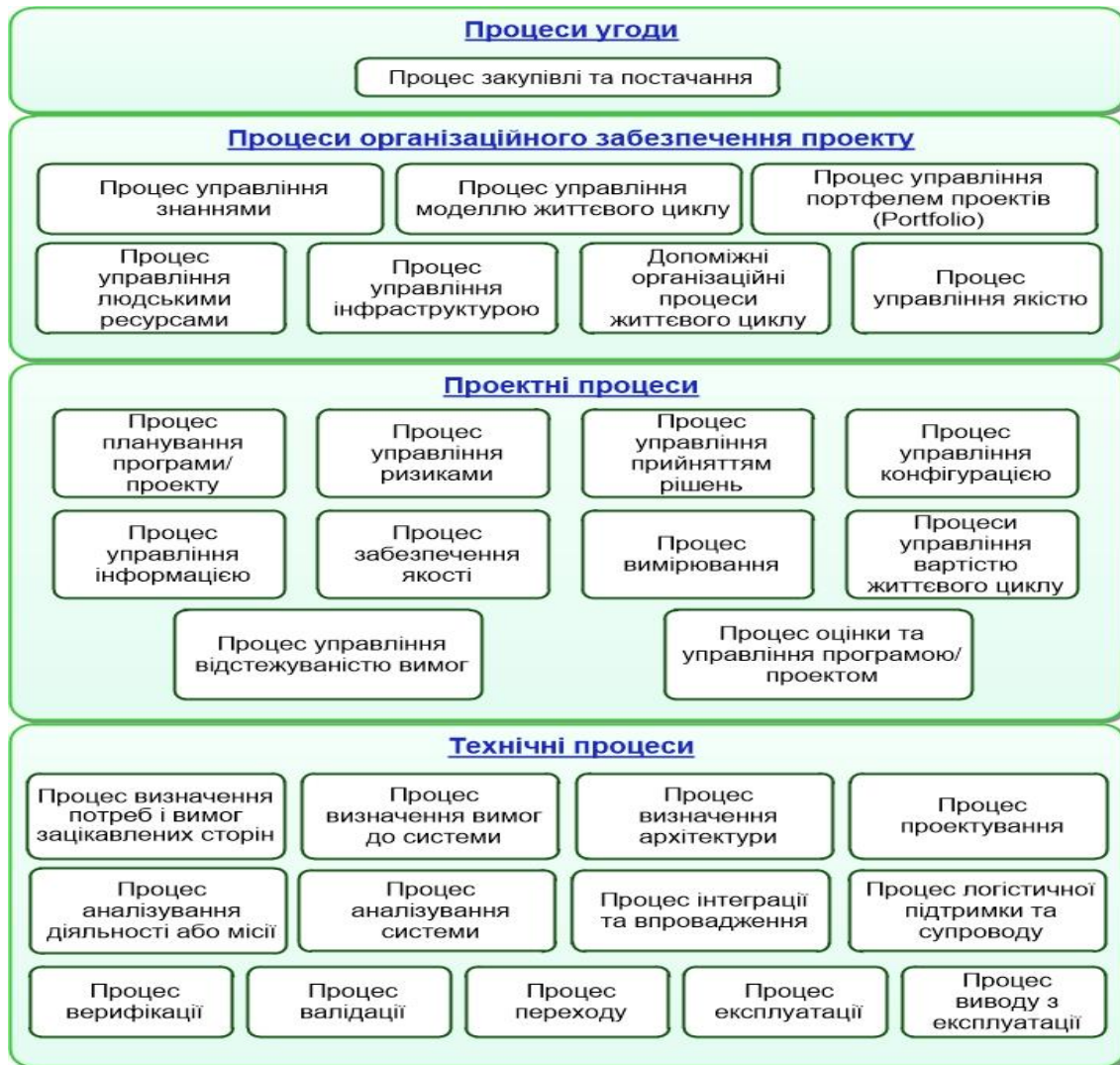


Рис.1 Процеси життєвого циклу інформаційних систем

Найбільш складною задачею в ході управління життєвим циклом, на наш погляд, є організаційні рішення на боці Замовника. Оскільки таку рекомендовану кількість процесів для кожного проекту здатні організувати та виконувати лише відповідні проектні офіси, які на цей час просто відсутні.

Отже, перехід на сучасні підходи управління життєвим циклом інформаційних систем в наших реаліях буде достатньо складним та ще попереду.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC/IEEE 15288:2016 (ISO/IEC/IEEE 15288:2015, IDT) Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем

Гарко І.І., Міронова В.Л.

Київський національний університет імені Тараса Шевченка

м. Київ, Україна

[*garko.iryana@gmail.com*](mailto:garko.iryana@gmail.com)

[*vicky.mironova@gmail.com*](mailto:vicky.mironova@gmail.com)

ВИКОРИСТАННЯ СЕРВІСУ ONLINE TEST PAD ДЛЯ ПРОВЕДЕННЯ ТЕСТУВАННЯ ПІД ЧАС ДИСТАНЦІЙНОГО НАВЧАННЯ ПРИ ВИКЛАДАННІ ПРОГРАМУВАННЯ МОВОЮ JAVA

The talk is devoted to the use of multifunctional service Online Test Pad for testing during distance learning when teaching programming in Java.

Keywords: *testing, programming, Java, distance learning.*

У зв'язку з ситуацією, викликаною пандемією COVID-19 на території України, заклади вищої освіти змушені перейти на дистанційне навчання студентів. Це поставило нові виклики перед викладачами та студентами, адже виникла проблема зміни методики організації навчального процесу: знайти платформи, які допомогали б організувати навчання, підвищити ефективність онлайн-занять та забезпечити об'єктивність оцінювання студентів.

Зупинимось детальніше на проблемі оцінювання студентів, а саме на використанні багатофункціонального сервісу Online Test Pad для проведення тестування при викладанні програмування мовою Java. Звичайно, існує велика кількість систем, за допомогою яких можна проводити тестування, проте є потреба, щоб обрана система дозволяла створювати різноманітні типи завдань для перевірки знань студентів. Зокрема, при викладанні програмування, необхідно використовувати не просто запитання на відтворення теорії, а здебільшого завдання практичного характеру, які б дозволяли перевірити рівень набуття навичок програмування. Серед них можна виокремити завдання на опис результату роботи програми або завдання на доповнення коду, щоб отримати заздалегідь вказаний результат [1].

Система Online Test Pad [2] дозволяє створювати тести із запитаннями понад 15 типів, серед яких завдання, що передбачають заповнення пропусків. До того ж, такі завдання можна використовувати в двох модифікаціях: заповнити пропуски, обравши необхідний елемент зі списку, або самостійно вписавши текст у спеціально відведені поля. Такі задачі дозволяють зацентувати увагу студентів на

ключових моментах написання коду, що в свою чергу допоможе в самостійному написанні програмного коду (рис.1).

У завданнях на заповнення пропусків, вписуючи текст у спеціально відведені поля, потрібно зосередити увагу на виборі місць пропусків, які будуть заповнювати студенти, чітко продумавши всі варіанти їх заповнення для отримання бажаного результату. Система Online Test Pad дозволяє вказати кілька альтернативних варіантів, які будуть захищені в якості правильної відповіді.

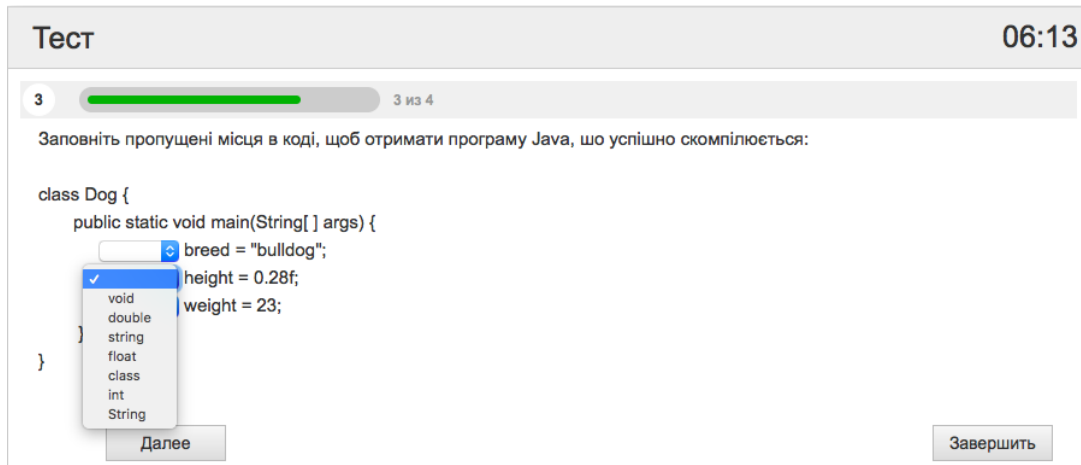


Рис. 1 – Приклад завдання із заповненням пропусків

Серед переваг сервісу Online Test Pad варто також відмітити, що при формулюванні запитань є можливість використовувати фрагменти коду, написані різними мовами програмування (Java, C++, C#, Python та ін.) з підсвічуванням синтаксису. Це дозволяє зробити завдання на опис результату роботи програми більш читабельними та зрозумілими (рис. 2).

Об'єктивність оцінювання знань студентів у системі Online Test Pad забезпечується тим, що сервіс дозволяє зі створеного банку питань (в якому запитання можна об'єднувати в окремі групи) генерувати тести для кожного студента випадковим чином, вказуючи необхідну кількість запитань з кожної групи. Така особливість сервісу сприяє тому, щоб в одному тесті не було однотипних запитань, а також унеможливорює наявність двох однакових тестів, що в свою чергу не дає студентам можливості «списувати» один в одного. Крім того, для того, щоб запобігти тому, що студенти будуть гуглити відповідь на запитання, в налаштуваннях тесту є можливість заборонити копіювання тексту завдання в буфер обміну.



Рис. 2 – Приклад завдання з підсвічуванням синтаксису

Підводячи підсумки щодо використання багатофункціонального сервісу Online Test Pad для проведення тестування під час дистанційного навчання, хотілося б звернути увагу на кілька моментів. По-перше, даний сервіс можна використовувати як для забезпечення поточного оцінювання знань студентів, так і для підсумкового контролю. По-друге, перевагою використання системи є також те, що при тестуванні студенти миттєво бачать результат проходження завдань, що дозволяє звернути їх увагу на проблемні моменти та змушує доопрацювати навчальний матеріал дисципліни.

Таким чином, впровадження онлайн-тестування, значно підвищує ефективність навчання та дозволяє учасникам навчального процесу краще організувати робочий час під час дистанційного навчання.

ЛІТЕРАТУРА

1. Гарко І.І. Інноваційні підходи до навчання бакалаврів технічних спеціальностей на прикладі викладання мови JAVA // Матеріали III Міжнародної науково-практичної конференції "Прикладні системи та технології в інформаційному суспільстві", 1 жовтня 2019 р., Київ, Україна, С. 45-47.

2. Online Test Pad <https://onlinetestpad.com/>

3. Гарко І.І. Використання багатофункціональних сервісів для проведення тестування під час дистанційного навчання в закладі вищої освіти // Екстремне дистанційне навчання в Україні: Колективна монографія / За ред. В.М. Кухаренка, В.В. Бондаренка – Харків: Вид-во КП «Міська друкарня», 2020. – 409 с.

Гладка О. М., Карпович І. М., Живий Я. В.

Національний університет водного господарства та природокористування,
м. Рівне, o.m.hladka@nuwm.edu.ua

ПРИКЛАДНА ПРОГРАМА РОЗПІЗНАВАННЯ ЛІТЕР

An algorithm and an implemented software module for recognizing Latin alphabet characters entered by the user in the drawing area ("hand-drawn") or from downloaded images have been developed. The process of optical character recognition is based on the contouring of letters with their subsequent description using the Freeman's chain code.

Keywords: *optical character recognition; Freeman's chain code; contouring*

Оптичне розпізнавання символів (ОРС або англ. optical character recognition, OCR) – це механічне або електронне переведення зображень рукописного, машинописного чи друкованого тексту в послідовність кодів, що використовуються для представлення в текстовому редакторі. Розпізнавання символів широко використовується для конвертації книг і документів в електронний вигляд, для автоматизації систем обліку в бізнесі або для публікації тексту на веб-сторінках. Оптичне розпізнавання тексту дозволяє редагувати текст, здійснювати пошук слова чи фрази, зберігати його в компактнішій формі, демонструвати або роздруковувати матеріал, не втрачаючи якості, аналізувати інформацію, а також застосовувати до тексту електронний переклад, форматування чи перетворення в мовлення.

Оптичне розпізнавання тексту є досліджуваною проблемою в галузях розпізнавання образів, штучного інтелекту і комп'ютерного зору. Зокрема, методи ОРС застосовуються для розпізнавання підписів, які використовуються в банку та інших закладах з високим рівнем безпеки; для розпізнавання текстури, що використовується при ідентифікації за відбитками пальців; для розпізнання номерних знаків автомобілів в радарях тощо.

Процес ОРС складається з кількох етапів, що включають сегментацію зображення, вилучення ознак та класифікацію, кожен з яких є окремою і доволі складною проблемою. Підсумковий етап ОРС – це класифікація оптичних візерунків, які містяться в цифровому зображенні, що відповідають літерно-цифровим та іншим символам.

Зазвичай, етап попередньої обробки зображення передбачає бінаризацію (у випадку зображення в сірих тонах – це просто питання вибору порогового значення); сегментацію – розділення зображення на окремі символи, позначення

та виокремлення їх; морфологічну обробку – виділення ізольованих плям і дірок у символах, для чого використовується оператор більшості чи ін.

У розробленому алгоритмі як засіб для вилучення ознак було використано найпростіший метод – ланцюговий код Фрімена. І хоча ланцюговий код є хорошим методом кодування зображень і компактним способом представлення контуру об'єкта, він має серйозні недоліки, коли використовується як дескриптор форми об'єкта (текстури, символу). Він застосовний лише на контурних фігурах; чутливий до піксельного шуму, що може призводити до накопичення помилок; на ланцюговий код впливає вибір початкової точки, а також орієнтація і масштаб контуру.

Розроблений програмний модуль, призначений для розпізнання латинських символів, намальованих від руки, або взятих із зображень, які завантажені з диска, являє собою форму з кнопками, текстовими полями та областю для малювання (рис. 1, 2).

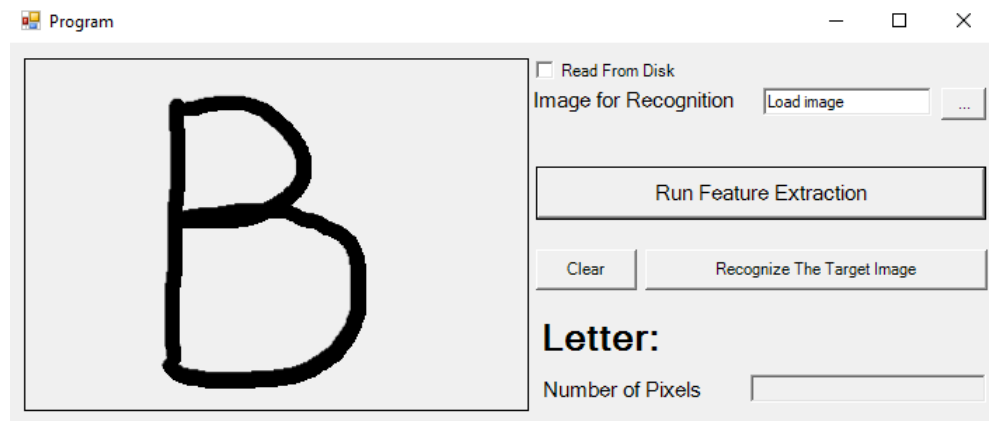


Рис. 1. Початковий інтерфейс програми з намальованою від руки літерою

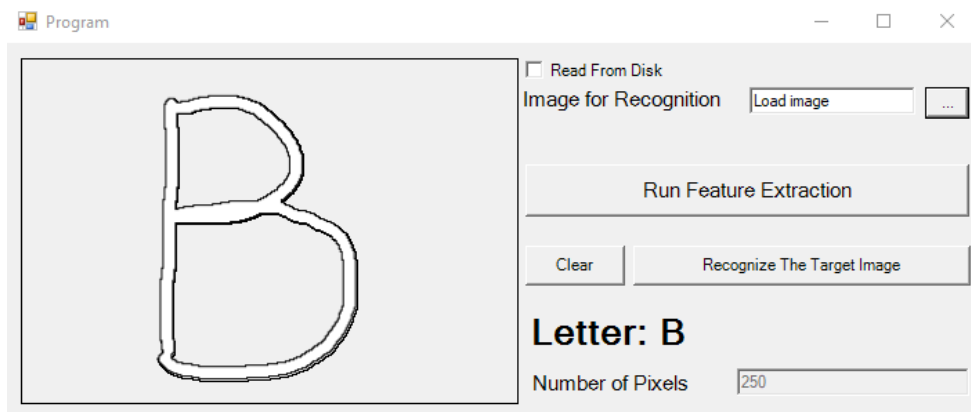


Рис. 2. Результат роботи програми з відконтурованим символом і розпізнаною літерою «В»

Розроблене програмне забезпечення є лише початковим етапом дослідження і має обмежену сферу застосування, оскільки манера написання літер та багато інших чинників можуть впливати на точність розпізнавання символу. В перспективі на основі цього застосунку планується розробити досконаліше

програмне забезпечення із ширшим функціоналом для розпізнавання цифр, слів, речень, рукописного тексту з відповідним «навчанням» системи.

Глушкова В.В.,

*ИК им. В.М.Глушкова НАНУ, г. Киев,
verakiev170@gmail.com;*

Карпец Э.П.,

*ИК им. В.М.Глушкова НАНУ, г. Киев,
keleonora@ukr.net*

ИСТОРИЯ РАЗВИТИЯ ТЕХНОЛОГИЙ ИНТЕРАКТИВНОГО УПРАВЛЕНИЯ В УКРАИНЕ

The paper provides an overview of the scientific achievements of Cybernetics Institute (Ukraine) in the development of technologies of the interactive management of economic and social objects in real time. The periods of formation and the main difficulties of creating are described. The feasibility of using these developments in modern digital transformations is being considered.

Keywords: *technologies real-time interactive management of complex objects , digital economy, innovation , digital infrastructure optimization.*

Одной из важнейших технологий в современной цифровой экономике является **технология интерактивного управления сложными объектами в реальном режиме времени**. По данным Forrester (Fenwick et al., 2017) [1] технология интерактивного управления относится к наиболее значимым технологиям, обеспечивающим цифровую трансформацию бизнеса и экономики.

В последние годы интерактивные технологии принято рассматривать как элемент организации образовательного процесса или систем коммуникации, при котором человеко-машинное взаимодействие имеет циклический характер. При этом в управлении экономикой и бизнес-процессами внедрение данных технологий менее заметно и происходит, подчас, бессистемно.

Целью данной работы есть необходимость осмыслить научное наследие по разработке **технологий интерактивного управления сложными объектами в реальном режиме времени** с точки зрения применения данного опыта в условиях масштабной цифровой трансформации.

Идея использовать *технологии интерактивного управления в реальном времени* в государственных масштабах возникла еще в период становления кибернетической науки. В 1964 году 20-го века в Институте кибернетики под руководством В.М. Глушкова был создан первый в мире проект управления экономикой страны в реальном режиме времени – ЕГСВЦ(Единая Государственная Сеть Вычислительных Центров)[2], который впоследствии был преобразован в проект ОГАС (ОбщеГосударственную Автоматизированную Систему учета и обработки информации)[3].

В докладе [4] В.М.Глушков классифицирует периоды истории развития информационных технологий управления в Украине, выделяя три этапа:

1) первый этап - конец 50-х – начало 60-х гг. прошлого века. В этот период решались в основном простые задачи вычислительного плана для расчета статистики, счетоводства, материальных запасов и т.д.

2) второй период продолжался до начала 70-х гг. и ознаменовался расцветом математического моделирования. Тогда казалось, что с помощью ЭВМ и моделирования можно решать любые наиболее сложные и масштабные задачи управления экономикой, социальными процессами и т.д.

3) однако с накоплением опыта расчетов и просчетов стало очевидным, что «во многих случаях единственно возможный путь решения сложных задач управления обществом состоит в использовании вычислительных машин в режиме диалога в реальном масштабе времени»[4].

Отметим, какие проблемы возникают при решении задач подобного рода.

1. Сложности в нахождении и применении наиболее адекватных моделей, описывающих тот или иной объект, процесс. Часто приходится работать с разными моделями, т.е. с некоторым заранее заданным множеством моделей, каждый раз, выбирая наиболее подходящую для новых данных и новых процессов.

2. Работа с постоянно меняющимися в течение времени данными. По сути это есть работа с BigData.

3. Работа с информацией, выраженной в качественных показателях, а не в количественных.

4. Существование противоречия «между сложностью задач, стоящих перед современным обществом, с одной стороны, и личным характером знаний и ответственности, необходимых для их решения, с другой стороны» [4].

В.М. Глушков отмечал, что интерактивное управление (человеко-машинное управление кибернетическими системами), является одним из главных путей эффективного решения многих сложных и глобальных проблем, стоящих перед

человечеством: управление экономикой в государственном и международном масштабе, экологией, космосом и др.

В институте кибернетики АН УССР в 70-х годах было предложено и реализовано много новаторских разработок этого направления.

Создавались АСУ (Автоматизированные Системы Управления) предприятиями, министерствами и отраслями, Для управления технологическими и экономическими объектами разрабатывались пакеты прикладных программ, аккумулирующие математические модели, которые могли быть применимы при работе с этими объектами, В дальнейшем создавались экспертные системы и системы поддержки принятия решений различного назначения,

Для автоматизации работы с неколичественными процессами в киевском Институте кибернетики была, например, разработана система реализующая идею коллективного мозга. Эта система позволяла «осуществлять в вычислительной машине определенный обмен мнениями с многими сотнями и тысячами экспертов в разных, но взаимосвязанных областях» [4].

Проблему больших данных предполагалось решать за счет создания ОГАС (ОбщеГосударственной Автоматизированной Системы учета и обработки информации), где управление экономикой страны предполагалось вести в реальном режиме времени от каждого рабочего места до макроэкономического уровня.

В.М.Глушков предложил, а в Институте кибернетики разработали и создали уникальную даже на сегодняшний день систему интерактивного управления и оперативного планирования экономикой СССР в реальном режиме времени – ДИСПЛАН (Диалоговая Система ПЛАНирования)[5]. Глушков писал, что «ДИСПЛАН - это не просто очередная модель планирования на верхнем уровне, а принципиально новая технология планирования на всех уровнях, основанная на индустриальной базе машинной информатики»[6].

Оперируя современной терминологией, уже тогда (на концептуальном уровне) постулировалось, что задача не сводится к разработке и управлению в реальном режиме времени отдельными технологическими, организационными или бизнес процессами, а предполагается интеграция информационно-коммуникационных технологий (ИКТ) во всю социально-экономическую среду.

Следует учитывать, что фактически за последние десятилетия существенно изменилась не только технологическая компонента, но усложнилась и социально-экономическая среда. Нарушение важных макроэкономических пропорций влияет на углубление дисбалансов как для мировой экономики, так и экономики отдельной страны, что требует разработки интерактивных средств поддержки

принятия решений для согласования всей цепочки социально-экономических процессов.

В Украине в последнее время практическое применение интерактивных технологий управления затруднено тем, что приходится моделировать деятельность большого количества экономических структур (агентов), находящихся под влиянием последствий финансово-экономического кризиса, политической нестабильности, экологических и эпидемиологических угроз. Сейчас возникла необходимость мониторинга и согласованного преобразования структурных диспропорций в экономике страны, которые искажают базовые функциональные связи между производством и денежным обращением. Фактически на базе современных инновационных технологий и соответствующего математического аппарата стоит задача управления не самими социально-экономическими процессами, а их постоянным изменением.

При этом важна единая концептуальная, технологическая и организационно-экономическая платформа для интеграции всех сфер человеческой деятельности. Однако, реализация в последние годы организационных задач становления цифровой экономики, как составного элемента информационного общества, происходила в Украине довольно быстро, а подчас и спонтанно. Это обусловлено как стимулирующим действием внешнеэкономической среды, так и потребностью стабилизации национальной экономики. Институциональные меры, такие как разработка Концепции развития цифровой экономики и общества в Украине на 2018-2020 годы, соответствующего Плана мероприятий по ее реализации и процесс согласования законодательной базы с интересами высокотехнологичных компаний [7], - разрабатывались достаточно форсировано. В результате имеем быстро подготовленную институциональную базу, но вместе с тем остается без детальной проработки много вопросов как практического, так и методологического характера.

Важной задачей является определение структурных преобразований, которые позволят максимально использовать инновационный потенциал для внедрения такого элемента цифровой экономики, как сбалансированное формирование цифровой инфраструктуры, что позволит повысить конкурентоспособность как традиционных промышленных видов экономической деятельности, так и быстро развивающейся сферы услуг. Следует учитывать, что этот процесс должен сопровождаться соответствующим совершенствованием цифровых навыков и компетенций работников, которые будут отвечать потребностям высокотехнологичных рабочих мест.

Решение данного вопроса считают одним из стратегических на пути к гармонизации структурно-организационных аспектов цифровой экономики Украины с соответствующими компонентами в странах Европы.

Рассматривая пути решения данного вопроса, мало кто из чиновников вспоминает о накопленном опыте по созданию автоматизированных систем управления технологическими процессами (АСУ ТП), АСУ предприятий и учреждений, а также подготовке персонала соответствующего уровня. Забывают об основных принципах автоматизации, сформулированных В.М.Глушковым еще в 1974 году в его работе «Введение в АСУ»[8], таких как наличие *системного подхода* при решении задач, *единства ближних и дальних целей*, *принципа первого руководителя* и др.

Концептуальное и научное обоснование системного подхода к реализации масштабных цифровых преобразований в социально-экономической среде, которые были разработаны в Институте кибернетики, могут быть успешно использованы на современном этапе цифровизации. Особенно в части соблюдения принципов автоматизации управления [8] и использования математического аппарата, разработанного для адекватного мониторинга, анализа и моделирования экономических и социальных процессов в системах принятия решений различных уровней.

ЛИТЕРАТУРА

1. Цифровізація економіки України: трансформаційний потенціал. За редакцією В.П.Вишневецького, С.І Князева. - Київ , 2020. - С.47.
2. ПРЕДЭСКИЗНЫЙ ПРОЕКТ (предварительный вариант) Единой Государственной сети вычислительных Центров СССР (ЕГСВЦ) [Электронный ресурс]. – Режим доступа: <http://ogas.kiev.ua/library/predeskyznyj-proekt-predvartelnyj-varyant-edynoj-gosudarstvennoj-sety-vychyslytelnyh-tsen-0>.
3. Глушкова В.В., Жабин С.А. ОГАС В. М. Глушкова: История проекта построения информационного общества. [Электронный ресурс]. – Режим доступа: <https://commons.com.ua/uk/ogas-v-m-glushkova-istoriya-proekta-postroeniya-informatsionnogo-obshhestva/>
4. Глушков В.М. Некоторые проблемы использования вычислительных машин для управления социальными процессами. [Электронный ресурс]. – Режим доступа: <http://ogas.kiev.ua/glushkov/nekotorye-problemy-yspolzovanyua-vychyslytelnyh-mashyn-dlya-upravlenyya-sotsyalnymy-protses>
5. Глушков В.М. ДИСПЛАН — новая технология планирования. Управляющие системы и машины. - 1980.- № 6.- С. 5–10.

6. Глушков В.М., Каныгин Ю.М. Основы экономики и организации машинной информатики. - Киев – 1981. - 64с. URL: <http://ogas.kiev.ua/library/osnovy-ekonomyky-y-organyzatsyy-mashynnoj-unformatyky-833>.

7. Концепція розвитку цифрової економіки та суспільства в Україні на 2018-20120 роки.- Розпорядженням Кабінету Міністрів України від 17 січня 2018 року, №67-р.URL:<http://zakon.rada.gov.ua/laws/show/67-2018-%D1%80>

8. Глушков В.М. «Введение в АСУ», Киев.- 1974. – 321с.

Гнатієнко Г.М.,

*кандидат технічних наук, факультет інформаційних технологій,
Київський національний університет імені Тараса Шевченка, g.gna5@ukr.net*

Гнатієнко В.Г.,

*студент Інституту прикладного системного аналізу,
Національний технічний університет України «Київський політехнічний
інститут імені Ігоря Сікорського», м. Київ, ambience@ukr.net*

ТЕХНОЛОГІЯ ТЕСТУВАННЯ З ВИКОРИСТАННЯМ ЗАКРИТИХ ЗАПИТАНЬ ПРИ МНОЖИННОМУ ВИБОРІ ВАРІАНТІВ ВІДПОВІДЕЙ

Розглянуто систему «Іспит» автоматизованої підтримки процедур оцінки знань у різних предметних областях. Запропоновано технологію тестування респондентів з використанням закритих запитань, орієнтовану на множинний вибір варіантів відповідей.

Ключові слова: *тестування, оцінювання, множинний вибір, закриті запитання, тестове завдання, формалізація.*

Рассмотрена система «Испит» автоматизированной поддержки процедур оценки знаний в различных предметных областях. Предложена технология

тестирования респондентов с использованием закрытых вопросов, ориентированная на множественный выбор вариантов ответов.

Ключевые слова: *тестирование, оценка, множественный выбор, закрытый вопрос, тестовое задание, формализация.*

The system «Icnum» of automated support of knowledge assessment procedures in different subject areas is considered. The technology of testing respondents using closed questions, focused on multiple choice of answer options, is proposed.

Keywords: *testing, evaluation, multiple choice, closed question, test task, formalization.*

Процедура тестування застосовується в різних галузях людської життєдіяльності: програмуванні, техніці, медицині, психіатрії, освіті тощо. Зокрема, у навчальній діяльності важливим елементом та одним з найважливіших компонентів є контроль. Причому, педагогічний контроль виконує одночасно кілька функцій: навчальну, діагностичну, оціночну, стимулюючу, розвиваючу, виховну тощо.

Тестування є зручним, але неоднозначним способом оцінювання знань [1]. Ця процедура містить немало «підводних каменів», елементи неоднозначності, недостатньої обґрунтованості. Існує багато думок щодо доцільності використання тестів: з одного боку тести розглядаються як засіб позитивного перетворення навчального процесу в бік його технологізації, зниження трудомісткості та об'єктивності; з іншого – в тестах вбачається засіб приниження ролі педагога, а результати тестування вважаються недостатньо достовірними. Наприклад, є інформація, що Ілон Маск вважає тести неефективними і пропонує від них відмовитися, оскільки вони загубили американську освіту. Однак, слід зазначити, що саме тестування поступово стає основною формою складання іспитів.

Водночас невірний підхід до організації тестування або необґрунтована оцінка можуть бути причиною апеляцій, демотивації опитуваних, претензій до викладачів, закидів щодо несправедливого та непрозорого оцінювання, спорів,

разночитань та іншого роду непорозумінь. Тому дослідження деяких нетривіальних типів запитань, які використовуються при тестуванні, є актуальним та необхідним. Незважаючи на всебічну і почасти обґрунтовану критику, тестування освітнього процесу має цілу низку переваг:

- воно є якісним та об'єктивним способом оцінювання, оскільки стандартизовано процедури проведення та перевірки показників якості тестових завдань для усіх опитуваних у групі;

- тест є достатньо точним інструментом, оскільки шкала оцінювання тесту залежить від кількості запитань, які до нього включено, і може значною мірою варіюватися;

- це об'ємний інструмент, який дозволяє визначити рівень знань опитуваного по усій навчальній дисципліні у цілому та по окремих її розділах;

- це м'який інструмент, який ставить усіх опитуваних в однакові умови, використовуючи єдину процедуру та єдині критерії оцінювання;

- є справедливим методом оцінювання знань, який ставить усіх опитуваних в однакові умови в процесі контролю та процесі оцінювання знань, суттєво усуваючи суб'єктивізм викладача: є інформація, що тестування дозволяє знизити число апеляцій більше ніж у тричі;

- є економічно ефективним адже основні витрати при цьому способі оцінювання мають одноразовий характер і є значно нижчими, ніж при письмовому чи усному контролі.

Види тестових завдань. Тестові завдання традиційно поділяються на дві великі групи:

- тестові завдання закритого типу;

- тестові завдання відкритого типу.

У цій роботі будемо досліджувати завдання закритого типу – коли кожне запитання супроводжується варіантами відповідей, з яких слід вибрати декілька

вірних. У свою чергу, закриті завдання з кількома варіантами вірних відповідей передбачають різні варіанти вибору:

- завдання з множиною варіантів – вибір одного варіанта відповіді з наведеного списку;
- альтернативний вибір: випробовуваний повинен відповісти «так»/«ні»;
- визначення відповідності: випробуваному пропонується встановити відповідність елементів двох списків;
- встановлення правильної послідовності – розташувати елементи списку в певній послідовності, тобто розв'язати задачу ранжування;
- множинний вибір: вибір кількох варіантів відповідей з наведеного тестового варіанту переліку відповідей.

Система «Іспит». Автоматизовану систему «Іспит» підтримки процедур оцінки знань з різних учбових та виробничих дисциплін розроблено у складі програмного комплексу «Персонал» [2, 3] та впроваджено у різних підрозділах кількох підприємств [3, 4]. Систему «Іспит» розроблено з метою автоматизованої підготовки користувачів до проведення деяких стандартизованих класів іспитів. Система функціонує під управлінням MS Windows, написана у середовищі *DELPHI*. Ця автоматизована система призначена для експлуатації в організаціях та установах, діяльність яких пов'язана з ситуаціями складання іспитів, які можуть бути достатньою мірою формалізовані.

Розробка єдиної методології експертних оцінок в автоматизованій системі базується на класифікації запитань залежно від варіантів відповідей [5]. Прикладом є використання варіантів запитань з можливими відповідями типу: «Так-Ні», «один з декількох», «декілька із багатьох», «число», «інтервал», «нечіткий інтервал», «слово», «одне або декілька речень». Для розширення можливостей та сфер застосування системи «Іспит» було розроблено та реалізовано у вигляді програмного забезпечення різні типи запитань.

Програмна система «Іспит» повністю автоматизує процес перевірки значної

кількості типів іспитів, а також передбачає ведення бази даних про учасників іспиту та формування звітних документів. Причому перевірка робіт ведеться на комп'ютерах, з'єднаних в локальну мережу. На одному з них встановлюється керуюча програма, на решті – програми перевірки робіт.

Система «Іспит» містить підсистеми протоколювання та документування інформації, яка здійснює безумовний запис проведення будь-якого іспиту до відповідних файлів. Цей важливий елемент діалогового сеансу передбачено з метою уникнення зловживань у процесі складання іспитів.

Постановка задачі. З метою розвитку математичного забезпечення системи «Іспит» було розроблено додаткову опцію, яка обґрунтовує та авто-матизує процедуру тестування при множинному виборі варіантів відповідей.

Розглянемо формальне описання множинного вибору у закритих запитаннях при тестуванні. Зазначимо, що моделі та методи множинного вибору на базі аксіоми незміщеності досліджувалися також у монографії [6].

Нехай задано множину варіантів відповідей $a_i \in A$, $i \in I = \{1, \dots, n\}$, кількість яких дорівнює n , $n = |A|$. Частина відповідей n_1 , $n_1 < n$, є вірними і вони складають підмножину A^1 , $A^1 \subset A$, а інша частина відповідей n_0 , $n_0 < n$, є помилковими і вони складають підмножину A^0 , $A^0 \subset A$, причому $A^1 \cup A^0 = A$. Крім того, будемо вважати, що усі запропоновані тестовим завданням відповіді $a_i \in A$, $i \in I$, є рівноцінними.

Для багатьох тестових завдань така постановка є природньою та логічною. Наприклад, вибрати серед заданих варіантів чисел ті, які є дільниками заданого числа. Можна навести багато варіантів такого роду завдань. Тобто, такий підхід має місце у повсякденному житті і задача його формалізації при тестуванні є актуальною. Особливість таких задач полягає у тому, що вони відображують відому істину: «Скільки людей – стільки думок». Тому розв'язок має бути

обґрунтованим такою мірою, яку підказує логіка його побудови, політика оцінювання, визначена організаторами тестування, здоровий глузд тощо.

Алгоритм оцінювання. Запропоновано застосовувати алгебраїчний підхід до визначення результатів оцінювання, який успішно використовується у теорії прийняття рішень та при застосуванні технологій експертного оцінювання. При алгебраїчному підході формалізація передбачає обчислення та обґрунтування усіх можливих варіантів відповідей. Максимальна кількість балів за достовірно вибрану підмножину варіантів дорівнює B . Кількість балів за правильно вибраний елемент підмножини вірних відповідей $b = B/n_1$.

Задачі, які апріорно мають залежність від суб'єктивної складової, неможливо розв'язати без застосування евристики. Пропонується евристична формула визначення бальної оцінки за вибір варіантів відповідей у вигляді множини, яку породжують відповіді респондента: $V \subset A$. Причому, кількість елементів $\nu = |V|$ у множині V може бути різною: від 0 до n , $0 \leq \nu \leq n$. Будемо позначати кількість вірних відповідей, вибраних опитуваним, через ν_1 , а кількість невірних відповідей, які він визначив як вірні – через ν_0 , $\nu_1 + \nu_0 = \nu \leq n$. Відповідно, кількість варіантів відповідей, які не задіяно у реакції респондента на запитання, дорівнює $n - \nu$.

Евристика E1. Вводиться значення штрафу k за кожне неспівпадання відповіді, яке дорівнює:

– E1.1 – деякому обґрунтованому коефіцієнту k , який відображує суб'єктивне уявлення організаторів тестування про «ціну помилки», наприклад, $k = 2$;

– E1.2 – значенню виразу $k = 1 + p_0$, де p_0 – ймовірність невірної відповіді;

– E1.3 – значенню деякої встановленої експертами функції $k = f_{E1}(n_0, p_0)$, яка залежить від кількості невірних відповідей та їхньої ймовірності.

Евристика E2. За неповну відповідь, тобто коли $\nu < n_1$, передбачається часткове пропорційне приписування балів:

– E2.1 – відповідно до співвідношення одержаних вірних відповідей $\nu_1 \leq \nu$, до загальної кількості вірних відповідей n_1 ;

– E2.2 – значення деякої встановленої експертами функції $f_{E2}(n_1, p_1)$, де p_1 – ймовірність одержання вірної відповіді.

Звичайно, частково вірна відповідь може бути вгадана респондентом з більшою ймовірністю, але і бали за неї приписуються також пропорційно менші.

Евристика E3. Для ситуацій, коли респондентом не вибрано жодної відповіді ($\nu = 0$) або усі відповіді позначені, як вірні, тобто $\nu = n$, то штрафом є нульова оцінка результату – за відсутність вибірковості: $B = 0$.

Важливою та неоднозначною є ситуація, коли опитуваний не визначив жодної вірної відповіді. У цьому випадку опитуваним може бути зазначено різна кількість невірних відповідей. Залежно від політики планування тестових завдань та позиції особи, що приймає рішення, зазначена ситуація може бути описана та регламентована додатковою евристикою.

Евристика E4.1. При відсутності вірних відповідей оцінка завжди дорівнює нулю, незалежно від кількості помилкових відповідей.

Евристика E4.2. При нульовій кількості вірних відповідей менша кількість невірних відповідей є переважнішою від більшої кількості невірних відповідей.

Для формалізації цієї евристики скористаємося нижнім граничним значенням описаної ситуації. Для цього розглянемо ситуацію $c(\nu_1 = 1, \nu_0 = n_0)$, коли опитуваний визначив одну вірну відповідь і усі n_0 невірних. Відповідно до описуваної технології, значення оцінки визначається такою евристикою.

Евристика E5. Будемо вважати, що ситуація $c(\nu_1 = 0, \nu_0 = 1)$ є наступною за ситуацією $c(\nu_1 = 1, \nu_0 = n_0)$ і погіршує результуючу оцінку на один крок, тобто $c(\nu_1 = 0, \nu_0 = 1) = c(\nu_1 = 1, \nu_0 = n_0) - c(\nu_1 = 1, \nu_0 = n_0 - 1)$. Наступні ситуації визначення результуючої оцінки розраховуються одним із способів:

– E5.1 – спадна функція: $c(\nu_1 = 0, \nu_0 = i) = c(\nu_1 = 0, \nu_0 = i - 1) / k$ для $i = 2, \dots, n_0$.

– E5.2 – ситуація $c(v_1 = 0, v_0 = n_0)$ є рівноцінною з ситуацією $v_1 + v_0 = n$: $c(v_1 = n_1, v_0 = n_0)$ тобто наслідком її є нульова оцінка респонденту. У цьому випадку оцінки за різну кількість невірних відповідей ($v_0 = 1, \dots, n_0$) при нульовій кількості вірних відповідей ($v_1 = 0$) визначаються таким чином:

$$c(v_1 = 0, v_0 = i) = c(v_1 = 1, v_0 = n_0) - i * c(v_1 = 1, v_0 = n_0) / n_0, \quad i = 1, \dots, n_0.$$

Приклад. Нехай розглядається ситуація побудови тестового завдання з такими параметрами: $n = 5$, $n_1 = 3$, $n_0 = 2$. Без зменшення загальності, будемо вважати, що у варіантах відповідей на тестове запитання перші три відповіді є вірними, а останні дві – помилковими. Тобто запитання поставлено так, що вірні та помилкові варіанти відповідей можна представити у вигляді вектора: $(1, 1, 1, 0, 0)$.

У векторах, які відповідають відповідям респондента, елементи будемо позначати таким чином: респондентом вибрано вірну відповідь – «1», вибрано невірну відповідь – «0», відсутність відповіді – «*».

При побудові цього ілюстративного тестового оцінювання застосовуються евристики E1.1, E2.1 та E3. Таким чином, евристики E1, E2, E3 трансформуються у такі варіанти відповідей та обчислюються такі оцінки за них.

$$\text{Відповідь 1: } (1, *, *, *, *)v(*, 1, *, *, *)v(*, *, 1, *, *) = 1/3;$$

$$\text{Відповідь 2: } (1, 1, *, *, *)v(*, 1, 1, *, *)v(1, *, 1, *, *) = 2/3;$$

$$\text{Відповідь 3: } (1, 1, 1, *, *) = 1;$$

$$\text{Відповідь 4: } (1, *, *, 0, *)v(*, 1, *, 0, *)v(*, *, 1, 0, *)v(1, *, *, *, 0)v(*, 1, *, *, 0)v(*, *, 1, *, 0) = 1/3/2 = 1/6;$$

$$\text{Відповідь 5: } (1, *, *, 0, 0)v(*, 1, *, 0, 0)v(*, *, 1, 0, 0) = 1/3/4 = 1/12;$$

$$\text{Відповідь 6: } (1, 1, *, 0, *)v(*, 1, 1, 0, *)v(1, *, 1, 0, *)v(1, 1, *, *, 0)v(*, 1, 1, *, 0)v(1, *, 1, *, 0) = 2/3/2 = 1/3;$$

$$\text{Відповідь 7: } (1, 1, *, 0, 0)v(*, 1, 1, 0, 0)v(1, *, 1, 0, 0) = 2/3/4 = 1/6;$$

$$\text{Відповідь 8: } (1, 1, 1, 0, *)v(1, 1, 1, *, 0) = 1/2;$$

$$\text{Відповідь 9: } (1, 1, 1, 0, 0) = 0.$$

При побудові тестового контенту можна використати евристики, які будуть мати інші закономірності та відповідати іншим конфігураціям відповідей. Залежно від вибору евристик, змінюється чутливість функції, яка визначає значення результуючої оцінки. Але проблема підборутаких евристик не є темою цієї роботи.

Перспективи дослідження. У подальшому слід дослідити модифікації описаного підходу та розвитку ідеї множинного тестування закритого типу:

- ввести оцінки або обчислювати числові значення вірності кожної відповіді чи кластеризувати варіанти вірних відповідей за значимістю;

- враховувати показники складності запитань та відповідей, наприклад, залежно від кількості комбінацій варіантів правильних та неправильних відповідей чи інших чинників;

- розглядати вибір будь-якої кількості закритих запитань з множини відповідей – коли опитуваному невідомо, яка кількість відповідей є правильною, ускладнюючи таким чином виконання завдання;

- вводити відповіді різної ваги або різної близькості до ідеальної, хоча це суперечить деяким принципам тестування;

- враховувати коефіцієнти схожості відповідей та еталону – відповідно до алгебраїчного підходу.

Висновки. У роботі запропоновано новий підхід до обчислення оцінки при тестуванні з використанням закритих запитань, орієнтованих на множинний вибір. Підходи, які використовувалися раніше на практиці, пропонувалися, перш за все, через їхню простоту. Проте у зв'язку з розвитком м'яких обчислень, підходи які раніше використовувалися на практиці, можуть бути доповнені і слід розрізняти, наприклад, повністю невірну відповідь від частково невірної.

Позитивною рисою запропонованого підходу є прозорість апріорно заданих організаторами тестування правил, відсутність ситуацій невизначеності під час проведення процедури оцінювання, монотонність поведінки функції, яка відображує інтегральну оцінку за відповіді. Відповідно до запропонованої технології, визначення результуючої оцінки є обгрунтованою та формалізованою

процедурою. Крім того, технологія допускає можливість подальшого удосконалення описаного підходу.

ЛІТЕРАТУРА

1. Буйницька О.П. Інформаційні технології та технічні засоби навчання. Навч. посіб. – К.: Центр учбової літератури, 2012. – 240 с.
2. Гнатієнко Г.М. Формалізація задач управління персоналом з урахуванням моделі компетенцій//Вісн. Черкаського держ.технологічного ун-ту. №4, 2005, С.200-206.
3. Бондарчук Ю.В., Гнатиенко Г.Н. Применение модели компетенций при решении задач управления персоналом//Proceeding of the XII-th International Conference “Knowledge-Dialogue-Solution”, June 20-25, 2006, Varna (Bulgaria). – Sofia, FOI-COMMERCE - 2006. – p.165-172.
4. Бондарчук Ю.В., Гнатиенко Г.Н. Управление системой обучения компании с использованием программного комплекса “Персонал”//Proceeding of the Second International Conference “Modern (e-) Learning”, July 1-5, 2007, Varna (Bulgaria). – Sofia, FOI ITHEA - 2007. – p.201-205.
5. Гнатієнко Г.М., Снитюк В.Є. Математичне та програмне забезпечення задач обробки експертної інформації при проведенні іспитів //Искусственный интеллект. – 2010. – №3. – С.638-647.
6. Снитюк В.Є., Юрченко К.Н. Интеллектуальное управление оцениванием знаний. – Черкасы, 2013. – 262 с.

Гончаренко Н. А.

Київський національний університет ім. Тараса Шевченка, м. Київ

rapid.gepard@gmail.com

DARK WEB ЯК ЧАСТИНА ВСЕСВІТНЬОЇ ПАВУТИНИ ТА ЙОГО ВПЛИВ НА СУСПІЛЬСТВО

The visible side of the Internet includes sites that can be found through an ordinary search, while the invisible side — the deep Web — includes sites or networks that cannot be accessed by regular means. This includes databases, academic journals, private networks and so on. Most of the content located in the deep Web exists in websites that require a search that is not implicitly illicit. However, an intensive search will find the dark Web. The dark Web is a small portion of the deep Web that has been intentionally hidden. While innovative methods have been developed for monitoring content on the visible Web in recent years, there are almost no similar tools for the dark Web. Providing evidence showing that the dark Web has turned into a major platform for global terrorism and criminal activities is crucial in order for the necessary tools to be developed for monitoring all parts of the Internet.

Keywords: *Internet, Deep Web, Dark Web, IP, network, anonymity, cybercrime, security, WWW, Tor, onion.*

Багато з нас використовують терміни Інтернет та Всесвітня павутина (World Wide Web) як взаємозамінні, але насправді вони не є синонімами. Інтернет та Web – це дві окремі, хоча і пов’язані речі. Інтернет – масивна мережа мереж (мережева інфраструктура), що з’єднує мільйони комп’ютерів у всьому світі, утворюючи одну систему, в якій будь-який комп’ютер може спілкуватися з будь-яким іншим комп’ютером, якщо вони обидва підключені до цієї мережі. З іншого боку, Всесвітня павутина, або просто Web – це спосіб доступу до інформації через Інтернет або ж модель обміну інформацією, яка побудована на самій верхівці Інтернету. Для передачі даних Web використовує протокол передачі гіпертексту (HTTP) – єдиний метод, за допомогою якого транспортуються дані від відправника до отримувача. Проте Інтернет, а не Web, також використовується ресурсами електронної пошти, робота яких спирається на SMTP та FTP протоколи. У свою чергу, Web – лише частина Інтернету, хоч і досить велика. Нарешті, Deep Web – це, простіше кажучи, частина Web, яка прихована від очей рядового користувача. До нього не можуть отримати доступ звичайні пошукові

системи. Цей масивний підрозділ Інтернету в 500 разів більший за видимий Інтернет.

Як результат, виділяють три якісно різні рівні Web-простору:

- Загальнодоступна мережа: зазвичай вона відноситься до незашифрованої мережі. Цей сегмент Web має відносно низьку анонімність, оскільки більшість веб-сайтів регулярно ідентифікують користувачів за їхньою IP-адресою.

- Deep Web: стосується вмісту в Інтернеті, який не є частиною загальнодоступної мережі. Проведемо аналогію: супер-агент мусить виконати ціль X у локації Y. Але замість того, щоб шукати Y за картою, йому доведеться відвідати Y безпосередньо. На агента чекають для виконання X за умови, якщо йому буде відома адреса Y, але при цьому він не матиме ніяких вказівок, як туди дістатися. Інтернет занадто великий, щоб його могли повністю охопити пошукові системи; таким чином, глибока павутина значною мірою завжди присутня. У Deep Web, як правило, згадуються веб-сторінки, що невидимі для засобів традиційних пошукових систем. Найчастіше для сканування глибоких веб-ресурсів використовують спеціальні веб-сканери, які на основі ключових термінів, наданих користувачами або зібраних з інтерфейсів запиту, звертаються до відповідної веб-форми.

- Dark Web (темна павутина): частина глибокої павутини, до якої можна отримати доступ лише за допомогою певного програмного забезпечення, конфігурацій або авторизації, часто використовуючи нестандартні протоколи та порти зв'язку. Onion-маршрутизація використовується для доступу до таких веб-сайтів, сукупність яких називається мережею Tor. Трафік при такій маршрутизації багаторазово шифрується, а потім надсилається через кілька мережевих вузлів, які називаються onion-маршрутизаторами. Як тільки хтось «лущить цибулю», кожен маршрутизатор видаляє шар шифрування, щоб розкрити інструкції маршрутизації, і надсилає повідомлення наступному маршрутизатору, де процес повторюється. Цей прийом заважає стороннім вузлам дізнатися походження, пункт призначення та вміст передаваних даних.

Схема на рис.1 відображає різницю між Deep Web, Dark Web та мережею Інтернет.

Щодня наша активність в Інтернеті залишає сліди, які формують нашу цифрову ідентичність у віртуальному просторі. Анонімність використання Інтернету гарантується тоді, коли адреси Інтернет-протоколу (IP) неможливо відстежити. Отже, темна павутина – це частина глибокої павутини, яка була навмисно прихована та недоступна для стандартних веб-браузерів. Темні веб-сайти служать платформою для користувачів Інтернету, для яких анонімність є критично необхідною умовою, оскільки такі сайти не тільки забезпечують захист

від несанкціонованих користувачів, але також зазвичай включають шифрування для запобігання моніторингу.

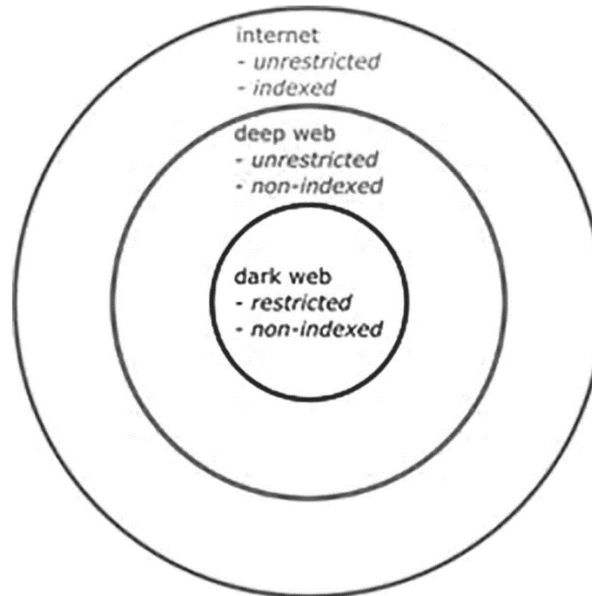


Рис. 1. Відмінності між Deep Web, Dark Web та Internet

Порівняно відомим інструментом для доступу до контенту, що знаходиться в Dark Web, є мережа Tor. Мережа Tor – це анонімна мережа, доступ до якої можна отримати лише за допомогою спеціального веб-браузера, який називається браузером Tor. Вперше дебютований як проект Onion Routing (Tor) у 2002 році Американською морською дослідницькою лабораторією, він був методом анонімного спілкування в Інтернеті. Оскільки Tor спрямовує Інтернет-трафік через всесвітню добровільну мережу серверів, приховуючи інформацію про користувача та уникаючи будь-яких заходів моніторингу, це робить Dark Web дуже доречним ресурсом для кіберзлочинців, які постійно намагаються приховати свій незаконний промисел. Також можливість серфінгу просторами Інтернету з повною анонімністю сформувала платформу, яка дозріла до того, що її використання у деяких країнах вважається незаконною діяльністю. Подібна діяльність, зокрема, найчастіше охоплює:

- ринки збуту заборонених речовин;
- шахрайство з кредитними картками та викрадення особистих даних;
- витіки конфіденційної інформації;
- продаж крадених товарів;
- зброя та екзотичні тварини;
- тероризм;
- незаконні фінансові операції;

- hidden wiki;
- азартні ігри;
- та ін.

Інша відома мережа під назвою I2P надає багато тих самих функцій, що і Тог, однак I2P була спроектована як мережа в Інтернеті, в якій трафік циркулює тільки її в межах. Варто відмітити, що Тог забезпечує кращий анонімний доступ до відкритого Інтернету, а I2P забезпечує більш надійну модель роботи «мережа в мережі». Слід також зазначити, що Тог пропонує можливість користувачу контролювати свою історію переміщень. Для деяких соціальних груп суспільства даний механізм несе, на противагу, досить вагоме позитивне значення: наприклад, інсайдери мають змогу повідомляти новини, які влада з певних причин воліє приховати для журналістів введенням цензури; правозахисники отримують широке поле для боротьби з репресивними діями своїх урядів; дисиденти можуть уникнути контролю авторитарних режимів.

Темна павутина також є найкращим каналом для обміну таємними документами. Анонімні повідомлення мають важливе місце в нашому політичному та соціальному дискурсі. Багато людей бажають приховати свою особистість через побоювання щодо політичної чи економічної розправи.

Професор Австралійського національного університету Пітер Грабоскі (Peter Grabosky) зазначає, що віртуальна злочинність нічим не відрізняється від злочинності в реальному світі – вона просто відбувається в іншому, новому середовищі: «Віртуальна злочинність в основному така ж, як і реальна злочинність, з якою ми знайомі. Безумовно, деякі прояви є новими, але велика кількість злочинів, скоєних за допомогою комп'ютерів або проти них, відрізняється лише в площині сприйняття суспільством. Хоча технологія реалізації, а особливо її ефективність, може бути безпрецедентною, злочин [все одно] принципово знайомий. Мова йде не про що інше, як про звичайний злочин, вчинений докорінно неординарним методом».

Безпека в темній павутині має вирішальне значення для зміцнення впевненості та надійності використання інформаційних технологій. Відсутність безпеки в кіберпросторі підриває довіру до інформаційного суспільства. Прикладом цього є достатня кількість інцидентів по всьому світу, що часто призводять до крадіжки грошей, активів та конфіденційної військової, комерційної та економічної інформації, а тому невпинно зростає потреба в захисті особистої інформації, фондів та активів і навіть національної безпеки. Як результат, сфера дії кібербезпеки набуває інтересу як з боку державного, так і приватного секторів. З появою комп'ютерних та ІТ-програм, кіберзлочинність стала значним викликом у всьому світі. Тисячі кіберзлочинців щодня намагаються

атакувати комп'ютерні системи, щоб незаконно отримати до них доступ через Інтернет. Щомісяця випускаються сотні нових комп'ютерних вірусів та спам, які намагаючись пошкодити комп'ютерні системи, викрасти чи знищити їх дані. Такі загрози є дорогими не лише з точки зору кількості, але й з точки зору якості. В останні роки експерти дедалі більше турбуються про захист комп'ютерних та комунікаційних систем від зростаючої кількості кібератак, включаючи:

- навмисні спроби несанкціонованого доступу до комп'ютерних систем з метою викрадення важливих даних;
- здійснення незаконних фінансових переказів;
- порушення цілісності і маніпулювання даними;
- виконання будь-яких інших незаконних дій.

З розвитком комп'ютерної безпеки зміцнення стійкості мережі посилюється. Відповідно до звіту Австралійського центру кібербезпеки (ACSC), культура суспільства пристосувалась до цього середовища, зосередившись на цілях з низьким ризиком та високою винагородою за їх досягнення, та з акцентом на розробці методологій соціальної інженерії для здійснення нових атак. Крім цього, всюдисуща природа Інтернету дозволила таким особам отримувати більш деталізовані профілі користувачів мережі шляхом експлуатації та аналізу їх цифрових слідів, що призвело до вищих показників атак типу фішинг, крадіжок особистих даних та шахрайства, а також до розробки вузькоспеціалізованих інструментів шкідливого програмного забезпечення.

Висновок. Відсутність видимої діяльності в нетрадиційних мережах, таких як Deep Web і, зокрема, Tor, не обов'язково означає, що вони не існують. Насправді, згідно з основоположним принципом, який керує темною павутиною, цю діяльність просто важче помітити. Цілком можливо, що переважна більшість веб-сайтів може виходити в Інтернет у визначений час, мати коротке вікно активності, а потім зникати, роблячи себе більш складними для відстеження. Темна павутина має потенціал для розміщення дедалі більшої кількості шкідливих служб та заходів, кількість яких, на жаль, з плином часу тільки збільшується. Дослідники з питань безпеки повинні бути пильними і знаходити нові способи виявлення майбутніх шкідливих ресурсами, щоб якомога швидше боротися з новими загрозами в інформаційному просторі.

ЛІТЕРАТУРА

1. Erdal Ozkaya, Rafiqul Islam. Inside the Web. 2019. CRC Press, Taylor & Francis Group. P. 8, 10.

2. Michael Chertoff and Toby Simon. The Impact of the Dark Web on Internet Governance and Cyber Security. No. 6 – February 2015. Centre for International Governance Innovation and the Royal Institute for International Affairs. P.2-5.

Горіцький М.В.,

Київського національного університету ім. Т. Шевченка,

м.Київ

mgoritskyi@gmail.com

ОРГАНІЗАЦІЙНО - ТЕХНОЛОГІЧНІ ЗАСАДИ СТВОРЕННЯ ПРОГРАМНОЇ СИСТЕМИ ЕЛЕКТРОННОГО БАНКІНГУ

The thesis considers the concept, essence and purpose of Internet banking systems, identifies their advantages, described proposed software and technological solution.

Keywords: *bank, banking, online-banking, application, payment, payment transactions.*

Електронний банкінг - це загальна назва технологій дистанційного банківського обслуговування, а також доступ до рахунків та операцій, що надається у будь-який час та з будь-якого пристрою, що має доступ до мережі Інтернет [1].

Суттєва економія часу - це основна перевага електронного банкіngu, адже він дозволяє не здійснювати візит банківської установи для проведення розрахункової операції. У таблиці 1 представлено порівняння витрат часу при проведенні однієї розрахункової операції у відділенні банку та через електронний банкінг.

Таблиця 1 - витрати часу для підготовки та проведення однієї банківської операції [2]

Операція	Звичайний банківський платіж	Електронний банкінг
Укладання платіжного документу	4 хв	4 хв
Перевірка платіжного документу	2 хв	2 хв
Друк платіжного документу на принтері	2 хв	0 хв
Поїздка у банк та з банку	1 год	0 хв

Обслуговування у банку (за умови відсутності черг)	15 хв	0 хв
Загальний час	1 год 23 хв	6 хв

Зазначимо, що система електронного банкінгу суттєво економить час для проведення однієї банківської операції. Така перевага зумовлює стабільний ріст використання цього методу при проведенні платіжних операцій. За даними українського “Ощадбанку”, у 2014 році лише 20% транзакцій здійснювалися через дистанційні канали (електронний банкінг, оплата картою у магазині, тощо), а у 2019 - вже 87% [3].

Варто зазначити, що така популярність новітніх способів розрахунків зумовлена науково-технологічним прогресом загалом, та розвитком інформаційних технологій зокрема. Банки витрачають значні кошти у створення та підтримку власних програмно-технологічних рішень електронного банкінгу. Однак, такі системи у більшості профільовані лише на їх власників, а клієнт може здійснювати операції тільки за наявності відкритого рахунку у цьому банку. Це створює певні незручності, особливо, коли людина користується послугами кількох банків. У такому випадку, йому необхідно встановлювати прикладні застосунки усіх банків на власний смартфон, а також запам'ятовувати способи авторизації (найчастіше це логін та пароль), що не є зручно. Саме тому виникає потреба в уніфікованому рішенні, використовуючи яке, клієнт міг би здійснювати необхідні розрахункові операції з власними картками в одному місці.

Пропоноване мною рішення - це програмна система електронного банкінгу у вигляді клієнт-серверного застосунку, з можливістю збереження платіжних карт в єдиному місці - персональному електронному гаманці, та можливістю їх подальшого використання для сплати електронних платежів, здійснення банківських переказів з картки на картку, перегляд статистики за операціями тощо. Для доступу до власного гаманця, користувач зможе скористатися як веб-застосунком у браузері, так і мобільними застосунками для Android чи iOS. Основною перевагою запропонованого рішення є можливість зміни зовнішнього вигляду головного екрану клієнтського застосунку відповідно до потреб користувача. Це надасть змогу користувачу самостійно вирішувати, які програмні частини для нього більш пріоритетні та необхідні для швидкого доступу.

ЛІТЕРАТУРА

1. Інтернет-банкінг для фізичних осіб - путівник [Електронний ресурс] — Режим доступу до ресурсу: https://bankchart.com.ua/e_banking/statti/internet_banking_dlya_fizichnih_osib_putivnik
2. Лосевская С.А. Интернет – банкинг и его роль в системе банковского обслуживания / С.А. Лосевская // Вестник Донского государственного аграрного университета. – 2013. - №2 – С.52-58.
3. Отделения банков теряют популярность в Украине [Електронний ресурс] – Режим доступу до ресурсу: <https://economics.segodnya.ua/economics/finance/otdeleniya-bankov-teryayut-populyarnost-v-ukraine-1336516.html>.

Давидько С.В.

Університет митної справи та фінансів, м. Дніпро
davydco.serhiy@gmail.com

ПЕРСПЕКТИВИ І ПЕРЕВАГИ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО РЕЗИДЕНТСТВА В УКРАЇНІ

The article describes the e-Residency system. The experience of Estonia in the implementation of such a system is considered, described the path taken by the former Soviet country. Statistical data and comparisons with the Ukrainian realities are given, identified advantages of this system for the Ukrainian economy.

Keywords: *e-residency, Estonia, international experience, digital transformation*

За словами президента України Володимира Зеленського: «Одним із пріоритетних завдань української влади нині є розвиток цифрової економіки країни та цифровізація державних послуг, адже це не лише звільняє громадян від зайвої бюрократії, а й допомагає в боротьбі з корупцією».[1] Новостворене міністерство цифрової трансформації займається радикальним реформуванням системи взаємодії між суб'єктами держави: міністерствами, бізнесом, громадянами. І в планах є запуск системи електронного резидентства, за основу якої взято естонський досвід впровадження подібних систем.

Попри такі позитивні плани, коронакриза що вдарила по Україні спричинила призупинення частини бізнесу в період березень-травень 2020 р., і послаблення податкового навантаження для нього. Все це призвело до значного невиконання

державного бюджету 2020 року, відповідно державний дефіцит буде покриватись залученням додаткового фінансування.

Електронне резидентство - видана державою цифрова ідентифікація і статус, який надає підприємцям доступ до цифрового ділового середовища країни.[2]

Впровадження системи e-residency сприятиме залученню іноземців в українське бізнес середовище, і служитиме додатковим джерелом податкових надходжень для держави, покращить позиції України у світових рейтингах як країни з високим ступенем розвитку технологій та інновацій, призведе до приросту іноземних інвестицій.[3]

В Естонії подібна система була запущена в 2014 році і популярність системи зумовлена значним розвитком електронного уряду, легкістю ведення бізнесу, простою для розуміння системою оподаткування і дуже низьким рівнем корупції. Україна та Естонія мають багато спільних рис, по-перше, їх об'єднує радянське минуле, по-друге, це країни, що на початку 1990-х почали будівництво самостійних та демократичних держав, проголосивши курс на співпрацю з Європейським Союзом і НАТО.

Що цікаво, з моменту незалежності в 1991 році Естонія вважалася однією з найбільш корумпованих країн у регіоні, зокрема й у правоохоронних органах, щоб не брати й не давати хабарів, був викоренений факт безпосереднього контакту з держслужбовцями завдяки впровадженню системи так званої електронної держави. Уже з середини 2000-х років в Естонії діє єдиний державний інтернет-сервер eesti.ee, в який входить більше ста порталів з надання різних послуг жителям країни.

В Україні ініціатива по впровадженню електронного резидентства вже запущена і до 1 липня 2022 р. очікуємо впровадження системи. [4]

В Естонії к-сть населення станом на початок 2020 року становила 1 329 млн., кількість зареєстрованих учасників в системі e-citizenship станом на 29.06.2020 становить 70 344 осіб, що становить вже 5,3% від кількості населення, що доволі вражає, враховуючи що система працює з грудня 2014 року. Динаміка реєстрації зображена на рис. 1.

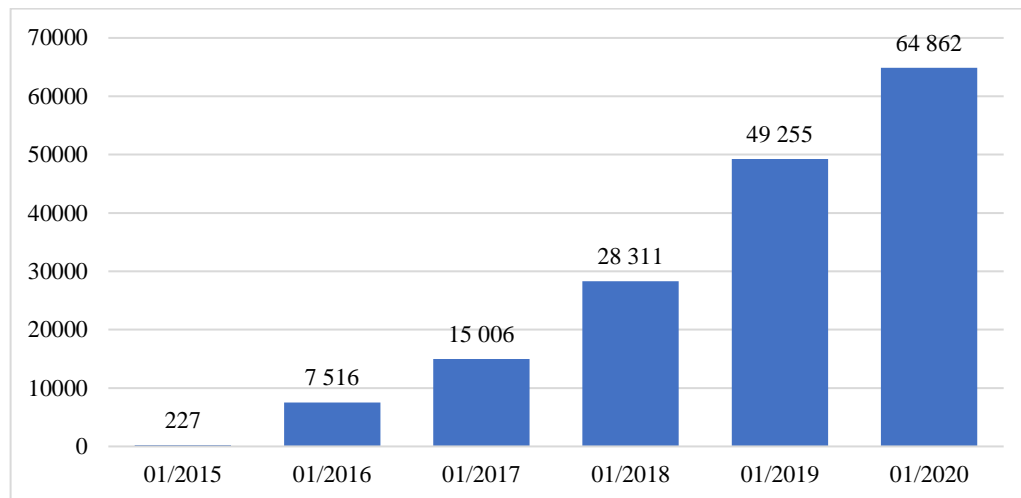


Рис. 1. Динаміка реєстрації в естонській системі e-residency

До речі, Україна лідирує за кількістю учасників-резидентів естонської системи, переважно це особи і підприємства з ІТ сфери.[5] Це можна пояснити перевагами, які надає естонська система для них, а саме доступ до європейського ринку а також платіжних систем: Stripe, Klarna PayPal, які в Україні не працюють. (Табл. 1)

З причин, що спонукали скористатися естонською системою учасники називають: ведення міжнародного бізнесу, який не прив'язаний до локації – 31,2%, перенесення бізнесу до Естонії – 20,7%.

Звертаю увагу на те, що дана система електронного резидентства в Естонії була впроваджена тоді, коли країна вже стала зрілою digital державою, яка в 2005 році надала можливість проводити президентські вибори через інтернет через систему i-voting. А отже країна вже мала що запропонувати громадянам інших країн, адже 99% державних сервісів переведено в електронний формат і необхідності відвідувати країну немає.

Таблиця 1 Рейтинг країн серед учасників e-residency в Естонії

№	Країна	Учасників
1	Фінляндія	5 464
2	Росія	4 792
3	Україна	4 375
4	Німеччина	4 221
5	Китай	3 559

Що стосується України, то курс на діджиталізацію був взятий з початком президентства В. Зеленського, з того часу була запущена система «Дія», яка надає можливість оцифрувати основні документи, система е-малятко для спрощення

оформлення документів при народженні дитини, система «Трембіта», яка являється аналогом естонської X-Road.

В Україні є всі шанси повторити успіх Естонії, адже є всі умови для цього: зацікавлена верхівка влади, розвинутий ІТ сектор, перспективна економіка, що розвивається.

ЛІТЕРАТУРА

1. Офіційний портал президента України [Електронний ресурс]. – Режим доступу: <https://www.president.gov.ua/news/volodimir-zelenskij-nasha-globalna-meta-robuduvati-krayinu-z-58593>
2. Державний сервіс «Дія» [Електронний ресурс]. – Режим доступу: <https://diia.gov.ua/news/zapuskayemo-elektronne-rezidentstvo-v-ukraini>
3. Офіційний портал Міністерства цифрової трансформації [Електронний ресурс]. – Режим доступу: <https://thedigital.gov.ua/news/pratsyuemo-shchob-za-kilka-misyatsiv-v-ukraini-zyavilis-pershi-e-rezidenti>
4. Урядовий портал [Електронний ресурс]. – Режим доступу: <https://www.kmu.gov.ua/npas/pro-realizaciyu-eksperimentalnogo-proektu-iz-zaprovadzhennya-ta-realizaciyi-v-ukrayini-elektronnogo-rezidentstva-i250620-648>
5. Офіційний портал e-residency Естонії [Електронний ресурс]. – Режим доступу: <https://e-resident.gov.ee/dashboard/>

Домрачев В.М.

КНУ імені Тараса Шевченка, mirp@ukr.net

Семененко Т. О.

Сумський державний університет,

t.semenenko@uabs.sumdu.edu.ua

Третиник В.В.

Київський політехнічний інститут ім. Ігоря Сікорського,

viola.tret@gmail.com

МОДЕЛЮВАННЯ ВПЛИВУ ДИНАМІКИ ОБЛІКОВОЇ СТАВКИ НА ЕКОНОМІЧНЕ ЗРОСТАННЯ В УКРАЇНІ

The perspectives of improvement of methods of regulation of macroeconomics in Ukraine is described.

Keywords: *macroeconomics, money stability, interest rate.*

Пандемія COVID-19 спричиняє істотний вплив на поточний стан світової та української економіки. Різні країни розробляють власні програми боротьби з економічною кризою. Більшість країн вдаються до застосування у таких програмах, зокрема інструментів грошово-кредитної політики. При цьому більшість центральних банків використовують політику зміни облікової ставки до рівня, який би сприяв підтримці економіки. У деяких випадках застосовують навіть механізм від'ємної облікової ставки [1, 2].

Переоцінити значення правильної організації фінансової системи складно, адже принцип організації грошових потоків і кредитних, зокрема, формує істотний вплив на стабільність, продуктивність і справедливість функціонування економіки.

Аналізуючи грошово-кредитну політику, можемо констатувати, що після світової фінансової кризи центральні банки більшості країн агресивно знизили номінальні процентні ставки, у багатьох випадках до нуля або майже до нуля (рис.1).

Останніми роками все більше центральних банків вдавалися до політики низьких ставок. Деякі з них, зокрема Європейський центральний банк і центральні банки Данії, Швейцарії, Швеції і Японії, почали експериментувати з від'ємними процентними ставками, по суті, змушуючи у такий спосіб банки сплачувати за зберігання їх надмірних грошових коштів в центральному банку. Мета таких сценаріїв - спонукати банки надавати такі кошти в кредит, щоб сприяти подоланню слабкості економічного зростання після світової фінансової кризи.

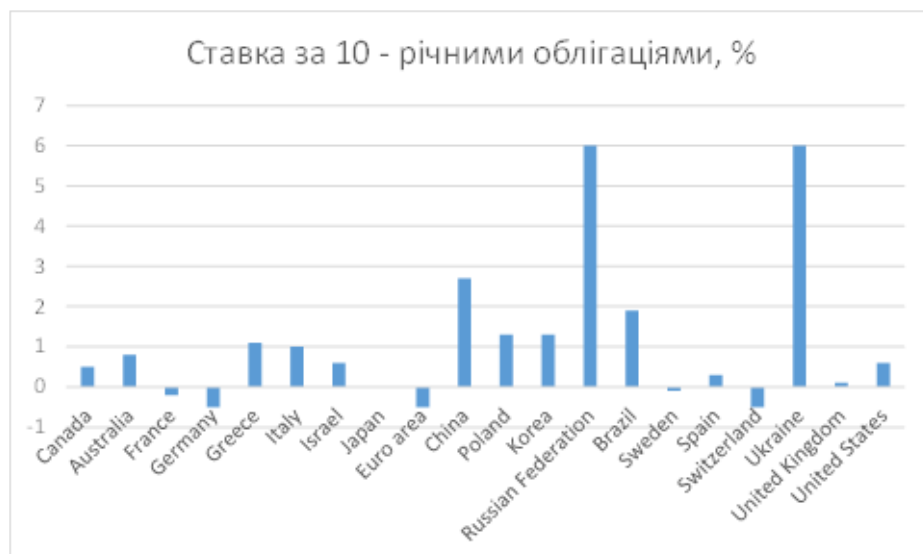


Рисунок 1. Порівняльні значення ставок за 10 річними облігаціями різних країн, станом на 01.07.20 (джерело даних: www.economist.com).

Проте все не так просто. Від’ємні процентні ставки несуть певну загрозу фінансовому ринку. Відсотки - це вартість кредиту або вартість грошей. Це – сума, яку позичальник погоджується сплатити за право користуватися грошима кредитора з урахуванням пов’язаних з цим ризиків. Концепції економічної теорії, що лежать в основі формування процентних ставок, різняться за базовими постулатами. Одні вказують на взаємодію між пропозицією заощаджень і попитом на інвестиції, інші - на взаємодію пропозиції грошей і попиту на них. Але жодна концепція не говорить про можливість існування від’ємної процентної ставки.

У цьому аспекті щодо ситуації в Україні та дій Національного банку України, за нової влади так і не відбулась його націоналізація; значний вплив на дії НБУ все ще мають олігархічні структури. Наразі в Україні спостерігається збільшення кредитування оптової та роздрібною торгівлі. Високі процентні ставки не сприяють розвитку виробництва (рис.2).



Рисунок 2. Розподіл кредитів банків України станом на 01.07.20 (власні розрахунки, джерело даних: НБУ).

Згідно з результатами дослідження, представленими в таблиці 1, на сьогодні маємо негативний вплив динаміки облікової ставки на динаміку ВВП в Україні. Це свідчить про те, що грошово–кредитна політика в Україні залишається хибною.

Таблиця 1 - Залежність динаміки ВВП (GDPR) від динаміки облікової ставки (obl_stavka) в Україні (кореляція на часових рядах 1991-2019 рр., власні розрахунки одержані у пакеті SPSS, джерело даних: НБУ).

Correlations

	obl_stavka	GDPR
obl_stavka	1	-.688**
GDPR	-.688**	1

	Sig. (2-tailed)		.000
	N	28	28
GDPR	Pearson Correlation	-.688**	1
	Sig. (2-tailed)	.000	
	N	28	28

У результаті проведеного аналізу, автори пропонують такі рекомендації для уряду та НБУ:

- забезпечення стабілізації банківської системи України, яка сприятиме відновленню виробництва;
- встановлення оптимального рівня облікової ставки, яка буде сприяти відновленню економічного зростання в Україні;
- проведення більш незалежної грошово–кредитної політики з метою запобігання гіперінфляції;
- посилення регулювання діяльності банків в Україні, зокрема, перегляд значення економічних нормативів регулювання;
- запровадження жорсткого контролю за обігом коштів між учасниками ринку з метою використання коштів для потреб економіки та інвентаризація майнових прав суб’єктів господарської діяльності.

ЛІТЕРАТУРА

1. Батковський В.А. Політика процентних ставок центральних банків у кризових умовах / В.А.Батковський, В.М.Домрачев. Вісник НБУ, №9, вересень 2009, - С. 14 – 16.
2. Уолш Карл. Монетарная теория и монетарная политика / Карл Уолш . М.: Издательский дом «Дело», 2014. – 632 с.

Дудзінський Ю. М., Манічева Н. В., Найденко О. В.
Одеський національний політехнічний університет
м. Одеса, Україна
ymanichev@ukr.net

ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ NI MULTISIM ДЛЯ ДОСЛІДЖЕННЯ ТА АНАЛІЗУ БІОМЕДИЧНОЇ АПАРАТУРИ

A method of using the NI Multisim software and its models for studying and analyzing the circuitry capabilities of biomedical equipment is proposed.

Key words: *modeling, circuitry, analog and digital circuits, microprocessors, circuit editor, biomedical equipment.*

Сучасне електронне обладнання, що використовується в медичній діагностиці, фізіотерапії та медико-біологічних дослідженнях, досить складно в розробці, аналізі та вивченні. Ефективність досліджень, аналізу та розробки медичної апаратури істотно зростає, коли поряд з теоретичними знаннями існує можливість отримання практичних навичок розробки, вивчення і аналізу електричних схем діагностичної та фізіотерапевтичної апаратури, блоків обробки біомедичної інформації, програм, що реалізують функції управління засобами медичної електроніки і електротехнічних систем на основі мікропроцесорів.

Комп'ютерне моделювання при роботі з медичною апаратурою дозволяє розглядати, аналізувати та розробляти значно більшу кількість приладів біомедичного технологічного обладнання вже на стадії проектування. Також виникає можливість застосовувати комп'ютерне моделювання як альтернативу використанню дорогого устаткування, яке у свою чергу дозволяє розширювати можливості вивчення, регулювання, експлуатації та обслуговування біомедичних технологічних апаратів [1-4].

Multisim містить ряд функцій, корисних для процесу аналізу та навчання: інструменти, що спрощують управління експериментами з програмного інтерфейсу, функції підтримки роботи з проектною групою, призначення дефектів компонентів схеми, установку глобальних і локальних обмежень та подібне [2, 3].

З точки зору економічної політики та оптимізації робочих процесів на медичних виробництвах, у біомедичних лабораторіях, в університеті при вивченні біомедичної інженерії одночасне застосування великого числа програм досить накладне, що призводить до збільшення ПЗ. Тому необхідно знайти таке

універсальне ПО, яке б мало всі якісними характеристиками спеціальних програм [1, 4].

Навчальна версія Multisim дозволяє проектувати і моделювати релейно-контактні схеми, широко використовувані в системах управління біомедичної апаратури. Використання в навчальній версії Multisim макетування допомагає викладачам продемонструвати найважливіший етап створення прототипу при проектуванні схем, дозволяючи показати студентам процес і результат макетування в тривимірному вигляді [1-4].

Програмне середовище NI Multisim – це сучасна система комп'ютерного моделювання і комплексного аналізу схем електронних пристроїв, що дозволяє інтерактивно досліджувати створені схеми за допомогою засобів аналізу і віртуальних приладів [1-3]. Можливості програми дозволяють розглядати, вивчати і аналізувати як окремі вузли електронної медичної апаратури, так і спрощені схеми фізіотерапевтичних і діагностичних приладів.

Широкі можливості NI Multisim дозволяють включити в нього крім вивчення схем множення, стабілізації та обмеження напруги, джерел струму на біполярних і польових транзисторах, спектрального аналізу сигналів різної форми, вивчення биття при вимірюванні швидкості кровотоку, також аналіз схем фізіотерапевтичного і діагностичного обладнання – детектора брехні, електрокардіографа, електроакупунктурного стимулятора та ще багато різного. Таким чином, ми маємо можливість самостійно здійснювати підключення вимірювальних приладів, а також налагодження, складання і перевірку схем на працездатність [5].

Оптимальне використання програмного забезпечення NI Multisim дозволяє здобувачам самостійно моделювати реальні аналогові та цифрові схеми, електричні схеми та складні електронні вузли електронної медичної апаратури, а також схеми управління електричними двигунами постійного току в діагностичних та фізіотерапевтичних пристроях [6].

Показано, що віртуальні схеми відповідають реальним електричним системам з високим ступенем достовірності. Запропонована можливість дистанційного навчання із застосуванням програмного забезпечення NI Multisim, яка дозволяє використовувати здобувачам замість фізичних експериментів методи комп'ютерних моделей медичної діагностичної та терапевтичної апаратури, завдяки цьому біомедична інженерія виходить на новий сучасний рівень.

ЛІТЕРАТУРА

1. Хернитер, М.Е. Multisim: Современная система компьютерного моделирования и анализа схем электронных устройств / М.Е. Хернитер. – М.: Издательский дом ДМК пресс, 2006. – 488 с.: ил.
2. [Carlos, Navarro M.](https://ru.scribd.com/doc/36528195/Multisim-Instruction-Manual) Multisim User Manual. National Instruments Corporation. [Electronic resource] Режим доступа: <https://ru.scribd.com/doc/36528195/Multisim-Instruction-Manual>
3. National Instruments, Руководство пользователя [Electronic resource] Режим доступа: <http://www.twirpx.com/file/2084021/>
4. Манічева Н.В., Дудзінский Ю.М., Жукова А.В. Струмінні акустичні випромінювачі для біотехнологій. / Ю.М. Дудзінский, Н.В. Манічева, А.В. Жукова // Журнал «Біомедична Інженерія». – м. Київ, Україна – № 4, квітень 2017. – С. 33–36.
5. Найденко Е.В. Использование программной среды NI MULTISIM при подготовке студентов направлений «Электромеханика» и «Электротехника» / Е. В. Найденко, Е.Ю.Маевская // Электротехнические и компьютерные системы. – Киев: Техника, 2017. – Вып.24(100). – С.164-168.
6. Найденко Е.В. Применение программной среды NI MULTISIM при изучении дисциплины «Микропроцессорная техника» / Е.В. Найденко // Электротехнические и компьютерные системы. – Киев: Техника, 2017. – Вып. 25(101). – С.465-469

Зайцев С.О., Кучанський В.В.

Інститут електродинаміки Національної академії наук України
kuchanskiyvladislav@gmail.com

ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ПОТУЖНОСТЕЙ ТЕПЛОВИХ ЕЛЕКТРОСТАНЦІЙ МЕТОДОМ ДИНАМІЧНОГО ПРОГРАМУВАННЯ

This section discusses the method of optimization of locations and installed capacity of thermal power plants of the power system.

Keywords: *Optimization of power systems operation modes, nonlinear programming, software package, dynamic programming method*

Організація роботи електричних мережі об'єднаної енергетичної системи України (ОЕС) включає широке коло питань. До них відносяться: оптимізація паливно-енергетичного балансу, розміщення виробництв і трудових ресурсів, оптимізація розподілу навантаження електричними станціями за їх типом, визначення доцільних місць спорудження електростанцій визначених потужностей, оптимізація потоків в енергетичній системі [1, 2, 3]. Як зазначено в [2] структура генеруючих потужностей ОЕС України з точки зору забезпечення ефективного регулювання потужності в енергосистемі є неоптимальною. При цьому 62% генерації електричних станцій ОЕС України припадає на теплові електростанції (ТЕС, ТЕЦ, блок-станції). Тому, зважаючи на широке коло питань, які потребують одночасного розв'язку, організація роботи теплових станцій електричної мережі особливо в маневрених режимах при покритті добових графіків навантаження є складною актуальною задачею. Одним із шляхів вирішення якої є використання методів оптимізації розвитку складних систем-об'єктів, що характеризуються значною кількістю параметрів.

Класично для розміщення і вибору потужностей теплових електростанцій використовується лінійна модель вагомим недоліком є неможливість врахування нелінійності економічних характеристик, та дискретності зміни встановлених генеруючих потужностей електростанцій, що оптимізуються [4].

Метод динамічного програмування позбавлений цього недоліку. Динамічне програмування — один з найбільш потужних методів оптимізації при вирішенні завдань нелінійного програмування, який дозволяє представити процес у вигляді послідовності окремих етапів [5]. При використанні методу функція, що мінімізується, повинна бути подільною, тобто дорівнювати сумі функцій окремих змінних:

$$f(x_1, x_2, \dots, x_j, \dots, x_n) = f_1(x_1) + f_2(x_2) + \dots + f_j(x_j) + \dots + f_n(x_n)$$

Алгоритм методу динамічного програмування реалізовано в пакеті програм, який призначений для визначення оптимальної потужності та вибору місць теплових електростанцій. При розробці пакету основна увага приділялась реалізації гнучкості та функціональній простоті інтерфейсу, який має логічно представлені на екрані монітора елементи управління.

Введення інформації здійснюється за допомогою імпорту даних з редактору Excel або шляхом вводу даних про елементи мережі у відповідні таблиці програми. В пакеті програм передбачений синтаксичний контроль вихідної інформації про елементи електричної мережі, передбачена обробка можливих помилок в процесі виконання програми. При введенні помилкової інформації на

екран монітора виводяться відповідні повідомлення для інформування користувача.

Програма дозволяє визначити оптимальну сумарну генеруючу потужність електростанцій, що споруджуються в пунктах в залежності від відомих функцій приведених витрат на спорудження і експлуатацію станцій.

Проведені розрахунки показали, що запропонований алгоритм вибору оптимальної потужності електричних станцій, який використовує метод динамічного програмування, має досить високий рівень збіжності, стійкість до вибору початкових наближень.

ЛІТЕРАТУРА

1. Козирський В. В., Тугай Ю. І., Бодунов В. М., Гай О. В. (2011) Інтеграція поновлюваних джерел енергії в розподільні електричні мережі сільських регіонів *Технічна електродинаміка*, (5), 63-67.
2. План розвитку Об'єднаної енергетичної системи України на 2017-2026 роки URL: <https://ua.energy/wp-content/uploads/2016/12/Proekt-Planu-rozvytku-OES-Ukrayiny-na-2017-2026-roku.pdf> (дата звернення: 21.09.2020)
3. Зайцев Є.О., Кучанський В.В. Аналіз методів контролю втрат потужності на корону в лініях електропередавання. *«Технічні науки в Україні: сучасні тенденції розвитку»*: Всеукраїнська інтернет-конференція студентів, аспірантів та молодих вчених 20-21 листопада 2019 р., Київ, Україна. С. 14-16.
4. Blinov I., Zaitsev I.O., Kuchanskyu V.V. Problems, methods and means of monitoring power losses in overhead transmission lines. *Systems, Decision and Control in Energy I* / за ред. V.P. Babak, V. Isaienko, A.O. Zaporozhets. 279: Springer, 2020, P. 123-136. DOI: 10.1007/978-3-030-48583-2_8.
5. Denardo E. V. *Dynamic Programming: Models and Applications* / Eric V. Denardo. NY: Dover Publications, 2003.

Карчева Г.Т.

*Університет банківської справи, м. Львів
anna.karcheva@gmail.com*

Карчева І.Я.,

*ТОВ «ШОП-ЖСМ»
ira.karcheva@gmail.com*

НОВІ ПІДХОДИ ДО РЕГУЛЮВАННЯ ДІЯЛЬНОСТІ БАНКІВ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Was substantiated the necessity of embedding new approaches to regulation of bank activities in terms of digital society. Digital regulation must be flexible, working in real time, using digital technologies, machine modelling, automated methods of control and risk prevention in real time.

***Keywords:** regulation of banks, concept “Bank 4.0”, risks, digital technologies.*

Протягом останніх років ситуація в банківському секторі України залишається складною, що підтверджується рейтингом Всесвітнього економічного форуму. В 2019 році за компонентою WEF «9. Фінансова система» Україна зайняла 136 позицію, а за показником «Стабільність фінансового сектора» – останнє місце серед країн, що приймали участь - 141 позиція зі скоринговою оцінкою – 57,6 (зі 100 можливих) та тенденцією до погіршення. За індексом «Стабільність банків» Україна входить в десятку країн з найнижчим рівнем стабільності банків – 131 позиція з оцінкою 37,4 серед 141 країни, що приймали участь в рейтингуванні (табл. 1).

Основними причинами нестабільності банківського сектору є високі кредитні ризики та низька якість кредитних портфелів банків, насамперед державних банків, на які припадає більше 60% активів банківської системи. Незважаючи на вжиті заходи, банкам не вдалося суттєво знизити кредитний ризик. Майже половина наданих банками кредитів залишається проблемними (на 01.01.2020 – 48,36%).

Зауважимо, що відповідно до міжнародної практики банк вважається проблемним, якщо проблемні кредити становлять більше 5-10 % кредитного портфеля. Ситуація ускладнюється тим, що найгіршу якість кредитного портфеля мають банки з державною участю, непрацюючі кредити яких становлять 63,5% (Приватбанк – 78,4%), в банках іноземних банківських груп – 32,5%, з приватним капіталом – 18,6% (рис. 1). Зауважимо, що проблемні кредити в розвинутих банківських системах становлять до 3% [2].

Таблиця 1

Фінансова система (Financial system)

Індекс компоненти	Значення		Скорингова оцінка		Ранг	
	2018	2019	2018	2019	2018	2019
9. Фінансова система				42,3		136
Фінансова глибина проникнення в економіку (Depth)				30↓		97
9.01. Кредитування приватного сектора, % до ВВП		47,5		50↓		76
9.02. Фінансування малого і середнього бізнесу		3,4		39,2↓		112
9.03. Наявність венчурного капіталу		3		33,7↑		80
9.04. Ринкова капіталізація		4		4,0↓		112
9.05. Обсяг страхової премії		1,4		23,4↓		78
Стабільність фінансового сектора (Stability, 0 –100)				57,6↓		141
9.06. Стабільність банків (1-7)		3,2		37,4↑		131
9.07. Непрацюючі кредити від загальної суми		54,5		0		139
9.08. Кредитний розрив, %		-30,8		100,0=		1
9.09. Коефіцієнт достатності регулятивного капіталу		13,7		93,0↓		120

Джерело: розроблено авторами за даними [1]

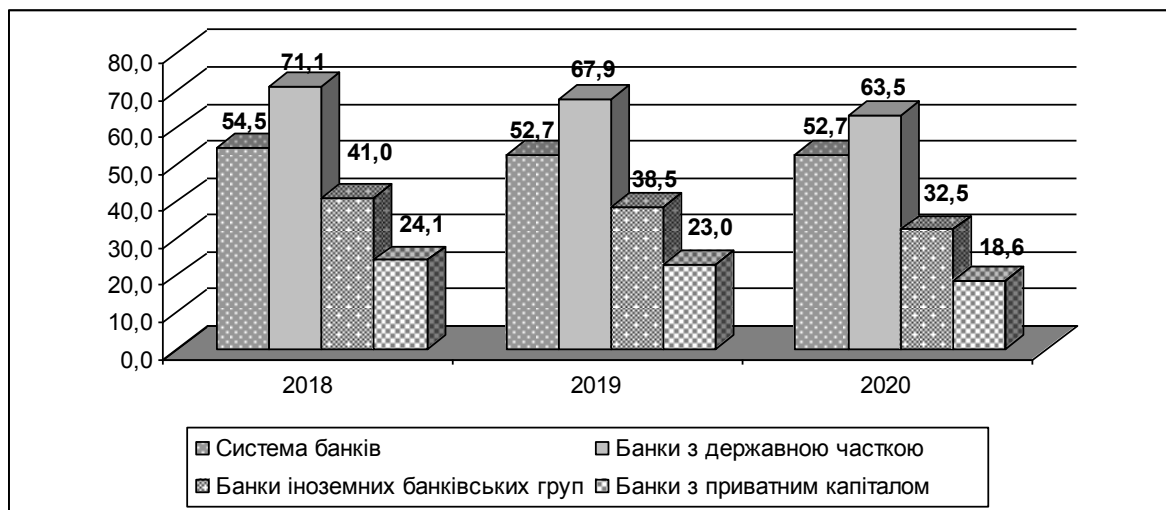


Рис. 1. Непрацюючі кредити в розрізі груп банків станом на 1 січня 2018-2020 рр.

Джерело: розроблено авторами за даними офіційного сайту НБУ

Наслідками високих кредитних ризиків зазвичай стають: репутаційні втрати; зменшення клієнтських надходжень; збільшення витрат, пов'язаних з формуванням резервів та роботою над проблемною заборгованістю; виникнення додаткових ризиків; недостатньо ефективного використання обмежених банківських ресурсів.

Для успішного розв'язання проблем і забезпечення ефективного функціонування і стабільного розвитку банківської системи України, підвищення її системної стійкості і ролі в соціально-економічному розвитку країни та здійсненні прогресивних структурних перетвореннях в економіці важливу роль відіграє підвищення ефективності регулювання та нагляду діяльності банків, впровадження міжнародних стандартів і, передусім, розроблення механізмів стимулюючого банківського регулювання на основі ризик-орієнтованого нагляду як за окремими банками, так і за банківськими групами, що ґрунтуються на використанні цифрових технологій [3].

Зауважимо, що Національний банк України в 2018 р. розпочав впровадження нової системи нагляду за банками – supervision review and evaluation process (SREP), яка ґрунтується на SREP в ЄС. Оцінюючи позитивно використання системи SREP при здійсненні нагляду за банками, в той же час запропонована система недостатньо враховує ризики використання банками інноваційних цифрових технологій, впровадження банками інноваційних концепцій «Банк 3.0», «Банк 4.0» в своїй діяльності, а також нові підходи щодо цифрового регулювання діяльності банків.

В умовах зростання конкуренції, посилення вимог регулятора, постійних зовнішніх і внутрішніх загроз, банки повинні постійно реалізовувати нові стратегії розвитку і просування на ринку, які б забезпечили ефективність, конкурентні переваги, стабільність і зростання. За таких умов основне завдання інноваційної діяльності полягає в тому, щоб перетворити потреби суспільства на нові можливості для прибуткового ведення бізнесу. Саме на активній взаємодії банку та клієнта будуються інноваційні концепції «Банк 2.0», «Банк 3.0» і «Банк 4.0», відповідно до яких головними рисами банку майбутнього є орієнтація на розвиток високотехнологічних продуктів і послуг, інноваційна онлайн-направленість, орієнтація на мобільні технології та інтеграція із соціальними медіа [4].

За останні 40 років банки перейшли від відділення – як єдиного каналу доступу до банківських послуг – до мультиканального, потім до омніканальності і, нарешті, до цифрової омніканальності для клієнтів, взаємодіючих з банком в цифровому форматі. Порівняльний аналіз концепцій традиційного банкінгу, Банк

2.0, Банк 3.0, Банк 4.0 дозволив визначити такі основні тенденції інноваційного розвитку цифрових банків (необанків):

- 1) мобільні комунікації;
- 2) соціальні технології;
- 3) необмежені пропускні можливості мереж, величезні обсяги зберігання даних та їх обробки завдяки використанню хмарних сховищ і обчислень, здійснення моделювання грошових потоків і кредитних послуг, обробка *Big Data* (інформаційних масивів великого обсягу з високою швидкістю зростання);
- 4) API-інтерфейси, співробітництво з конкурентами;
- 5) інтелектуальний аналіз даних – складна обробка даних для пошуку зв'язків між різними розрізненими фрагментами даних;
- 6) використання нової моделі банківського бізнесу *VaaS – Banking as a Service*, що передбачає перетворення банкінгу на компонентний бізнес, конструктор. Багатокомпонентний банк – основа *VaaS*-методу, при якому складні банківські додатки існують у вигляді веб-сервісів.

Для сучасного цифрового банку електронний канал обслуговування стає спільною платформою для всіх інших каналів взаємодії: мобільного, телефоном, через Інтернет, у відділеннях. На зміну багатоканальному обслуговуванню приходить омніканальне, відповідно до якого всі канали обслуговування є інтегрованими і в клієнта зникає необхідність вибору або зміни каналу обслуговування. В розпорядженні клієнта може бути кілька каналів одночасно. Впроваджується проактивна випереджальна взаємодія з клієнтами в різних життєвих ситуаціях, замість реактивного обслуговування у відділеннях банку [4].

Банк 4.0 – це нова концепція банкінгу, що базується на принципах, де банкінг органічно вбудований в цифрове середовище. Банк 4.0 дасть можливість користуватися банківськими послугами в будь-якому місці в будь-який час, враховуючи звички і спосіб життя клієнта. В нових умовах індикаторами успіху будуть не обсяги наданих кредитів, нарощування активних операцій, а здатність до впровадження нових цифрових технологій. Найбільш поширені інноваційні моделі банківського бізнесу:

Розумний багатоканальний банк, що базується на мультиканальній інтеграції, що фокусується на цифрових каналах і інтегрованій архітектурі;

Соціально зорієнтований банк – орієнтується на соціальні мережі для залучення та зміцнення зв'язків з клієнтами;

Банкінг у вигляді «Фінансової/нефінансової цифрової екосистеми» - банк використовує переваги мобільних технологій, може стати для клієнтів «єдиним вікном» для задоволення всіх релевантних потреб останніх.

В умовах активного впровадження цифрових технологій та інноваційних концепцій діяльності банків, виникає потреба в нових підходах до регулювання діяльності банків, впровадженні цифрових технологій в наглядові процеси. Регулятор має визначити нові інструменти цифрового регулювання діяльності банків у режимі реального часу, оскільки в умовах активного впровадження банками цифрових технологій ризик «зараження» набуває особливої загрози через можливість прискорення його розповсюдження.

В умовах цифровізації потрібно нове регулювання діяльності банків. Традиційні підходи до регулювання діяльності небанків, які функціонують відповідно до інноваційних концепцій Банк 3.0, Банк 4.0, не спрацьовують. І, як зазначає Бретт Кінг, «найвірогідніша загроза при впровадженні інноваційної концепції 4.0 полягає в тому, що ми будемо неправильно регулювати фінансову галузь і не зуміємо відновити її в достатній мірі, щоб наші інститути зберегли конкурентоспроможність на світових ринках» [5, с.48].

Нові інструменти регулювання діяльності банків мають враховувати, з одного боку, активну цифровізацію банківської діяльності, яка супроводжується новими можливостями, загрозами і ризиками для стабільності і безпеки банків, а з іншого боку, впровадження цифрових технологій в процедури регулювання і нагляду за банками, яке має базуватися на таких принципах:

- банківське регулювання та нагляд має здійснюватися в реальному режимі часу з використанням цифрових технологій, базуватися на аналізі великих обсягів даних, використанні штучного інтелекту для контролю транзакцій, моніторингу ділової поведінки на ринку. Це дозволить унеможливити виникнення ситуації, яка склалася в банківській системі України щодо проблемних кредитів, нарощування інсайдерських операцій, відмивання грошей.

- регулювання має бути гнучким, сприйнятливим до нових технологій і використовувати автоматизовані методи контролю та упередження ризиків в реальному часу. Важливим буде уміння застосовувати в своїй діяльності хмарні технології і не тільки для нових та існуючих учасників ринку, але й для регуляторів.

- машинне моделювання процесів регулювання. Вважається, що нові підходи до регулювання мають базуватися на результатах експерименту, проведеного Управлінням з фінансового регулювання і нагляду Великобританії, щодо впровадження «машинного регулювання» (machine-executable regulation) - правил, що записуються не словами, а комп'ютерним кодом [5].

Отже, нові підходи до регулювання діяльності банків в умовах активного використання цифрових технологій передбачають використання нових цифрових

інструментів, і перш за все передбачають перехід від норм, що містять вимоги до політики і процесів, - до автоматизованого нагляду і правил, розроблених саме для функціонування банків в цифровому середовищі. Б. Кінг стверджує [5], що до 2030 року в обов'язки регулятора не буде входити розроблення нормативно-правової бази та перевірка дотримання встановлених вимог. Банківський нагляд буде здійснюватися автоматично і максимально оперативно, майже в реальному часі, реагувати і вносити корективи в ринкову практику. Вважається, що такі цифрові зміни в системі регулювання відбудуться швидко, за 10-15 років.

ЛІТЕРАТУРА

1. The Global Competitiveness Report, 2019.
2. Механізми забезпечення ефективності та конкурентоспроможності банківської системи та економіки України : монографія / [Г. Т. Карчева, А. Я. Кузнецова, Н. Р. Швець та ін.] ; за заг. ред. д-ра екон. наук Г. Т. Карчевої. — Київ : ДВНЗ «Університет банківської справи», 2019. —311 с.
3. Карчева Г.Т. Фінансовий стан банків та розвиток механізмів стимулюючого банківського регулювання // Сучасні тенденції стійкого фінансово-економічного розвитку та механізми їх реалізації в глобальному вимірі: монографія / за заг. ред. Т.М. Болгар. – Дніпро: Університет імені Альфреда Нобеля, 2020. – 220 с.
4. Карчева І. Я. Сучасні тенденції інноваційного розвитку банків України в контексті концепції Банк 3.0 / І. Я. Карчева // Фінансовий простір. – 2015. – № 3 (19). – С. 299–309.
5. Кинг Б. Банк 4.0: Новая финансовая реальность. Издательство «Олимп-Бизнес», 2020.- 486 с.

ВИРОБЛЕННЯ ДОКАЗОВОЇ ДЕРЖАВНОЇ ПОЛІТИКИ В УМОВАХ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

The article considers a new trend in public policy making - evidence-based policy, which became possible due to the introduction of digital innovations in government activities. The state and prospects of evidence-based policy in Ukraine, the problems that hinder its successful implementation are analyzed.

Keywords: *evidence-based policymaking, digital economics, public policy analysis, Big data, program monitoring and evaluation.*

У розвинених країнах світу останні 20 років набув поширення новий тренд у формуванні й реалізації державної політики – вироблення доказової політики (або політики, що ґрунтується на доведених фактах, англ. – *evidence-based policy*) – це підхід до вироблення політики, коли рішення щодо подальшого курсу дій ґрунтуються на строго встановлених, перевірених фактах і доказах. Для його впровадження вирішальною є наявність відповідної інфраструктури – правових норм, демократичних інститутів, розвиненого громадянського суспільства, *Big data* з відповідними можливостями комфортного опрацювання даних, алгоритмів штучного інтелекту, належно підготовлених креативних фахівців і активної політичної підтримки з боку творців політики. Фактично йдеться про переосмислення на вищому технологічному рівні аналізу політики як комплексу процедур щодо підготовки проектів рішень органів влади з використанням порівняльного аналізу альтернативних варіантів вирішення суспільних проблем. Нові можливості для підготовки більш обґрунтованих програм створює розвиток цифрової економіки на основі новітніх інформаційно-комунікативних технологій. Насьогодні в країнах ОЕСР, в ЄС рішення центральних і місцевих органів влади практично у всіх ситуаціях базуються на процедурах аналізу доказової політики, для чого створено відповідне інституціональне, зокрема, інформаційне забезпечення.

В Україні від початку 2000-х років здійснюються кроки (не завжди послідовні) на шляху впровадження доказової політики завдяки застосуванню підходів аналізу політики для обґрунтування рекомендацій органам влади при підготовці програмних документів. В останні п'ять років були внесені зміни (2015

р.) до Закону України «Про державну службу», де зазначено, що держслужба – це діяльність щодо аналізу державної політики (у ст.1); у Регламент Кабінету Міністрів України, де було імплементовано вимогу дотримуватись циклу політики при її розробці (ст. 3¹). У лютому 2020 р. було затверджено новий варіант Регламенту (набуде чинності з 1 січня 2021 р.), де значно посилені вимоги до аналітичного обґрунтування урядових програмних документів. Реформовані міністерства, затверджені відповідні професійні стандарти для виконавців аналізу політики. Проте ситуація з якістю державного програмування поки відчутно не покращується.

Вузьким місцем залишається наявність підготовлених для реалізації згаданих процедур високопрофесійних кадрів, а також розуміння необхідності проведення повноцінного аналізу політики всіма стейкхолдерами, в першу чергу, керівниками органів влади. Іншою вагомою причиною є, на перший погляд, дрібниця – термінологічна плутанина навколо вживання поняття «ефективність» у законодавстві і практиці його використання при впровадженні процедур моніторингу і оцінювання політики. І, нарешті, можливості плідного використання в країні кращих світових практик використання можливостей цифрового розвитку обмежуються станом *Big data*, які з багатьох причин ще не стали драйвером цифрових трансформацій в українському суспільстві.

Kozlenko M., Lazarovych I., Kuz M.

Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine

mykola.kozlenko@pnu.edu.ua

DEEP LEARNING APPROACH TO SIGNAL PROCESSING IN INFOCOMMUNICATIONS

Digital communications techniques based on random, chaotic, or noisy carriers are well known and successfully used in a number of applications. Simple on-off or amplitude shift noise keying modulation schemes are among the most popular. In this paper, we propose to use a classification model based on an artificial dense neural network and a deep learning approach for software-defined demodulation of spread spectrum signals.

Keywords: *spread spectrum; communication system; amplitude noise shift keying; digital communications; demodulation; software defined radio; machine learning; deep learning; artificial neural network; deep neural network; interference immunity; bit error rate; symbol error rate.*

Digital communications based on spread spectrum technology is very popular area in the communication field. Spread spectrum signals have time-bandwidth product greater than one. Nowadays there are some classical approaches to generating and processing of such signals: spreading bandwidth of sinusoidal signals, using of non-sinusoidal waveforms, dynamic chaos-based methods, using of noise carrier, etc. All approaches except the last utilize pseudo-random techniques and noise-like signals. This limits the benefits of complex signals using. This paper investigates the performance of communication system where the amplitude of the band-limited Gaussian noise represents binary information symbols and deep artificial neural network is responsible for demodulation and detection.

The amplitude noise shift keying modulation scheme is very simple. If the transmitted binary information symbol is “mark” then the transmitter radiates a band-limited white Gaussian noise signal. Inactive state of the noise generator represents the transmission of the symbol “space”. The processing of received signal is performed at the receiver side. The received signal is a sum of the convolution of the transmitted signal waveform with the channel impulse response and the channel interference. Demodulation is performed using artificial dense neural network over a symbol duration interval. The output of the last neuron layer (in this case it is a single neuron) represents the demodulator output at the end of the each symbol interval.

The interference immunity of amplitude noise shift keying demodulation based on dense neural network was obtained for the first time as a result of this research. It has been proved that the proposed method is competitive with other well-known methods. The noise immunity is greater than immunity of “power reception” method for at least 3.5 dB. The method can be used as core physical technology for the data exchange in wide area of applications. It has very low probability of interception by design. The time complexity was evaluated and real-time processing capability was proven. The reinforcement learning ideology can be used to implement the cognitive radio concept.

REFERENCES

1. D. Torrieri, *Principles of spread-spectrum communication systems*. [Place of publication not identified]: Springer, 2019, doi: 10.1007/b99535
2. M. Kozlenko and V. Vialkova, "Software Defined Demodulation of Multiple Frequency Shift Keying with Dense Neural Network for Weak Signal Communications," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 590-595, doi: 10.1109/TCSET49122.2020.235501.
3. M. Kozlenko, I. Lazarovych, V. Tkachuk and V. Vialkova, "Software Demodulation of Weak Radio Signals using Convolutional Neural Network," *2020 IEEE 7th International Conference on Energy Smart Systems (ESS)*, Kyiv, Ukraine, 2020, pp. 339-342, doi: 10.1109/ESS50319.2020.9160035.
4. M. Kozlenko and A. Bosyi, "Performance of spread spectrum system with noise shift keying using entropy demodulation," *2018 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Slavske, 2018, pp. 330-333, doi: 10.1109/TCSET.2018.8336213.
5. T. Wu, "CNN and RNN-based Deep Learning Methods for Digital Signal Demodulation," *Proceedings of the 2019 International Conference on Image, Video and Signal Processing - IVSP 2019*, 2019.

Комісаренко О.С.

*Національний транспортний університет, м. Київ,
olenakomisarenko@ukr.net*

Баранов Г.Л.

*Національний транспортний університет, м. Київ,
baranovgl2018@gmail.com*

Чака О.Г.

*Інститут фізіології ім. О.О. Богомольця НАН України, м. Київ
lenchaka@ukr.net*

ТЕХНОЛОГІЇ СТВОРЕННЯ ФУНКЦІОНАЛЬНИХ МАТЕРІАЛІВ ЗА ЗАМОВЛЕННЯМИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

The digital technologies for construction future materials are prosed. It has been recalled that the use space-time-codes allows to visualize the technologies information of formation of the structure state the function materials. The basic concept of the STC in the domain $\{0,1\}$ are considered.

The factsheet the physical process, described by STC equation is characterized by a large number of diverse parameters. To reduce the difficulty an approach based on similar cases transformations is offered. The proposed method allows solve actual problem of optimal choice for construction the function materials and to comes to improve its effectiveness.

Key words: *digital technologies, future materials, human participation, smart order, single-minded information, space-time-codes.*

Цифрові технології в сучасному інформаційному суспільстві набувають суттєвого поширення у різних галузях людської діяльності на базі автоматизованих робочих місць з програмно-апаратними комплексами (ПАК), розумними мережами (SN – smart network), інтелектуальними телекомунікаціями (ITS), включаючи глобальний Internet. Покращення показників ефективності згаданих засобів інформаційних систем та технологій (IST) досягається за рахунок швидкого масштабування програмуємих додатків мультиагентної інтелектуальної взаємодії (МІВ). Лише кількісне зростання числа $n \rightarrow n_{max} \rightarrow n_{sup}$ значно спрощує функціональні операції, що необхідні для зростання об'ємів учасників МІВ (human participation and automation chatbot), які насамперед реалізують сутність інформаційних індустріальних революцій [1,2]. За цим принципом нумерації більшості елементів спеціалізованого кортежу (біт, байт, файлів,

перемиканих та розгалужених структур) реально з'являються (виникають) Internet речі [3]. Свобода маніпуляції для формування нових описів з таких кортежів обмежена лише кількістю $C_n^m = \frac{n!}{m!}$ комбінацій у переліку складові можуть замовляти клієнти, як замовник та інтелектуальний агент системи (IAS), де таким чином означеному виборі речей конкретного зобов'язання.

Значно більша складність програмування виникає при спробах опису замовлень на рівні та особливо на штучні функціональні матеріали (FM) [4,5]. Вони обов'язково повинні (як носії необхідних та достатніх властивостей) проявляти функціональну стійкість у сфері експлуатаційного застосування FM. Тоді головна мета – безпека життя FM в умовах дії факторів впливу реального нестационарного природного середовища (НПС) на об'єкти техно-природних компонентів (ТПК). Майбутнє життя людства все більше пов'язано з ТПК у критичних середовищах: космічному всесвіті; акваторіях морів та океанів; підземних сферах комунікації та індустріальна інфраструктура. Бізнес на базі новітніх FM вже зараз змінює наземні біосферні оазиси з захистами життєвих циклів; агропромислові комплекси керованого землеробства [6] тощо. Саме замовлення FM на майбутнє не може з'явитись зразу у повному, достовірному та точному описі для всіх ситуацій у об'єктах ТПК. Причини обумовлені тим, що вони неперервно взаємодіють у власних індивідуальних життєвих циклах (ЖЦ) з незалежним (нами не керованим) НПС. Зовнішні та внутрішні прояви факторів впливу для об'єктів складних динамічних систем (СДС) [7] ТПК НПС специфічно гетерогенні та [8] різні. Вони суто гетерогенні відповідно до вкладеності численних елементів (n_0, n_i) різних (протилежних, антиподних, асиметричних, природних та штучно керованих) учасників взаємовідношень між НПС ($n_0 \rightarrow \infty$) та СДС ($n_i < n_{sup} \ll n_0$) на (МЕ – мета, МА – макро, МІ – мікро та нано) контактних сферах об'єктно інтегрованих ЖЦ. Зараз актуальність мікро та нано форм проникнення (Covid-19) з макро зон НПС до життєвих й визначальних органів людини та створення пандемії у ТПК найбільш висвітлюється у Internet джерелах [9,10]. Вибір техніко-технологічних рішень (ТТР) для гарантування функціональної стійкості кожної особи (IAS, human participation, ПЕВО – поліергатична виробнича організація) потребує обґрунтування FM, мінімізації ризиків, максимізації тривалості ЖЦ, реального застосування наявних ресурсів в умовах самозахисту та тривалого терміну очікування з розв'язання актуальної проблеми масштабно й повсякмісно.

Інтелектуальність якісних замовлень на майбутні FM (або цілий комплекс взаємопов'язаних наноматеріалів) означає повноту й достовірність описів

стосовно умов взаємодії у природних 3D вимірних просторах, що охоплюють, як зовнішні на далеких відстанях загрози так й внутрішні реальні нано розмірні процеси змін мікро ЖЦ під час реагуванні об'єктів СДС на гетерогенні фактори (одночасно разом у просторі та часі) НПС. Нажаль передбачення (прогноз) майбутнього завжди обмежено [2,6,7] інтервалом наступного кроку Δt моделювання необмеженого Всесвту. Мова повинна описати майбутні взаємодії [8,10] між ТПК↔НПС, FM↔СДС, СДС↔ТПК на відповідно різних ієрархічних рівнях відкритих систем з внутрішніми особливостями МІВ. Якість потрібних даних (у кінцевому вимірі Big Data) залежить від обізнаності експертів-наукової спільноти інформаційного суспільства. Але й на ергатичних рівнях (human participation) виникають непорозуміння ряду базових понять, які застосовують експерти (фізики-хіміки-біологи-медики-інженери-конструктори-технологі-експлуатанти техніки-менеджери-фінансисти) у відповідно різних галузях людської діяльності у цілісному сучасному інфологічному суспільстві [1,2]. Поняття на різних людських (іноземних мовах тощо) словах різні наприклад, «проникнення». Але це базове поняття обов'язково повинно бути гармонізовано з реченням, текстом опису, цілісним тематичним замовленням [7,8] на FM.

Практика тлумачних словників фіксує деякі аспекти граматично достовірного застосування означеного поняття «проникнення». Але для адекватної інтерпретації, яка потрібна для отримання FM згідно (smart order) замовлення, необхідно зберігати тотожність у вигляді еквівалентів з лише однозначним (const) тлумаченням у межах повного циклу пошуку ефективних процесів створення конкретного (майбутнього, а зараз поки ще не відомого) FM [6-9].

Кожний конкретний FM, що потребує замовник, у даному прикладі повинен бути достовірно точно описаний за напрямками характеристикації: геометрії «координат» місце положення визначальних точок та особливості специфічної топології «формотворення» простору; граничних умов на площинах – поверхнях граней тіла об'єкта, «який» проникає та «куди», «що» входить, втікає, індукує, активізує; фізики процесів проникнення «яким чином» та відповідно «якими силами», моментами, формами, енергії; кінематичних траєкторій проникнення «яким таким чином» відбувається рух у означеному просторі; динаміки зміни явищ коли під час «якого» здійснення відбувається дане проникнення конкретних форм матеріального носія. Можливо продовжувати перелік запитань та необхідних описів характеристикації замовлення по зв'язаним розділам та темам. Головна умова повний (максимально $n_{max} < n_{sup}$ на досягнутому рівні суспільної обізнаності сучасних наукових експертів) опис умов та вимог для ефективного моделювання [7,8,10]. В той же час характеристикація за критеріями безпеки ЖЦ

повинна означати саме сутність форм матеріального проникнення: твердого, рідини, газу, плазми, елементарних часток тіла; лінійного, криволінійного, гвинтового, плоского, сферичного та іншого фронту хвильових процесів; маси, заряду, потоку, однорідного чи неоднорідного носія; механічної, акустичної, гідравлічної, теплової, хімічної, біологічної, соціальної, фінансової, електромагнітної взаємодії; причин та наслідків, а також ланцюгів та розгалужень від початку до кінцевого завершення проникнення у конкретній цільовій формі існування. Реально та за фактом значне різноманіття змін контрольних параметрів та критеріїв ефективності під час реагування шарів FM на прояв факторів впливу НПС можливо реєструвати за результатами моделювання за допомогою ПАК, засобів ITS та Internet. Численні розрахунки на основі цифрових даних модельного опису мають відомі обмеження: спрощення моделі відносно реального об'єкта та явищ для прийняттого часу очікування результатів у вигляді параметризованих таблиць та графіків перехідних процесів обмеженої точності; невідповідне застосування методу у конкретному типовому програмному модулі (ТПМ) без контролю можливостей втрати чисельної стійкості (розходимість або зациклювання) обчислювального процесу обумовлює нераціональні витрати ресурсів IST на отримання цільового результату; обмеження (спрощення, прискорення, неповнота) тестування розрахункових моделей (Big Data) та методів й ТПМ може у великих масштабах взаємообумовлених розрахунків провести до абсурдних (не достовірних, неправдоподібних) результатів комплексного моделювання СДС та режимів функціонування ТПК.

За результатами наших досліджень запропонована IST на принципах саме символічних (нечисленних) обчислень засобами комп'ютерної алгебри для необхідних математичних символічних перетворень (МСП) [10] з метою отримання корисних цільових форм (КЦФ) – розв'язків за наступними критеріями:

- Витрат часу IAS мінімальні, кінчені, включаючи освоєння ПАК КМ-ПД є доступність операційної системи та середовища МІВ у «хмарах»;
- Ефективність та швидкість імпорту/експорту описів КЦФ;
- Швидкість МСП у заданих типових задачних варіацій атрибутів;
- Доступність відомих алгебраїчних функцій для описів явищ; швидкість процедур синтезу композицій з застосуванням предикатів, підстановок, процесів створення інноваційних властивостей;
- Зручність візуалізації результатів по кожній КЦФ та в цілому згідно повної концептуально-семантичної цільової моделі (КСЦМ) об'єкта, включаючи описи властивостей та взаємодії FM у НПС.

Окрім тематичного за сумісністю FM спеціалізованого пакета КМ-ПД запропоновану методологію (але з більшими витратами наявних ресурсів ITS) зможе використовувати самостійно IAS, які володіють іншими відомими пакетами МСП наприклад: Maple (www.maplesoft.com); Mathematica (www.wolfram.com); MATLAB (www.mathworks.com); Mathcad (www.mathworks.com); O-Matrix (www.omatrix.com); Scilab (www.scilab.org).

В означених пакетах існуючі засоби ITS забезпечують традиційні чисельні методи обробки цифрових параметрів, які згруповані у групових табличних характеристиках (ГТХ) без даних для обчислень табличним процесом типу Excel, а також й для прискорення покращення моделювання об'єктів СДС (запропонованими засобами МСП, графіків перехідних процесів обмеженої точності; включаючи Р-перетворення Г.Є. Пухова [11,12]).

Результуюча інтегрована ефективність комплексного моделювання згідно описів тематично означених понять на базі символічних КСЦМ та накопичених у пам'яті КМ-ПД КЦФ з ієрархічними та мережними описами з застосуванням просторово-часових кодів STC (Space-Time-Code) обумовлена технологією цифровізації повного набору моделей, методів та учасників МІВ, які активізують структурні відношення: ергатично суспільного моделювання майбутніх ТПК у НПС; моделювання КЦФ практичного тематичного досвіду достовірного (гарантованого) результату з фіксуванням опису у STC для подальших розрахунково-базисних моделей РБМ будь-якої складності у 3D вимірному просторі причин впливу та наслідків реагування; процедурно обчислювального моделювання з застосуванням фрагментів РБМ за потребами синтезу інноваційної розрахунково оперативної моделі (РОМ) за потреб гарантування достовірності замовлених у вигляді переліку властивостей (стосовно розмірної кількості та бажаної корисної якості FM). Ці ситуативні варіюємо, змінюємо, модифікуємо, переконфігуруємо у процесах синтезу майбутнього результату КЦФ алгебраїчно й логічно (предикативно) гарантують точність, достовірність та надійність майбутніх ТТР необхідних для експлуатації ТПК у НПС без відмов, накопичення дефектів, аварійних подій (у сенсі крупних втрат ресурсів) та катастроф (масштабних форс-мажорних обставин). Саме візуалізація STC понять, описів, критеріїв, вимог, обмежень, заборон, а також контроль ефективності ресурсів КМ-ПД (КЦФ, МСП, РОМ, РБМ, ГТХ) та тестування практикою застосування всіх наявних засобів ITS для експлуатації ТПК в умовах ризиків впливу НПС з гарантованим результатом безпеки життя на тривалих інтервалах отримання прибутку забезпечує експертам описи послідовної технології з процесів створення FM з замовленими властивостями.

ЛІТЕРАТУРА

1. Schwab K. Fourth industrial revolution / K. Schwab – М.: Eksmo.-2016.
2. Self-organization of the human mind and the transitions from Paleolithic to behavioral modernity Yury N. Kovalyov, Ncer M. Mkhitaryan Igi-global.com/book/self-organization-human-mind-transition/233934
3. <https://www.imena.ua/blog/top-10-scope-iot/#:~:text=%D0%9D%D0%B0%D0%BF%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%2C%20%D1%96%D1%81%D0%BD%D1%83%D1%8E%D1%82%D1%8C%20%D1%80%D0%BE%D0%B7%D1%83%D0%BC%D0%BD%D1%96%20%D1%82%D0%B5%D1%80%D0%BC%D0%BE%D1%81%D1%82%D0%B0%D1%82%D0%B8%2C%20%D0%BA%D0%BE%D0%BD%D0%B4%D0%B8%D1%86%D1%96%D0%BE%D0%BD%D0%B5%D1%80%D0%B8,%D1%8F%D0%BA%D1%96%20%D0%B2%D0%B8%D0%BA%D0%BE%D0%BD%D1%83%D1%8E%D1%82%D1%8C%20%D0%B7%D0%B2%D0%B8%D1%87%D0%B0%D0%B9%D0%BD%D1%96%20%D0%B4%D0%BE%D0%BC%D0%B0%D1%88%D0%BD%D1%96%20%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97.>
4. Y.A. Mikhailn Structural polymer composite materials SPB: Scientific principles and technologies, 2008. 822 pp.
5. Polymer composite materials: structure, properties, technology / Edited by A.A. Berlin. SPB.: Professed. – 2008.-552 p.
6. Кравчук В.І. Інформаційна технологія прогнозування та випробування майбутньої аграрної техніки / В.І. Кравчук, Г.Л. Баранов, О.С. Комісаренко / Техніко-технологічні аспекти розвитку та випробування нової техніки і технології для сільськогосподарського виробництва. Зб.наукюпрюУкр НДПВТ ім. Л.Погорілого, Дослідницьке, 2018-вип.22(36). – с.10-15, с.27-34.
7. Баранов Г.Л., Макаров А.В. Структурное моделирование сложных динамических систем / Баранов Г.Л., Макаров А.В. – Киев: Наукова думка, 1986. – 272с.
8. Баранов Г.Л., Артеменко В.Л., Чака А.А. Система інформаційно-аналітичного забезпечення технології підвищення безпеки руху транспорту // Вісник НТУ. Вип. 42. – К.: НТУ, 2008 р. – С.23-27.
9. <https://www.who.int/ru/emergencies/diseases/novel-coronavirus-2019>
10. Структурне моделювання та символічні перетворення для управління рухом транспортних засобів: монографія / Баранов Г.Л., Носовський А.М., Пнін В.В., Тихонов І.В., Васько С.М.: М-во освіти і науки України. – К.: ДП «Інформ. – аналіт. агентство», 2014. – 310.

11. Пухов Г.Е. Дифференциальные преобразования функций и уравнений / Пухов Г.Е. – К.: Наукова думка. 1980. – 419с.

12. Пухов Г.Е. Дифференциальные спектры и модели / Пухов Г.Е. – К.: Наукова думка. 1990. – 184с.

Котенко Н.О.

Киевский национальный торгово-экономический университет, г. Киев,

[*kotenkono@knuce.edu.ua*](mailto:kotenkono@knuce.edu.ua)

Жирова Т.О.

Киевский национальный торгово-экономический университет, г. Киев,

[*zhyrova@knuce.edu.ua*](mailto:zhyrova@knuce.edu.ua)

ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА В УСЛОВИЯХ СМЕШАННОЙ РАБОТЫ УЧЕБНОГО ЗАВЕДЕНИЯ

Every educational institution today faces the question of the quality organization of the educational process. Due to the COVID-19 pandemic, the vast majority of educational institutions are forced to switch to blended learning. The effectiveness of a mixed form of organization of the educational process largely depends on a properly selected and configured LMS. If an educational institution chooses an open source or limited functionality LMS, then you should pay attention to the possibility of integrating this system with other services. For example, Moodle integration with Microsoft Teams or Google Classroom.

Keywords: *blended learning, LMS, Moodle, Teams, Google Classroom.*

Вопрос дистанционного обучения возник достаточно давно. Первые попытки его организации были предприняты еще задолго до появления Интернета. Уже в 1969 году в Великобритании появился первый университет полноценного дистанционного образования – Открытый Университет (Open University).

Дистанционное образование – это возможность учиться и получать необходимые знания отдаленно от учебного заведения в любое удобное время. Процесс обучения построен на использовании различных коммуникационных средств. По окончании такого обучения студенты получают соответствующие сертификаты.

Нужно осознавать разницу между дистанционным образованием и организацией образовательного процесса в дистанционной форме. Пример ведущих университетов мира свидетельствует о том, что качественное образование возможно и при существенно меньшем количестве аудиторных занятий, чем в украинских учебных заведениях. Но это требует грамотного применения онлайн-технологий с соответствующими методическими подходами, обеспечивающими эффективное сочетание непосредственной и опосредованной формы взаимодействия студентов и преподавателей в виде смешанного обучения [1].

Смешанное обучение – стиль обучения, при котором сочетаются технологии дистанционного обучения и очное взаимодействие для привлечения студентов, удобства обмена информацией, выставления оценок и увеличения каналов общения между преподавателями и студентами.

С началом карантинных мероприятий, вызванных эпидемией COVID-19, перед всеми образовательными учреждениями встал вопрос о выборе форм и средств взаимодействия. Готовность образовательного учреждения к решению стоящих вопросов была прямо пропорциональна развитию дистанционного образования в нем. Тем, у кого оно было формальным, пришлось приложить немало усилий к решению возникших задач. Одной из основных задач оказалась задача, связанная с подбором правильных онлайн-технологий. С ослаблением карантинных мероприятий очень популярным стало смешанное обучение.

Эффективное внедрение смешанного обучения предполагает наличие учебной платформы, интегрированной с внутренними системами учета и документооборота, которые используются в учебном заведении [1], то есть, наличие качественной системы дистанционного обучения.

Системы дистанционного обучения или LMS (Learning Management Systems) позволяют качественно организовать учебный процесс и отслеживать успеваемость слушателей посредством создания онлайн-курсов или виртуальных классов, доступных в любое время и в любой точке мира где есть Интернет. Все учебные материалы при этом сохраняются в одном месте, их удобно просматривать и адаптировать в зависимости от целей обучения и сферы деятельности компании или организации.

Сегодня в мире известно более 600 LMS. По данным Edutechnica [2] уже несколько лет подряд самыми популярными LMS является Blackboard, Canvas, D2L Brightspace, и Moodle. Если говорить о Open Source LMS, то долгое время в Украине и мире ведущее место занимает Moodle. Сводная информация по этим платформам приведена в таблице 1.

Результаты опроса о состоянии использования технологий дистанционного обучения в учреждениях высшего образования Украины [3] свидетельствуют о недостаточно высоком уровне культуры использования LMS в образовательном процессе как со стороны преподавателей, так и со стороны студентов.

Наполнение коммерческих LMS Blackboard, Brightspace и других во многом зависит от выбранного тарифного плана, установленных плагинов и прочего. В образовательных учреждениях Украины они не являются популярными.

Moodle и Canvas – самые популярные бесплатные LMS с открытым исходным кодом, ориентированные, прежде всего, на организацию взаимодействия между преподавателем и слушателем, они также подходят для организации дистанционных курсов и поддержки очного обучения. Однако Moodle и Canvas являются относительно бесплатными, поскольку дополнительные (расширенные) возможности – платные.

Таблица 1

LMS	Blackboard	Canvas	Brightspace	Moodle
Open Source	-	+	-	+
Назначение	K-12 schools, Higher Education, Government, Business	K-12 schools, Higher Education, Business	K-12 schools, Higher Education, Corporate Learning	K-12 schools, Higher Education, Workplace
Платформа	Windows Mac Linux Android	Windows Mac Linux Android	Windows Mac Linux Android	Windows Mac Linux Android
Интеграция с Google	+	+	+	+
Интеграция с Microsoft	+	+	+	+

Поскольку среди многих LMS в Украине Moodle является самой популярной, остановимся более подробно на возможностях ее совершенствования без использования платных тарифных планов. Это возможно благодаря интеграции Moodle с Microsoft Teams или с Google Classroom.

Microsoft Teams и Google Classroom – это две образовательные программы, причем первая достаточно новая в образовательной среде, а вторая популярная уже давно и получила еще большую популярность из-за COVID-19. Также, в

значительной степени их популярности способствует доступность, ведь каждый, кто имеет аккаунт Google, имеет учетную запись Google Classroom.

Google Classroom – это бесплатный веб-сервис, разработанный Google для школ и других образовательных учреждений, благодаря которому можно упростить процесс создания, хранения, распространения и проверки заданий. Основная цель Google Classroom – упорядочить процесс обмена файлами между преподавателями и слушателями, упростить процесс дистанционного обучения.

Microsoft Teams – это универсальная платформа для общения, сотрудничества и обучения, сочетающая постоянные чаты на рабочем месте, видеовстречи, сервисы хранения файлов и возможность интеграции программ. Платформа имеет расширения, которые можно интегрировать с продуктами, не принадлежащие Microsoft.

Microsoft Teams рекомендуется использовать при подготовке IT-специалистов, поскольку кроме поддержки образовательного процесса эта среда позволяет формировать ряд soft skills. Также она приучает студентов к среде, в которой им, с большой вероятностью, придется работать в будущем.

Сравнительную характеристику Microsoft Teams та Google Classroom предоставлено в таблице 2.

Таблица 2.

Характеристики	Microsoft Teams	Google Classroom
Корпоративная почта	+	-
Система оповещений	+	+
Связь с внутренними программами	OneDrive,	Google Drive,
Чат	+	-
Видеосвязь	+	+
График проведения мероприятий	+	-

Google Classroom и Microsoft Teams имеют свои положительные и отрицательные стороны, но оба они являются эффективными инструментами обучения. Преимуществом Google Classroom является доступность, а Microsoft Teams – функциональность. Дополнение Moodle одним из указанных сервисов способствует повышению уровня предоставления образовательных услуг.

ЛИТЕРАТУРА

1. Рекомендации по внедрению смешанного обучения в учреждениях профессионального, перед высшего и высшего образования. URL:

<https://mon.gov.ua/storage/app/media/vishcha-osvita/2020/zmyshene%20navchanny/zmishanenvchannia-bookletspreads-2.pdf>

2. LMS Data – Spring 2020 Updates. URL: <https://edutechnica.com/category/edtech/>

3. Информационно-аналитическая справка о результатах опроса о состоянии использования технологий дистанционного обучения в учреждениях высшего образования Украины. URL: <https://cutt.ly/NfntLMe>

4. Microsoft Teams. URL: <https://www.microsoft.com/uk-ua/microsoft-365/microsoft-teams/free>

5. Classroom Help. URL: <https://support.google.com/edu/classroom#topic=6020277>

Краснощок В.М.

Київський національний університет імені Тараса Шевченка

Київ, Україна

kivinme@ukr.net

ОБРОБКА ВЕЛИКИХ НЕСТРУКТУРОВАНИХ ДАНИХ В РОЗПОДІЛЕНИХ СЕРЕДОВИЩАХ

The article discusses the problems that arise during storage and retrieval in large cloud databases, the parameters of the models used to process various large data..

Key words: *Big Data Storage, NoSQL, MongoDB, search encryption schemes, data model, distributed environments, cloud bases.*

Розподілене середовище – це віртуальний обчислювальний простір, який може обмежуватися однією розподіленою системою, а може містити кілька взаємодіючих розподілених систем. Такий віртуальний обчислювальний простір надається користувачеві у вигляді систематизованого сховища інформаційних і програмних ресурсів, має певну структуру, зрозумілу систему адресації ресурсів і певні моделі обчислювальних процесів або бізнес-процесів конкретного користувача. Бізнес-процеси користувача є проблемно-орієнтованими, відповідають певним видам його робіт. Користувач звертається до бізнес-процесів, які, у свою чергу, відвантажують необхідні ресурси для своєї роботи.

Учасниками взаємодії в розподіленому середовищі виступають окремі сутності, якими можуть бути користувачі, прикладні програми та інші обчислювальні ресурси.

У базовій моделі клієнт-сервер всі процеси в розподілених системах поділяють на дві групи. Процеси, що реалізують деяку сервіси, наприклад, службу файлової системи чи бази даних, які називають серверами (servers). Процеси, що запитують сервіси в серверів шляхом посилання запитів та наступного очікування відповіді від сервера, називають клієнтами (clients). Взаємодія клієнтів і сервера, відома також як режим роботи запит-відповідь.

Найбільш відомими розподіленими середовищами, в широкому сенсі, є хмарні сховища, які представляють собою модель зберігання даних у комп'ютері, в якій цифрові дані зберігаються в логічні пули, а фізичне зберігання охоплює кілька серверів (зазвичай, у кількох місцях).

Найбільш визнаними в Україні сховищами даних є: Dropbox, Microsoft OneDrive, Box, OziBox, Syncplicity, Google Drive, MediaFire, OpenDrive, Mega. Найбільш вагома їх перевага перед іншими сховищами – безкоштовність зберігання даних. Разом з тим всі вони дозволяють зберігати обсяг даних від кількох до декількох десятків гігабайт, високу швидкість доступу до даних та безпеку роботи з даними.

Всі ці середовища підходять фізичним особам, але не завжди юридичним особам, які є невеликими фірмами чи організаціями. Обсяг даних в таких установах може бути значним, порівняно з простором, що виділяють перелічені сервіси чи швидкість та доступ до них будуть суттєво обмежені. Виходом в такій ситуації може стати написання застосунку (клієнтської частини) до сервісів, які пропонують зберігання більшого обсягу, а за безпеку даних відповідатиме клієнтська частина програми. Тобто все шифрування та дешифрування проходитиме на клієнтській частині, а в хмарному сховищі будуть зберігатися неструктуровані зашифровані дані [1].

Зберігання даних передбачає використання баз даних, а неструктурованість цих даних надає перевагу базам даних з технологією NoSQL. Такі бази даних дозволяють зберігати неструктуровані дані в довільному, зручному для користувача, форматі, обробляти та швидко повертати дані на запити довільної складності.

Незалежно від застосовуваного шифрування, в більшості баз даних з технологією NoSQL, наприклад MongoDB, швидкий пошук здійснюється завдяки індексації даних. У MongoDB індекси представлені В-деревими.

У В-дерев є дві головні властивості, які роблять їх ідеальною складовою організацією індексів в базах даних. По-перше, вони забезпечують ефективно

виконання самих різних запитів, в тому числі, пошук за збігом, за діапазоном, сортуванням, за випадковим збігом префіксів і з застосуванням тільки самих індексів. По-друге, В-дерева залишаються збалансованими після вставки і видалення ключів [3].

Основними перевагами В-дерев є:

- у всіх випадках корисне використання простору вторинної пам'яті становить понад 50%. Зі зростанням ступеня корисного використання пам'яті не відбувається зниження якості обслуговування;
- довільний доступ до запису реалізується за допомогою невеликої кількості підоперацій (звернення до фізичних блоків);
- в середньому досить ефективно реалізуються операції включення та видалення записів; при цьому зберігається природний порядок ключів з метою послідовної обробки, а також відповідний баланс дерева для забезпечення швидкої довільної вибірки;
- постійна впорядкованість за ключем забезпечує можливість пакетного оброблення.

Ключовим для швидкого пошуку у великих базах даних є модель даних. Кожна модель даних найкраще підходить для певного набору застосунків і вимог з урахуванням її моделі предметної області, моделей доступу до даних і варіантів використання. Будь-яка модель предметної області, яка дозволяє розділяти і розподіляти свої дані за документами, може використовувати базу даних документів.

Документо-орієнтована СУБД [2] – це спеціально призначена для зберігання ієрархічних структур даних (документів) і зазвичай реалізована за допомогою підходу NoSQL. В основі документо-орієнтованих СУБД є документні сховища, які мають структуру дерева (лісу). Структура дерева починається з кореневого вузла і може містити кілька внутрішніх і листових вузлів. Листові вузли містять дані, які при додаванні документа заносяться в індекси, що дозволяє навіть при досить складній структурі знаходити місце (шлях) шуканих даних. API для пошуку дозволяє знаходити за запитом документи і частини документів. На відміну від сховищ типу ключ-значення, вибірка за запитом до документного сховища може містити частини великої кількості документів без повного завантаження цих документів в оперативну пам'ять.

Сховища ключів-значень (Key-Value) є зазвичай моделями даних, які використовуються переважно для застосунків, що оточують дані, наприклад, профіль користувача, електронні листи, коментарі до блогу / статті, інформація про сеанс, дані про кошик покупок, огляди продуктів, відомості про продукти і

таблиці пересилання за інтернет-протоколу (IP). Сховище ключ-значення відмінно підходить для зберігання повних веб-сторінок. У цьому випадку URL може використовуватися як ключ, а вміст веб-сторінки – як значення.

Графічні бази даних (Graph) пропонують ефективний спосіб управління і об'єднання даними. Корпоративні дані зазвичай пов'язані між собою, і графічні бази даних для їх зберігання забезпечують простіше управління контентом. Концепція взаємно пов'язаного світу, роль якої зростає після появи соціальних мереж та Інтернет речей, може використовувати той факт, що графічні бази даних дозволяють інтегрувати різні різні взаємопов'язані дані з різних джерел.

Сховища з широкими стовпцями (Wide column store) – це також модель для зберігання великих даних. Ці бази даних вважають найбільш придатними для розподілених систем. Вони використовують таблиці, рядки і стовпці, але на відміну від реляційних баз даних, назви та формат стовпців може бути різним у різних рядках таблиці. Їх можна розуміти як двовимірну базу даних «ключ-значення».

Таким чином, при роботі з великими даними, які зберігають у хмарних базах даних, необхідно велику увагу приділяти моделі зберігання даних і безпеки роботи з даними. Для цього можна скористатися вже готовими рішеннями, які пропонують великі компанії і корпорації при роботі з хмарними базами даних, так і розробляти свої варіанти шифрування з подальшим зберіганням цих даних. Незважаючи на переважання на ринку баз даних реляційних СУБД, технологія NoSQL є досить перспективною і в рамках цієї технології пропонують прогресивніші механізми пошуку у великих базах даних.

ЛІТЕРАТУРА

1. Artem Storozhuk Шифрование в базах данных SQL с возможностью поиска https://dou.ua/lenta/articles/searchable-encryption/?fbclid=IwAR1cUztFly8qv9JmoYzuXL0JsSFkuDgLGIn2szUwsgFDtZMphl6pms_w908 [in Russian];
2. Samiya Khan, Xiufeng Liu, Syed Arshad Ali, Mansaf Alam Storage Solutions for Big Data Systems: A Qualitative Study and Comparison. Available at: <https://arxiv.org/ftp/arxiv/papers/1904/1904.11498.pdf> (Accessed 28 Feb 2020) [in English];
3. Кайл Бэнкер. MongoDB в действии./ Пер. с англ. Слинкина А. А. - М.: ДМК Пресс, 2012. - 394с.

Кобижча І.І.,

Київського національного університету ім. Т. Шевченка,

м.Київ

igorkobyzhcha@gmail.com

СУЧАСНІ ТЕХНОЛОГІЇ І МЕТОДИ РОЗРОБКИ ВЕБ-ЗАСТОСУНКІВ

The thesis considers a list of modern technologies and methods of website development, as well as identifies their advantages and disadvantages in the development and maintenance, and is use by customers.

Keywords: *internet, web service, e-commerce, framework, trends, technology.*

Технології і методи веб розробки іноді змінюються швидше, ніж їх можна впровадити. Щоб залишатися на крок попереду, важливо зосереджуватися на тенденціях, техніках і підходах, які набувають популярності.

Сьогодні є багато різних методів і засобів створення сайтів, які можна поділити на три категорії:

1. Розробка в конструкторі сайтів, наприклад Wix, Squarespace;
2. Розробка на CMS (Content management system), наприклад Wordpress, Joomla;
3. Самостійна розробка сайтів.

У кожного з цих способів є свої переваги і недоліки.

Створюючи сайт з «нуля», на виході отримуємо унікальний і персоніфікований продукт, який буде вирішувати певні завдання клієнта. Переваги власноруч створеного сайту в тому, що його функціональність буде профільована для ефективного вирішення конкретної бізнес-задачі, його легше оптимізувати і просувати в пошуку. З недоліків можна виділити те, що розробка продукту буде дорожчою і займе більше часу.

Найпопулярнішими фреймворками нині є React.js, Vue.js та Angular.js.

За допомогою React.js розробники можуть створювати повторно використовувані компоненти (reusable components), кожен з яких буде з власним станом [1]. Якщо на сторінці необхідно оновити лише один компонент, React змінює лише його, а не оновлює всю сторінку. Для цього він використовує Virtual DOM – спосіб представлення UI (інтерфейс користувача), який зберігається в пам'яті і постійно синхронізується з реальним DOM. Такі великі компанії, як Airbnb, Instagram і Netflix вже використовують React, цей фреймворк є надійним і ефективним. React Native – це фреймворк, який дозволяє створювати

кроссплатформені застосунки для iOS і Android. Фреймворк використовує ту ж саму технічну базу, що і React.

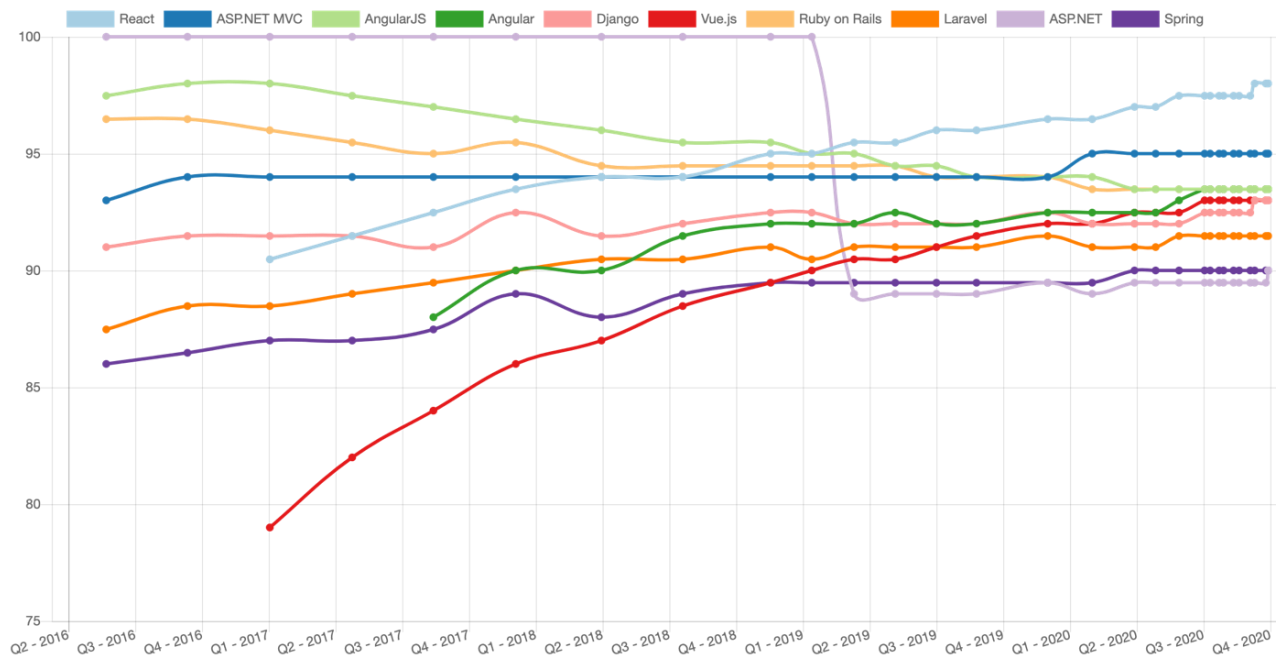


Рисунок 1. Популярність веб-фреймворків

Vue.js – це JavaScript фреймворк, який завдяки маленькому розміру (20 кб), швидкості і гнучкості показує найкращу продуктивність порівняно з іншими фреймворками [2]. Vue – прогресивний фреймворк, це означає, що якщо у вас вже є проєкт, то можна використати Vue лише на певній частині цього проєкту, і все буде працювати без проблем. На жаль, великі компанії, як Facebook і Google поки не підтримують цей фреймворк, але популярність зростає з кожним днем.

Angular вважається одним з найкращих фреймворків для веб розробників. Цей фреймворк розробив і підтримує Google. Angular дозволяє розробникам створювати потужні веб застосунки, він використовується для створення високопродуктивних і великомасштабних веб-застосунків [3]. Застосунки, створені за допомогою цього фреймворку, прості в обслуговуванні.

Використовуючи останні тенденції веб-розробки, можна покращити роботу своїх веб-застосунків. Загалом, кожен веб-фреймворк вартий уваги. Деякі з них вже мають велику базу користувачів і заручились підтримкою компаній, отже немає жодних ризиків при використанні їх у своїх проєктах.

ЛІТЕРАТУРА

1. React – A JavaScript library for building user interfaces [Електронний ресурс] — Режим доступу до ресурсу: <https://reactjs.org/docs/glossary.html#components>

2. Vue.js [Електронний ресурс] — Режим доступу до ресурсу: <https://vuejs.org/>

3. Angular – Features & Benefits [Електронний ресурс] — Режим доступу до ресурсу: <https://angular.io/features>

Луценко В. В.

*Київський національний університет імені Тараса Шевченка,
vladyslav.lutsenko99@gmail.com*

ОРГАНІЗАЦІЯ БЕЗПЕЧНОЇ РОБОТИ ПРИ ВИКОРИСТАННІ ЕЛЕКТРОННОЇ ПОШТИ

This article presents the main threats to the use of e-mail, the benefits of its use and the main methods of protection against threats.

Keywords: *e-mail, password, protection, internet, viruses, spam, antivirus, management policies.*

Використання електронної пошти займає значне місце в діяльності підприємств будь-якої сфери. Багато чинників серед яких: електронний документообіг, цифровий підпис, сприяють поширенню та розвитку використання електронної пошти. Також безсумнівним плюсом є її зручність у використанні та порівняно низька ціна. А, зазвичай, використання електронної пошти є безкоштовним. Звісно, при використанні електронної пошти виникають загрози інформаційної безпеки, які можуть стати причинами витоку персональної або конфіденційної інформації.

Серед таких загроз можуть бути:

- завантаження вірусів та шкідливих доповнень
- спроби запуску системних команд
- унеможливлення роботи або вихід з ладу операційної системи
- витоки конфіденційної інформації
- перенавантаження поштового клієнту
- втрата контролю над поштовою скринькою і т.д.

Задля ефективного захисту електронної пошти необхідна ієрархічна система керування безпекою та ефективністю, яка повинна містити в собі[1]:

- контроль на системотехнічному рівні

- контроль над користувачами: їхнє реєстрування, створення адресних книг, переліків розсилання тощо
- контроль над інформаційними потоками
- протидія зараженню комп'ютерними вірусами
- забезпечування конфіденційності шляхом аналізування структури та вмісту електронних листів

При використанні корпоративної електронної пошти на підприємстві доцільним є створення відповідної політики використання електронної пошти. Вона містить критерії котрі визначають ознаки виникнення критичних ситуацій та необхідні дії при виникненні таких ситуацій. На підставі використання правил, умов та дій працює система моніторингу електронної пошти. Одним з прикладів може слугувати система захисту поштового сервера за допомогою TrendMicro Scan Mail for MS Exchange.

Даний програмний засіб можливо запустити з віддаленого терміналу при умові попереднього встановлення продукту TrendMicro. У цій системі передбачено централізоване керування. Автоматично забезпечується захист у реальному часі для тільки створених поштових скриньок. Антивірусне сканування поштових повідомлень здійснюється у фоновому режимі або спеціалістом з безпеки вручну. При виявленні зараженого повідомлення відправникові, одержувачам та адміністраторові надсилається попередження щодо цього інциденту. Співробітники не мають прав доступу щоб вимкнути сканування пошти, аби передати шкідливий файл, оминаючи систему безпеки.

При скануванні використовується активний фільтр повідомлень. Адміністратором мережі можуть вибиратися типи електронної пошти й даних, які сервер пропускати або не пропускати за допомогою фільтра на підставі інформації в їхніх заголовках: домена, звідки відправлене повідомлення, або вмісту полів From (Відправник), To (Кому) і Subject (Тема)[2]. Це може використовуватися для боротьби зі спамом.

Коли повідомлення потрапляє до системи захисту, відбувається повна перевірка та аналіз листа, його структури та вмісту. Дана система працює з усіма типами файлів. Система моніторингу виконує:

- контроль відправників та одержувачів повідомлень
- фільтрування повідомлень за їхнім розміром, датою, типом долучених файлів
- визначення реального типу долучених файлів за сигнатурою, тобто за двійковим кодом.

Одним з найпоширеніших видів захисту є шифрування листів на транспортному рівні, який забезпечує безпеку повідомлення в процесі передачі через Інтернет. Даний метод схожий на вкладення листа в конверт, тобто можна побачити звідки та куди направляється повідомлення, проте його зміст можна побачити тільки після відкриття так званого «конверта».

Інший метод захисту пошти — це повне шифрування даних. Сутність даного методу полягає в тому, що лист шифрується у відправника, а розшифровується в одержувача, при цьому в процесі передачі воно має зашифрований вигляд. Навіть якщо дані будуть перехоплені, зміст їх буде неможливо прочитати. Існують плагіни для браузерів і поштових клієнтів, що реалізують цю технологію, тим самим значно спрощують роботу.

Отже, можна зробити висновок що при роботі з електронною поштою є багато загроз та проблем, які вирішені тільки частково. Необхідно приділяти увагу заходам безпеки для унеможливлення витоку інформації. Основними рекомендаціями для захисту електронної пошти є:

1. Використання політики керування
2. Використання шифрування даних
3. Встановлення антивірусу
4. Використання шифрування на транспортному рівні
5. Впровадження спеціальних фільтрів та мережевих екранів
6. Створення політики доступу
7. Використання спеціальних поштових сервісів та систем

ЛІТЕРАТУРА

1. Бурикін О. Б., Кулик В. В., Рубаненко О. Є., Малогулко Ю. В. *Вінницький національний технічний університет*. Система оптимального керування режимами локальних електричних систем з відновлюваними джерелами енергії. 2016. С. 2.
2. Електронний посібник. *Тернопільський національний технічний університет ім. І. Пулюя*. 2019. С. 42.
3. Безпека пошти: основні рекомендації для захисту скриньок від онлайн-загроз – [Електронний ресурс] – Режим доступу: <https://eset.ua/ua/news/view/659/bezopasnost-pochty-vneshniye-i-vnutrenniye-factory-zashchity-pochty>
4. Захист електронної пошти – [Електронний ресурс] – Режим доступу: <https://faq.in.ua/articles/29-zakhyst-elektronnoyi-poshty.html>

Мазютинець Г. В.,

ДВНЗ «Ужгородський національний університет»,
м. Ужгород, e-mail: gabbi.maz@uzhnu.edu.ua

Маляр М. М.,

ДВНЗ «Ужгородський національний університет»,
м. Ужгород, e-mail: mykola.malyar@uzhnu.edu.ua

Шаркаді М. М.,

ДВНЗ «Ужгородський національний університет»,
м. Ужгород, e-mail: marianna.sharkadi@uzhnu.edu.ua

НЕЧІТКІ МОДЕЛІ У СИСТЕМІ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ

In the Ukrainian economy of the recent period, after numerous crises, reforms, post-crisis and transition periods, market relations are deepening, their quality and role is growing, and thus the impact on the direct functioning of enterprises is increasing. The financial security of the enterprise plays a special role in the activities of the enterprise in the long run. Require special attention to the study and analysis of financial and economic activities of enterprises, expanding the scope of production activities, finding tools for their effective operation, as well as finding sources of funding. The works of many leading Ukrainian and foreign scientists are devoted to the problems of financial security of methodological and scientific-practical nature. Despite the significant amount of research work on this issue, a large number of problems in the field need further development and improvement.

This publication proposes a scientific approach to determining the levels of financial security, which is a state of protection of enterprises from unforeseen negative changes. The authors propose modeling the level of financial security of enterprises using fuzzy set theory. To assess the complex indicator of the level of financial security, it is proposed to formalize the type of integrated indicator, which can be used to conduct a comprehensive assessment of enterprises.

Keywords: *financial and economic security, level of financial security, fuzzy model.*

Вступ. Для суб'єкта господарювання економічна безпека розглядається як стан, за якого забезпечується його економічний розвиток і стабільна діяльність, гарантується захист його фінансових і матеріальних ресурсів. Враховуючи, що в цьому випадку мова йде про складну систему, доречно навести визначення,

запропоноване Л. Донцем: «система економічної безпеки підприємства являє собою обмежену безліч взаємозалежних елементів, що забезпечують безпеку підприємства і досягнення ним цілей бізнесу» [1]. Серед факторів, які не можна залишити осторонь, порушуючи проблеми економічної безпеки, є вплив на економічну та фінансову діяльність стрімкого розвитку інформаційних та інноваційних технологій, зокрема науково-технічного прогресу в цілому, оскільки саме вони є сьогодні необхідною складовою конкурентоспроможності та подальшого розвитку. Забезпечення фінансової безпеки пов'язане з плануванням, прогнозуванням і передбаченням багатьох факторів внутрішнього і зовнішнього середовища. При цьому вкрай важливим є системний, комплексний підхід, що базується на ефективному використанні відповідного інформаційно-аналітичного забезпечення, логіки та моделювання із залучення сучасного математичного апарату. Оскільки врахувати всі фактори впливу та потенційні загрози складно або просто неможливо, потрібно визначити пріоритети, після чого розглянути, обрати, адаптувати або побудувати модель, застосування якої зумовлює та визначає вибір заходів щодо забезпечення фінансової безпеки.

Постановка задачі. Нехай для певного суб'єкта економічного господарювання відома множина кількісних і якісних показників його функціонування, а також відома історія цих показників за певні періоди часу. Виникає завдання передбачити оцінку рівня економічної безпеки даного суб'єкта господарювання.

У процесі досягнення поставленої задачі необхідно: визначити та охарактеризувати модель оцінки рівня фінансової безпеки підприємства; здійснити аналіз фінансового стану підприємства; побудувати модель оцінки рівня фінансової безпеки підприємства.

Адекватні математичні моделі для управління фінансово-економічною безпекою вимагають всебічного врахування факторів невизначеності, пов'язаних з особливостями функціонування підприємств в сучасних ринкових умовах. Вплив даних факторів ускладнює отримання необхідних правильних та обґрунтованих рішень, що обумовлює практичну важливість обробки нечітких даних та необхідність використання нечітко-множинного підходу.

Для аналізу стану рівня фінансової безпеки і прогнозування загроз сьогодні будуються моделі із застосуванням апарату нечітких множин. Це дає можливість поєднання кількісних даних та лінгвістичних змінних з метою отримання оцінки з урахуванням прогнозованих ризиків і загроз. Для цього формується перелік обмежень, у рамках яких має функціонувати система безпеки та описуються групи показників, що характеризують ці обмеження. Розгорнутий перелік факторів

обмежень може враховувати обмеження від тих, що зумовлені законодавством держави і особливостями діяльності саме в цій країні, до обмежень, пов'язаних зі специфікою діяльності в конкретній галузі та унікальною структурою самого суб'єкта господарювання. Для оцінки створюється шкала, за допомогою якої лінгвістичним змінним ставиться у відповідність певні кількісні показники. Будуються функції належності із застосуванням методу експертних оцінок.

Розроблено багатофакторну нечітко-множинну модель аналізу рівня фінансової безпеки підприємства, що дозволяє розрахувати інтегральний показник фінансової безпеки підприємства на основі відповідної системи груп факторів, розподілених за нечіткими рівнями.

Фінансовий рівень підприємства може бути оцінений на основі значень узагальнених груп показників[2]. У свою чергу, комплексне значення кожної з груп показників було розраховане за кількісними та якісними критеріями оцінок. Для цього, пропонується методика формалізації критеріїв оцінки за допомогою функцій належності. Запропоновано найбільш вживані види функції належності, які можуть задавати множину критеріїв для розглядуваної задачі. Множина критеріїв розбивається на групи відносно описання тим чи іншим видом функції належності[3]. Для кожного моменту часу за всіма групами показників отримуємо згортання цих показників в межах своїх груп відповідно. Після цього, на основі логічного висновку, можемо отримати рівень фінансової безпеки підприємства.

Висновки.

Запропонований підхід дозволяє моделювати рівень фінансової безпеки підприємства за допомогою апарату нечіткої математики, що дозволить об'єктивізувати суб'єктивність міркувань експертних висновків для прийняття управлінських рішень.

ЛІТЕРАТУРА

1. Донець Л.І., Ващенко Н.В. Економічна безпека підприємства: навч. пос. — К.: Центр учбової літератури, 2008. — 240 с.
2. Маляр М.М. Нечіткі моделі і методи оцінювання кредитоспроможності підприємств та інвестиційних проектів : монографія / М.М. Маляр, В.В. Поліщук. — Ужгород : РА «АУТДОР-ШАРК», 2018. — 174 с.
3. Polishchuk V. Technology to Improve the Safety of Choosing Alternatives by Groups of Goals/ V. Polishchuk// Journal of Automation and Information Sciences. — Begell house, Inc, New York, 2019. — Volume 51, 2019 Issue 9. — P.66-76. DOI: 10.1615/JAutomatInfScien.v51.i9.60.

Макаренко О.С.

ННК «ІПСА» КПІ ім. Ігоря Сікорського

Київ, Україна

makalex51@gmail.com

Самородов Є.Л.

ННК «ІПСА» КПІ ім. Ігоря Сікорського

Київ, Україна

esamor2@gmail.com

Морева О. О.

ННК «ІПСА» КПІ ім. Ігоря Сікорського

Київ, Україна

olga_moreva@ukr.net

Патіоха А.А.

ННК «ІПСА» КПІ ім. Ігоря Сікорського

Київ, Україна

alla_patio@ukr.net

ДОСЛІДЖЕННЯ ПРОЦЕСІВ МІГРАЦІЇ В НАУЦІ ТА ОСВІТІ З ВИКОРИСТАННЯМ МОДЕЛЕЙ ТА ГІС.

The results of a systematic analysis of an important applied problem of external and internal migration in the field of education and science are presented. Classes of models for studying these processes are offered. The choice of information platform for studying and modeling of these processes is considered.

Keywords: *migration, education, science, models, relational cartography, geographic information systems*

Загальноприйнятим в індустріальному світі є визнання того, що значною мірою розвиток промисловості, добробуту суспільства та прогрес в інших галузях залежить від розвитку освіти та науки. При цьому сама наука та техніка створює нові можливості для розвитку освіти та науки. Як приклад можна навести дистанційну освіту з застосуванням інформаційних технологій, психології, віддаленого доступу, математичного моделювання. Дослідженням з цих питань та розробці відповідних засобів для практичних застосувань присвячено дуже багато зусиль з залученням великих коштів (як держбюджетних, так і комерційних). Україна як невід'ємна частина світової спільноти теж посідає певне місце серед інших країн і є учасником таких процесів. Але Україна з певних причин (особливо

специфічних для пост-радянських країн в процесі трансформації) має свої специфічні задачі в галузі освіти та науки, які потребують вирішення задач з реформування галузі освіти та науки, суттєвого покращення процесу навчання, перегляду задач фінансування освіти та науки та багато іншого. Також нагальною потребою для України є забезпечення сталого розвитку освіти та науки. Треба зауважити, що багато установ та спеціалістів займаються цими питаннями. Але насправді є велика кількість проблем, які поки що не є вирішеними (а іноді навіть не є чітко сформульованими). Тому нагальною потребою в українських реаліях є більше залучення для розгляду проблематики та прийняття практичних рішень сучасних наукових підходів, в першу чергу системного аналізу, математичного моделювання, засобів аналізу даних, в тому числі просторових з залученням геоінформаційних систем [1-5].

Стан розвитку науки та освіти у світі зараз визнається визначним для розвитку економіки, промисловості та добробуту найбільш розвинутих країн, про що свідчить, наприклад, присудження нобелівської премії 2018 з економіки П. Ромеру за моделювання впливу знань на розвиток економіки. Є також величезна кількість теоретичних та прикладних досліджень та розробок пов'язаних з знаннями. В Україні теж виконана певна кількість досліджень в галузі науки та освіти. Але зараз в зв'язку з перехідним станом України, новими викликами та критичними проблемами виникає потреба розв'язку нових задач з застосуванням моделювання та інформаційних технологій.

Однією з критичних задач, що має довготривалий вплив на розвиток України має міграція науковців і студентів з наукових напрямків. Раніше ця проблема обговорювалась в пресі або середовищі науковців або освітян без спроб більш формального розгляду. Дещо глибше питання ставилися профільними інституціями – НАНУ, НАПНУ, інститутами та дослідниками. Але як правило це розглядалось на рівні констатації факту небезпечної міграції з збором та застосуванням статистики (В. Ковтунець, О. Попович, Е. Стадник і інші). Але зараз назріла можливість розробки моделей, методів та програмного забезпечення для прогнозування в галузі перебігу можливих варіантів міграції.

Звісно, неможливо розв'язати зразу всі необхідні для освіти та науки України задачі відразу. Для цього планується застосувати моделі з класу звичайних диференційних рівнянь, їх систем, клітинних автоматів, нейромереж, мультиагентних систем, системної динаміки та теорії мереж. Головною особистістю рішення є врахування балансів потоків від'їзду та повернення та їх залежність від внутрішніх та зовнішніх умов. При цьому для роботи з реальними просторовими даними планується застосувати геоінформаційні системи [6, 7].

Але процеси міграції в Україні не можна вивчати без врахування міжнародного стану. Для врахування зовнішнього впливу слід використовувати зовнішні відкриті дані, які повинні входити складовою частиною для моделей і рішень. Для інтеграції методів і моделей процесів міграції в науку та освіту зовнішні і внутрішні дані повинні бути приведені до "спільного знаменника", тобто використовувати стандартизовані способи зберігання та подання інформації.

Найбільш придатними форматами даних з точки зору сумісності є інструкції INSPIRE. Відповідно до цих стандартів можливо комбінувати дані з різних джерел, повторно їх використовувати, застосовуючи розподілену сервісну архітектуру (SOA), а для дослідження міграційних процесів наукових кадрів рекомендується використовувати такі продукти: AtlasSF, Giscuit і GeoNetwork.

ЛІТЕРАТУРА

1. Макаренко О. С. Аналіз та сценарії геополітичних та геоeкономічних процесів і місце в них України. Тези міжнар. Науково-практичної конференції «Україна в системі змін парадигми світопорядку ХХ-ХХІ століть». К.: Ун-т. ім. Грінченко. 2016. С. 46-50

2. Makarenko A. Towards system analysis and modeling of global sustainable development. Proc. EMCSR-2014, Vienna, April, 2014. pp. 427-430.

3. Makarenko A., Kirvelis D. The Ukrainian bifurcation point in innovative technologies and education as a contrast to the development of Lithuania. International business: Innovations, Psychology, Economics, 2013. vol.4, n.1(6). Pp. 7-16

4. Z. Klestova, A. Makarenko Conflict of Interest between Eastern and Western Scientific Systems. Science and Engineering Ethics, 2002. Vol.8 , pp. 387-392.

5. Makarenko A., Kirvelis D. The Ukrainian bifurcation point in innovative technologies and education as a contrast to the development of Lithuania. International business: Innovations, Psychology, Economics, 2013. vol.4, n.1(6). Pp. 7-16

6. Самородов Є.Л., Морева О. О., Патіоха А.А. Вибір інформаційної платформи для відображення міграційних процесів наукових кадрів. Матеріали міжнародної науково-практичної конференції “Інформаційні технології та комп’ютерне моделювання” 18-22 травня 2020 року, Івано-Франківськ. 2 с.

7. Макаренко О.С., Самородов Є.Л. Геоінформаційні системи як засіб підтримки реформ. Задачі, приклади та можливості. Матер. П’ятої міжнародної наук.-практ. Конференції Інформаційні технології та комп’ютерна інженерія. Івано-Франківськ 27-29 травня 2015. С. 51-52.

Малишев О. В.

*Інститут проблем математичних машин і систем НАН України, м. Київ,
oleg_malyshev@ukr.net*

ЖИТТЄВИЙ ЦИКЛ СИСТЕМИ: ПОГЛЯД З ВИСОТИ ПТАШИНОГО ПОЛЬОТУ

The system life cycle has recently been viewed by many as an interesting and promising object of modeling and management. But the system life cycle and something that includes it, at least from the point of view of the need to manage it, are not the same things. In this regard, suspicions arise about the need to consider some meta-level, for which, perhaps, it will be necessary to look for an appropriate subject, appealed to attend to it.

Keywords: *system, life cycle, model, meta-model, management, object of management, subject of management.*

Останнім часом усе більший інтерес користувачів, замовників, творців систем та інших категорій зацікавлених у системах осіб викликає проблематика підтримки життєвого циклу системи. Насамперед, це стосується складних систем, підтримка життєвих циклів яких пов'язана із значними витратами. Працює не зовсім очевидне припущення, що шляхом упорядкування процесів підтримки ці витрати можуть бути суттєво зменшені. Але зрозуміло, що будь-яке упорядкування діяльності неминуче потребує додаткових значних зусиль і витрат ресурсів, зекономити які можливо лише за рахунок використання апробованих ефективних моделей діяльності, тобто застосування формального підходу [1]. Наразі існують, як мінімум численні нормативні документи, що містять такі моделі - насамперед, це міжнародні стандарти ISO (ISO/IEC/IEEE) під загальною рубрикою «Systems and software engineering» (українською мовою – «Інженерія систем і програмного забезпечення»), де окреме місце займають стандарти, присвячені проблематиці управління життєвим циклом систем (ЖЦС). Деякі з них уже набули статус державних стандартів України (ДСТУ). Крім того, відповідно до узятого Україною курсу на членство в НАТО. ця частина її нормативного поля розвивається з урахуванням продукції Бюро Стандартизації НАТО (NATO Standardization Office - NSO), а саме, документів категорії «Allied Administrative Publication» (AAP). Кожний з цих нормативних документів (стандартів) присвячений окремому певному аспекту ЖЦС, тому виникає цілком природне бажання уможливити охопити «середньозважений» ЖЦС у цілому мета-моделлю ЖЦС (див. рис. 1).

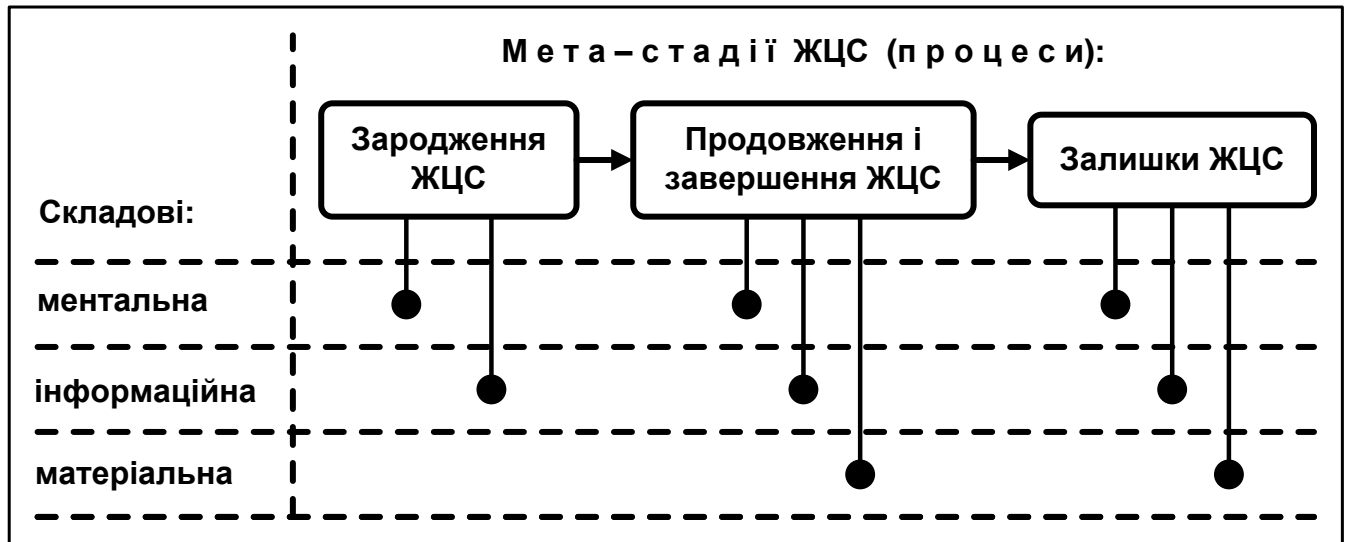


Рис. 1. Мета-модель ЖЦС

Мета-модель оперує поняттями мета-стадій ЖЦС (процесів) та їх складових - ментальної, інформаційної та матеріальної.

Мета-стадія «Зародження ЖЦС» включає в себе, насамперед, ментальні напрацювання щодо самої системи - стадія концепції (concept) ЖЦС [2, 3]). Але на цій мета-стадії у поле зору неминуче попадають також інші аспекти - можливі зацікавлені сторони, системи забезпечення тощо:

зацікавлена сторона (stakeholder) – «фізична особа чи організація, що має право, частку, претензії або інтерес до системи або її характеристик, які відповідають їхнім потребам й очікуванням» [2, 3]; приклади: кінцеві користувачі-особи, кінцеві користувачі-організації, прихильники, розробники, виробники, тренери, супроводжувальна сторона, фахівець зі списання, покупець, постачальник і регуляторні органи. Деякі зацікавлені сторони можуть мати інтереси, що конфліктують з іншими зацікавленими сторонами або системою;

система забезпечення (enabling system) – «система, яка підтримує цільову систему, під час етапів життєвого циклу, але не обов'язково вносить безпосередній внесок в її функції під час експлуатації» [2, 3]; приклад: якщо цільова система переходить на стадію промислової експлуатації, для цього потрібна відповідна платформа.

Безсумнівно, що на цій мета-стадії виникає «зародок» моделі витрат на життєвий цикл (Life Cycle Cost – LCC [4]), «приреченої» розвиватись і супроводжувати весь ЖЦС, реагуючи на зовнішні та внутрішні для нього зміни.

На цій мета-стадії так чи інакше виникає інформаційна складова, зокрема, документація.

Мета-стадія «Продовження і завершення ЖЦС» включає в себе такі стадії ЖЦС: розроблення (development), виробництво (production), використання (utilization), підтримання (support) та утилізація (retirement) [2, 3]. Цікаво, що гнучкість стандартів проявляється у тому, що вони допускають порушення «природної» послідовності стадій і навіть появу «циклів» [5]. Типова діяльність на цих стадіях поділяється на процеси, які поділяються на такі групи [2, 3]: процеси угоди (agreement processes), процеси організаційного забезпечення проекту (organizational project-enabling processes), процеси технічного управління (technical management processes) та технічні процеси (technical processes) [2, 3].

На стадіях використання і підтримання:

значно розширюється коло зацікавлених сторін;

з примноженням упроваджених примірників системи значно розширюються усі складові мета-стадії;

розширюється номенклатура здійснюваних видів діяльності – зокрема, виникає потреба у проведенні навчань;

разом із набуттям досвіду експлуатації системи виявляються її недоліки відносно декларованих можливостей і відносно рівня, можливо зростаючого, потреб, які система покликана задовольняти.

Усе це і багато чого іншого викликає загострення проблеми забезпечення адекватного управління. Так, стандарти ідентифікують окремі процеси саме як процеси управління, але уважне ознайомлення з ними (стандартами) виявляє цікавий факт: у них згадується багато сутностей, що розглядаються як об'єкти управління (management) – наприклад, спроможність, зміна, скарга, інцидент, інформаційна безпека тощо. Це означає, що на кожній стадії ЖЦС треба здійснювати обґрунтований відбір «потрібних» об'єктів управління і обґрунтовану відмову від «непотрібних». Кожний відібраний об'єкт управління потребує розроблення і впровадження відповідного контуру управління. До цього треба додати, що між окремими контурами управління треба виявляти і врахувати існування суттєвих взаємозв'язків між ними.

Інформаційна складова мета-стадії створюється і розвивається з урахуванням запропонованої в [6] системи інформаційних елементів (документації).

Закінчення цієї мета-стадії пов'язують зі стадією утилізації. Так, дійсно, немає ніякого сенсу зберігати матеріальні залишки системи, хіба що для виставлення у музеї. Але зрозуміло, що від системи повинні зберегтись залишки інформаційні. І ніхто не може вимагати стерти залишки ментальні, які, до речі, як і інформаційні, можуть дати поштовх для зародження нової системи. Тому мета-

модель включає мета-стадію (процес) «Залишки ЖЦС»

Резюме: дана робота – це спроба «явочним порядком» показати об’єктивність існування мета-рівня для власне рівня ЖЦС. За умови визнання його існування, чи не виникає потреба в уведенні у розгляд суб’єкта, що мав би ним опікуватись?

ЛІТЕРАТУРА

1. Малишев О.В. Моделювання діяльності у процесах управління життєвим циклом систем (ескіз формального підходу). – У кн. «Математичне та імітаційне моделювання систем. Тези доповідей XV-ї Міжнародної науково-практичної конференції - МОДС 2020», м. Чернігів, 2020. - С. 356-360.

2. International Standard ISO/IEC/IEEE 15288 First edition 2015-05-15 Systems and software engineering — System life cycle processes. - 118 p.

3. ДСТУ ISO/IEC/IEEE 15288:2016 (ISO/IEC/IEEE 15288:2015, IDT) Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем. – Київ, ДП «УкрНДНЦ», 2018. – 90 с.

4. NATO Standard AAP-20 NATO Programme Management Framework (NATO Life Cycle Model) Edition C Version 1 October 2015. – 78 p.

5. Technical Report ISO/IEC TR 24748-1 First edition 2010-10-01 Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management. - 86 p.

6. International Standard ISO/IEC/IEEE 15289 Third edition 2017-06 Systems and software engineering — Content of life-cycle information items (documentation). - 98 p.

Малишев О. В.

Інститут проблем математичних машин і систем

НАН України, м. Київ,

oleg_malyshev@ukr.net

Калмиков В.Г.

Інститут проблем математичних машин і систем

НАН України, м. Київ

vl.kalmykov@gmail.com

КОНЦЕПТУАЛЬНА МОДЕЛЬ ПЛАНУВАННЯ ДІЯЛЬНОСТІ НА ОСНОВІ СПРОМОЖНОСТЕЙ

One approach to improving an organization's activities is an approach aimed at regulating its capabilities. This approach is applied in many fields of activity, but most extensively and consistently in the defense sphere of developed countries, NATO, and more recently in Ukraine. In this paper, we propose a conceptual model of accounting and use of capabilities. This model has two components: static and dynamic. The static component of the model is a set of entities, relationships between them, as well as attributes of entities and relationships between entities. The main entities are capability and carrier of capability. The proposed model can be used as the basis for creating the appropriate information technology.

Keywords: *activity, organization, capability, process, model, capability carrier, requirement.*

Удосконалення механізмів здійснення людьми своєї практичної діяльності є чи не найважливішим чинником прогресу. Основним суб'єктом діяльності виступає організація (англ. organization) – «особа чи група людей, які мають свої власні функції з відповідальністю, повноваженнями та взаємовідносинами, щоб досягати своїх цілей» [1]. Серед відомих підходів до удосконалення діяльності, зокрема, планування діяльності, окреме місце займає такий, що спирається на поняття «спроможності», тобто для досягнення певних цілей організація має володіти певними спроможностями. Цей підхід застосовується у різних видах діяльності (див., наприклад, [2-5]), зокрема, у такій важливій сфері діяльності як оборонне планування, що має місце у багатьох розвинених країнах, починаючи з США [6], і на міжнародному рівні - в НАТО [7]. Не так давно до цього руху приєдналась і Україна [8]. Але аналіз численних матеріалів, присвячених підходу, призводить до думки, що відносна новизна підходу потребує зусиль щодо його доосмислення, що і є метою даної роботи.

У [1] спроможність (англ. capability) визначається наступним чином: «здатність об'єкта отримувати вихід, який відповідатиме вимогам до цього виходу». Для цього «отримання виходу» необхідно запустити певний процес (англ. process) – «сукупність взаємопов'язаних або взаємодійних робіт, що використовують входи для створення запланованого результату» [1], в якому входи перетворюються у результат (вихід) за рахунок участі у процесі певного об'єкта - носія спроможності.

У загальному випадку необхідну трансформацію входу у вихід можуть здійснювати різні, і навіть принципово різні носії спроможностей і, якщо підняти на рівень організації, то вона має володіти не однією, а певним спектром взаємопов'язаних спроможностей.

Сподівання на успішність процесу є обґрунтованими, якщо на момент його початку спроможність, яка має бути задіяна у процесі, відповідає певним вимогам – знаходиться не нижче певного рівня. Такі вимоги можуть бути виражені кількісно та/або якісно.

Визначення фактичного рівня спроможності у її носія отримується у результаті відповідного процесу оцінювання.

Відповідно розрізняються носії спроможностей номінальні і фактичні. Номінальний носій спроможності - це абстракція, що визначається назвою об'єкта і вимогами до нього, зокрема, вимогами до номінальних рівнів його спроможностей.

Фактичний носій спроможності - це реальний об'єкт, що є втіленням номінального з точністю до фактичних обставин. Серед усього іншого такий об'єкт характеризується своєю присутністю у світі (як мінімум, має певні координати місцезнаходження) та наявними (фактичними) спроможностями, бажано, з оцінками їх рівней.

На основі обговорених вище понять побудована концептуальна модель предметної області планування на основі спроможностей, що складається з двох складових: статичної і динамічної.

Статична складова моделі - це набір сутностей, відношень між ними і атрибутів сутностей і відношень між сутностями. Розрізняються такі сутності: спроможність, тип спроможності, метамодель опису спроможності, опис спроможності, вимога до спроможності (кількісна та/або якісна), оцінка спроможності (кількісна та/або якісна), тип носія спроможності, носій спроможності номінальний, носій спроможності фактичний, метамодель опису носія (номінального) та його спроможностей, опис/вимоги до носія номінального

та його спроможностей - кількісні та/або якісні, оцінка носія спроможності (фактичного) – кількісна та/або якісна, місцезнаходження носія спроможності.

Що стосується атрибутів елементів (сутностей і відношень), то вони поділяються на дві групи: а) загальні атрибути (для всіх елементів) та б) специфічні атрибути (індивідуальні для кожного елемента).

До загальних атрибутів відносяться: унікальний ідентифікатор елемента, дата/час включення елемента в модель, дата/час логічного виключення елемента з моделі.

Динамічна складова – діяльність, підтримувана моделлю, зміст якої може коливатись у певних межах.

Особливостями концептуальної моделі, що пропонується, є наступне: чітке розділення номінального і фактичного планів діяльності;

жорстка відповідність фактичного плану номінальному може розглядатись як бажана, але допускається існування номінальних носіїв спроможностей, що не набули свого «втілення» на фактичному плані, і фактичних носіїв спроможностей, що не «втілюють» жодного номінального носія;

декларація відповідності фактичного носія номінальному не вимагає, наприклад, їх повного структурного ізоморфізму.

Модель, що пропонується, може бути покладена в основу інструментальної підтримки виконання важливих задач, у тому числі, оборонного планування.

ЛІТЕРАТУРА

1. ДСТУ ISO 9000:2015 - Системи управління якістю - Основні положення та словник термінів. – Київ, ДП «УкрНДНЦ» 2016. – 73 с.
2. Методологія визначення спроможності служб управління персоналом державних органів. – Національне агентство України з питань державної служби. - М. Київ, 2019. – 19 с.
3. Звіт про результати оцінки рівня спроможності служб управління персоналом державних органів, які здійснюють підготовку та реалізацію ключових національних реформ (звітний період 01.01.2018 — 30.11.2018). - [Електронний ресурс] – режим доступу: <https://i.factor.ua/ukr/journals/ds/2019/february/issue-2/article-42427.html>.
4. Тренінг для тренерів з управління людськими ресурсами для зміцнення спроможності службовців в об'єднаних територіальних громадах (22-23 жовтня 2018). – Офіс Ради Європи в Україні. - [Електронний ресурс] – режим доступу: <https://www.coe.int/uk/web/kyiv/-/training-of-trainers-on-human-resources-management-to-support-public-officials-in-amalgamated-hromadas>

5. Тренінг з розбудови спроможності: управління проектним циклом (м. Дніпро, 23-25 липня 2019 р.). - Суспільно-аналітичний центр «Інститут Республіка». - [Електронний ресурс] – режим доступу: <https://inrepublica.org.ua/>.
6. Manual For The Operation Of The Joint Capabilities Integration And Development System - JCIDS Manual. - 31 August 2018. – 341 p.
7. An Introduction to the NATO Defence Planning Process. - September 20, 2010. – 47 p.
8. Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України та Збройних Силах України. – Затв. МОУ 12.06.2017 р. – 49 с.

Міронова В.Л., Гарко І.І.

Київський національний університет імені Тараса Шевченка

Київ, Україна

vicky.mironova@gmail.com

Богданець Є.І

Національний транспортний університет

Київ, Україна

МЕТОДИКА ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ЦИФРОВОГО СУСПІЛЬСТВА

The report considers the characteristics and basic requirements for intelligent systems of the digital society and its components, methods and techniques of their interaction and integration.

Keywords: *Digital society, complex dynamic system, intelligent system.*

З огляду на невідпинні процеси формування цифрового суспільства (ЦС), розвитку інформаційного простору та інфраструктури, одним з важливих завдань сучасної науки стало забезпечення надійності, швидкодії та відмовостійкості систем, що забезпечують функціонування цифрового суспільства. Такі складні динамічні системи (СДС), що забезпечують виконання основних процесів цифрового суспільства, досліджуються в багатьох країнах світу.

У зв'язку с пандемією COVID-19 розвиток цифрового суспільства прискорився у декілька разів та розширив вимоги та функції інтелектуальних

систем цифрового суспільства (ІСЦС). Для стану адміністративної та економічної галузі у 2020р. та методологічного базису стосовно методик, методів, моделей та алгоритмів ІСЦС і забезпечення функціональної стійкості їх окремих модулів та системи в цілому характерне наступне:

1. Кожне сучасне підприємство повинно мати ІСЦС, а будь-яка існуюча його організаційна структура, що забезпечує обробку електронних даних індивідуума, належить до категорії СДС, у межах яких діють ергатичні вирішувальні системи (ЕВС), що цілеспрямовано забезпечують результуючі показники цифрової єдиної технологічної організації (ЦЄТО);

2. ЦЄТО раціональна, надійна та рентабельна лише за умов адекватного реагування на змінні фактори впливу оточуючого навколишнього середовища. Такий вплив не повинен змінювати функціональну стійкість гармонійної взаємодії між усіма внутрішніми підсистемами інтегрованих ІСЦС. Майбутні вимоги до обробки цифрових даних, як і сучасні, регламентуються відповідними міжнародними стандартами, рекомендаціями та правилами. Відомі з 2005 року стандарт ISO/IEC 20000-1 «Information technology - Service management. Specification» являє собою детальний опис вимог до системи менеджменту ІТ сервісів і відповідальність за ініціювання, виконання та підтримку в організаціях. Цей стандарт поступово розповсюджується на інші види високошвидкісних технологій за рахунок уніфікації апаратно-програмних засобів телекомунікації та диспетчерського управління.

3. Глобальні процеси інформатизації суттєво впливають на технологію взаємодії між підсистемами ЦЄТО, яка визначає життєві цикли планування, формування, розподілу, використання та утилізації усіх видів ресурсів ІСЦС, що забезпечують конкретні форми існування елементів роботи.

4. Системна ефективна організація ЦЄТО та відповідні оптимальні показники роботи існують лише за умов синергізму, коли гармонізація взаємодії зовнішніх та внутрішніх взаємовпливів гарантує мінімальні (задовільні для соціуму) відхилення між планом та фактом. Принципові розбіжності між майбутнім та минулим обумовлені значною (майже нескінченною) складністю навколишнього середовища, яке має власну ознаку СДС, що ніколи не співпадає з обмеженою, але також СДС ЦЄТО.

Головна умова синергізму мультиагентного розв'язку задач у межах ІСЦС – це забезпечення оптимальних режимів роботи ЕВС. Ця умова визначається як єдність взаємодії усіх частин системи у відповідності з однозначним розумінням інформаційно-образної динамічної моделі об'єкта (ІОДМ) ЦЄТО. У кожного агента цієї системи, згідно зі штатним та функціональним розподілом задач ЦЄТО, існує власна точка зору та індивідуальне бачення об'єкта. Тому

$IOДМ_i \neq IOДМ_j, \forall i, j = \overline{1, n}, i \neq j$ але $IOДМ_i \cap IOДМ_j \neq 0$, оскільки для ефективної взаємодії повинна бути загальна інформаційна частка, яка забезпечує коректність, адекватність та точність спільних дій у конкретній ситуації ІСЦС.

ЛІТЕРАТУРА

1. George D. Magoulas. Virtual reality in the e-Society/ Virtual Reality website // Електронний ресурс – режим доступу: https://www.researchgate.net/publication/228328279_Virtual_reality_in_the_e-Society
2. Jayashree S. Government to E-government to E-society/ Journal of Applied Sciences 10(19) // Електронний ресурс – режим доступу: https://www.researchgate.net/publication/49591267_Government_to_E-government_to_E-society

Наконечний В.С.,

Київський національний університет імені Тараса Шевченка, Київ
nvc2006@i.ua

Толюпа С.В.,

Київський національний університет імені Тараса Шевченка, Київ
tolupa@i.ua

Петренко А.І.,

Київський національний економічний університет імені Вадима Гетьмана, Київ
petrenko.anastasia@kneu.edu.ua

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ КІБЕРБЕЗПЕКИ В СВІТІ ІНТЕРНЕТ РЕЧЕЙ

The IoT encompasses a wide range of processes: sensing, computation, communication, time, context, and data, to name only a few. The IoT security has become more and more challenging these days. Since the idea of networking platforms and other sites are relatively new, most developers focus more on the product's overall

designing phase. This is also due to the IoT's nascent market. As a result, they have overlooked the importance of security and privacy of users and subscribers.

Keywords: *Internet of Things, cybersecurity, vulnerability, risks.*

Інтернет речей, аналітика великих даних і машинне навчання – це ті області науки і техніки, які бурхливо розвиваються та формують нове покоління комп'ютерних систем з використанням штучного інтелекту. Варто відмітити, що ці області є міждисциплінарними за своєю природою. Це дозволяє їм нагромаджувати як теоретичні основи, так і розвиватися в практичній площині.

Варто наголосити, що Інтернет речей - це не тільки холодильник, який сам замовляє улюблену їжу господаря, або чайник, який кип'ятить воду за запитом смартфона. Це також і розумні датчики на полях, дрони з камерами, завдяки яким можна віддалено моніторити стан ґрунтів, це датчики в громадському транспорті і єдині системи для моніторингу життя міста та окремого підприємства.

Cisco прогнозує, що до 2025 року до Інтернету буде підключено 75 млрд пристроїв [1]. Однак ці прогнози не враховують прискореного розвитку технологій і пристроїв. Комусь кількість підключених пристроїв може здатися заниженою. Це пов'язане з тим, що в розрахунках враховується все населення нашої планети, але більшість людей до сих пір не має доступу в Інтернет. Якщо ж враховувати тільки тих, хто користується Інтернетом, то кількість підключених пристроїв на одного користувача виявиться набагато вище.

Нові можливості підключення в Інтернеті речей відкривають велику і часто невідому зону атак. Пристрої і додатки можуть зберігати величезні склади персональних, робочих і корпоративних даних [2]. Тому фахівцям з безпеки потрібно виходити за рамки традиційних вимог до інформаційної безпеки (захист конфіденційності, цілісності і доступності).

Оскільки вразливість в IoT може нести фізичну загрозу для життя (медичні пристрої) або призвести до величезних збитків компаніям (контроль над літаками), особливу увагу потрібно приділяти захисту підключень, додатковому захисту пристроїв, моніторингу загроз і управлінню станом безпеки, а також захисту даних в частині хмарного сховища.

Проблема в тому, що більшість користувачів не замислюються про безпеку своїх даних і захисту пристроїв. Люди ставлять паролі, які легко зламати, не змінюють їх на маршрутизаторах, і в цілому дуже недбало ставляться до безпеки інформації [3]. Це призводить до зломів пристроїв розумного будинку, перебоїв роботи кардіостимуляторів, масштабних кібератак і витокам секретних даних.

Щоб зменшити ризик кібератак та злому, розробники повинні підтримувати конфіденційність даних, цілісність та доступність у всій ІТ-інфраструктурі всіма доступними їм способами, зважаючи на особливості пристроїв IoT (рис. 1).



Рис 1. Компоненти побудови системи захисту IoT

Розвиток концепції Інтернету речей та її впровадження в різні сфери передбачає наявність десятків мільярдів автономних пристроїв. Усі вони підключені до мережі та передають через неї відповідні їх функціоналу дані. Ці дані і функціонал є мішенню для зловмисників, а отже, повинні бути захищені відповідним чином.

Фактично, більшість IoT-пристроїв не забезпечені елементами захисту, мають доступні зовні інтерфейси управління, дефолтні паролі, тобто, мають всі ознаки веб-уразливості.

Всі ще пам'ятають події трьох-річної давності, коли ботнет Mirai шляхом підбору комбінацій дефолтних логінів і паролів злавав велику кількість камер і роутерів, які були в подальшому використані для наймогутнішої DDoS-атаки на провайдерські мережі UK Postal Office, Deutsche Telekom, TalkTalk, KCOM і Eircom [4]. При цьому «брутфорс» IoT-пристроїв здійснювався за допомогою Telnet, а роутери зламувалися через порт 7547 з використанням протоколів TR-064 і TR-069.

Найбільш резонансною була атака у 2016 році, що порушила нормальне функціонування DNS-оператора DYN, а разом з ним практично роботу «пів-інтернету» США [5]. Для атаки ботнетом були використані ті ж самі встановлені за замовчуванням логіни і паролі пристроїв.

Сьогодні більшість пристроїв IoT утворюють «закриті системи». В такій системі покупці не можуть змінювати наповнення пристроїв, а будь-яке втручання завдає непоправної шкоди системі. Тобто, усі заходи захисту мають бути вбудовані до виходу продукту на ринок. Для інформаційної безпеки така «безпека зсередини» є новою технологією захисту при виготовленні пристрою на заводі. Це стосується і класичних технологій безпеки, таких як шифрування, перевірка автентичності, перевірка цілісності, запобігання вторгнень і можливості безпечного оновлення. З огляду на тісний зв'язок апаратного і програмного забезпечення в моделі IoT, іноді простіше, щоб програми для захисту використовували розширення функцій апаратної частини і створювали «зовнішні» рівні безпеки.

Апаратний рівень - це всього лише перший крок, необхідний для комплексного захисту зв'язку і пристроїв. Комплексний захист вимагає інтеграції функцій управління ключами, захисту на основі хосту, інфраструктури OTA і аналітики безпеки [6].

Безпеку інтернету речей можна побудувати на фундаменті з чотирьох наріжних каменів: безпека зв'язку, захист пристроїв, контроль пристроїв і контроль взаємодій в мережі.

Відсутність навіть одного з наріжних каменів у фундаменті безпеки залишить широкий простір діям зловмисників. Наше життя залежить від літаків, поїздів і автомобілів, які перевозять нас, від інфраструктури охорони здоров'я та цивільної інфраструктури, яка дозволяє нам жити і працювати. Неважко уявити, як незаконне маніпулювання світлофорами, медичним обладнанням або незліченними іншими пристроями може привести до плачевних наслідків.

Велика кількість сучасних алгоритмів захисту інформації і, зокрема, шифрування, розраховані на застосування в ЕОМ в складі програмних комплексів без урахування оптимізації на апаратному рівні забезпечення [7]. Цей факт робить неможливим застосування більшості існуючих криптографічних алгоритмів в пристроях з обмеженою обчислювальною потужністю, малим обсягом і малим енергоспоживанням.

Безпека повинна бути передбачена на рівні проектування нових пристроїв, рішень і технологій. Якщо створювати рішення на початку безпечної платформи - можна позбутися від цілого ряду класичних проблем і вразливостей.

Захист співробітників, користувачів, цінних операційних технологій та бізнес-інвестицій за допомогою захищеної інфраструктури Інтернету речей вимагає комплексного підходу [8]. Досвідчені компанії, що займаються безпекою в Інтернеті речей, рекомендують застосовувати тристоронній підхід - захист даних, пристроїв і підключень.

Проблему, пов'язану з захищеністю IoT-девайсів, частково здатна вирішити сертифікація. Головна умова такої процедури, щоб вона була доступна виробникам і не перетворилася в чисту формальність.

Безпека IoT стає головним завданням для організацій, оскільки без міцної архітектури безпеки великі обсяги даних, що надходять через мережі і зберігаються в хмарах, можуть стати легкою здобиччю для хакерів. Щоб зменшити ризик кібератак та злому, розробники повинні підтримувати конфіденційність даних, цілісність та доступність у всій IT-інфраструктурі всіма доступними їм способами, зважаючи на ресурсні обмеження пристроїв IoT. Простого універсального рішення не існує, і для забезпечення безпеки недостатньо замкнути двері, залишивши вікна відкритими. Безпека повинна бути комплексною, інакше хакери просто скористаються найслабшою ланкою.

ЛІТЕРАТУРА

1. Смирнов О.С. Розвиток «Інтернету речей», доповненої реальності та комунікаційних технологій: стаття / К. С. Голохваст, О. В. Тумялис. – Далекосхідний федеральний університет – Режим доступу: <https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf>
2. UK Government Chief Scientific Adviser The Internet of Things: making the most of the Second Digital Revolution / посібник, 2014 – 40 с.
3. Тюрин В.А. Інтернет речей: нові можливості для світу та бізнесу – Мережа. Фактори – Режим доступу: <https://megamozg.ru/post/25334/>
4. Sundmaeker H. Vision and Challenges for Realising the Internet of Things / European Commission - Information Society and Media DG
5. Вічугова А. Криптографія в IoT та Big Data: захищені протоколи та мікросхеми [Електронний ресурс] – Режим доступу: <https://www.bigdataschool.ru/bigdata/iot-protocol-microchip-crypto-big-data.html>
6. Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития сети // Компания Cisco Systems. – 2011 [Електронний ресурс] – Режим доступу: <https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html>

7. IoT і проблеми безпеки – блог компанії Unet – 2018. [Електронний ресурс] – Режим доступу: <https://habr.com/ru/company/unet/blog/410849/>
8. Rouse M. “IoT security” – 2018. [Електронний ресурс] – Режим доступу: <https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security>

Наконечний В.С.

Київський Національний університет імені Тараса Шевченка

м. Київ

e-mail: nvc2006@i.ua

Кузьменко О.О.

Київський Національний університет імені Тараса Шевченка

м. Київ

e-mail: aleksandr.kuzmenko778@gmail.com

КЛАВІАТУРНИЙ ПОЧЕРК – МЕХАНІЗМ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА В ІНФОРМАЦІЙНІЙ СИСТЕМІ

In the annotation of the report there is the analysis of keyboard handwriting as behavioural biometrics of the person, and suggested the mathematical methods of the analysis of the data which is used to define the identify user inside information system. Also in this report three popular methods are specified, which can be used to analyze data.

Determined approaches which are uses with mathematical methods, such as:

- Student's t-test*
- Euclidean distance*

The further steps of continuation of research in this direction are specified.

Key words: *keyboard handwriting; biometric human identification; information system; data analysis.*

Для запобігання витоку інформації або несанкціонованого доступу до інформаційних систем використовуються різні засоби ідентифікації користувача такі як:

- атрибуtnі;
- парольні;

- біометричні;

Проблема атрибутних засобів у тому, що користувач, який має доступ до інформаційної системи може втратити свій атрибут – ключ, токен тощо. В іншому випадку атрибут доступу може бути втрачений або вкладений. Такою втратою може скористуватися зловмисник для отримання несанкціонованого доступу до системи.

Проблема паролних засобів полягає в тому, що користувач може забути пароль, пароль може бути підібраний, підглянутий під час набору або зчитаний за допомогою спеціального шкідливого програмного забезпечення.

Біометричні засоби можуть суттєво підвищити ступінь захисту інформаційних систем. Поведінкові характеристики користувача неможливо відтворити або вкрати, тому сучасність вимагає відмовитись від використання атрибутних та паролних засобів на користь біометричних.

Використання методів поведінкової біометрії, яка заснована на клавіатурному почерку не вимагає придбання додаткових дорогих пристроїв та спецтехніки.

Для отримання зразка клавіатурного почерку достатньо наявність звичайної стандартної клавіатури. Це робить даний метод простим, недорогим і ненав'язливим для користувача, також цей метод може бути застосовано таємно, що дозволить покращити існуючі комп'ютерні інформаційні системи.

Тому клавіатурний почерк людини є поведінковою особливістю, яка розвивається з плином часу і не може бути змінена, втрачена або забута.

У будь-якій поведінковій біометричній характеристиці можуть спостерігатися великі зміни в особливостях характеристики. Однак, вони повинні надати достатньо інформації, щоб ідентифікувати і визначити справжність особистості за шаблоном почерку.

Тому на основі вищесказаного запропоновано вважати клавіатурний почерк індивідуальним та унікальним для кожної людини, що може бути використано в процесі ідентифікації.

Для розпізнавання використовуються алгоритми розпізнавання клавіатурного почерку, які можна розділити на три групи[1]:

- алгоритми, які аналізують почерк вчасного введення пароля;
- алгоритми, які аналізують почерк після введення додаткового текстового фрагмента або фрази тощо;
- алгоритми, які постійно проводять прихований моніторинг клавіатурного почерку користувача.

Алгоритми першої групи забезпечують найбільшу швидкодію: користувачеві потрібно лише ввести свій логін і пароль. Однак точність в цьому випадку невисока, особливо в разі короткого пароля. Вхід може здійснюватися користувачем, а далі можлива підміна на іншу людину.

Алгоритми другої групи можуть забезпечити більшу точність, в порівнянні з першою групою. Однак на введення додаткового фрагмента тексту потрібен час, що може викликати негативні емоції у користувача, особливо в випадку, якщо йому часто доводиться проходити процедуру ідентифікації.

Алгоритми третьої групи дозволяють забезпечити високу точність. При цьому вони вимагають більше ресурсів. Перевагою цієї групи є можливість розпізнати зловмисника, який використовує комп'ютер, на якому раніше авторизувався студент.

Маючи шаблон клавіатурного почерку користувача стає можливо провести автентифікацію та ідентифікацію користувача. Для цього необхідно провести процедуру порівняння поточного зразка почерку і збереженого раніше шаблону.

Запропоновано використовувати такі алгоритми, як: Евлідова відстань[2] та t-критерій Стьюдента[3] для порівняння часу Hold (час утримання клавіші), DownDown (час між натисканням сусідніх клавіш) та UpDown (час між опусканням однієї клавіші і натисненням наступної).

Евклідова відстань (Евклідова метрика) — формула традиційної відстані між двома точками (1.1):

$$M = \sqrt{\sum_{i=1}^V (A_i - B_i)^2} \quad (1.1)$$

де M – розраховане значення Евклідової відстані; V – кількість вибірок часу Hold, DownDown, UpDown, що відповідає кількості аналізованих клавіш; A_i – час утримання клавіші з поточного зразка клавіатурного почерку користувача, що претендує на доступ; B_i – час утримання клавіші, що зберігається в шаблоні почерку.

Користувач буде успішно ідентифікований або його особа буде підтверджена, якщо розраховані значення Евклідової відстані менше встановленого в системі порога доступу.

Поріг доступу підбирається в залежності від вимог до розроблюваної системи. Основними вимогами для систем захисту інформації є ймовірності виникнення помилок першого і другого роду[4].

t-критерій Стьюдента – загальна назва для класу методів статистичної перевірки гіпотез (статистичних критеріїв), які засновані на розподілі Стьюдента. Найбільш розповсюджені випадки застосування t-критерію пов'язані з перевіркою рівності середніх значень у двох вибірках.

t-критерій Стьюдента використовується для визначення статистичної значущості відмінностей середніх величин. Може застосовуватися як у випадках порівняння незалежних вибірок, так і при порівнянні пов'язаних сукупностей.

Алгоритм Стьюдента порівняння двох вибірок:

1. Порахувати середнє значення вибірок.
2. Порахувати стандартне відхилення вибірок.
3. Порахувати критерій Стьюдента за допомогою формули (1.2):

$$t = \frac{|M_1 - M_2|}{\sqrt{\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}}} \quad (1.2)$$

де M_1 - середнє арифметичне еталонної вибірки; M_2 - середнє арифметичне вибірки не авторизованого користувача; σ_1 – стандартне відхилення еталонної вибірки; σ_2 – стандартне відхилення вибірки; N_1/N_2 – об'єми вибірок.

Отримане значення t-критерію Стьюдента необхідно правильно інтерпретувати. Для цього необхідно знати кількість досліджуваних в кожній групі. Знаходимо число ступенів свободи f за формулою (1.3):

$$df = (N_1 + N_2) - 2 \quad (1.3)$$

де N_1/N_2 – кількість значень у вибірках;

Після цього визначаємо критичне значення t-критерію Стьюдента для необхідного рівня значущості (наприклад, $p = 0,05$) і при даному числі ступенів свободи df по таблиці критичних значень Стьюдента.

Порівнюємо критичне і розраховане значення критерію:

- якщо розраховане значення t-критерію Стьюдента дорівнює або більше критичного, знайденого по таблиці, робимо висновок про статистичної значущості відмінностей між порівнюваними величинами;

- якщо значення розрахованого t-критерію Стьюдента менше табличного, отже відмінності порівнюваних величин статистично не значимі.

Таким чином клавіатурний почерк посідає важливе місце в біометричній ідентифікації користувача, як один з найефективніших методів. Даний метод дешевий, не потребує дорогого й спеціального програмного забезпечення та простий у використанні.

Правильно обрані методи аналізу даних (Евклідова відстань та t-критерій Стьюдента) швидко обчислюють правильність та точність критеріїв за допомогою яких ідентифікується користувач інформаційної системи. В майбутньому, на думку автора, клавіатурний почерк може витіснити біометричну ідентифікацію за відбитком пальця та паролню.

ЛІТЕРАТУРА

1. Сидоркина И.Г., Савинов А.Н. Три алгоритма управления доступом к КСИИ на основе распознавания клавиатурного почерка оператора // Вестник Чувашского университета, 2013. – 293-301 с.
2. https://en.wikipedia.org/wiki/Student%27s_t-test
3. https://en.wikipedia.org/wiki/Euclidean_distance
4. Широчин В. П., Кулик А. В., Марченко В. В. Динамическая аутентификация на основе анализа клавиатурного почерка. - http://www.masters.donntu.edu.ua/2002/fvti/aslamov/files/bio_autentification.html

Ніколаєв М.О.

Київський національний університет

імені Тараса Шевченка

nikitok95@gmail.com

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ТА АЛГОРИТМІЧНОГО КОДУВАННЯ ПРИ ПРОГОЗУВАННІ ЦІН ТА ОЦІНЦІ РИЗИКІВ МАЙБУТНІХ ПЕРІОДІВ НА СВІТОВИХ ФІНАНСОВИХ РИНКАХ

Consideration of paradigmatic algorithms and statistical methods of research and forecast of financial indicators. A model of the machine set algorithm has been developed, data based on statistical indicators have been predicted.

Keywords: *artificial intelligence, algorithms, financial markets*

Машинне навчання, розробка алгоритмів з використанням технології "BigData" стає невід'ємною частиною будь-якого дослідження. Інформаційні системи та технології увійшли на перший план при дослідженні та прийнятті рішення щодо аналітичних рішень у будь якій сфері виробництва чи бізнесу.

Проте занадто велика популярність цих технологій накладає ще й питання доцільності даних, справедливого сприйняття методу розрахунків, отримання результатів та підходу до формулювання висновків. Крім зростання популярності великих даних загалом, спостерігається підвищення інтересу до різних неструктурованих джерел інформації. Тепер для участі у аналітичній діяльності користувачам потрібно навчитися визначати, яка інформація корисна, а яка ні. Big Data представляють величезну користь для сегмента активного управління. Пов'язані з ними технології, такі як машинне навчання і штучний інтелект – це інструменти для повного доступу до великої кількості неструктурованих даних і їх аналізу.

Постановка проблеми. В даному дослідженні буде необхідно вирішити такі проблеми:

- Розробити власні приклади алгоритмів машинного навчання, алгоритмів прийняття рішень на товарних та фінансових ринках
- Отримати аналітичні дані прогнозів скорельовані за різними методами аналізу
- Показати приклади роботи алгоритмів, які самокорегуються з отриманням потоку нових даних

- Провести дослідження впливу закладених алгоритмів та результати машинного навчання на різних прикладах.

Аналіз останніх досліджень і публікацій.

У процесі трансформації фінансової ринку майже кожні десять років з'являється новий підхід до інструментів аналізу та прогнозування фінансових ринків. Теоретичний фундамент машинного навчання було закладено Янсенем Стефаном у його праці “Машинное обучение для алгоритмической торговли на финансовых рынках. Практикум”. На думку Янсена С., цінові котирування на фінансових ринках є ніщо інше як статистичний фрактал, який утворений поведінковими та соціально економічними діями учасників ринку.

Мета публікації. Дослідження проблем застосування алгоритмів із застосуванням елементів машинного навчання, та результатів його використання на фінансових ринках.

ТЕОРЕТИЧНІ ОСНОВИ

Реальні дані складніше, ніж «ціни, попит і пропозиція», це так звана проблема економетрики.

Стандартна процедура в фінансовій математиці - коли тимчасові ряди цін, оброблені за допомогою “time series differentiation”, після чого побудована модель розподілу і показано, що ця модель описує ці дані, безвідносно того, чи це ARIMA або стохастичне диференціальне рівняння Фоккера-Планка.

У чому тут проблема?

- Дані на ринках спочатку не структуровані, а економетричні моделі використовують красиву послідовність цін.

- Дуже низьке відношення сигналу до шуму.

- Видалення пам'яті часових рядів

- Фінансові моделі в більшості своїй працюють з максимально неінформативними даними, ще й обробляючи їх неправильно і пояснюючи патерни “in-sample”.

МЕТОДИ ДОСЛІДЖЕННЯ

Перший метод це бек тестування або “in-sample”. Бек тестування - це процедура перевірки стратегії на історичних даних одного або декількох фінансових інструментів, щоб зрозуміти, як стратегія б відпрацювала «в минулому», і на основі цього оцінити ризики її поведінки в майбутньому.

Почнемо з того, що ціни «в минулому» - це всього лише одна з реалізацій складного стохастичного процесу, і навіть якщо ми могли б його змодельювати, то перевіряти треба було б не на одній випадковій реалізації, а на сотнях тисяч.

Більш того, бек тестування - це все один великий і красивий набір даних in-sample. Зробити модель, яка добре заробить в минулому, - простіше простого, питання тільки в тому, як вона відпрацює на живому ринку.

Бек тестування - не може бути частиною процесу експериментування через проблеми множинної перевірки гіпотез, систематичних помилок відбору і схильності до підтвердження своєї точки зору.

Інший метод, це метод кореляції і лінійні залежності.

Коефіцієнт кореляція пояснює міру лінійної залежності між двома випадковими величинами. Більш того, кореляція в теорії, означає причинно-наслідковий зв'язок.

Проблема в тому, що фінансові дані дуже шумні і схильні до або розрідженості, або викидів. В результаті кореляційні або коваріаційні матриці на таких даних вважаються. Але якщо цю проблему ще можна вирішити акуратною обробкою даних і поліпшеними алгоритмами, то проблему лінійної залежності ніхто не відміняв.

Очевидно, що залежності в фінансових ринках нелінійні, дані не підлягають нормальному розподілу, і кореляція не може їх пояснити в принципі, не кажучи вже про те, що розподіл даних постійно змінюється.

РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Отримані результати дослідження показують, що традиційні статистичні методи не відображають дійсності у нераціональній поведінці фінансових ринків. Тому при машинному навчанні стратегій та аналізу, треба застосовувати комплексних підхід з переміною даних на багатьох рівнях.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Висновків, яких можна було дійти згідно отриманих результатів, це:

- використовувати сирі дані про ціни, а не підготовлені графіки цін
- вибірка має бути незалежною і не порушуватися ключова гіпотеза про розподіл даних.
- дослідження значимості факторів на крос-
- p-values в реальному житті не можуть визначити якість змінних через нереалістичних обмежень до задачі.
- Бек-тестування взагалі не може бути єдиним у дослідженні для позитивного результату, перевіряти необхідно всі описані вище кроки, які стосуються тільки машинного навчання.

ЛІТЕРАТУРА

1. Black Hung-Han, Chen Lawrence, Hunter Harry, Poteat Kristin Snow, Machine learning systems and methods, , 2008, с. 2-17. <https://patents.google.com/patent/US20050267850A1/enF>.

2. Н.Н. Шаповалова , Розробка навчальної платформи для побудови, навчання та дослідження моделей штучного інтелекту, 2018, с. 115

3. Eric John Dluhos, Bradley Lloyd Wilk, Genetic Algorithm And Genetic Programming System, 2017 , 17-29 с.

4. David Peter Bullivant, Paul Burton Robertson, Mark Andrew Sagar, System for neurobehavioral animation, 2018с.

5. https://en.wikipedia.org/wiki/Machine_learning.

6. López de Prado, Marcos, The 7 Reasons Most Econometric Investments Fail (Presentation Slides) (April 16, 2019). Available at SSRN: <https://ssrn.com/abstract=3373116> or <http://dx.doi.org/10.2139/ssrn.3373116>.

Новіцька Т. В.

*Національний педагогічний університет
імені М. П. Драгоманова, Київ, Україна
radugga2009@gmail.com*

ВИКЛИКИ ТА ОСВІТНІ ТЕХНОЛОГІЇ У КОНТЕКСТІ ПІДГОТОВКИ ФАХІВЦІВ МАТЕМАТИЧНИХ (ФІЗИЧНИХ) СПЕЦІАЛЬНОСТЕЙ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Nowadays there is strong interest of modern scientists to pressing issues on the development of innovative educational technologies influence on personality and methods of effective and optimal use in the educational process of higher education. Considered issues related to the use of innovative information technology in learning mathematics.

Key words: *innovative educational technologies, innovation, educational technology, training process, mathematical discipline.*

Підготовка фахівця в сьогоденних умовах процес складний та не однозначний. Перш за все, це пов'язано з тим, що суспільство в період

глобалізації розвивається за умов впливу на нього інноваційних технологій. В цих умовах освіта повинна виконати стратегічне завдання, з одного боку допомогти створити інноваційне середовище на основі новітніх наукових досліджень, а з іншого, підготувати спеціаліста, який мислив би і діяв інноваційно. Такі тенденції змушують освітян задуматися над тим яким має бути сучасна особистість. Зрозуміло, що вона має бути наділена комунікативними здібностями, мати блискучі знання, виважено приймати рішення, критично мислити. Завданням вищої освіти стає формування цілісного світогляду, певної життєвої позиції випускника ЗВО, який вже володіє високими професійними знаннями та навичками відповідно до вимог суспільства. Стає зрозуміло, що суспільство «чекає» від вищів формування нового типу особистості, яка б мислила і діяла інноваційно.

Усвідомлення знань як важливого ресурсу розвитку цивілізації в умовах зростання впливу інтернет-технологій, засобів мобільної комунікації та цифрових ресурсів, що забезпечують можливості ефективного використання інтелектуальних ресурсів, – все це визначає принципово нові підходи до можливостей практичного використання знань.

Вузькоспеціалізованого професійного мислення, яке домінує сьогодні в освіті, недостатньо для вирішення глобальних проблем людства. Виникає потреба трансформації існуючої системи освіти.

Таким чином, пошук нових моделей освіти, зокрема, моделей математичної та природничої освіти актуалізовано як сучасними викликами сьогодення, так і потребою у становленні особистості, яка відповідає запитам ХХІ століття.

Характерними ознаками сучасної освіти має стати відмова від шаблонного мислення, підтримка ініціатив молоді, орієнтації на розвиток творчого потенціалу, індивідуальний підхід до кожного студента.

Усе вище зазначене, стає ще більш актуальним в умовах дистанційного навчання. Оскільки забезпечити надання якісних освітніх послуг стає неможливо без використання сучасних технологій при цьому з урахуванням особливостей спеціальності та кожної окремої дисципліни, що викладається. Актуальними постають питання готовності усієї освітньої системи та кожного окремого викладача до таких умов підготовки фахівців. Особливо це стосується викладання дисциплін математичного та природничого блоку.

Отже, сучасні підходи до підготовки фахівців мають орієнтуватися на використання інноваційних освітніх технологій, зокрема інформаційно-комунікаційних, навчання з доступом до цифрових ресурсів, тощо.

ЛІТЕРАТУРА

1. Філософія освіти: навчальний посібник / [за загальною редакцією В. Андрущенко, І. Предборської]. – К. : Вид-во НПУ ім. М.П.Драгоманова, 2009. – 330 с.
2. Кошечко Н. Інноваційні освітні технології навчання та викладання у вищій школі / Н. Кошечко // Вісник Київського національного університету імені Тараса Шевченка. Педагогіка. – 2015. – Вип. 1. – С. 35-38. – Режим доступу: http://nbuv.gov.ua/UJRN/vknutshp_2015_1_10.

Онуфрик О.І.

Прикарпатський національний університет імені Василя Стефаника
м. Івано-Франківськ
olehonufryk@gmail.com

MODERN ALGORHITMS IN NATURAL LANGUAGE PROCESSING

Over the last decade, artificial intelligence has made great strides. People meet it every day. Artificial intelligence consists of many areas, such as computer vision, speech, text recognition, and more. Natural language processing algorithms occupy a significant niche in the field of artificial intelligence. Companies such as Google, Apple, and Amazon use them in their voice assistants.

Keywords: *artificial intelligence, algorithms, natural language, analysis.*

Introduction

Natural language processing is a field that combines artificial intelligence, computer science, computational linguistics and explores the problem of analysis and synthesis of natural language. Natural language processing algorithms allow the creations of intelligent systems that are able to generate, translate and determine the emotional color of the text, communicate with the end-user(chat-bot systems), and voice assistants (Alexa, Google Assistant).

Research

Word2vec is a technique for natural language processing. It uses neural network to learn word associations from large datasets. Once the model is trained – it can suggest words for a sentence. Itself, word2vec represents each distinct word with a particular list

of numbers called a vector. Word2vec can utilize either of two architectures: continuous bag-of-words or continuous skip-gram.

The intuition of word2vec is that instead of counting how often each word ω occurs near Ω we will instead train a classifier on a binary prediction task. “Is a word ω likely to show up near Ω ?” We do not actually care about this prediction task, instead we will take the learned classifier weights as the word embeddings. The benefit of this approach is – we can just use running text as implicitly supervised training data for a classifier. A word $\acute{\omega}$ that occurs near to the word Ω considered as correct answer to our question “Is a word ω likely to show up near Ω ?”, so that, need for any sort of labeled data disappear.

Word2vec learns embeddings by starting with an initial set of embedding vectors and then iteratively shifting the embedding of each word ω to be more like the embeddings of words that occur nearby texts, and less like the embeddings of words that do not occur nearby. For training a binary classifier it is require having negative examples. Basically, skip-gram uses more negative examples that positive ones. For each pair (t, c) training instances we will create k -negative examples, each containing of the target word t and a noise word. Noise word means a random word from the lexicon that is not equal to the target word t .

Continuous bag-of-words takes the context of each word as the input and tries to predict next word corresponding to the context. For example – the sentence is “Have a good night” and the input to the neural network is the word “good”. Here we are trying to predict a target word using a single input word “good”. By predicting the target word – we learn the vector representation of the target word. The input is a vector of size V . The hidden layer contains N neurons and output layer – a vector of size V . The hidden layer neurons copy the weighted sum of inputs to the next layer. The described model uses single context word to predict the target. Also, it is possible to use multiple context words. The only difference is – to calculate hidden layer inputs, model take an average over all the C context word inputs.

Conclusions

During the research was found advantages and disadvantages word2vec approach in natural language processing. Both, continuous bag-of-words, and continuous skip-gram defined by word2vec are good models to predict target word in sentence. Continuous bag-of-words architecture – the model predicts the target word from a surrounding context word. Continuous skip-gram architecture – the model uses the target word to predict the surrounding context words. Continuous bag-of-words architecture is faster that continuous skip-gram architecture, but continuous skip-gram architecture is better for infrequent words.

LITERATURE

1. Jurafsky Daniel. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition. Daniel Jurafsky, James H. Martin. - 3rd edition. - Prentice Hall, 2019. - 621 p.

2. Natural Language Processing with Python – Analyzing Text with the Natural Language Toolkit. Steven Bird, Ewan Klein, and Edward Loper

Орехов О.А.,

ФТІ НТУУ “КПІ ім.Ігоря Сікорського”,

м.Київ, o.oriekhov@kpi.ua

Орехова Н.А.,

Інститут кібернетики ім.В.М.Глушкова

НАН України, м.Київ

**ЗАСТОСУВАННЯ АНСАМБЛЕВИХ МЕТОДІВ ДЛЯ
ПРОГНОЗУВАННЯ ЕПІДЕМІЧНОЇ СИТУАЦІЇ (НА БАЗІ КЛАСИЧНОЇ
SIR-МОДЕЛІ)**

The paper proposes an ensemble method for predicting the development of an epidemic based on the classical SIR model. The computational experiments showed a higher agreement (in comparison with the classical model) of the calculated data with experimental observations

Key words: *SIR model, epidemic, ensemble methods*

SIR-модель є одним з основних інструментів прогнозування перебігу епідемії. Її перевагою є відносна простота і інтуїтивна прозорість, а недоліком – недостатня точність прогнозування в умовах гетерогенних середовищ з коефіцієнтами, що змінюються у часі або при переході від однієї групи учасників моделі до іншої.

Для побудови моделі, яка б спиралася на переваги SIR-моделі, але б більш точно описувала реальний перебіг подій, було зроблено спробу використати оригінальну SIR-модель як основу ансамблю моделей з статичними у часі, але

різними для різних груп учасників характеристиками, що впливають на відмінність поведінки окремих SIR-моделей як складових ансамблевої моделі.

Будемо вважати, що окрема SIR-модель (згідно з [1]) визначається параметрами $M = M(N, \beta, \gamma)$, де

N – розмір популяції,

β – середня кількість контактів окремої особи в одиницю часу,

γ – коефіцієнт середньої прогнозованої тривалості одужання (в днях),

та залежними від часу змінними

S – ‘susceptible’ – кількість осіб, що піддані ризику зараження,

I – ‘infected’ – кількість осіб, що є інфікованими,

R – ‘recovered’ – кількість осіб, що відновилися (одужали).

Якісний аналіз окремої класичної SIR-моделі надає наступний шаблон її поведінки в залежності від значень параметрів:

1. при поступовому збільшенні коефіцієнтів β і γ та досягненні певного порогового значення ендемічний перебіг перетворюється на епідемічний, в якому певна частка популяції залишається неураженою на всьому протязі епідемії,

2. подальше збільшення хоча б одного з вказаних коефіцієнтів скорочує час настання максимуму для I ,

3. значення максимуму I також зростає при цьому,

4. кількість «неушкоджених» в кінці ($S - R$) зменшується до нуля.

Умовно кажучи, в залежності від значень β і γ можливі більш «гострі» і більш «консервативні» сценарії.

Для різних значень параметрів класична SIR-модель має лише один максимум для I , що не збігається з фактичними спостереженнями.

Тому було розглянуто дві задачі оптимальної апроксимації даних спостереження лінійною комбінацією двох і трьох SIR-моделей з наступними припущеннями:

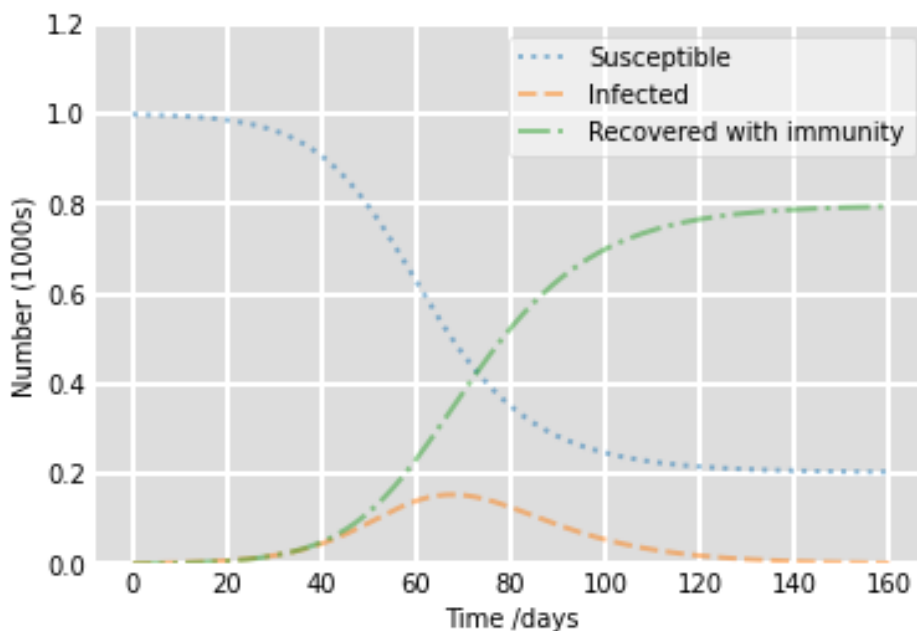
$$(2): M^{(2)} = M_1 + M_2, N_1 \ll N_2, \beta_1 > \beta_2, \gamma_1 \cong \gamma_2$$

для ансамбля з двох моделей, і

$$(3): M^{(3)} = M_1 + M_2 + M_3, N_1 \ll N_2 \ll N_3, \beta_1 > \beta_2 > \beta_3, \gamma_1 \cong \gamma_2 \cong \gamma_3$$

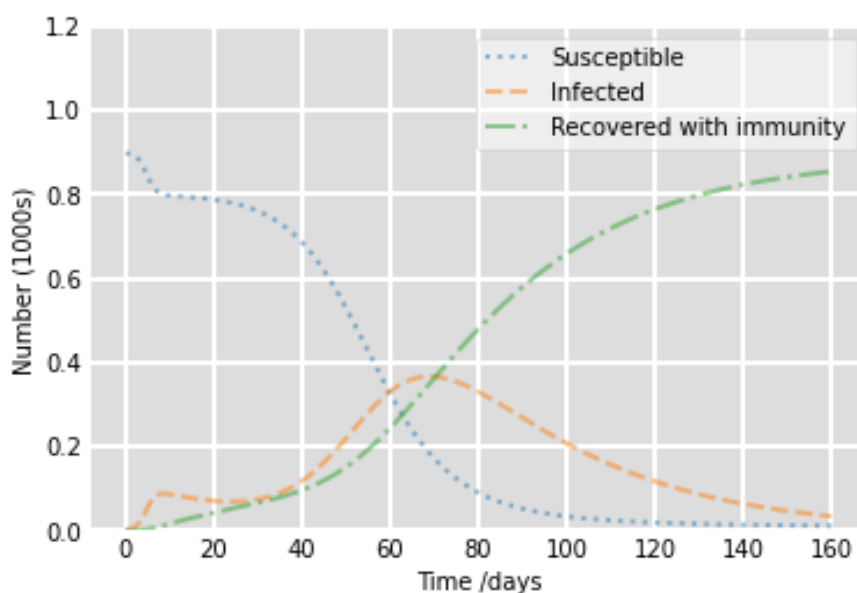
для ансамбля з трьох моделей. Визначення ансамбля моделей для машинного навчання є в багатьох джерелах, наприклад, в [2]. Саму SIR-модель було взято з джерела [3] і на її базі побудовано ансамбль з двох і трьох моделей, з якими виконано низку машинних експериментів.

Приклад моделювання можливого перебігу епідемії для при використанні ансамбля з двох SIR-моделей міститься на мал.1, можливу поведінку ансамблю з



Мал. 1. Приклад динаміки перебігу епідемії, що її описує класична SIR-модель

двох моделей наведено на мал.2, один із можливих варіантів перебігу епідемії, який можна змодельовати ансамблем з трьох моделей, наводиться на мал.3.

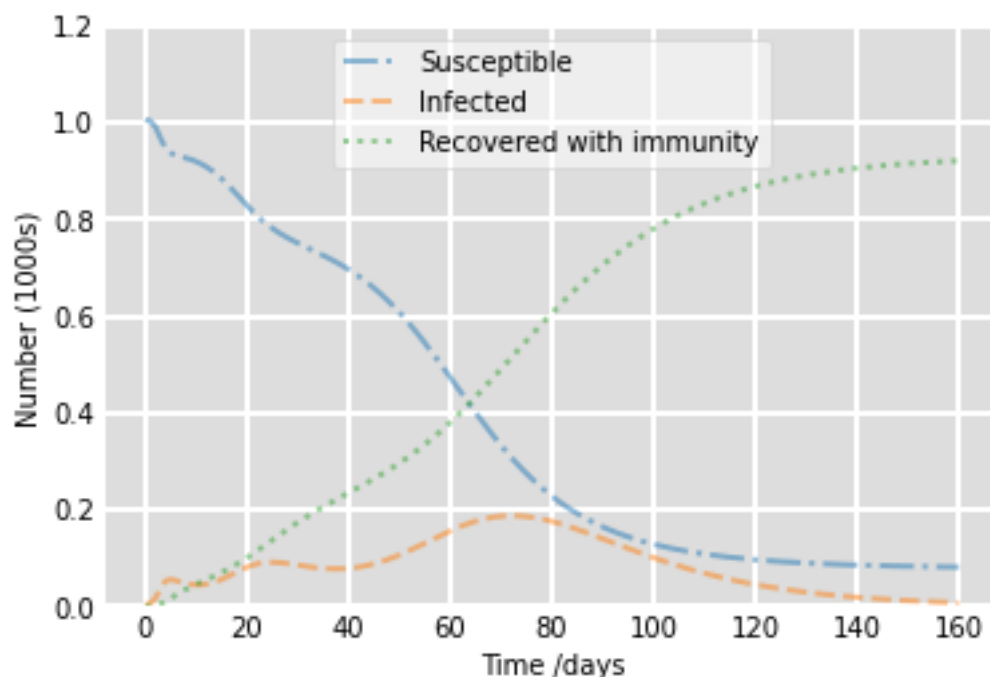


Мал. 2. Приклад динаміки перебігу епідемії, що її описує ансамбль з двох SIR-моделей

Висновок. Проведене моделювання і обчислювальні експерименти свідчать про можливість декількох (двох або більше) хвиль епідемії за умов, якщо для різних соціальних груп, що беруть участь в процесі інфікування їхніх членів, виконуються наступні умови:

1. Вони є суттєво різними за розміром
2. Вони характеризуються суттєво різними за величиною коефіцієнтами розповсюдження інфекції.

Додатково слід зазначити, що заходи, спрямовані на перешкоджання розповсюдження хвороби, зменшують пікове значення змінної I , але подовжують термін епідемічного стану.



Мал. 3. Приклад динаміки перебігу епідемії, що її описує ансамбль з трьох класичних SIR-моделей

ЛІТЕРАТУРА

1. https://en.wikipedia.org/wiki/Compartmental_models_in_epidemiology
2. Witten, I.H., Frank, E. and Hall, M.A. (2011) *Data Mining: Practical machine learning tools and techniques*. (Third Edition). Morgan Kaufmann, USA.
3. <https://scipython.com/book/chapter-8-scipy/additional-examples/the-sir-epidemic-model/>

Павелко Т. М.

Київський національний університет імені Тараса Шевченка

м. Київ, Україна

TarasPavelko@i.ua

ЗАСТОСУВАННЯ МІКРОКОНТРОЛЕРІВ У ЗВ'ЯЗЦІ З ІНФОРМАЦІЙНОЮ СИСТЕМОЮ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ЗАГАЛЬНООСВІТНЬОЇ ШКОЛИ

The approaches to the construction of IoT devices based on microcontrollers are analyzed. The architecture of the device and the algorithm of interaction with the previously implemented electronic document management system in secondary school have been developed. Key words: Internet of Things, microcontrollers.

Keywords: *Internet of Things, microcontrollers.*

Сьогодні надзвичайно важко уявити велику організацію без власної інформаційної системи. Перш за все, тому, що це найпростіший та найефективніший спосіб збереження та обробки інформації. Але у сучасному розумінні інформаційна система являє собою дещо більше. Вона може не тільки зберігати інформацію, введену користувачем безпосередньо, але й модифікувати її автоматизовано, миттєво формувати лаконічні звіти з величезних масивів інформації та багато чого іншого.

Раніше такого набору функцій було достатньо, але зараз замовники вимагають все більшої й більшої автоматизації різноманітних процесів, що часто не можливо без реєстрації тих чи інших фізичних подій. Як це можна вирішити? По-перше, необхідно підібрати датчик, який здатний зареєструвати потрібну нам подію (датчик вологості, коли потрібно повідомити системі про початок дощу, датчик освітленості для визначення початку світлового дня тощо). Найпримітивніші датчики віддають аналоговий сигнал на виході, який потрібно перетворити в цифровий за допомогою аналогово-цифрового перетворювача. Більш серйозні зчитувачі виконані у вигляді модулів, які на борту уже мають АЦП. По-друге, необхідно застосувати контролер з примітивним кодом, який на фізичному рівні зчитує дані з датчиків та взаємодіє з модулем зв'язку з навколишнім світом (Ethernet, Wi-Fi, Bluetooth). Ну й, звичайно, необхідно реалізувати API, за допомогою якого контролер відправить на сервер отримані дані на опрацювання системою (див. рис.1).

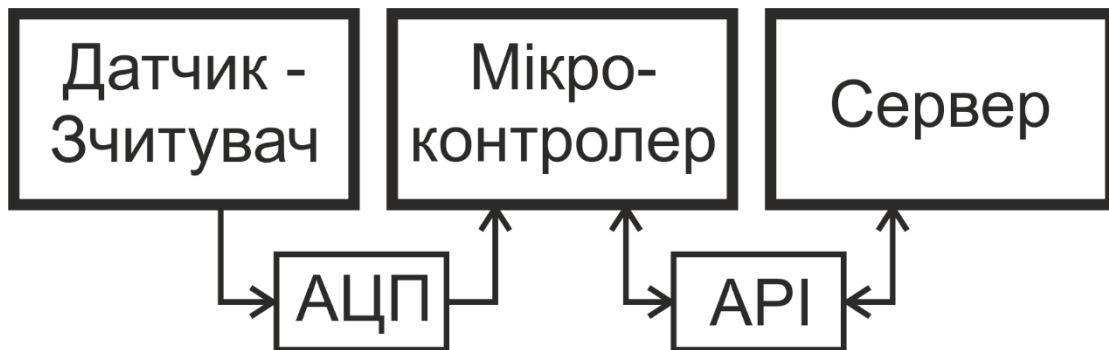


Рис. 1 – Спрощена схема взаємодії апаратного зчитувача фізичних подій з інформаційною системою

Прикладом подібної реалізації є впровадження функції щоденної ідентифікації учнів у інформаційну систему школи. Це дозволяє реєструвати час прибуття кожного конкретного учня, а також автоматизувати виставлення відміток про не прибуття на урок.

Індивідуальним ключем учня було обрано карту з вмонтованою RFID міткою. Для зчитування даних з таких карток застосовано цифровий модуль RC522. В якості мікроконтролера використано ESP8266, адже він являє собою потужний мікроконтролер + Wi-Fi модуль на одній платі.

Після піднесення учнем карти до зчитувача, отримується унікальний ID цієї карти й передається мікроконтролеру, який за допомогою HTTP протоколу передає дані на сервер, що, в свою чергу, формує запит до бази даних на перевірку існування такого ID. У разі успішного проходження всіх попередніх етапів буде створено новий запис в таблиці прибуття учнів.

ЛІТЕРАТУРА

1. Из чего состоит IoT [Електронний ресурс] // Habr. – 2019. – Режим доступу до ресурсу: <https://habr.com/ru/post/436708/>.
2. ESP8266 прошивка, программирование в Arduino IDE [Електронний ресурс] // Habr. – 2016. – Режим доступу до ресурсу: <https://habr.com/ru/post/371853/>.

Панасюк О. І.,

Київський національний університет імені Тараса Шевченка,

м. Київ, Україна

panasiuk0756@gmail.com

ПРОГРАМНІ РІШЕННЯ ДЛЯ ВЗАЄМОДІЇ МІЖ СЕРВІСАМИ ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Modern software solutions for creation of effective interaction between services of applied information systems are analyzed. The architectural features and prospects of using RabbitMQ and Apache Kafka for event processing scenarios in medical information systems are considered.

Key words: *applied information systems, message broker, stream scenarios, event processing*

Важливою складовою реформування системи охорони здоров'я в Україні є впровадження електронних медичних інформаційних систем, які дозволяють автоматизувати всі основні процеси, пов'язані з роботою медичних закладів, забезпечують обмін медичною інформацією і підтримують можливості інтеграції з іншими системами і програмами [1]. В зв'язку з цим, обґрунтований вибір програмних рішень для взаємодії між сервісами таких прикладних систем набуває все більшого значення. RabbitMQ та Apache Kafka – це дві системи з відкритим кодом та комерційною підтримкою, які охоче приймаються підприємствами. Випущена в 2007 році RabbitMQ була основним компонентом обміну повідомленнями для систем з сервісно-орієнтованою архітектурою (SOA). Сьогодні вона також використовується для випадків з інтенсивними потоками повідомлень. Apache Kafka – це новіший інструмент, який був розроблений в 2011 році спеціально для поточкових сценаріїв [3].

Метою нашої роботи було провести аналіз необхідних програмних рішень для створення ефективної взаємодії в розподіленій сервісно-орієнтованій архітектурі медичної інформаційної системи.

Проаналізовано архітектурні відмінності систем RabbitMQ та Apache Kafka. Брокер повідомлень загального призначення RabbitMQ використовує варіанти шаблонів спілкування запит/відповідь, точка-точка та публікація/підписка. В цій системі реалізована модель розумного брокера/німого споживача, тобто послідовна доставка повідомлень споживачам приблизно з такою ж швидкістю, як брокер контролює стан споживача [4]. Слід відмітити зрілу платформу, що добре підтримується, доступна для Java, клієнтських бібліотек, .NET, Ruby, node.js, a

також пропонує десятки плагінів. Зв'язок може бути синхронним або асинхронним. RabbitMQ надає розподілені сценарії розгортання. Багатовузловий кластер не покладається на зовнішні служби, однак певні плагіни формування кластера можуть використовувати DNS, API, Consul.

За архітектурою Apache Kafka – стійка, швидка та масштабована платформа повідомлень і потоків публікацій-підписок [2]. Це довготривале сховище повідомлень функціонує як журнал, запущений у кластері серверів, який зберігає потоки записів у темах (категоріях). Повідомлення складаються із значення, ключа та позначки часу. Реалізовано модель німого брокера/розумного споживача – не намагається відстежувати, які повідомлення читають споживачі, а зберігає лише непрочитані повідомлення. Apache Kafka зберігає всі повідомлення протягом певного періоду часу. Потрібні зовнішні служби для запуску, в деяких випадках Apache Zookeeper [4,5].

Apache Kafka пропонує набагато вищу ефективність, ніж брокери повідомлень, такі як RabbitMQ. Apache Kafka використовує послідовний ввід/вивід дискової підсистеми для підвищення продуктивності, що робить її придатною для впровадження черг. Вона може досягти високої пропускної здатності (мільйони повідомлень за секунду) за допомогою обмежених ресурсів, що необхідно у випадках використання великих масивів даних. RabbitMQ також може обробляти мільйон повідомлень за секунду, але вимагає більше ресурсів, близько 30 вузлів [3]. Використовувати RabbitMQ для тих самих випадків, що і Apache Kafka, можливо, але потрібно буде поєднувати його з іншими інструментами, такими як Apache Cassandra.

Apache Kafka надає брокера повідомлень і була розроблена для сценаріїв обробки потоків [2]. Ця система підтримує такі випадки використання, як метрики, відстеження активності, агрегування журналів, обробка потоків, журнали комітів та джерело подій. Особливо підходять для Apache Kafka наступні сценарії обміну повідомленнями [3,5]:

- потоки зі складною маршрутизацією, пропускною здатністю 100 тисяч подій за секунду і більше, із принаймні один раз розділеним упорядкуванням;
- програми, що вимагають історію потоку за умови «повідомлення прочитано хоча б один раз»;
- джерело подій, реагування моделей системи на послідовність подій;
- потокова обробка даних у багатоступеневих конвеєрах, конвеєри генерують графіки потоків даних у реальному часі.

RabbitMQ доцільно використовувати, коли веб-серверам потрібно швидко реагувати на запити. Це позбавляє від необхідності виконувати ресурсомісткі дії,

поки користувач чекає результату. RabbitMQ також є зручним для передачі повідомлення різним одержувачам для споживання або для розподілу навантажень між працюючими сервісами під великим навантаженням (20 тисяч і більше повідомлень за секунду). Сценарії використання RabbitMQ включають [4,5]:

- програми, які повинні підтримувати застарілі протоколи, такі як STOMP, MQTT, AMQP, 0-9-1;
- детальний контроль узгодженості/набору гарантій на основі кожного повідомлення;
- складна маршрутизація до споживачів;
- програми, яким потрібні різноманітні можливості обміну повідомленнями: публікації/підписки, із запитом/відповіддю, точка-точка.

Досвід впровадження і використання Apache Kafka в рамках рефакторингу і розширення функціоналу системи для роботи з асинхронними подіями проаналізовано на прикладі медичної інформаційної системи ТОВ «ХЕЛСІ ЮА». Вибір Apache Kafka був обумовлений тим, що ця система за своєю архітектурою є журналом (log) повідомлень, а не чергою. В зв'язку з цим, вона є ефективнішим засобом передачі сповіщень про події в ситуації, коли декілька сервісів мають відреагувати на повідомлення. Сповіщення зберігається певний час, незалежно від того, обробили його чи ні. Суттєвою перевагою Apache Kafka є краща масштабованість, ніж у RabbitMQ, завдяки чому вона більше підходить для високонавантажених систем. Таким чином, використання Apache Kafka дозволяє забезпечити найбільш ефективну взаємодію в розподіленій сервісно-орієнтованій архітектурі сучасної медичної інформаційної системи.

ЛІТЕРАТУРА

1. eZdorovya. Адміністратор Центральної бази даних eHealth України [Електронний ресурс]. – Режим доступу до ресурсу: <https://ehealth.gov.ua/>
2. Introduction to Apache Kafka [Електронний ресурс] // Apache Kafka. A distributed streaming platform. – Режим доступу до ресурсу: <https://kafka.apache.org/intro>
3. Levy E. Kafka vs. RabbitMQ: Architecture, Performance & Use Cases [Електронний ресурс] // Blog Upsolver, 2019. – Режим доступу до ресурсу: <https://www.upsolver.com/blog/kafka-versus-rabbitmq-architecture-performance-use-case>
4. Potapov E.A. RabbitMQ против Kafka: два разных подхода к обмену сообщениями [Електронний ресурс] // Блог компании ITSumma. 2018. – Режим доступу до ресурсу: <https://habr.com/ru/company/itsumma/blog/416629/>

5. Stiller E. RabbitMQ vs. Kafka. An architect's dilemma [Електронний ресурс] // Better Programming, 2020. – Режим доступу до ресурсу: <https://medium.com/better-programming/rabbitmq-vs-kafka-1ef22a041793>

Передерій Н.О.,

Студент групи УІС-21,

КНУ ім. Тараса Шевченка, м Київ

nick.perederiy@gmail.com

АНАЛІЗ ПЕРЕВАГ І НЕДОЛІКІВ ВИКОРИСТАННЯ ПАТЕРНУ EVENT SOURCING ПРИ ПОБУДОВІ ПРОГРАМНИХ СИСТЕМ Е-КОМЕРЦІЇ

***Анотація.** Проаналізовано переваги та недоліки використання патерну Event Sourcing у роботі з даними у великих комерційних проектах.*

***Ключові слова:** CRUD, Event Sourcing, робота з даними*

***Аннотация.** Проанализированы преимущества и недостатки использования паттерна Event Sourcing при работе с данными в больших коммерческих проектах.*

***Ключевые слова:** CRUD, Event Sourcing, работа с данными*

***Abstract.** Analyzed the advantages and disadvantages of using the Event Sourcing pattern in working with data in large commercial projects.*

***Key words:** CRUD, Event Sourcing, working with data*

Для більшості застосунків, що працюють з даними, типовою є підтримка поточного стану даних за рахунок оновлення у міру роботи з ними. Наприклад, у традиційній моделі створення, читання, оновлення та видалення (CRUD), оброблення даних – це зчитування даних зі сховища, внесення певних змін і оновлення їх поточного стану новими значеннями [1].

Такий підхід має деякі обмеження:

- Системи CRUD виконують операції оновлення безпосередньо у сховищі даних, що може негативно впливати на продуктивність і швидкість реагування і обмежувати масштабованість системи в цілому.
- У домені для спільної роботи з великою кількістю паралельних підключень користувачів з'являється ймовірність виникнення конфліктів оновлення даних, оскільки операції оновлення виконують для окремого елемента даних.
- За відсутності додаткового механізму аудиту, що записує деталі кожної операції в окремий журнал, історія змін не зберігається.

Патерн Event Sourcing (джерело подій) визначає підхід до оброблення операцій з даними на основі послідовності подій, кожна з яких записується в інкрементоване сховище. Код застосунку відправляє ряд подій, що примусово описують кожну дію з даними в сховищі подій, де вони зберігаються. Кожна подія описує набір змін до даних (наприклад, додавання нового елемента у список). Сховище подій виступає як система запису поточного стану даних. Зазвичай, воно публікує ці події для сповіщення підписників і, за необхідності, надає їм можливість обробляти ці події. Аналізуючи реалізації цих підходів у різних комерційних проектах, можна виділити такі переваги та недоліки застосування патерну Event Sourcing.

Переваги:

- Зберігання тільки доменних подій дає можливість визначати стан програмної системи у будь-який момент часу в минулому.
- Події є незмінними. Їх збереження виконується інкрементованою операцією.
- Події – це об'єкти, що описують деякі виконані дії та дані, необхідні для їх опису.

- Можливість запобігання конфліктів, що виникають у разі паралельного оновлення даних, оскільки виключається необхідність безпосереднього оновлення об'єктів у сховищі даних.
- Код застосунку, що створює події, не пов'язаний із кодом систем, що підписані на ці події. Це, у свою чергу, збільшує гнучкість і масштабованість системи.

Недоліки:

- Це рішення є більш складним порівняно з застосуванням традиційного CRUD підходу.
- Повна реалізація патерну потребує зміни архітектури більшої частини програмної системи.
- Реалізація патерну потребує використання бази даних, створеної спеціально для джерел подій (наприклад, Event Store), або документо-орієнтованої бази даних (Azure Cosmos DB, MongoDB, Cassandra, CouchDB, або RavenDB) [2].
- Між додаванням подій у сховище, їх публікацією та обробкою підписниками існує деяка затримка.

Зазначимо, що використання патерну Event Sourcing вирішує більшість проблем традиційних підходів роботи з даними. Проте, у більшості випадків, реалізувати цей патерн повною мірою не є тривіальною задачею. Як і більшість патернів, патерн Event Sourcing має рекомендаційний характер, і не є рішенням усіх проблем, тому для кожного окремого випадку слід обирати свій підхід, ретельно зваживши всі переваги та недоліки.

ЛІТЕРАТУРА:

1. Mike Wasson, Christopher Bennage and others. «Event Sourcing pattern» [<https://docs.microsoft.com/en-us/azure/architecture/patterns/event-sourcing>]

2. Cesar de la Torre, Bill Wagner, Mike Rousos «Microservices Architecture for Containerized .NET Applications». Edition 3.1.2, p. – 144. Microsoft. 2020. [<https://aka.ms/microservicesebook>]

Підлужний Д. О.

Київський національний університет імені Тараса Шевченка,

м. Київ, Україна

d.pidluzhnyi@gmail.com

ВИКОРИСТАННЯ СУЧАСНИХ АЛГОРИТМІВ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ ПІД ЧАС ПАНДЕМІЇ COVID-19

In this paper, the author considers the prospects of bypassing the mask occlusion in image classification and processing. Possibilities and methods for improving the recognition process of people wearing masks or other objects are discussed.

Keywords: *Image classification, image processing, face recognition, neural networks, occlusion in image processing and recognition*

Одними з основних проблем з розпізнавання обличчя людини нині є розпізнавання обличчя з різних точок зору, а також розпізнавання з певними перешкодами, що в останній час набуло найбільшої актуальності, оскільки більшість людей в публічних місцях захищає обличчя, одягаючи медичну маску, або саморобну маску з підручних матеріалів. Тому задача розпізнавання погіршується багаторазово, так як більша частина обличчя є закритою. Рот і ніс охоплюють інформацію, корисну як для розпізнавання, так і для етапу виявлення, який передує цьому.

Тому, якщо не знайти спосіб розпізнавати обличчя за його частинами, Face ID в телефонах та банківські операції при використанні маски будуть недоцільні. А пошукові системи людей нейромережею стануть неефективними. Під час тестування, проведеного національним інститутом стандартів і технологій, з понад 89 найкращих комерційних алгоритмів розпізнавання обличчя коефіцієнт помилок при накладанні цифрових масок для обличчя становив від 5% до 50% у поєднанні із фотографіями тієї самої людини без маски. При виконанні тесту було використано 6,2 млн зображень 1 млн людей [1].

У цілому нині можна виділити три основні методи для боротьби з цією проблемою такі як: уникання частини фото, що не містить корисної для розпізнавання інформації при обробці зображення; відновлення регіону, що закривається маскою за допомогою зображень з уже чинної бази даних; поділ зображення на частини та застосування алгоритму розпізнавання до кожної частини, порівнюючи результати з базою даних [2].

Для виконання перевірки ефективності алгоритмів можна використовувати відкриту базу даних Real-World-Masked-Face-Dataset [3], що містить велику кількість обличчя з масками. База даних поділяється на набір даних розпізнавання обличчя з маскою (MFDD), набір даних розпізнавання обличчя в масках (RMFRD) та набір даних із розпізнаванням, що імітують наявність маскування (SMFRD) [2].

Ще однією цікавою темою для дослідження, пов'язаною з цією проблематикою, є розпізнавання наявності маски або інших об'єктів, що закривають частину обличчя. Більшість людей, які користувалися якими-небудь застосунками, що використовують розпізнавання обличчя, стикалися з проблемою неможливості розпізнавання та обминання об'єкта при розпізнаванні. Наприклад, такі застосунки як Instagram та Snapchat використовують розпізнавання обличчя для створення фільтрів в режимі реального часу, або на основі вже наявної фотографії. Такі сервіси практично не можуть якісно розпізнати об'єкт, тому вважають маску чи інший об'єкт як частину обличчя, що у свою чергу, надає не зовсім коректні результати.

ЛІТЕРАТУРА

1. Звіт національного інституту стандартів і технологій про точність розпізнавання обличчя з маскою з використанням алгоритмів щодо COVID-19 [Електронний ресурс] - Режим доступу до ресурсу: <https://doi.org/10.6028/NIST.IR.8311>

2. Ефективний метод розпізнавання обличчя під маскою під час пандемії COVID-19 Walid Hariri [Електронний ресурс] - Режим доступу до ресурсу: <https://assets.researchsquare.com/files/rs-39289/v1/68fdc679-44c5-4949-bb3b-e5ad1bfc1ef0.pdf>

3. База даних з реальними фото людей в масках (RMFRD) [Електронний ресурс] - Режим доступу до ресурсу: <https://github.com/X-zhangyang/Real-World-Masked-Face-Dataset>

Пікуляк М.В., Корнута В.Р.

ДВНЗ «Прикарпатський національний університет імені В.Стефаника»

mykolapikulyak@gmail.com; atunrok888@gmail.com

ВДОСКОНАЛЕННЯ ЕВРИСТИЧНОГО АЛГОРИТМУ ПОШУКУ ОПТИМАЛЬНОГО МАРШРУТУ ДО ПАРКУВАЛЬНОЇ ЗОНИ

Abstract. The analysis of known algorithms for determining the route is performed and the algorithm A is improved, which allows to increase the speed of processing program results and expand the scope of its application.*

Keywords: heuristic algorithm, parking zone, weight function, route determination.

Вступ. Сьогодні на ринку програмних продуктів представлено чималу кількість сервісів, що дають можливість прокласти маршрут до потрібної точки та мають необхідну базу паркувальних зон. Проте багато з них мають недоліки, пов'язані із ліцензійними обмеженнями, недостатньою повнотою вихідних просторових даних та неможливістю застосування власних алгоритмів.

Крім цього виникає необхідність у розробці додаткових функцій подібних сервісів, пов'язаних із проведенням деталізованого аналізу отриманих результатів пошуку, можливістю застосування на місцевостях із складним ландшафтом, підтримкою актуальності даних. Тому розробка подібних програмних додатків є актуальною задачею, яка вимагає подальшого їх дослідження та розробки нових і вдосконалення відомих алгоритмів обробки.

Аналіз відомих алгоритмів. Усі відомі алгоритми для визначення маршруту, по якому можна потрапити з однієї точки в іншу, можна розбити на дві групи:

- алгоритми, що дозволяють визначити оптимальний шлях;
- алгоритми, що дозволяють знайти субоптимальний шлях.

Алгоритми першої групи потребують детального дослідження простору станів задачі. Найпростішим способом пошуку оптимального шляху є повний перебір всіх можливих маршрутів. Це гарантує знаходження оптимального шляху. Але на практиці частіше за все такий спосіб неможливо використати із-за надмірних накладних витрат, оскільки він потребує зберігання в пам'яті усієї досліджуваної області.

Прикладом алгоритмів пошуку субоптимальних шляхів є евристичні алгоритми, які дозволяють на кожному кроці максимально наблизитись до

кінцевої точки. Однак при пошуку одного з найближчих до оптимального шляху слід враховувати, що спочатку важко точно передбачити, який саме варіант буде обраний. У цьому випадку можна використовувати різні алгоритми при виборі напрямку на кожному кроці. Найбільш раціональним у такій ситуації здається розробка окремих алгоритмів для різних класів задач на базі алгоритмів визначення оптимального шляху із застосуванням евристик, що враховують специфіку даної проблемної області.

Багато алгоритмів мають схожу проблему: отриманий з їх допомогою шлях виглядає не найкоротшим. Для її вирішення потрібно або використовувати оптимізацію шляху, або застосовувати алгоритм, в якому вже використовуються функції, які дозволяють отримати найкоротший шлях в дискретній моделі [1].

Можна узагальнити наступні найбільш ефективні алгоритми на основі яких розробляються похідні:

- алгоритм Дейкстри (використовується для знаходження оптимального маршруту між двома вершинами). Перевагою даного алгоритму є простота реалізації та можливість його застосування в графах з невеликою кількістю вершин. З огляду на структуру схеми міста, програма, що написана з використанням алгоритму Дейкстри буде виконуватися повільно, а розподіл пам'яті не буде раціональним [2].

- алгоритм Флойда (для знаходження оптимального маршруту між усіма парами вершин). Цей алгоритм призначений для вирішення завдання пошуку всіх найкоротших шляхів на графі. Також він розпізнає наявність негативних циклів. Недоліком його застосування є те, що він містить три вкладені цикли, тобто має кубічну складність. Тому при його застосуванні буде використовуватися великий обсяг пам'яті, що є не раціональним рішенням [3].

алгоритм Беллмана-Форда (для знаходження найкоротшого шляху від однієї вершини графа до всіх інших). Його відмінною рисою є можливість застосування до графів з довільними, в тому числі негативними, вагами. Алгоритм використовує повний перебір всіх вершин графа, що призводить до великої втрати часу та потребує значного обсягу пам'яті.

Імплементация алгоритму A^* для системи прокладання маршруту до паркувальної зони.

Алгоритм мобільної системи прокладання маршруту до найближчого паркінгу для автомобілів на базі ОС Android повинен базуватися на удосконаленому алгоритмі A^* і працювати на вуличній мережі, яка моделюється як граф. Вузлами в графі будуть представлені переходи чи дороги, що не мають наскрізного проїзду (тупики), а ребрами – вуличні сегменти. В удосконаленому

алгоритмі необхідно врахувати, що граф спрямований, а це означає, що є обмеження напрямку (наприклад, враховується рух в одну сторону вулиці). Ребро з обома напрямками означає, що можливе управління на вулиці в обох напрямках, незалежно від структурних умов, які можуть відокремити смуги [4].

Блок-схема вдосконаленого алгоритму A* представлена на рис.1:

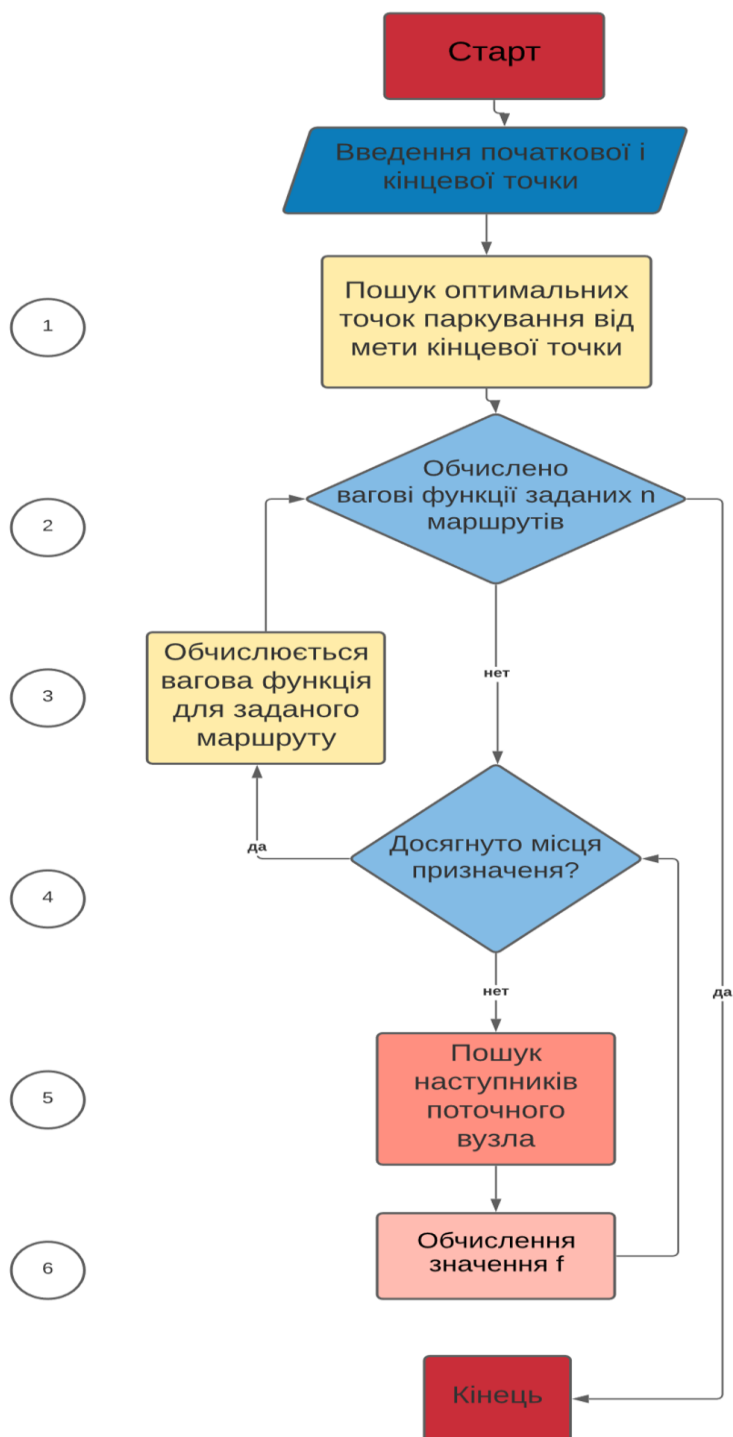


Рис. 1. Блок-схема вдосконаленого алгоритму

Робота алгоритму розпочинається з того, що спочатку відбувається пошук паркувальних точок в заданому оптимальному радіусі для водія. На наступному кроці ми перевіряємо, чи є закінчений обрахунок вартості маршрутів. Якщо так, то алгоритм закінчується; якщо ні, тоді слідує четвертий крок.

З четвертого по шостий крок знаходиться найкоротший шлях за допомогою функції оцінки:

$$f(x) = g(x) + h(x),$$

де:

g – визначає витрати від початкового вузла до вузла x ;

h – описує евристичні орієнтовні витрати від x до кінцевого вузла.

Вузол визначається як поточний, якщо він має найменше значення f .

На другому кроці виконання алгоритму перевіряється чи поточний вузол є цільовим вузлом. Якщо так, то алгоритм закінчується. Якщо ні, слідує крок 3.

Коли вивчається поточний вузол x , то відбувається визначення та вивчення всіх його наступників. Для кожного наступника y обчислюється функція $f(y)$.

На п'ятому кроці обчислюються затрати на шлях до вузла x , а саме $g(x)$ і затрати від поточного вузла x до його наступника.

На шостому кроці обчислюється функція:

$$f(y) = g(y) + h(y),$$

де:

$g(y)$ – це затрати від початкового вузла до вузла y ;

$h(y)$ – оцінює затрати від вузла наступника на цільовий вузол з евристикою.

В кінці $f(y)$ оцінює спадковий вузол y .

Після вищевказаного відбувається перехід на четвертий крок, і кроки 4-6 повторюються до досягнення цільового вузла.

Якщо був зроблений перехід до цільового вузла, то відбувається третій крок, який здійснює обрахунок вагової функції всього маршруту. Далі йде перевірка чи було обраховано ваговий коефіцієнт всіх маршрутів. Якщо так, алгоритм закінчується.

Отже, вагова функція складається з часу проїзду від поточного вузла до наступного вузла, ймовірності паркування на ділянці дороги, яка зв'язує поточний і наступний вузол, а також коефіцієнт оптимального віддалення.

Не тільки вагова функція, але і евристика адаптована для алгоритму паркування. В якості евристичної функції береться евклідова відстань від вузла наступника до цільового вузла, розділеного на константу. Константа складається із рекомендованої швидкості руху та не повинна переоцінювати витрати для вулиць у місті.

Порядок кроків алгоритму – це функція оцінки витрат з допомогою евристики і призводить до формування паркувальних точок маршрутизації.

У більшості випадків A^* обчислює найшвидший або найкоротший шлях, тому функція витрат включає лише час проїзду або на довжину дорожньої лінії. Проте, щоб вирішити проблему паркування автомобіля з найменшою витратою часу на подолання відстані до потрібної точки, потрібно також враховувати вірогідність паркування і час пішого проходження до кінцевої точки маршруту.

Висновок. В результаті проведеного дослідження виконано аналіз відомих алгоритмів визначення маршруту та запропоновано вдосконалений евристичний алгоритм пошуку, що дає можливість підвищити швидкість обробки отриманих результатів та розширити застосування додатку у відповідності до змін ландшафту.

Практична реалізація даного алгоритму дозволить побудувати сервіс, який вирішить проблему паркування автомобіля з найменшою витратою часу на подолання відстані до потрібної точки.

ЛІТЕРАТУРА

1. Delling, D.; [Sanders, P.](#); Schultes, D.; [Wagner, D.](#) (2009). Engineering route planning algorithms. Algorithmics of Large and Complex Networks: Design, Analysis, and Simulation. Springer. с. 117–139. [doi:10.1007/978-3-642-02094-0_7](https://doi.org/10.1007/978-3-642-02094-0_7).
2. [Dijkstra E. W. A note on two problems in connexion with graphs](#) (англ.) // [Numer. Math](#) / [F. Brezzi](#) – Springer Science+Business Media, 1959. – Vol. 1, Iss. 1. – P. 269–271. — ISSN [0029-599X](#); [0945-3245](#) — [doi:10.1007/BF01386390](https://doi.org/10.1007/BF01386390)
3. [Томас Кормен](#); [Чарльз Лейзерсон](#)[en], [Рональд Рівест](#) (1990). [Вступ до алгоритмів](#) (вид. 1st). MIT Press і McGraw-Hill. ISBN [0-262-03141-8](#). Секція 26.2, «The Floyd–Warshall algorithm», С. 558–565 та секція 26.4, «A general framework for solving path problems in directed graphs», С. 570–576.
4. Електронний ресурс : <http://www.raywenderlich.com/4946/introduction-to-a-pathfinding>.

Пирог М.В.

Київський національний університет імені Тараса Шевченка

м. Київ, Україна

mykola.pyroh@ukr.net

Дуля Д.В.

Київський національний університет імені Тараса Шевченка

м. Київ, Україна

daryna_dulia@knu.ua

ПОРІВНЯННЯ ПЛАТФОРМ .NET CORE ТА NODE.JS ЯК ТЕХНОЛОГІЙ ВЕБ-РОЗРОБКИ

In this paper, the authors consider web development platforms .Net Core and Node.js, analyze their advantages and disadvantages. The authors aimed to conduct a comparative analysis to understand the capabilities of the platforms, their scope of application, the complexity of work and mastery of the proposed technologies. The analysis presented for future development platforms.

Keywords: *.NET Core, Node.js, web development.*

З розвитком інформаційних технологій, збільшенням обчислювальних потужностей персональних комп'ютерів та серверів ускладнилось і програмне забезпечення. Ці зміни, в тому числі, не обійшли стороною сферу веб-розробки.

Якщо від початку сайти створювали за допомогою HTML (англ. HyperText Markup Language – мова гіпертекстової розмітки) та оформлювали через CSS (англ. Cascading Style Sheets – каскадні таблиці стилів), то на даний час веб-сайти та веб-застосунки отримали свій розвиток та профільні інструменти, що здатні забезпечити розробку щораз складніших програмних застосунків.

Згідно даних опитування проведеного порталом Stack Overflow [1] за останні два роки найбільш популярними платформами для веб-розробки стали Node.js [2] та .NET. Варто відзначити, що під .NET ми розуміємо як саму платформу .NET так і .NET Core [3] яку ми виберемо для подальшого аналізу.

Платформа Node.js має відкритий вихідний код, розроблена на рушії Google V8 для опрацювання мови JavaScript, що своєю чергою написаний мовами C++ та C. Дана платформа дозволяє виконувати скрипти на стороні сервера та передавати результат їх роботи клієнту, що дозволяє зменшити навантаження та кількість інформації, що необхідно опрацювати на стороні користувача. Node.js дозволяє створювати продукт для Windows та Unix-подібних систем.

Платформа .NET Core стала переосмисленням класичного .NET. Ця платформа також отримала відкритий вихідний код та, на відміну від .NET, можливість працювати з Windows та Unix-подібними системами. Робота з .NET Core ведеться мовою C#.

Після короткого огляду платформ можемо зробити попередній висновок, що з платформою .NET Core працювати важче, адже необхідно знання додаткової мови програмування на відміну від Node.js де робота ведеться на JavaScript, що на сьогодні є обов'язковою для оволодіння будь-яким веб-розробником. В свою чергу C# має перевагу у вигляді строгої типізації, що ставить більше вимог перед розробником проте захищає його від помилок, що супроводжують динамічну типізацію в JavaScript.

Відзначимо, що платформа Node.js на 7 років старша за .NET Core та має більшу спільноту розробників, що пояснює ширше представлення інструментів та модулів для розробки – приблизно у 6 разів.

З іншого боку при розробці веб-застосунку на .NET Core розробник отримує вбудовану можливість працювати з багатопоточністю сучасних серверів та процесорів, що позитивно впливає на можливості таких продуктів та їх подальшу підтримку. В свою чергу Node.js має балансувальники навантаження та інструменти керування сервісами і трафіком, що з нашої точки зору є вирішенням питання багатопоточності на рівні надбудов [4].

Проведемо синтетичні тести для аналізу швидкодії платформ на базі TechEmpower Web Framework Benchmarks [5]. Результати наступні:

Best database-access responses per second, single query, Azure D3v2 Instances (8 tests)													
Rnk	Framework	Best performance (higher is better)		Errors	Cls	Lng	Plt	FE	Aos	DB	Dos	Orm	IA
1	aspcore-mw-ef-pg	16,188	100.0% (11.7%)	0	Mcr	C#	NE	kes	Lin	Pg	Lin	Ful	Rea
2	nodejs-postgres	12,225	75.5% (8.8%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea
3	aspcore-mw-ef-pg	10,817	66.9% (7.8%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea
4	typexi-ef-pg	8,645	53.4% (6.2%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea
5	typexi-postgres	3,533	21.8% (2.5%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea
6	hapi-postgres	1,573	9.7% (1.1%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea
7	express-ef-pg	534	3.3% (0.4%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea
8	express-ef-pg-postgres	477	2.9% (0.3%)	0	Plt	JS	njs	Non	Lin	Pg	Lin	Ful	Rea

Рис. 1. Одноразове звернення до бази та отримання відповіді.

На рисунку 1 представлений результат роботи систем на платформах .NET Core та Node.js в умовах одноразового звернення клієнта до бази та отримання у відповідь однієї строки з неї.

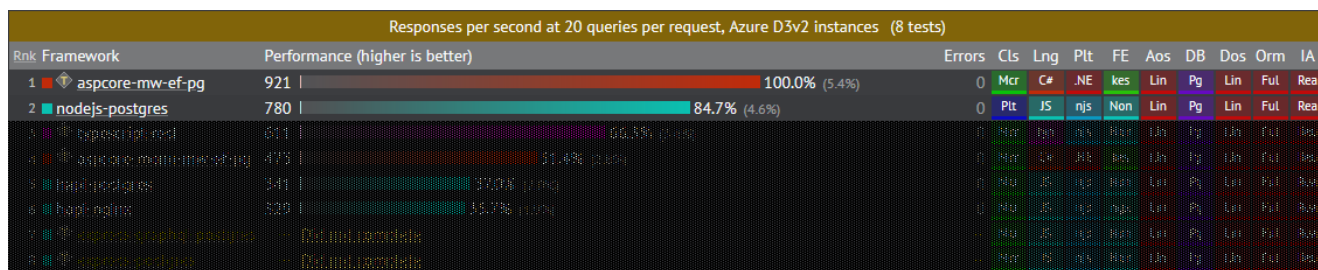


Рис. 2. Множинне звернення до бази та отримання відповідей.

На рисунку 2 представлений результат роботи систем на платформах .NET Core та Node.js в умовах множинного звернення клієнта до бази та отримання у відповідь на кожен запит множини строк.

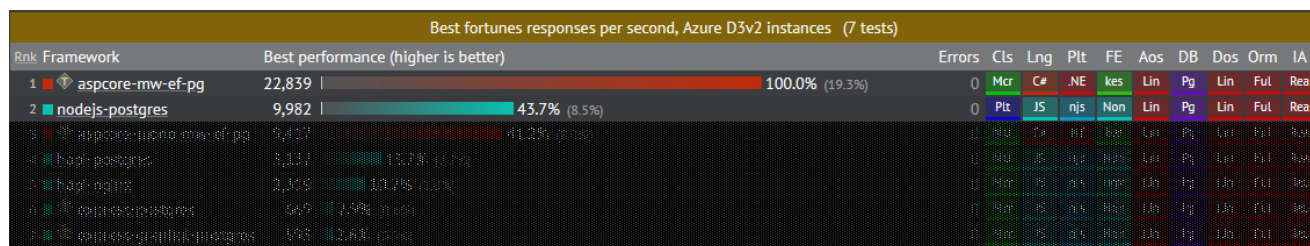


Рис. 3. Отримання повної бази клієнтом.

На рисунку 3 представлений результат роботи систем на платформах .NET Core та Node.js в умовах запиту клієнтом повної бази з сервера, її подальшої інтерпретації у звіт та передачі на сторону клієнта.

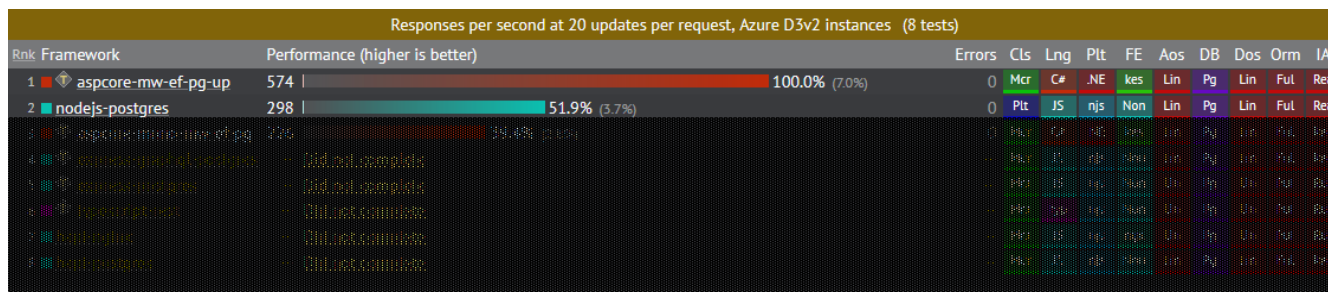


Рис. 4. Оновлення бази після запиту.

На рисунку 4 представлений результат роботи систем на платформах .NET Core та Node.js в умовах множинного звернення клієнта до бази, отримання з бази множини строк, їх модифікації та подальшого повернення в базу.

Пророблена нами робота показує певне домінування платформи .NET Core у синтетичних тестах. Проте відзначимо, що такі тести не можуть в повній мірі дати уявлення про реальні умови роботи описаних вище платформ. З огляду на

отримані результати та вивчені матеріали вважаємо за можливе стверджувати, що обидві платформи є конкурентно здатними, а перевага однієї платформи над іншою може бути визначена виключно технічним завданням конкретного проекту.

Ми вважаємо за необхідне додати, що матеріал дослідження був написаний до офіційного виходу стабільної версії платформи .NET 5, що має нівелювати необхідність існування трьох платформ компанії Microsoft та фактично об'єднати їх в один допрацьований, стабільний, кросплатформний інструмент.

ЛІТЕРАТУРА

1. 2020 Developer Survey [Електронний ресурс] // Stack Overflow. – 2020. – Режим доступу до ресурсу: <https://insights.stackoverflow.com/survey/2020>.
2. Node.js [Електронний ресурс] // OpenJS Foundation – Режим доступу до ресурсу: <https://nodejs.org/en/>.
3. .NET [Електронний ресурс] // Microsoft – Режим доступу до ресурсу: <https://dotnet.microsoft.com/>.
4. Горшков М. .NET Core vs Node.js [Електронний ресурс] / Максим Горшков // Хабр. – 2020. – Режим доступу до ресурсу: <https://habr.com/ru/post/506282/>.
5. TechEmpower Web Framework Benchmarks [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techempower.com/benchmarks/>.

Пирог М.В.

Київський національний університет імені Тараса Шевченка

м. Київ, Україна

mykola.pyroh@ukr.net

Борсук О.С.

Київський національний університет імені Тараса Шевченка

м. Київ, Україна

borsuk_alexandra@knu.ua

ФРЕЙМВОРК ANGULARJS ТА БІБЛІОТЕКА REACT.JS ЯК ІНСТРУМЕНТИ РОЗРОБКИ ДИНАМІЧНИХ ВЕБ-ЗАСТОСУНКІВ

In this paper, the authors consider the web development tools AngularJS and React.js. The authors conducted a comparative analysis of the capabilities of platforms, scope of their application, the complexity of their work. The question of prospects for further development of the proposed technologies is considered.

Keywords: *AngularJS, React.js, web development.*

Розвиток сфери веб-розробки сприяв перетворенню статичних сайтів написаних на складні динамічні програмні застосунки, що будуються на базі багатьох допоміжних інструментів. Таким чином веб-розробники розширюють функціонал та можливості роботи з програмним забезпеченням через всесвітню мережу.

Згідно опитування проведеного порталом Stack Overflow [1] найбільш популярною мовою, що використовується в веб-розробці є JavaScript. Розглядаючи інструментарій, що було розроблено за час існування цієї мови програмування ми звернули увагу на рейтинг фреймворків та бібліотек для JavaScript. Чільні місця цього рейтингу посідають бібліотека React.js [2] та фреймворк Angular.

Зважаючи на нашу націленість саме на мову JavaScript було прийнято рішення для порівняння використовувати не фреймворк Angular, а його вихідний варіант Angular.js [3].

Фреймворк Angular.js – JavaScript-фреймворк з відкритим програмним кодом, який розробляє Google. Призначений для розробки односторінкових додатків. Створений з метою розширення браузерних застосунків на основі шаблону «модель-вид-контролер» (MVC), а також спрощення їх тестування та розробки. Фреймворк працює зі сторінкою HTML, що містить додаткові атрибути і пов'язує області вводу або виводу сторінки з моделлю, яка є звичайними

змінними JavaScript. Значення цих змінних задаються вручну або отримуються зі статичних або динамічних JSON-даних.

Оскільки Angular.js є повноцінним фреймворком в нього за замовченням вбудована широка бібліотека шаблонів, розширень для HTML та система керування пакетами. До недоліків фреймворку можемо віднести різноманітність структур з якими працює розробник, що ускладнює його вивчення. Не в останню чергу Angular.js повільніший за React.js через свою відносно громіздку структуру, виконанні на стороні клієнта та роботу з реальним DOM.

Бібліотека React.js – відкрита JavaScript бібліотека для створення інтерфейсів користувача, яка покликана вирішувати завдання часткового (динамічного) оновлення вмісту веб-сторінки. Розробляється Facebook і спільнотою індивідуальних розробників. React.js дозволяє розробникам створювати великі веб-застосунки, які використовують дані, котрі змінюються з часом, без перезавантаження сторінки. Його мета полягає в тому, щоб бути швидким, простим, масштабованим. React.js обробляє тільки користувацький інтерфейс у застосунках. Як бібліотеку інтерфейсу користувача React.js найчастіше використовують разом з іншими бібліотеками, такими як Redux.

Як бібліотека React.js потребує доповнень для розширення своїх можливостей, що одночасно можна розглядати як недолік так і перевагу оскільки розробник вільний у виборі підходів до розробки та застосуванню модулів в межах бібліотеки. React.js завдяки виконанню на стороні сервера. Ще однією перевагою бібліотеки React.js ми вважаємо не пряму роботу з DOM, а взаємодію з віртуальним DOM [4], що дозволяє зробити процес розробки зручнішим, а кінцевий програмний продукт більш динамічним.

Повертаючись до аналізу статистики порталу Stack Overflow можемо констатувати, що кількість проектів де використовується React.js вдвічі більша за кількість проектів з використанням Angular.js. Проте, важливо відзначити, що Angular.js активно замінюється фреймворком Angular на базі TypeScript, у випадку порівняння останнього з React.js відставання у кількості проектів скорочується до 15-20%.

У майбутньому розвитку розглянутих нами технологій варто відзначити і суб'єктивні думки розробників щодо згаданих інструментів.

Таким чином у рейтингу улюблених фреймворків та бібліотек для веб-розробки React.js посідає друге місце, поступаючись, з невеликим відривом, фреймворку ASP.NET Core. В той же час у рейтингу найбільш небажаних у роботі інструментів Angular.js посідає перше місце. Найбільш бажаним для використання в роботі, за даними опитування, було визнано React.js.

Підсумовуючи проведену нами роботу можемо впевнено стверджувати про наявність динаміки щодо відмови від використання Angular.js на проектах на користь бібліотеки React.js та фреймворку Angular. Відзначимо, що хоч React.js і є більш популярним та поширенішим у колах веб-розробників, цю бібліотеку важче опанувати за Angular.js причиною чого є варіативність роботи з нею.

ЛІТЕРАТУРА

1. 2020 Developer Survey [Електронний ресурс] // Stack Overflow. – 2020. – Режим доступу до ресурсу: <https://insights.stackoverflow.com/survey/2020>.
2. AngularJS [Електронний ресурс] // Google – Режим доступу до ресурсу: <https://angularjs.org/>.
3. React.js [Електронний ресурс] // Facebook, Inc. – Режим доступу до ресурсу: <https://reactjs.org/>.
4. Что такое Virtual DOM? [Електронний ресурс] // Хабр. – 2015. – Режим доступу до ресурсу: <https://habr.com/ru/post/256965/>.

Плескач В.Л.

*Київський національний університет імені Тараса Шевченка, Київ
v_pleskach@ukr.net*

Плескач М.В.

*Київський національний університет імені Тараса Шевченка, Київ
pleskachmarija@gmail.com*

ІНДЕКС РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ ТА ЕЛЕКТРОННИХ ПУБЛІЧНИХ ПОСЛУГ В УКРАЇНІ: 2020

The research represents a review of current condition of implementation e-government measures. The article demonstrates Ukraine's rating in the international arena on the development of e-government in 2020. This research also outlines the issue of low implementation rate of practical measures in this sphere.

Key words: *E-Government Development Index, public e-services.*

Вступ. Створення можливостей для отримання людиною електронних публічних послуг, організація належних умов для звернення людини до органів публічної влади із використанням мережі Інтернет є одними із важливих напрямків упровадження *електронного урядування* як форми організації державного управління, що сприяє підвищенню ефективності, відкритості та прозорості суб'єктів публічної адміністрації із використанням інформаційно-комунікаційних та цифрових технологій для формування нового типу держави, орієнтованої на задоволення потреб людини [1, с.11].

«Електронна послуга», відповідно до Стратегії розвитку інформаційного суспільства в Україні, схваленої Розпорядженням Кабінету Міністрів України від 15 травня 2013 року за № 386-р, є послугою, що надається громадянам та організаціям в електронному вигляді за допомогою інформаційно-комунікаційних технологій [2].

Фахівці до електронних послуг відносять: усі електронні адміністративні послуги, онлайн оплату комунальних послуг, телекомунікаційних послуг, придбання товарів у Інтернет-магазинах тощо [3, с. 20].

Спроби створити повноцінні сервісні платформи *електронного урядування* робилися в Україні ще із 2001 року, однак лише у 2015-2016 роках почали реалізуватися більш конкретні заходи у цьому напрямку. Так, згідно з рейтингом E-Government Development Index (EGDI), у 2016 році Україна займала 62-е місце серед 193 країн та покращила свою позицію порівняно із 2014 роком на 25 пунктів. Це пояснюється створенням відповідної державної установи (станом на 2016 рік – це було Державне агентство з питань електронного урядування України), що мало здійснювати забезпечення сфери електронного урядування в Україні. [4, с. 66].

Однак, незважаючи на те, що у вищевказаний період в Україні було частково створено відповідну нормативно-правову базу з питань електронного урядування (хоч і не без низки таких недоліків, як неповнота, несистемність, недостатня взаємоузгодженість із міжнародними нормами), відсутність належного втручання та регулювання державою процесів розбудови інформаційного суспільства, а також подальшого впровадження електронного урядування призвело до того, що у 2018 році Україна опинилася вже на 82 місці *Індексу розвитку електронного урядування*.

Доцільно зазначити, що Індекс розвитку електронного урядування (E-Government Development Index (EGDI)) розраховується за методологією Організації Об'єднаних Націй, і демонструє ступінь готовності країн до реалізації та

використання електронного урядування, у тому числі надання адміністративних та інших публічних послуг онлайн.

Цей Індекс складається один раз на два роки Департаментом економічного та соціального розвитку Організації Об'єднаних Націй (Department of Economic and Social Affairs, UN DESA), і який, в свою чергу, складається із таких показників, як-от: стан цифрової (інформаційно-телекомунікаційної) інфраструктури; людський капітал; якість електронних державних послуг. Зазначимо, що у 2020 році Україна посіла у Індексі розвитку електронного урядування 69 місце (0,7119 пунктів), піднявшись порівняно із 2018 роком на 13 позицій [5] (рис.1).

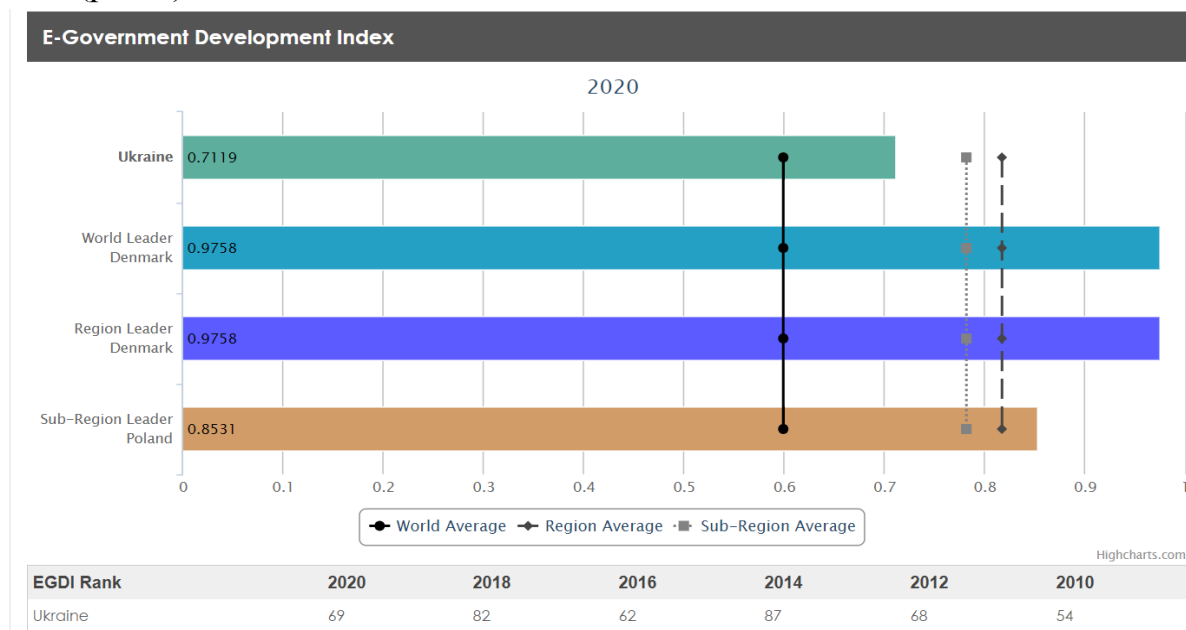


Рис.1

У розрізі показників: стан цифрової (інформаційно-телекомунікаційної) інфраструктури; людський капітал; якість електронних державних послуг ситуація в Україні у 2020 році виглядає таким чином:

- за показником *Якість електронних державних послуг (Online Service Index)*, рис. 2, Україна має 0,6824 пункти, відстаючи від світового лідера – Республіки Корея (Південної Кореї) майже на половину показників.

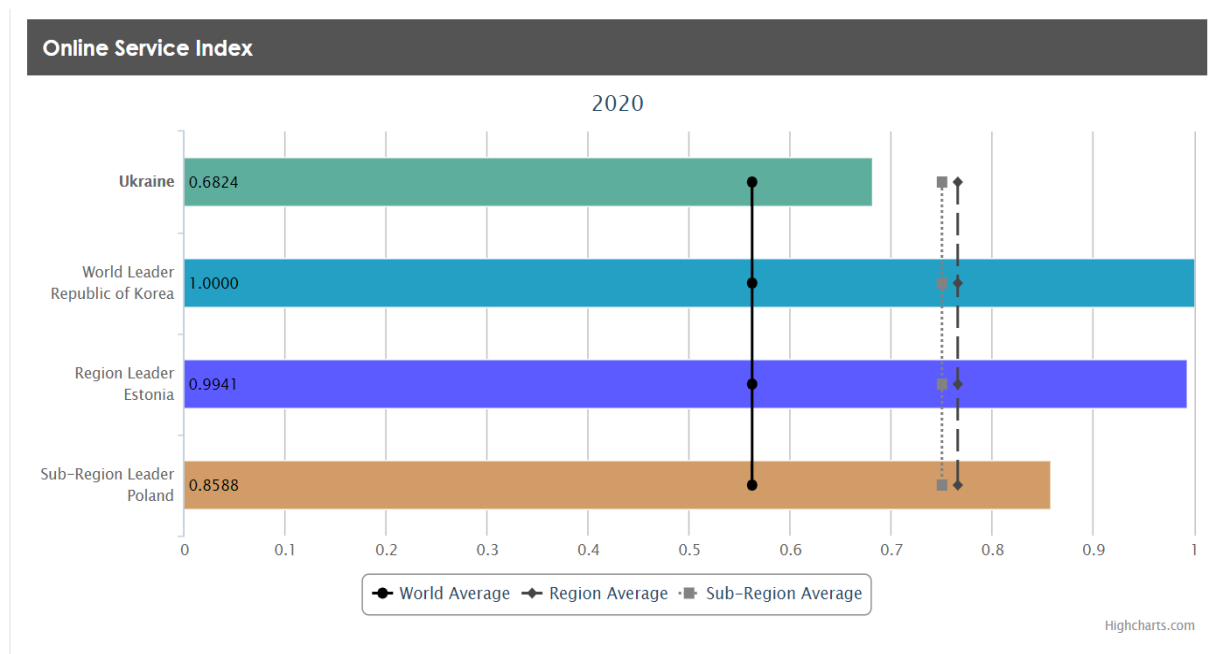


Рис.2

- за показником *Стан цифрової (інформаційно-телекомунікаційної) інфраструктури (Telecommunication Infrastructure Index)* (рис.3), Україна має лише 0,5942 пункти, що на половину менше від таких розвинутих світових країн-лідерів, як Республіка Корея (Південна Корея), Естонія.

Зазначимо, що за Індексом розвитку інформаційно-комунікаційних технологій (International Telecommunication Union: ICT Development Index 2017) Україна також суттєво поступається у показниках, адже займає лише 79 місце зі 176 країн з індексом 5.62 [6].

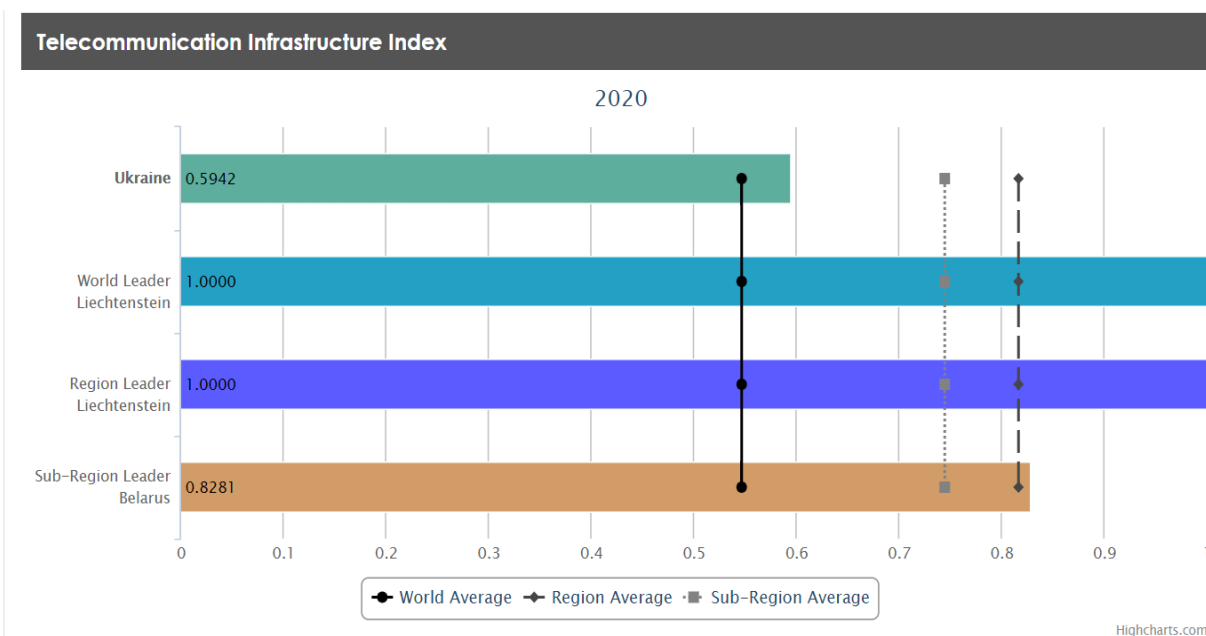


Рис.3

- за показником *Людський капітал (Human Capital Index)* Україна знаходиться у дещо ліпшій ситуації, адже має 0,8591 пунктів із можливих 1,0000, рис.4.

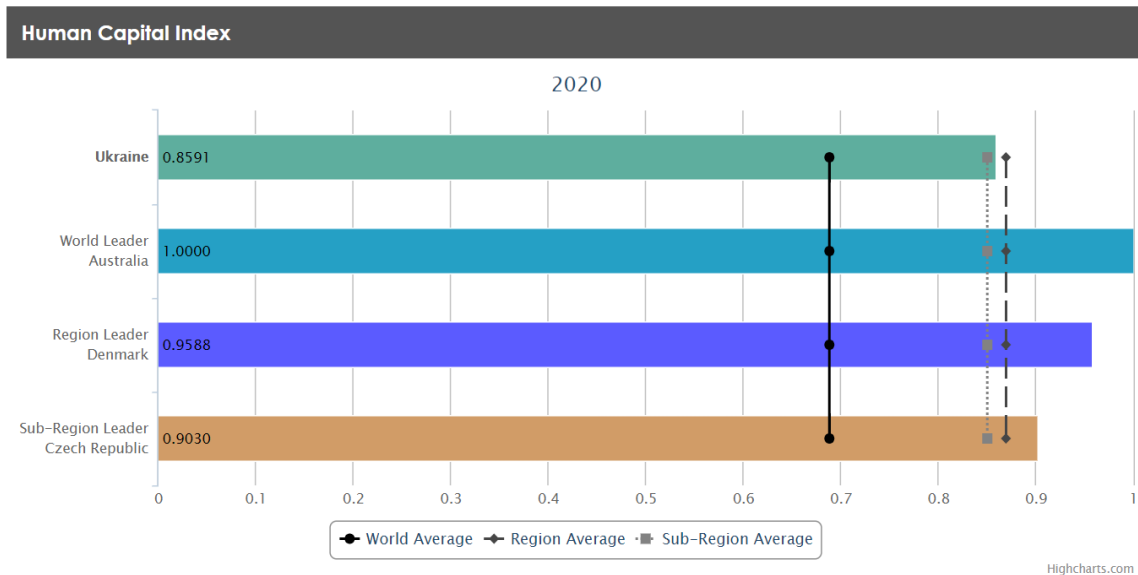


Рис.4

Враховуючи те, що значення Індексу розвитку електронного урядування розраховується як середнє арифметичне трьох його показників (підіндексів) – ІКТ-інфраструктури, людського капіталу та електронних державних послуг, відставання хоча б за одним із них суттєво погіршує показники України в цілому.

Як впливає із вищевказаного, Україна значно піднялась за показниками електронного урядування у 2020 році, у тому числі завдяки впровадженню низки практичних заходів у сфері електронного урядування, а саме:

- створенню у 2019 році профільного міністерства – Міністерства цифрової трансформації, яке є центральним органом виконавчої влади, що відповідає за формування та реалізацію державної політики у сфері цифровізації, відкритих даних, національних електронних інформаційних ресурсів, інтероперабельності – взаємодії мережевих систем на базі уніфікованих інтерфейсів або протоколів, впровадження електронних послуг та розвиток цифрової грамотності громадян;

- прийняттю низки нормативно-правових актів, необхідних для регулювання цієї сфери, зокрема:

- Концепції розвитку системи електронних послуг в Україні, схваленої Розпорядженням Кабінету Міністрів України від 16 листопада 2016 р. за № 918-р, метою якої є визначення напрямів, механізму і строків формування ефективної

системи електронних послуг в Україні для задоволення інтересів фізичних та юридичних осіб через розвиток і підтримку доступних та прозорих, безпечних та некорупційних, найменш затратних, швидких та зручних електронних послуг [7];

- *Плану заходів щодо реалізації Концепції розвитку системи електронних послуг в Україні на 2019-2020 роки*, затвердженого Розпорядженням Кабінету Міністрів України від 30 січня 2019 р. № 37-р, за яким передбачено: визначення оновленого переліку послуг для першочергового впровадження їх надання в електронній формі відповідно до суспільних потреб; забезпечення впровадження надання пріоритетних послуг в електронній формі; забезпечення реалізації принципу єдиного вікна («one-stop-shop») для надання електронних послуг фізичним та юридичним особам; модернізація наявних та створення нових веб-порталів (офіційних веб-сайтів суб'єктів владних повноважень), через які надаються електронні послуги (сервіси), відповідно до єдиних вимог для розроблення, ведення та інтеграції (взаємодії) офіційних веб-сайтів суб'єктів владних повноважень; інтеграція веб-порталів (офіційних веб-сайтів суб'єктів владних повноважень), через які надаються електронні послуги (сервіси) з інтегрованою системою електронної ідентифікації та автентифікації; розроблення пропозицій щодо оптимізації (об'єднання) надання послуг «За життєвими та бізнес-ситуаціями» тощо [8];

- *Указу Президента України «Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг»* від 29 липня 2019 року за № 558/2019, згідно з яким затверджено ряд необхідних заходів, спрямованих на забезпечення належного функціонування та захисту даних у національних електронних інформаційних ресурсах, доступності та зручності електронних послуг для фізичних та юридичних осіб, а також запобігання корупції під час надання таких послуг [9];

- *Постанови Кабінету Міністрів України «Деякі питання цифрового розвитку»* від 30 січня 2019 р. № 56, якою визначено засади реалізації органами виконавчої влади принципів державної політики цифрового розвитку [10];

- *Закону України «Про електронні довірчі послуги»*, яким визначено правові та організаційні засади надання електронних довірчих послуг, правові та організаційні засади здійснення електронної ідентифікації [11];

- *Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг*, затвердженого Постановою Кабінету Міністрів України від 18 грудня 2018 р. № 1215, який встановлює механізм проведення

процедури оцінки відповідності вимогам до кваліфікованих надавачів електронних довірчих послуг та послуг, що ними надаються [12];

- *Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності*, затвердженого Постановою Кабінету Міністрів України від 19 вересня 2018 р. № 749, який визначає вимоги щодо використання, у тому числі отримання, кваліфікованих електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності із використанням працівниками державних установ засобів кваліфікованого електронного підпису [13];

- *Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування*, затверджених Наказом Державного агентства з питань електронного урядування України від 27 листопада 2018 року за № 86 [14];

- *Постанови Кабінету Міністрів України «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів»* від 10 травня 2018 р. № 357, яка встановлює Порядок, який визначає механізм організації електронної інформаційної взаємодії державних електронних інформаційних ресурсів [15];

- *організації надання електронних публічних послуг* через Єдиний державний портал адміністративних послуг (<https://my.gov.ua/>), а також через Єдиний державний веб-портал електронних послуг «Портал Дія» (<https://diia.gov.ua/>), на якому нині доступними є 27 публічних послуг онлайн [https://zn.ua/ukr/TECHNOLOGIES/diya-proponuye-koristuvacham-27-poslug-343453_.html].

Висновки. Попри впровадження вищевказаних кроків, доводиться констатувати про низькі темпи їх реалізації в Україні, що підтверджується останніми показниками Індексу розвитку електронного урядування.

На жаль, в Україні так і не було прийнято профільного *Закону України «Про публічні електронні реєстри»*, яким би було якісно врегульовано правовідносини у сфері створення, функціонування та інформаційної взаємодії державних, комунальних та інших реєстрів, кадастрів та інформаційних систем.

Зважаючи на те, що Україна у 2020 році в цілому продемонструвала позитивну динаміку щодо впровадження заходів електронного урядування, зокрема електронних публічних послуг, подальше сповільнення темпів їх

реалізації може призвести до суттєвої втрати позицій України на міжнародній арені.

Також зазначимо, що паралельне функціонування кількох веб-порталів публічних послуг з одного боку покращує доступ фізичних та юридичних осіб до них, однак з іншого, створює деякою мірою плутанину для користувачів, і замість існування уніфікованого державного веб-порталу електронних послуг, де було б зосереджено усі електронні публічні послуги (як адміністративні, так і ті, що можуть надавати державні й недержавні установи), такі послуги досі розосереджуються по різних веб-платформам.

ЛІТЕРАТУРА

1. Електронне урядування та електронна демократія. Навчальний посібник, 2017, ч. 1. Вступ до курсу. Концептуальні засади електронного урядування та електронної демократії. – [Електронний ресурс]. – Режим доступу: <https://egap.in.ua/biblioteka/e-uriaduvannia-ta-e-demokratii-a-navchalnyi-posibnyk/>.
2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#n8>.
3. Електронне урядування та електронна демократія. Навчальний посібник, 2017, ч. 10. Електронні послуги. – [Електронний ресурс]. – Режим доступу: <https://egap.in.ua/biblioteka/e-uriaduvannia-ta-e-demokratii-a-navchalnyi-posibnyk/>.
4. Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020). Концептуальні засади (версія 1.0). Hi-Tech Office Ukraine. – [Електронний ресурс]. – Режим доступу: <https://ucco.org.ua/uploads/files/58e78ee3c3922.pdf>.
5. E-Government Development Index. – [Електронний ресурс]. – Режим доступу: <https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukraine/dataYear/2020>.
6. ICT Development Index. – [Електронний ресурс]. – Режим доступу: <https://gtmarket.ru/ratings/ict-development-index>.
7. Про схвалення Концепції розвитку системи електронних послуг в Україні : розпорядження Кабінету Міністрів України від 16 листопада 2016 р. № 918-р. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/918-2016-%D1%80#Text>.
8. Про затвердження плану заходів щодо реалізації Концепції розвитку системи електронних послуг в Україні на 2019-2020 роки : розпорядження

Кабінету Міністрів України від 30 січня 2019 р. № 37-р. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/37-2019-%D1%80#Text>.

9. Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг : указ Президента України від 29 липня 2019 року № 558/2019. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/558/2019#Text>.

10. Деякі питання цифрового розвитку : постанова Кабінету Міністрів України від 30 січня 2019 р. № 56. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text>.

11. Про електронні довірчі послуги : закон України від 5 жовтня 2017 року № 2155-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 400.

12. Про затвердження Порядку проведення процедури оцінки відповідності у сфері електронних довірчих послуг : постанова Кабінету Міністрів України від від 18 грудня 2018 р. № 1215. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1215-2018-%D0%BF#Text>.

13. Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності : постанова Кабінету Міністрів України від 19 вересня 2018 р. № 749. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/749-2018-%D0%BF#Text>.

14. Про встановлення Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування : наказ Державного агентства з питань електронного урядування України від 27.11.2018 № 86. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z1462-18#Text>.

15. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів : постанова Кабінету Міністрів України від від 10 травня 2018 р. № 357. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/357-2018-%D0%BF#Text>.

16. На порталі «Дія» вже можна отримати 27 публічних послуг онлайн. – [Електронний ресурс]. – Режим доступу: https://zn.ua/ukr/TECHNOLOGIES/diya-proponuye-koristuvacham-27-poslug-343453_.html.

Поліщук Д.О.

Факультет інформаційних технологій

Київського національного університету ім. Т. Шевченка,

м.Київ

polishchukdaria@gmail.com

«ВЕБ-СЕРВІС ІЗ ПІДТРИМКИ ДІЯЛЬНОСТІ КІНОТЕАТРУ»

У тезі розглянуто поняття, місце та роль веб-сервісів із підтримки діяльності кінотеатру, визначено їх переваги, описано запропоноване програмно-технологічне рішення.

The thesis considers the concept, place and role of a web service to support cinema activities, identifies their advantages, described proposed software and technological solution.

Ключові слова: веб-сервіс, кінотеатр, сфера розваг, купівля квитків, API, SPA

Keywords: web service, cinema, entertainment, buying tickets, API, SPA

Розваги в наш час вважають найважливішою частиною повсякденного життя сучасної людини. Вони, поряд з освітою, мають можливість вагомо впливати на загальні положення в суспільстві. Звісно, активна інноваційна діяльність не є виключенням і в такій сфері розваг як кінотеатр.

Зараз інновації мають помітний внесок у зміцнення позицій сервісної діяльності, підвищенню конкурентоспроможності послуг серед інших сфер. Інноваційний розвиток сфери розваг дозволяє задовольняти потреби суспільства, підвищуючи якість і рівень життя. Сталий розвиток країни залежить від її економічних перспектив. А на них, у свою чергу, впливають новітні розробки, в тому числі і в індустрії розваг. Інтелектуальна діяльність, завдяки якій відбуваються поліпшення в виробничо-технічному, організаційному і соціально-економічному напрямках розваг, стає найважливішим ресурсом людського прогресу.

Нині в Україні маємо достатній вибір кінотеатрів – від малих до великих. Багато з них вже зараз пропонують своїм відвідувачам скористатись найсучаснішими технологіями та відчутти переваги інновацій у цій сфері. Найважливішими перевагами наявних рішень є :

- цілодобова підтримка і постійний сервіс на місцевому рівні;
- оперативність реагування та увага до користувачів;
- одночасна робота з різними формами оподаткування;
- автоматичне отримання звітів про продані квитки за зміну, готівкової / безготівкової виручки;
- автоматичне отримання будь-якої довідкової інформації за кількістю замовлених місць, придбаними квитками, касирам, знижкам тощо;
- продуманий, зручний і інтуїтивно зрозумілий інтерфейс;
- розгалужена звітність та аналітика за багатьма параметрами, що забезпечує підтримку прийняття рішень.

Пропоноване мною рішення – це веб-сервіс, призначений для використання у кінотеатрах. Він допомагає автоматизувати та підтримувати роботу кінотеатру, що надає змогу збільшити попит на використання веб-сервісів для кінотеатрів за рахунок доступності та простоти впровадження цього веб-сервісу, тому що він можливий для швидкого розгортання різними кінотеатрами, а також є можливість доопрацювання унікального дизайну для користувачів.

У зв'язку з підтримкою життєдіяльності кінотеатру потребує функціонування клієнтських застосунків, що забезпечують можливість здійснення онлайн-вибору та купівлі квитків у кінотеатр, та системи адміністрування, створений веб-сервіс містить блок публічного API, що дозволяє здійснювати інтеграцію з ним у вигляді створених веб-застосунків або мобільних застосунків, а також систему адміністрування, що створена з використанням мови програмування JavaScript та клієнтської бібліотеки React у парадигмі SPA-застосунку. Ця парадигма дозволяє здійснювати перехід між веб-сторінками без

повного перезавантаження сторінки, а також уникати потреби у повторному завантаженні виконуваних клієнтських файлів у веб-браузер, що є перевагою вказаного рішення.

Список використаної літератури

1. Business plan for implementation in E-Square Entertainment and Movie Theater – [Електронний ресурс]. – Режим доступу: <https://www.slideshare.net/SHAURYAZZZZZZZZZZ/business-plan-to-launch-movie-theater>
2. James Snell Programming Web Services with SOAP / James Snell, Doug Tidwell, PavelKulchenko. – Publisher: O'Reilly MediaReleased: December 2001Pages: 264.
3. SaleTicket – [Електронний ресурс]. – Режим доступу: http://salesoft.com.ua/About_ST.html

УДК 336:1

Прокопенко Н.О.

аспірант відділу економіко-математичного моделювання та інформаційно-аналітичного забезпечення фінансово-економічних досліджень НДФІ «Академія фінансового управління», e-mail: Nadjezhda@ukr.net

Інформаційні технології в системі середньострокового бюджетного планування України

Процес складання проекту бюджету України та місцевих бюджетів неможливий без використання сучасних інформаційних технологій, а також інтегрованих прикладних інформаційних систем, які мають великі бази даних щодо планових і фактичних показників виконання бюджету за минулі періоди, а

також сукупність довідників щодо переліку державних програм, бюджетні класифікатори (наприклад, відомча, економічна та функціональна класифікації доходів і видатків бюджету), сукупність довідників для формування бюджету тощо. Підвищення рівня автоматизації процесів в бюджетному процесі та впровадження новітніх інформаційних технологій – є пріоритетним завданням уряду, адже, завдяки цьому можна досягнути прозорої системи моніторингу, контролю, звітності у бюджетному процесі, а також досягнути точнішого планування в подальшому.

Застосування інформаційних технологій призначено для створення бюджетних документів, оброблення даних, автоматичного формування аналітичної звітності на основі великих даних, що відображають динаміку показників бюджету у часовому вимірі та покращення обміну інформацією між учасниками бюджетного процесу.

Найбільш інтенсивний інформаційний обмін відбувається з Державною казначейською службою, зокрема, відправляються файли з інформацією про розпис бюджету, граничні обсяги видатків, а також зміни до них, у зворотному напрямку надається інформація про фактичні показники виконання бюджету на місцевому рівні, бюджетні запити, паспорти бюджетних програм і звіти про їх виконання.

Державна аудиторська служба надає Міністерству фінансів України інформацію про витрати бюджетних коштів не за призначенням або з порушенням бюджетного законодавства, а також визначає стягнення до державного бюджету при виявленні порушень.

Державна податкова служба надає Міністерству фінансів України показники податкової звітності платників податків та дані про стан розрахунків зі сплати податків, зборів та обов'язкових платежів.

Державна митна служба надає Міністерству фінансів інформацію про фактичне надходження доходів до державного бюджету, які включають митні збори, та дані про експортні та імпорتنі операції по основних товарних групах.

Міністерство розвитку економіки, торгівлі та сільського господарства надає Міністерству фінансів України планові показники економічного розвитку України в цілому та її регіонів зокрема, а також фактичні значення цих показників. За цими матеріалами Міністерство фінансів України здійснює розроблення стратегії розвитку бюджетної політики. З Верховною Радою України та Кабінетом Міністрів України проводиться обмін нормативними та аналітичними документами, які використовують при управлінні державними фінансами.

Головним розпорядникам бюджетних коштів (ГРБК) надаються граничні обсяги видатків державного бюджету. У свою чергу розпорядники надають Міністерству фінансів проект плану витрат коштів за бюджетними програмами, який потім узгоджується в Міністерстві фінансів та повертається головному розпорядникам. На рис.1 зображено схему інформаційних потоків у системі середньострокового бюджетного планування України.

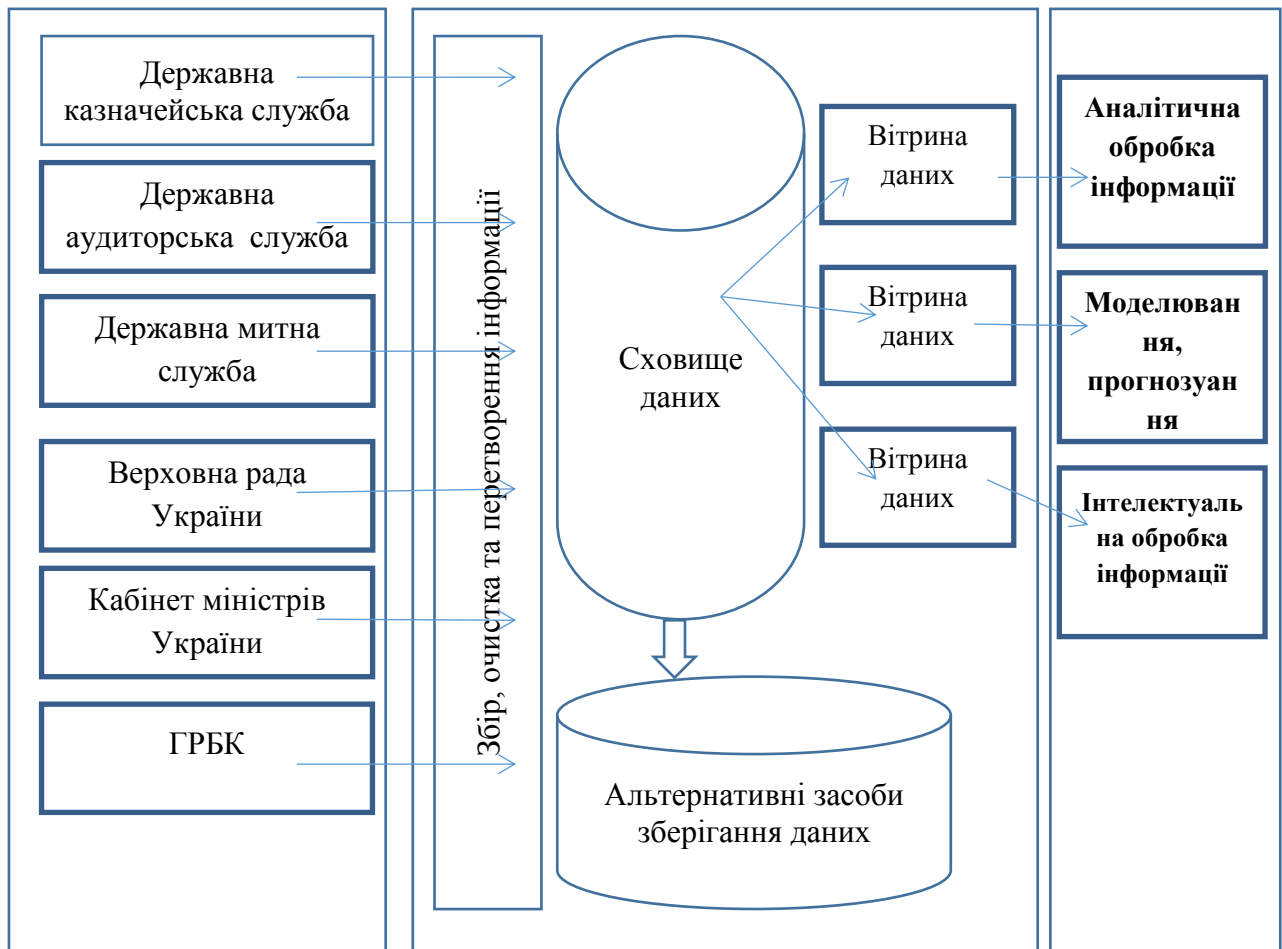


Рис.1 Інформаційні потоки у системі середньострокового бюджетного планування

За допомогою інформаційно-аналітичних систем Міністерства фінансів України можливо здійснити:

1. аналіз поточного рівня базових витрат, їх розподілу між напрямками та сферами витрат в розрізі ГРБК, аналіз розподілу витрат у рамках 3 видів класифікації бюджету, зокрема, програмної, функціональної та відомчої;
2. визначення планових витрат, які будуть мають разовий і не постійний характер у плановому періоді;
3. оцінку вартісних критерії, що будуть впливати на суму витрат державних послуг та соціального забезпечення (затверджені нормативи, як наприклад мінімальна заробітна плата, прожитковий мінімум, тарифна сітка тощо)

4. оцінку кількісних параметрів, які відповідно будуть впливати на суму державних витрат (демографічні прогнози, зміна рівня безробіття населення).
5. перевірку та коригування прогнозних показників за результатами актуалізації вихідної інформації, вдосконалення моделей оцінок.

Отже, система середньострокового бюджетного планування потребує узгодження та оброблення великих даних, яка надходить із багатьох державних органів. Для досягнення більшої точності та узгодження бюджетного плану країни із іншими прогнозами, наприклад соціально-економічного розвитку, демографічними прогнозами, прогнозами підтримання національної безпеки тощо необхідно досягнути можливості автоматичної перевірки відповідності показників різних сфер державного планування із бюджетним плануванням. Саме тому удосконалення інформаційно-аналітичних систем Міністерства фінансів України, у напрямку технічної можливості оброблення та порівняння показників стратегічних документів різних відомств, а також удосконалення процесу моделювання, через який можна відслідковувати не тільки бюджетну модель, а функціональний вплив інших прогнозів на бюджетні показники планового періоду.

Список використаних джерел:

1. Про затвердження Концепції діяльності Інформаційно-аналітичного центру Міністерства фінансів України: Наказ Міністерства фінансів України від 29.05.2004 N 364 – [Електронний ресурс]. – Режим доступу: [/https://zakon.rada.gov.ua/rada/show/v0364201-04#Text](https://zakon.rada.gov.ua/rada/show/v0364201-04#Text);
2. Про затвердження Концептуальної архітектури інформаційно-аналітичної системи Міністерства фінансів України: Наказ Міністерства фінансів України від 05.10.2004 N 630 – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0630201-04#Text>;
3. Стратегія реформування системи управління державними фінансами на 2017-2020 роки: Розпорядження Кабінету Міністрів України від 08.02.2017р. №142-р –

Електронний ресурс]. – Режим доступу:
<https://www.kmu.gov.ua/ua/npas/249797370>;

4. Плєскач В.Л. Інноваційні механізми стратегії фінансового управління: колективна монографія у 3-х т. / ДННУ «Акад. фін. управління» : за заг. ред. М.Я. Азарова. – К., 2013. – С. 384–428.

Пяташова Е. С.

*Київський національний університет ім. Тараса Шевченка, м.Київ
e.piatashova@gmail.com*

РОЗУМНА МЕРЕЖА. ПИТАННЯ ЩОДО КІБЕРБЕЗПЕКИ.

This article contains a short description of vulnerabilities and attacks related to smart-grid security.

Key words: *smart grids, smart grid security, smart grid vulnerabilities, smart grid threats.*

Традиційна електромережа в даний час перетворюється на інтелектуальну. Розумна мережа інтегрує в традиційну електричну мережу інформаційно-комунікаційні технології (ІКТ). Така інтеграція розширює можливості постачальників та споживачів електромереж, покращує ефективність та доступність енергосистеми, постійно контролюючи та керуючи потребами споживачів. Розумна мережа - це величезна складна мережа, що складається з мільйонів пристроїв та об'єктів, пов'язаних між собою. Вона використовує датчики, моніторинг, зв'язок, автоматизацію і комп'ютери для підвищення гнучкості, безпеки, надійності, ефективності та безпеки мережі. Така масивна мережа має безліч проблем безпеки та вразливостей.

Безпека залишається однією з найважливіших проблем у системах інтелектуальних мереж, враховуючи небезпеку та незручності, з якими можуть зіткнутися жителі та компанії, якщо мережа потрапить під атаку. Три основні цілі безпеки повинні бути включені в систему інтелектуальної мережі:

1. Наявність безперебійного живлення відповідно до вимог користувача
2. Цілісність переданої інформації
3. Конфіденційність даних користувача.

Щоб боротися з цими ризиками, треба зрозуміти, що таке «розумна мережа», як вона побудована, наскільки вона вразлива, і як ці уразливості можна мінімізувати і пом'якшити.

Системи “розумної мережі”, як правило, можна розділити на такі, що регулюють виробництво електроенергії, розподіл та передачу електроенергії, а також моніторинг електроенергії (наприклад, з домашніми лічильниками)

Основними системними компонентами інтелектуальної мережі є електрична побутова техніка, поновлювані джерела енергії, розумний лічильник, центр експлуатації електричних мереж та постачальники послуг

Розумна мережа включає в себе два типи зв'язку: домашня мережа (LAN) і широкопasmова мережа (WAN). LAN з'єднує домашні смарт-пристрої із смарт-лічильником. Мережа може спілкуватися за допомогою Zigbee, дротового або бездротового Ethernet або Bluetooth. WAN, навпаки, є більшою мережею, яка з'єднує розумні лічильники, постачальників послуг та електричну мережу. WAN може спілкуватися за допомогою WiMAX, 3G / GSM / LTE або волоконної оптики. Розумний лічильник діє як шлюз між внутрішніми пристроями та зовнішніми сторонами для надання необхідної інформації. Електрична мережа управляє розподілом електроенергії в інтелектуальній мережі, збирає споживане споживання електроенергії від розумних лічильників та надсилає повідомлення до інтелектуальних лічильників, коли це потрібно. Розумний лічильник приймає повідомлення від пристроїв у HAN та надсилає їх відповідному постачальнику послуг.

Використання мережі завжди несе за собою виклики безпеки. Вразливості, що є найбільш серйозними в інтелектуальних мережах:

1. Вразливості безпеки клієнта. Розумні лічильники автономно збирають величезні обсяги даних і передають їх комунальному підприємству, споживачеві та постачальникам послуг. Ці дані включають інформацію про приватних споживачів, яка може бути використана для висновку про діяльність споживача, використовувані пристрої та час, коли будинок вільний.

2. Вразливості фізичної безпеки. На відміну від традиційної енергосистеми, мережа інтелектуальних мереж включає багато компонентів, і більшість з них знаходяться поза приміщеннями комунального підприємства. Цей факт збільшує кількість небезпечних фізичних місць і робить їх вразливими до фізичного доступу.

3. Термін служби енергосистем. Оскільки енергосистеми співіснують із відносно нетривалими ІТ-системами, неминуче застаріле обладнання все ще

експлуатується. Це обладнання може діяти як слабкі точки безпеки і цілком може бути несумісним із поточними пристроями енергосистеми.

4. Неявна довіра між традиційними пристроями живлення. Зв'язок між пристроями в системах управління є вразливим до підробки даних, коли стан одного пристрою впливає на дії іншого. Наприклад, пристрій, що надсилає помилковий стан, змушує інші пристрої поводитись небажано.

5. Використання Інтернет-протоколу (IP), комерційного готового обладнання та програмного забезпечення. Використання стандартів IP у розумних мережах дає велику перевагу, оскільки забезпечує сумісність між різними компонентами. Однак пристрої, що використовують IP, за своєю суттю вразливі до багатьох мережевих атак на основі IP, таких як спуфінг IP, Tear Drop, Denial of Service та інші.

6. Наявність багатьох зацікавлених сторін. Може призвести до інсайдерських атак.

Щойно згадані вразливості можуть бути використані зловмисниками з різними мотивами та знаннями та можуть завдати мережі різного збитку. Ці зловмисники можуть спричинити широкий спектр атак, класифікованих за трьома основними категоріями: компонентно, протокольно та топологічно.

Компонентні атаки націлені на польові компоненти, що включають віддалений термінал (RTU). RTU традиційно використовуються інженерами для віддаленого налаштування та усунення несправностей пристроїв інтелектуальної мережі. Ця функція віддаленого доступу може бути піддана атаці, яка дозволяє зловмисним користувачам контролювати пристрої та видавати дефекти, такі як вимкнення пристроїв.

Протокольні атаки націлені на сам протокол зв'язку за допомогою таких методів, як зворотна інженерія та введення помилкових даних.

Топологічні атаки націлені на топологію інтелектуальної мережі, запускаючи атаку відмови в обслуговуванні (DoS), яка заважає операторам мати повний огляд енергосистеми, що спричиняє прийняття невідповідних рішень.

Інші найбільш поширені атаки включають в себе:

1. Поширення шкідливого програмного забезпечення. Зловмисник може розробляти шкідливе програмне забезпечення та поширювати його, щоб заразити розумні лічильники або сервери компанії. Шкідливе програмне забезпечення може бути використано для заміни або додавання будь-якої функції на пристрій або систему.

2. Доступ через посилання на базу даних. Системи управління реєструють свою діяльність у базі даних у мережі систем управління, а потім дзеркально

відображають журнали у бізнес-мережі. Якщо системи управління базами даних неправильно налаштовані, кваліфікований зловмисник може отримати доступ до бази даних бізнес-мережі, а потім використовувати свої навички для використання мережі системи управління.

3. Впорскування неправдивої інформації. Зловмисник може надсилати пакети, щоб вводити в мережу неправдиву інформацію, таку як неправильні дані лічильників, помилкові ціни, підроблені надзвичайні події тощо. Підроблена інформація може мати величезний фінансовий вплив на ринки електроенергії.

4. Доступність мережі. Оскільки інтелектуальна мережа використовує протокол IP та стек TCP / IP, вона стає предметом DoS-атак та вразливостей, властивих стеку TCP / IP. DoS-атаки можуть спробувати затримати, заблокувати або пошкодити передачу інформації, щоб зробити недоступними ресурси інтелектуальної мережі.

5. Підслуховування та аналіз трафіку. Суперник може отримати конфіденційну інформацію, контролюючи мережевий трафік. Приклади моніторингової інформації включають інформацію про майбутні ціни, структуру управління мережею та споживання енергії.

Оскільки розумна мережа вважається критично важливою інфраструктурою, слід виявити всі вразливі місця та впровадити достатні рішення для зменшення ризиків до прийняттого безпечного рівня.

Висновки:

Завдяки належній обізнаності щодо кіберзагроз, яке становить широке використання і впровадження «розумних мереж», можна безпечно пристосувати «розумну мережу» до адаптації до різних умов; і про це слід в основному подбати як на етапі планування, так і на етапі експлуатації для надійної, оптимізованої, надійно захищеної та стійкої системи електронежі.

ЛІТЕРАТУРА

1. Eric D. Knapp and Raj Samani, Applied Cyber Security and the Smart Grid Implementing Security Controls into the Modern Power Infrastructure.
2. A. R. Al-Alia, Rami Al-Dalkya, Mamoun Al-Mardinia and Wassim El-Hajjb, Smart Grid Security: Threats, Vulnerabilities and Solutions Fadi Aloula
3. Abdulrahman Okino Otuoze, Mohd Wazir Mustafa, Raja Masood Larik, Smart grids security challenges: Classification by sources of threats.

Пурський О.І., Кузнецов О.Ф., Медяник В.В.

Київський національний торговельно-економічний університет, м. Київ

Pursky_O@ukr.net, Alexandrfrk@ukr.net,

v_medyanyk_foais_17_10_b_d@knu.edu.ua

СПЕЦИФІКА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ WEB-СИСТЕМИ ОЦІНЮВАННЯ РІВНЯ РЕГІОНАЛЬНОГО РОЗВИТКУ

The software implementation of the Web-system for evaluating the level of socio-economic development of the regions of Ukraine has been implemented and the technology of its use has been developed. Modern software was chosen as tools for Web-application implementation: database - MySQL, software platform - Microsoft Silverlight 5.0 and C # programming language. Important aspects of the developed Web-system are automation of all settlement procedures and support of the computer network Internet which provides access to all its resources of territorially distributed users.

Keywords: *Web-system, socio-economic development, region, integrated indicator, factor analysis, expert evaluation.*

Програмна реалізація Web-системи оцінювання рівня соціально-економічного розвитку здійснена на основі алгоритму визначення інтегральних показників соціально-економічного розвитку представленого в попередній нашій роботі [1]. Алгоритм ґрунтується на спільному використанні статистичних методів факторного та методу експертного оцінювання. Характерною особливістю представленого алгоритму розрахунку інтегральних показників соціально-економічного розвитку є автоматизація механізму експертного оцінювання [2]. Даний алгоритм є основою функціонування Web-системи, розробленої з метою забезпечення доступу до функцій моніторингу показників соціально-економічних розвитку і використання в системі регіонального управління. Важливими аспектами розробленої Web-системи є автоматизація всіх розрахункових процедур та підтримка роботи в комп'ютерній мережі Internet, що забезпечує доступ до всіх її ресурсів територіально розподілених користувачів [3]. Варто також зазначити, що інтерфейс Web-додатку реалізовано у двох версіях: україномовний і англійськомовний варіанти. До складу Web-додатку входять наступні функціональні блоки:

- модуль аутентифікації користувача;

- база даних, що призначена для зберігання показників і результатів розрахунків предметної області, а також інформаційного наповнення елементів інтерфейсу Web-додатку;
- блок, що реалізує функції математичної моделі предметної області;
- шлюз для забезпечення взаємодії між Web-додатком і базою даних;
- інтерфейс, що забезпечує доступ до функцій веб-додатка.

Модуль аутентифікації користувача. Даний модуль забезпечує функціональне розмежування доступу до елементів управління Web-додатком і його ресурсів, відповідно до ролі користувача, а також здійснює перевірку коректності введених користувачем реєстраційних даних. Для доступу до функцій додатка необхідно ввести E-mail і пароль, що видаються адміністратором додатка. Також передбачена можливість доступу до базових функцій додатка в демонстраційному режимі. Даний модуль здійснює перевірку на відповідність введених користувачем даних із записами, що зберігаються у БД. У випадку коректного введення даних, модуль надає доступ до функціоналу і ресурсів Web-додатку відповідно до рівня доступу користувача, заданого адміністратором.

База даних: при розробці концептуальної моделі предметної області були визначені її сутності та взаємозв'язки між ними. Кожна сутність при розробці бази даних перетворюється в таблицю, кожному атрибуту сутності відповідає поле в таблиці бази даних.

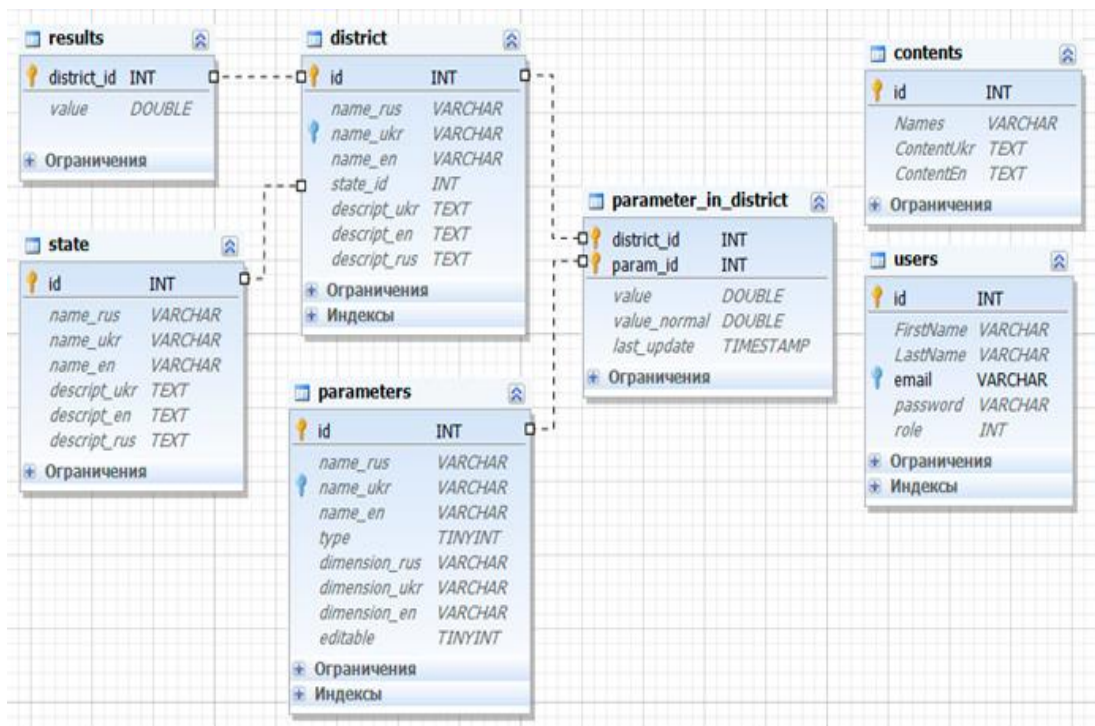


Рис. 1. Схема бази даних Web-додатку [3].

На рис. 1 представлена модель бази даних, яка використовується для визначення інтегральних показників соціально-економічного розвитку регіонів. Проектування масивів даних передбачає визначення їх складу, змісту, структури і вибір раціонального способу їх подання. База даних розроблена з використанням СУБД MySQL [4].

Програмну реалізацію математичної моделі розрахунку інтегральних показників соціально-економічного розвитку регіонів здійснено на мові програмування C#. Шлюз для забезпечення зв'язку із базою даних являє собою php-Інтерфейс, що забезпечує генерацію запитів до БД і формування результатів запитів [4, 5]. Зв'язок Web-додатку і php-шлюзу здійснюється за http-протоколом. На підставі параметрів методу GET http-протоколу формуються відповідні запити до БД [5]. Результуючі вибірки серіалізуються у форматі *.JSON, для передачі у Web-додаток [6]. При необхідності зберегти дані в БД, Web-додаток формує об'єкт у форматі *.JSON, в php-шлюзі відбувається десеріалізація об'єкта, отриманого методом POST http-протоколу, а також формування відповідних запитів до БД (REPLACE або UPDATE) [6, 7]. Інтерфейс Web-додатку реалізований на програмній платформі Microsoft Silverlight [8], і містить у собі наступні модулі: елементи управління, що забезпечують ідентифікацію користувача, верифікацію введених даних і надання доступу до функцій Web-додатку, відповідно до рівня доступу користувача; елемент управління, що забезпечує вибір мови (українська або англійська) Web-додатка; інтерактивне графічне представлення областей України (карта) із забезпеченням можливості вибору окремого регіону; блок відображення інформації про обраний регіон; модуль для одержання й редагування соціально-економічних показників для конкретного регіону, а також для активізації розрахунків інтегральних показників з виведенням проміжних результатів розрахунків; блок відображення результатів розрахунків інтегральних показників та кореляцій між соціально-економічними показниками у вигляді таблиць і діаграм; модуль адміністрування для додавання й редагування контенту Web-додатку і даних користувачів системи.

Додаток розрахований на роботу із трьома групами користувачів (адміністратори, редактори даних і звичайні користувачі) та забезпечує доступ до елементів управління залежно від рівня доступу конкретного користувача. Web-додаток реалізовано з використанням паттерну MVVM (Model-View-ViewModel). Структурна схема Web-додатку представлена на рис 2.

Для забезпечення функціонування Web-додатку на стороні сервера необхідна наявність: Apache 1.3 і вище або MS IIS 6.0 і вище; PHP 5.3 і вище; MySQL 5.1 і вище. На клієнтській машині потрібна наявність плагіна Microsoft

Silverlight для браузера, інсталяцію якого необхідно підтвердити при першому зверненні до сервера Web-додатку.



Рис. 2. Структурна схема розробленого Web-додатку [3].

ЛІТЕРАТУРА

1. Pursky, O. Computation algorithm for integral indicator of socio-economic development / O. Pursky, T. Dubovyk, I. Gamova, I. Buchatska // CEUR Workshop Proceedings – 2019. – Vol. 2393. – P. 919–934.
2. Мороз І.О. Визначення інтегральних показників соціально-економічного розвитку регіонів на основі експертних оцінок та методу головних компонент / О.І. Пурський, І.О. Мороз // Проблеми економіки. – 2013. – №2. – С. 230-236
3. Пурський О.І. Моніторинг соціально-економічного розвитку регіону: монографія / О.І. Пурський, О.А. Харченко, І.О. Мороз – К.: КНТЕУ, 2017. – 180 с.
4. Delaney K. SQL Server MVP Deep Dives/K. Delaney.–Manning Public, 2011.–688 р.
5. Котеров Д. PHP 5 в подлиннике / Д. Котеров, А. Костарев. – БХВ-Петербург, 2008. – 1104 с.
6. Белл Ч. Обеспечение высокой доступности систем на основе MySQL / Ч. Белл, М. Киндал, Л. Талманн: Пер. с англ. — М.: Изд-во «Русская редакция» 2012. – 624 с.
7. Suehring S. MySQL bible / S. Suehring. – NY.: Wiley Publishing Inc., 2002. – 686 p.

8. MacDonald M. Silverlight and ASP.NET Revealed / M. MacDonald. – Apress, 2007.
– 50 p.

Рогущина Ю.В.

*Інститут програмних систем НАН України, Київ,
Ladamandraka2010@gmail.com*

КІЛЬКІСНІ ОЦІНКИ СЕМАНТИЧНОЇ ПОДІБНОСТІ МІЖ ПОНЯТТЯМИ ПРЕДМЕТНОЇ ОБЛАСТІ ЯК ЗАСІБ МОДЕЛЮВАННЯ ІНТЕРЕСІВ КОРИСТУВАЧА

We propose to use semantic similarity estimation values proposed by user as a source of information about domain relevant to his/her interests. We consider various domain ontologies and search such one where semantic distances between concepts are more similar to user beliefs. Selected ontology is added to user profile and then can be used in various intelligent tasks such as information retrieval,

Keywords: *Semantic similarity, ontology, user profile.*

Вступ. В роботі аналізуються можливості використання мір семантичної подібності як засобу моделювання сфери інтересів користувача. У першому розділі розглядаються існуючі підходи до побудови множин семантично подібних понять (СПП) та параметри, на основі яких обчислюються семантичні відстані між поняттями. Основна увага приділяється онтологічному підходу та мірам, що використовують не тільки таксономічні зв'язки між поняттями, а враховують семантику відношень та подібність між властивостями понять. В другому розділі розглянуто проблеми, які виникають в процесі побудови СПП, яка адаптована до потреб окремого користувача. В третьому розділі запропоновано джерела інформації, які можуть бути зрозумілі користувачеві та придатні для автоматизованої генерації СПП. Запропоновано методи побудови таких персоніфікованих множин СПП на основі семантизованих Wiki-ресурсів.

Постановка задачі. Профілювання користувача та формальне відображення сфери його інформаційних інтересів є важливою складовою персоніфікованої обробки інформації в інтелектуальних системах. Виникає необхідність у розробці об'єктивних та автоматизованих методів відбору джерел знань (онтологій), що відповідають індивідуальним уявленням та потребам користувача. Для цього пропонується використовувати механізми семантичної подібності між поняттями предметної області (ПрО), які містяться в тезаурусі задачі користувача, та кількісні оцінки, що використовуються для їх оцінювання. Основна проблема полягає в тому, щоб на основі онтології ПрО, яка моделює знання про цю ПрО, побудувати тезаурус задачі – простішу для обробки модель того фрагменту ПрО,

що стосується певної поточної задачі користувача. *Тезаурус задачі* – це набір понять, для яких користувачем явно визначена семантична відстань до ключових слів запиту. Задачу користувача характеризують ПрО, для моделювання знань якої застосовуються онтології, та природномовний опис, який виокремлює певну підмножину цієї ПрО. Проблема полягає в тому, щоб серед великої кількості гетерогенних інформаційних ресурсів (ІР) з різними елементами структурування виокремити ті ІР, що потенційно можуть містити інформацію, яка необхідна користувачеві для розв’язання його задачі.

Семантична подібність та методи її оцінювання.

Семантично пов’язані поняття (СПП) задачі – це підмножина понять певної ПрО. Якщо для моделювання ПрО використано онтологічний підхід, тоді СПП є підмножиною понять онтології цієї ПрО. Для побудови СПП існує кілька шляхів, які можуть застосовуватися окремо або спільно. СПП можуть бути визначені користувачем безпосередньо (вручну – вибором з множини понять онтології або автоматизовано – за допомогою якогось механізму співставлення опису задачі з онтологією ПрО, що використовує лінгвістичні або статистичні властивості цього опису).

використанні знань з онтології ПрО та надають засоби їх обробки.

В СПП можуть включатися поняття, що пов’язані деякою підмножиною відношень цієї онтології (безпосередньо або через інші поняття онтології – за семантичними ланцюжками). Кожне поняття з СПП має вагу (позитивну чи негативну), яка визначає ступінь семантичної близькості поняття із задачею.

На відміну від випадку, коли СПП генерується за таксономією на основі припущення, що всі прямі відношення у таксономії мають однакову вагу, для СПП задачі різні відношення можуть мати різну вагу, наявність кількох семантичних ланцюжків між поняттями може враховуватися через сумування їх ваги. Крім того, принципова відмінність полягає в тому, що в СПП задачі оцінюється семантична близькість понять до задачі, а не між самими поняттями. Для автоматизації побудови СПП можуть використовуватися семантичні ланцюжки, для генерації яких застосовуються онтологічні знання щодо домену. *Семантичний ланцюжок* (СЛ – semantic chain) між поняттями x_1 та x_n онтології O – це послідовність $n-1$ пар понять, що пов’язані в онтології O одним з обраних відношень $r_k \in R_O: r_k(x_i) = x_{i+1} \in O \forall i, k$. Для побудови СЛ потрібно визначити: онтологію O ; початкове поняття онтології O x_1 ; набір відношень онтології $R_{sc} = \{r_k\} \subseteq R_O$; глибину пошуку в O .

До складу R_{sc} можуть входити відношення ”клас-підклас”, “екземпляр класу”, “екземпляр-значення x -ї властивості екземпляру” ($x = \overline{1, a}$), “ y -е відношення ПрО” ($y = \overline{1, b}$). Пари понять O , що пов’язані властивостями ПрО або властивостями екземпляру, можуть розглядатися як семантичні трійки.

Для побудови СЛ користувач може визначати ся не тільки конкретні відношення, а правила, за якими формуються такі множини відношень.

Наприклад, використовувати рекурсивно всі відношення, якими поняття А пов'язується із іншими поняттями онтології (наприклад, будувати СЛ для всіх понять, до яких можна перейти за Х кроків СЛ), що дозволяє будувати семантичне оточення для обраного поняття; або рекурсивно використовувати певні відношення онтології (наприклад, будувати СЛ для всіх понять, що пов'язані відношеннями “Співавтори” або “Є підрозділом”), що дозволяє будувати окремі структури за симетричними та транзитивними відношеннями певного специфічного типу. Таким чином, СПП – це підмножина понять онтології, що входять до складу набору СЛ, які побудовані за певним набором правил, визначених користувачем.

Вага кожного поняття у СПП залежить від правил, за якими був побудований відповідний СЛ. Кількісна оцінка залежить від специфіки ПрО (наприклад, в деяких випадках більш близькими є поняття з одного класу, в інших – поняття, що використовуються у характеристиках типового ІО).

Зараз існує багато різноманітних підходів до кількісної оцінки семантичної відстані між поняттями на основі онтологій. В [1] наводиться розгорнутий огляд та класифікація засобів вимірювання семантичної подібності на основі онтологій. На основі цього аналізу можна виділити кілька груп методів, які різняться не стільки формулами підрахунку кількісної оцінки семантичної подібності, скільки параметрами, які використовуються у цих формулах.

Багато мір обчислюється тільки на основі шляху між поняттями. Основна ідея таких оцінок полягає в тому, що подібність двох понять є функцією довжини шляху, що пов'язує поняття та їхні позиції в таксономії. Такий самий підхід може застосовуватися для довільної онтології ПрО. Наприклад, в [2] зазначає, що онтологію можна розглядати як спрямований граф, в якому поняття взаємопов'язані за допомогою зв'язків, переважно – таксономічних (is-a). Найпростіших спосіб оцінки СП між поняттями є обчислення мінімальної довжини шляху, що пов'язує відповідні онтологічні вузли за допомогою посилань is-a. Чим довший шлях, тим поняття семантично далекіші. Якщо визначити шлях $path(c_1, c_2) = l_1, \dots, l_k$ як набір посилань, що з'єднують поняття c_1 та c_2 , де $|path(c_1, c_2)| = k$ – довжина цього шляху, тоді, розглядаючи всі можливі шляхи між c_1 та c_2 , можна визначити семантичну відстань між ними як мінімальне значення цієї довжини:

$$SS_{Rada} = \min |path(c_1, c_2)| \quad (1)$$

Незважаючи на простоту подібних підходів, проблеми виникають через припущення про те, що різні ребра онтологічного графу відображають однакові семантичні відстані, що не завжди відповідає ПрО.

аналізувати найдовший шлях від кореня таксономії до поняття.

Інші міри базуються на аналізі шляху між поняттями та їх глибини в ієрархії. Наприклад, Ву та Палмер [3] визначають міру СП між поняттями c_1 та c_2 таким чином:

$$SS_{WP} = \frac{2H}{N_1 + N_2 - 2H} \quad (2),$$

де N_1 та N_2 – кількість зв'язків “is a” між c_1 та c_2 відповідно до найнижчого спільного родового об'єкта (subsumer) s , а H – кількість зв'язків “is a” між s та коренем таксономії.

Міри подібності на основі інформаційного контенту [4] визначають подібність двох понять визначається як інформаційний контент їх найнижчого загального родового об'єкта (subsumer) $LCS(c_1, c_2)$

$$SS_{re} = IS(LCS(c_1, c_2)) \quad (3).$$

Профілювання користувачів інтелектуальних ІС. Важливо відмітити, що профіль користувача має містити як більш статичну частину відомостей (сфера компетенцій користувача, його досвід, освіта та довгострокові інтереси), так і більш динамічну, що стосується поточної задачі або характеризує окремі аспекти інформаційних потреб. Зараз для формального подання статичної частини профілю користувача часто використовують онтології, а для динамічної можуть бути застосовані тезауруси, що базуються на цих онтологіях.

Перші системи моделювання користувачів були розроблені ще в 1970-х роках. Точність припущень щодо користувачів у моделюванні визначає ефективність адаптивних систем в цілому. Неправильне тлумачення потреб користувача призводить до неправильних рішень, що може спричинити втрату довіри, зниження мотивації користуватися системою тощо.

Для моделювати характеристик користувача існує два класичні підходи – моделювання користувачів перекриттям (overlay) [5], стереотипів та ключових слів [6].

Використання онтології ПрО для моделювання інтересів, потреб або цілей користувача дозволяє застосовувати стандартні формати представлення знань та загальнодоступні засоби логічного виведення. Модель користувача може складатися з підмножини понять із онтології ПрО. Це характерно для систем рекомендації, що представляють інтереси користувачів. Наявність / відсутність поняття в моделі користувача означає наявність / відсутність інтересу до відповідного поняття.

Багато проектів, що використовують онтології для моделювання характеристик індивідуального користувача, будують для користувачів не підмножини онтології ПрО, а індивідуальні мережі понять, що відображають персональні структури понять. Для подібних моделей використовують термін "персональні онтології" [7], щоб позначити індивідуальну точку зору на світ. Але це суперечить визначенню онтології як моделі, що представляє спільний погляд на ПрО. Тому зараз використовують термін "персональний погляд на онтологію" (POV – “personal ontology view”) [8]. Реалізації POV різняться в застосовних системах, але можна виділити дві основні варіанти: 1. POV, що представлений як підмережа онтології ПрО, 2. POV як унікальна концептуалізація, структура якої може відрізнятися від онтології ПрО.

Можливість повторного та спільного використання моделей користувачів потребують не тільки стандартизованого представлення ПрО, але й спільних

словників (common vocabularies) для опису самої моделі користувача. Тому розробка онтологій, що описують спільні профілі користувачів, є важливим напрямком досліджень, пов'язаних із застосуванням онтологій у моделюванні користувачів. Термін "профіль користувача" традиційно використовується для позначення складної структури знань, що містить різні статичні відомості про користувачів, такі як демографія, базові знання, когнітивний стиль тощо. Профіль користувача відрізняється від моделі користувача, яка зазвичай надає динамічне відображення лише якогось одного аспекту користувача (концептуальні знання, інтереси, уподобання тощо). Моделі користувачів можуть мати складну структуру і зберігати статичну інформацію про користувача, тоді як профілі користувачів можуть включати динамічний компонент, що відображає поточний стан певних характеристик користувача.

Одним з важливих елементів моделі користувача є модель його поточної задачі – тезаурус задачі. Цей тезаурус може бути побудований як множина СПП на основі обраної користувачем онтології ПрО за допомогою обраної користувачем міри семантичної відстані між поняттями або за набором спільних ознак.

Семантизовані Wiki-ресурси як джерело інформації для побудови СПП. Широко вживаним рішенням для створення Wiki-ресурсів є технологічна платформа MediaWiki [9], розроблена для створення найбільш відомого Wiki-ресурсу – Вікіпедії. Крім тексту, на Wiki-сторінках можуть використовуватися графіка, аудіо та відео. Інформація структурується за допомогою категорій та посилань між Wiki-сторінками. Semantic MediaWiki [10] – семантичне розширення MediaWiki, що дозволяє користувачеві автоматично інтегрувати інформацію з різних Wiki-сторінок та будувати семантичні запити. Для структурування інформації можуть використовуватися семантичні властивості, які змістовно пов'язують Wiki сторінку з константами різних типів та з іншими Wiki-сторінками. Виразні можливості семантизованого Wiki-ресурсу дозволяють співставляти його із відповідною онтологією [11], яка містить відомості, достатні для обчислення більшості оцінок семантичної відстані (наприклад, для оцінок (1)-(3)) між поняттями, що відповідають Wiki-сторінкам. З іншого боку, семантизований Wiki-ресурс є значно більш наочною формою подання інформації порівняно з онтологією, і ним можуть користуватися люди без спеціальних знань у сфері обробки знань. Тому пропонується для моделювання задачі користувача використовувати такі ресурси, де користувач самостійно обирає потрібні сторінки, а програмні засоби автоматично (за параметрами, що явно обирає користувач) генерують за ними множину СПП. Надалі такі СПП можуть використовуватися різними інтелектуальними застосуваннями для адаптації системи до індивідуальних потреб користувача. Приклад такого використання для семантичного пошуку наведено в [12]. (в цьому випадку онтологією користувача є Wiki-онтологія e-BUE). Цей тезаурус застосовується для персоніфікованого впорядкування результатів пошуку, що отримуються від зовнішніх ПС

(наприклад, від Google). В першу чергу користувач отримує ті інформаційні ресурси, які містять поняття, що семантично пов'язані (з позитивними коефіцієнтами) для нього з ключовими словами пошукового запиту. Для подібних цілей СПП можуть використовуватися в профілюванні користувачів в різноманітних рекомендуючих, консультуючих та навчальних інформаційних системах. Перспективи подальших досліджень пов'язані із тим, яким чином на основі кількісних оцінок, які користувач надає для визначення семантичної близькості між набором ключових слів (запитом) та поняттями ПрО, можна порівнювати пертинентність онтологій уявленням користувача. Наводяться методи порівняння та пропонуються результати їх використання. Четвертий розділ присвячено практичному використанню СПП для профілювання користувачів в інтелектуальних інформаційних системах.

ЛІТЕРАТУРА

1. Taieb, M. A. H., Aouicha, M. B., & Hamadou, A. B. (2014). Ontology-based approach for measuring semantic similarity. *Engineering Applications of Artificial Intelligence*, 36, 238-261.
2. Rada, R., Mili, H., Bicknell, E., & Blettner, M. (1989). Development and application of a metric on semantic nets. *IEEE transactions on systems, man, and cybernetics*, 19(1), 17-30.
3. Rada, R., Mili, H., Bicknell, E., & Blettner, M. (1989). Development and application of a metric on semantic nets. *IEEE transactions on systems, man, and cybernetics*, 19(1), 17-30.
4. Resnik, P. (1995). Using information content to evaluate semantic similarity in a taxonomy. *arXiv preprint cmp-lg/9511007*. – <https://arxiv.org/pdf/cmp-lg/9511007.pdf>.
5. Carr, B., & Goldstein, I. P. (1977). *Overlays: A theory of modelling for computer aided instruction* (No. AI-M-406). Massachusetts Inst Of Tech Cambridge Artificial Intelligence Lab.
6. Belkin, N. J., & Croft, W. B. (1992). Information filtering and information retrieval: Two sides of the same coin?. *Communications of the ACM*, 35(12), 29-38.
7. Huhns, M.N. and Stephens, L.M. (1999) 'Personal ontologies', *IEEE Internet Computing*, Vol. 3, No. 5, pp.85-87.
8. Kalfoglou, Y. and Schorelmmmer, M. (2003) 'Ontology mapping: the state of the art'. *The Knowledge Engineering Review*, Vol. 18, No. 1, pp.1-31
9. MediaWiki. – <https://www.mediawiki.org/wiki/MediaWiki>.

10. Krötzsch M., Vrandečić D., Völkel M. Semantic mediawiki // International semantic web conference, 2006, pp. 935-942. - https://link.springer.com/content/pdf/10.1007/11926078_68.pdf.

11.Рогушина Ю.В. Проблеми використання онтологічного аналізу для подання знань у wiki-ресурсах // Проблеми програмування, № 2, 2019. – С.17-37.

12.Rogushina J.V., Grishanova I.J. Ontological methods and tools for semantic extension of the media WIKI // Проблеми програмування, № 2-3, 2020. - С.77-88.

Saviak N.

*Vasyl Stefanyk Precarpathian National University,
Ivano-Frankivsk, email: saviak.nazar@gmail.com*

IMPROVED DEEP LEARNING ALGORITHM FOR SELF-DRIVING CARS CONTROL

This paper presents the method of machine learning algorithms combination for training self-driving cars. It improves the overall accuracy and speeds up the training process.

Keywords: *machine learning, self-driving car, algorithm, classification, linear regression, stochastic gradient descent, accuracy.*

Today, machine learning (ML) is among the hottest technologies for autonomous driving. One of the main challenges in autonomous driving systems that have ML components is to choose an appropriate training algorithm to get the most effective results [1].

This research aims at developing an optimized algorithm through the implementation and combination of classification (K-Nearest Neighbors algorithm), linear regression and stochastic gradient descent. Comparative analysis of the algorithms shows that the created one outperforms the other methods with a high accuracy.

The research is provided for the development of a simulator for self-driving cars training using machine learning. The optimized algorithm aims to speed up the training process and get more accurate results.

This method lies in subsequent usage of classification, linear regression and stochastic gradient descent.

Classification is a process of categorizing a given set of data into classes. Here it is used for clear determination of states, for example, turn, straight drive etc. Classification of discrete states based on analog signal explained in [2]. According to the defined state linear regression is performed.

Linear regression performs the task to predict a dependent variable value based on a given independent variable. So, this regression technique finds out a linear relationship between the input and output. Here it is used for accurate determination of such values like the wheel angle, speed etc.

The next step aims at the optimization of obtained data by the use of stochastic gradient descent. This method replaces the actual gradient (calculated from the entire dataset) by an estimate thereof (calculated from a randomly selected subset of the data). Especially in high-dimensional optimization problems this reduces the computational burden, achieving faster iterations in trade for a lower convergence rate [3].

To approve and assess an improvement of the described method the accuracy of algorithms in the training dataset is computed separately and in combination. The results are shown in the figure below:

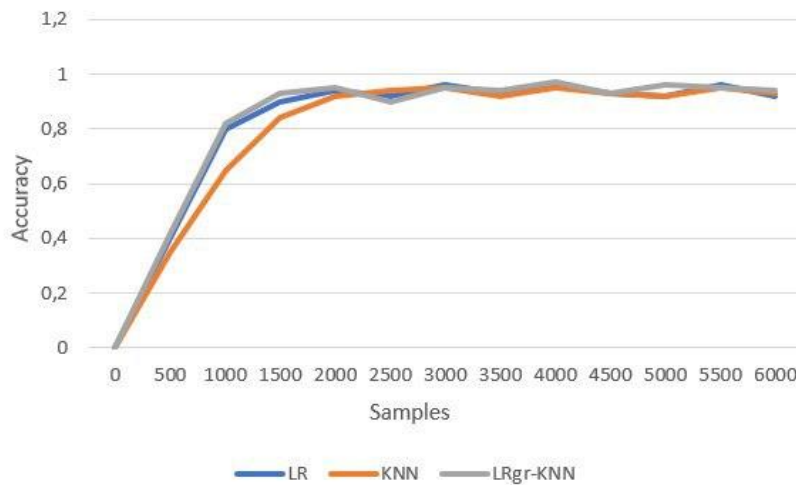


Fig. 1. Accuracy of used algorithms

According to the figure 1 it can be stated that subsequent usage of classification, linear regression and stochastic gradient descent gives higher accuracy in most cases of training the dataset for 94%.

During the research, it was established that the proposed approach of usage combination of methods allows to increase the overall accuracy of the training model, which enables to get more effective self-driving car behavior on the track.

REFERENCES

1. M. Cococcioni, F. Rossi, E. Ruffaldi and S. Saponara, "Novel Arithmetics to Accelerate Machine Learning Classifiers in Autonomous Driving Applications," *2019 26th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, Genoa, Italy, 2019, pp. 779-782, doi: 10.1109/ICECS46596.2019.8965031.
2. M. Kozlenko, I. Lazarovych, V. Tkachuk and V. Vialkova, "Software Demodulation of Weak Radio Signals using Convolutional Neural Network," *2020 IEEE 7th International Conference on Energy Smart Systems (ESS)*, Kyiv, Ukraine, 2020, pp. 339-342, doi: 10.1109/ESS50319.2020.9160035.
3. Bottou, Léon; Bousquet, Olivier (2012). "The Tradeoffs of Large Scale Learning". In Sra, Suvrit; Nowozin, Sebastian; Wright, Stephen J. (eds.). *Optimization for Machine Learning*. Cambridge: MIT Press. pp. 351–368. ISBN 978-0-262-01646-9.

Сайко В.Г. ,

*Київський національний університет імені Тараса Шевченка,
Київ, Україна, E-mail: vgsaiko@gmail.com*

Наритник Т.М.,

*Інститут електроніки та зв'язку Української академії наук,
Київ, Україна, E-mail:director@mitris.com*

Диль Є.А., Кузьмінський Ю.В.,

*Одеська національна академія зв'язку імені О.С. Попова,
Київ, Україна, E-mail:onazkafedratk@gmail.com*

ВИПРОМІНЮЮЧИЙ КОМПЛЕКС СУБТЕРАГЕРЦОВОГО ДІАПАЗОНУ ДЛЯ ЗАХИСТУ ОБ'ЄКТІВ ВІД НЕСАНКЦІОНОВАНОГО ПРОНИКНЕННЯ

The work is based on the authors' working hypothesis on the design of elements and nodes of the path of the radiating telecommunication system of the subterahertz range using microwave electronics technologies, which made it possible to propose new technical solutions to create in the terahertz range local oscillator.

Keywords: *terahertz lines, radiating installation, object protection.*

Постановка наукової проблеми в загальному вигляді.

Сьогодні випромінюючі телекомунікаційні системи субтерагерцового діапазону використовуються в якості так званою «нелетальної зброї» для або для обмеження здібностей людини (впливає на увагу, мислення), або на його знерухомлення (застосовуються спеціальні піни, клей або сітки), або на виведення з ладу життєво необхідних систем: джерел енергії, систем харчового постачання, засобів комунікації, систем спостереження і наведення і т.п.

До такої систем відносяться: лазерна зброя, системи з використанням інфразвукових генераторів, пристрої з електромагнітним імпульсом неядерного походження і зброя з речовинами, що руйнують основні елементи бойової техніки. Такі системи представляють сьогодні серйозну альтернативу не тільки вельми обмеженому ядерному потенціалу, а й поширеній класичній зброї. Крім того, воно відповідає міжнародним вимогам гуманізації збройного бою. В рамках програм з нелетального озброєння на даний час створюються технології спрямованої енергії, здатні зупиняти людей на великих дистанціях з мінімальним ризиком травм і непрямих збитків.

Формулювання мети дослідження й обґрунтування його актуальності.

В основу принципу роботи технологій спрямованої енергії покладено високотемпературний розігрів повітряного простору (понад 900 К) за допомогою вузьконаправленого радіовипромінювання, частота якого відповідає частоті максимального поглинання енергії молекулами атмосферного кисню і водяної пари. Відповідні спектральні діапазони розташовані в районі 60 і 118 ГГц, тому рекомендується використовувати як будь-який із зазначених ділянок спектра, так і їх сукупність. Абсолютне ж значення потужності розігріву залежить не тільки від стану атмосфери, але і від необхідної дальності дії, заданого перетину променя, форми і тривалості зондувальних імпульсів. За оцінками [1], для створення в сухому повітрі провідного каналу діаметром 1 см з температурою 4000 К верхній рівень енергії випромінювання в імпульсі повинен мати наступну залежність від протяжності каналу (див. табл.1):

Табл. 1 Залежність довжини каналу від енергії випромінювання

№ п/п	Протяжність каналу	Енергія випромінювання	Примітка
1	4 м	6,48 кДж	
2	20 м	32,4 кДж	
3	40 м	64 кДж	
4	41284 м	677,922 МДж	

За даними [1], при нагріванні сухого повітря від 2000 до 4000 К його провідність може бути підвищена від 10^{-6} до 1 См, причому повітряний канал з

діаметром поперечного перерізу в 1 см, розігрітий до 4000 К, може зберігати залишкову провідність протягом 50 мс після проходження мікрохвильового імпульсу [2]. Зазначених значень провідності в принципі може бути досить для реалізації транспорту електромагнітного імпульсу (ЕМІ) до об'єктів ураження по аналогії з лазерною іонізацією. Проте для підвищення провідності повітряного середовища використовується в якості вражаючого фактора так званий "плазмове удару" [2].

Відоме рішення в цій галузі під назвою Active Denial System (ADS) - яке має пристрій генерування та підсилення, хвильовідний тракт, антено-поворотний комплекс [3]. Пристрій генерування та підсилення побудовано на надпотужних гіротронах для генерації енергії міліметрових хвиль на частоті 95 ГГц на площі 1,5 метра і максимальної дальності 1000 м.

Недоліками такого рішення є те, що установка є високовольтна та потребує відповідні потужності компонентів і підсистем, включаючи систему терморегулювання і енергоустановку. Це ускладнює процес її оперативного управління та технічною експлуатацією.

Широковідоме також технічне рішення під званою "міліметрова атмосферна енергетична проєкційна система" (МАЕПС) [4]. МАЕПС містить пристрій на клістріні, циркулятор, хвильовід, хвильовідна секція, антено-поворотний комплекс, діелектричну лінзу, пристрій для забезпечення "плазмове удару".

В якості пристрою генерування та підсилення міліметрових хвиль використано пристрій на клістріні. Його випромінювання через циркулятор і хвилевід подається на герметизовану хвилевідну секцію з випромінюючим рупором. Зазначено, що герметизований рупор з апертурою 4,048 см забезпечує проходження 60 ГГц радіоімпульса тривалістю 6,32 мкс з еквівалентної потужністю випромінювання близько 19 МВт. Для формування плоского хвильового фронту використана діелектрична лінза. Для підвищення провідності повітряного середовища використовується пристрій для забезпечення так званого "плазмове удару".

Недоліками такого рішення є громіздкість конструкції, вона є також високовольтна та потребує відповідні потужності компонентів і підсистем, включаючи систему терморегулювання і енергоустановку. Це ускладнює процес її оперативного управління, технічною експлуатацією.

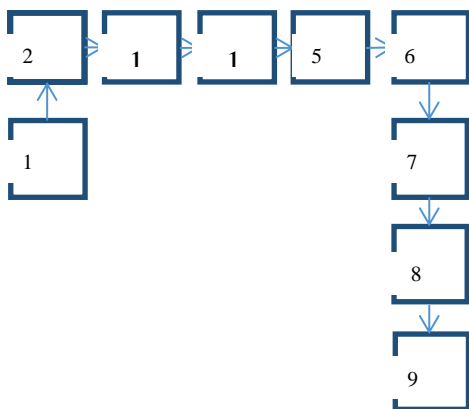
Виклад поставленого завдання.

Запропоноване авторами технічне рішення має за мету удосконалення високоенергетичної випромінюючої телекомунікаційної системи субтерагерцового діапазону. Поставлене завдання вирішується тим, що у високоенергетичній випромінюючій телекомунікаційній системі субтерагерцового діапазону пристрій генерування та підсилення виконано як послідовно з'єднані

задаючий опорний генератор, вихід якого підключений до послідовно з'єднаним множникам частоти з підсилювачами, твердотільним попереднім підсилювачем потужності, твердотільним проміжним підсилювачем потужності, вакуумним кінцевим підсилювачем потужності.

Технічний результат, на отримання якого спрямована корисна модель, - зменшення масо-габаритних характеристик і енергоспоживання компонентів і підсистем за рахунок застосування твердотільних підсилювальних пристроїв, що дозволяє потенційно зменшити масо-габаритні характеристики системи та енергоспоживання компонентів. Також при цьому спрощується процес технічної експлуатації системи. Сутність розробленого технічного рішення пояснюється кресленнями на фіг. 1, де зображена структурна схема високоенергетичної випромінюючої телекомунікаційної системи субтерагерцового діапазону для захисту об'єктів від несанкціонованого проникнення. На ній:

- 1 - задаючий опорний генератор,
- 2 - множники частоти з підсилювачами,
- 3 - твердотільний попередній підсилювач потужності,
- 4 - твердотільний проміжний підсилювач потужності,
- 5 - вакуумний кінцевий підсилювач потужності,
- 6 – циркулятор,
- 7 - хвильовід,
- 8 - хвильовідна секція,
- 9 – антено-поворотний комплекс.



Фіг.1

Ключовими елементами пропонованої системи в субтерагерцовому діапазоні частот являються радіоелектронні випромінюючі пристрої, здатні формувати сигнали необхідної потужності. Передавальний тракт побудований за гетеродинною схемою та забезпечує передачу сигналів на трасі в субтерагерцовому діапазоні частот в межах від 94 до 96 ГГц.

Високоенергетична випромінююча телекомунікаційна система субтерагерцового діапазону працює таким чином.

Побудова високоенергетичної випромінюючої телекомунікаційної системи субтерагерцового діапазону частот 94...96 ГГц базується на використанні високостабільного задаючого кварцового генератора з подальшим ланцюгом помножувальних і підсилювальних каскадів. Рівень підсилення встановлювався таким, щоб забезпечити оптимальний режим роботи помножувальних каскадів і необхідну потужність на виході.

У множників частоти з підсилювачами внаслідок перетворення частоти сигналу «угору», спектр сигналу з діапазону частот задаючого генератора переноситься у субтерагерцовий спектр 94-96 ГГц і після каскадів підсилення (твердотільний попередній підсилювач потужності, твердотільний проміжний підсилювач потужності, вакуумний кінцевий підсилювач потужності), подається на циркулятор, хвилевід, герметизовану хвилевідну секцію, на вхід антено-поворотного комплексу, маючи відповідну потужність та випромінюється за допомогою антени.

Високоенергетична випромінююча телекомунікаційна система генерує вузький спрямований (шириною до 0,5 градуса) радіопромінь в частотному діапазоні «вікна прозорості» 94-96 ГГц, який проникає в шкіру людини на глибину до 0.5 мм, нагріваючи її до і вище 45°C. При цьому в людини через певний нетривалий проміжок часу виникає нестерпний біль. Больова реакція на випромінювання інтенсивністю до 100 Вт/м² достатньо вагома, щоб заставити противника покинути поле бою.

Реакція на випромінювання виникає протягом 2-3 секунди, стає нестерпною через 5 секунд і зникає після відключення генератора або після того, як людина залишить зону опромінення. Якщо противник не покине зону протягом 250 секунд, він отримає опік шкіри. Прогнозована дальність ураження живої сили противника в межах 1 км і більше.

У пропонуваному технічному рішенні високоенергетичний випромінюючий тракт телекомунікаційної системи субтерагерцового діапазону частот побудований за гетеродинною схемою та забезпечує передачу сигналів на трасі в субтерагерцовому діапазоні частот в межах від 94 до 96 ГГц за допомогою високостабільного опорного генератора, множників частоти з підсилювачами, твердотільного попереднього підсилювача потужності, твердотільного проміжного підсилювача потужності, вакуумного кінцевого підсилювача потужності. У множників частоти з підсилювачами застосовується метод прямого перемноження частоти на лавинно-пролітних діодах з високим коефіцієнт корисної дії при великих коефіцієнтах примноження.

Так як випромінююча система має велику потужність, то побудова системи на основі малопотужного задаючого опорного генератора та підсилювачів потужності краще, ніж на основі потужного лампового генератора. В підсилювачах запропонованого рішення вихідний сигнал прецизійно прецизійно генерується на низькому рівні потужності, а потім підсилюється до рівня потужності, яка необхідна для передачі його за допомогою антени. Переваги підсилювачів полягають в тому, що вони здібні підтримувати стабільність формованих сигналів і збудження антенної системи. Ламповий клістрон має меншу гнучкість і, як правило, створює більше шуму та відповідно завад, ніж твердотільні підсилювачі потужності або підсилювачі на ЛБВ.

Висновок

В запропонованій системі, на відміну від [1-4], забезпечується зменшення масо-габаритних характеристик і енергоспоживання компонентів і підсистем випромінюючої телекомунікаційної системи субтерагерцового діапазону частот 94...96 ГГц за рахунок застосування пристроїв з напівпровідниковою технологією, що дозволяє потенційно отримати легшу систему менших розмірів, меншою вартістю і з скороченим часом готовності. Також при цьому спрощується технічна експлуатація комплексу та збільшуються функціональні можливості.

ЛІТЕРАТУРА

1. Пат. 5 624 592 США. Microwave facilitated atmospheric energy projection system / P.J.Paustian. H05B 6/80, Приоритет 29.04. 1997.
2. Пат. 6 111 237 США. Microwave facilitated atmospheric energy projection system / P.J.Paustian. H05B 6/80, Приоритет 29.08. 2000.
3. Нелетальное оружие армий мира. Часть 2. Опубликовано 04.06.2017. [Электронный ресурс] – Режим доступа к ресурсу: <http://integral-russia.ru/2017/06/04/neletalnoe-oruzhie-armij-mira-chast-2/>. (**аналог**).
4. Пат. 6 054 694 США. Microwave facilitated atmospheric energy projection system / P.J.Paustian. H05B 6/80, Приоритет 24.04. 2000. (**прототип**).

ЦИФРОВІЗАЦІЯ РИНКІВ ПОХІДНИХ ФІНАНСОВИХ ІНСТРУМЕНТІВ УКРАЇНИ В УМОВАХ ТРАНСФОРМАЦІЇ МІЖНАРОДНОГО РЕГУЛЯТОРНОГО ЗАКОНОДАВСТВА

The problems of digitalization, harmonization and implementation of new norms of international financial markets and the updated standard of interest rate to the national legislation are investigated. The main provisions of the paradigm platform for the transformation of the national market of financial derivatives are formulated

Keywords: *finance derivatives, credit risk, new «risk-free» interest rate*

Розвинений ринок капіталу є ключовим фактором сталого розвитку реального сектору економіки, особливо в часи несприятливої світової економічної кон'юнктури. Ефективна мобілізація, розподіл, перерозподіл і використання фінансових ресурсів забезпечуються обігом на ринку капіталу широкого спектру фінансових інструментів, ПФІ з наявними ліквідними схемами і стратегіями торгівлі, цифровими торговельними платформами, погашенням та сплатою доходу для суб'єктів ринків капіталу. В умовах пришвидшеної цифрової трансформації світового фінансового ринку до нових післякризових стандартів визначення ціни капіталу, розвиток і гармонізація національного фінансового ринку, на даний час, визначає майбутню конкурентоспроможність економіки України [1– 6].

Постановка проблеми. З 2010 року відбувається поетапна імплементація міжнародного законодавства щодо регулювання фінансових ринків, яке вже не використовує індикативну (безризикову) відсоткову ставку Libor у якості орієнтиру для короткострокових, середньострокових і довгострокових відсоткових ставок на міжбанківському ринку. З 2021 року згідно власного рішення FSA не буде її обчислювати і оприлюднювати. Ціноутворення кредитів, облігацій, інструментів фінансового ринку, ПФІ буде відбуватися за новим еталонним стандартом зі зміною методів його обчислення [2; 6]. Актуальною є проблема вжиття заходів щодо переходу від Libor до нового еталонного стандарту відсоткової ставки.

Аналіз останніх досліджень і публікацій.

У процесі трансформації фінансової системи законодавство щодо оцінювання кредитного ризику контрагента ПФІ транзакції грає вирішальну роль

для визначення цін фінансових інструментів. Теоретичний фундамент використання кредитних експозицій учасників транзакцій з ПФІ було закладено ще наприкінці минулого століття Д. Бріго, Р. Літценбергером, Е. Канабарро, Д. Даффі, Г. Цезарі, Р. Ярровим та іншими вченими [2; 3]. На думку Г. Паркера, М. Алстайна, С. Чоударі, провідних експертів ринків ПФІ, уряди і регулятори повинні забезпечити цифрову трансформацію фінансової системи у напрямку формування ефективного централізованого клірингу з метою захисту світової економіки від майбутніх криз [6].

Мета публікації. Дослідження проблем цифровізації, гармонізації і імплементації до національного законодавства нових нормалей фінансових ринків і оновленого еталону відсоткової ставки.

Піонерна стаття Фішера Блека, Майрона Шоулса, опублікована у 1973 році, була інноваційним проривом в обчисленні справедливої ціни європейського CALL опціону, яке було окремим розв'язком стохастичного диференційного рівняння, що давало змогу визначити ціну похідного фінансового інструменту для акції, на яку не сплачуються дивіденди [1]. Це рівняння визначало ціну європейського CALL і PUT опціонів на акції завдяки аналізу, до якого вдавалися Ф. Блек і М. Шоулс, використовуючи властивості стохастичного процесу для ціноутворення акцій – базового фінансового інструменту, на основі ризик-нейтрального ціноутворення, відсутності арбітражу, самофінансованого портфелю, реплікації його функції доходності і безперервної, безкоштовної торгівлі.

Після кризи, всі ці класичні припущення були зруйновані і зробили історією тривале існування безарбітражних методів Ф. Блека, М. Шоулса і Р. Мертона визначення справедливих цін ПФІ.

У затвердженій НБУ і НКЦПФ 16 січня 2020 року «Стратегії розвитку фінансового сектору України до 2025 року» підкреслюється роль імплементації ризик-орієнтованого підходу до нагляду за всіма учасниками фінансового ринку на основі прогнозування ціни інструментів фінансового ринку, похідних фінансових інструментів. За офіційною інформацією НБУ, станом на листопад 2019 року на ринку ОВДП в обігу знаходилися 34 випуски гривневих облігації, які приймаються НБУ для забезпечення виконання боргових зобов'язань. Динаміка безкупонної доходності за досліджуваний період з 2018 року визначається згідно постанови НБУ №627-рш від 20 вересня 2018 р. на основі нелінійної параметричної моделі Свенссона, табл. 1.2, модель №53 [2].

$$s_p = \beta_0 + \beta_1 \left(\frac{1 - e^{-p/\tau}}{p/\tau} \right) + \beta_2 \left(\frac{1 - e^{-p/\tau}}{p/\tau} - e^{-p/\tau} \right) + \beta_3 \left(\frac{1 - e^{-p/\tau_1}}{p/\tau_1} - e^{-p/\tau_1} \right), \quad (1)$$

де S_p – відсоткова ставка на споті для терміну p у роках. β_0 – незалежний довгостроковий фактор доходності, що визначає рівень знаходження кривої доходності, збільшення якого безпосередньо приводить до загального зростання/зменшення рівня відсоткових ставок. β_1, β_2 – середньострокові фактори кривої безкупонної доходності, що визначають її форму. τ_1, τ_2 – параметри, що впливають на напрям руху і опуклостей середньострокових відсоткових ставок кривої безкупонної доходності.

Із формули (1) зрозуміло, що у зв'язку із використанням в якості прийнятого НБУ стандарту прогнозування відсоткової ставки для гривневих ОВДП нелінійної моделі Свенссона з щоденним її розрахунком, прогнозовані відсоткові ставки уявляють собою спектри кривих безкупонної доходності для гривневих ОВДП із вбудованим опціоном CALL.

$$P = \sum_{t=1}^n (CF_t \times e^{-s_t \times d_t}) + P_{CALL}, \quad (2)$$

Для прогнозування складних процесів (2) ціноутворення ОВДП, які відносяться до гібридних ПФІ – облігацій із вбудованим опціоном CALL, необхідно визначати стаціонарність цього процесу. Розв'язання цієї задачі здійснено на основі розширеного критерія Дікі-Фулера для лінійної стохастичної авторегресійної інтегрованої моделі ковзного середнього, включаючи незалежні фактори впливу і з одночасним визначенням оптимальних параметрів [3]. Узагальнений вигляд таких стохастичних моделей прогнозування ціни ОВДП можна представити так:

$$\Delta^d X(t) = MA_0 + \sum_{i=1}^p MA_i \Delta^d X(t-i) + \sum_j^q AR_j L^j \Delta^d X(t-j) + \sum_{k=1}^s \alpha_k F_k(t), \quad (3)$$

де, AR_i - авторегресійні параметри процесу ціноутворення ОВДП, MA_i - коефіцієнти ковзного середнього, Δ^d - оператор інтегрування процесу ціноутворення порядку d , α_k - коефіцієнти зовнішніх незалежних факторів. На основі результатів дослідження стаціонарності процесів ціноутворення для всіх 34 випусків ОВДП, виявлено що майже всі процесі ціноутворення ОВДП є нестаціонарними. Розрахунками встановлено, що точність результатів прогнозування ціни ОВДП у вигляді кореляції прогнозованих значень ціни ОВДП за отриманими моделями і справедливої ціни ОВДП коливається від 82 до 93 відсотків.

Логіка проведення економічного аналізу фінансових ринків, ринків ПФІ, монетарної політики повинна бути парадигмальною платформою національного

законодавства щодо регулювання фінансових ринків. Основними положеннями цієї парадигмальної платформи є такі:

- Формування сучасної інформаційно-технологічної інфраструктури для ефективного функціонування ринку похідних фінансових інструментів на основі впровадження економічних механізмів для автоматизованого визначення їх справедливої ціни в умовах наявного арбітражу і відсутності безризикової відсоткової ставки;

- Законодавче вирішення проблеми управління ризиками в умовах імплементації післякризової парадигми визначення ціни капіталу із використанням мультидисконтування і застосуванням централізованого клірингу, маржі, варіаційної маржі, нетінгу, ліквідаційного нетінгу за умови дефолту контрагента.

ЛІТЕРАТУРА

1. Black F., Scholes M. The Pricing of Options and Corporate Liabilities. *Journal of Political Economy*. 1973. № 81, May–June. P. 637–654.

2. Силантьєв С.О. Міжнародна практика використання похідних фінансових інструментів : монографія / С.О. Силантьєв. — К. : КНЕУ, 2017. — 399 с.

3. Силантьєв С.О. Похідні фінансові інструменти : теоретичні та прикладні аспекти : монографія / С.О. Силантьєв. — К. : КНЕУ, 2012. — 310 с.

4. Силантьєв С.О. Менеджмент похідних фінансових інструментів : практикум / Силантьєв С.О. — К. : КНЕУ, 2009. — 399 с.

5. Силантьєв С.О. Менеджмент похідних фінансових інструментів : навч. посіб. / Силантьєв С.О. — К. : КНЕУ, 2010. — 279 с.

6. Parker G., Van Alstyne M., Choudary S. *Platform Revolution: How Networked Markets Are Transforming the Economy And How to Make Them Work for You*. New York; London: W. W. Norton & Company, 2016. 352 p.

Симонов Д.І.

*Інститут кібернетики ім. В.М. Глушкова НАН України, м. Київ
simonov_d@ukr.net*

Симонов Є.Д.

*ННК «ІПСА» [НТУ України "КПІ ім. І. Сікорського"](#), м. Київ
e.simonov@gmail.com*

ПЛАНУВАННЯ ТА УПРАВЛІННЯ ЛАНЦЮГАМИ ПОСТАЧАННЯ

The paper considers modern methods of planning and analysis of supply chains; analysis comprises the advantages and disadvantages of methods, their varieties and functionalities; recommendations for improving planning and management methods have been developed.

Keywords: *Supply Chain Management, transformation model, supply chain management, modeling of structural equations, axiomatic research approach, quantitative empirical research.*

Ланцюг постачання - це три або більше економічних одиниці (організації або особи), що безпосередньо беруть участь у зовнішніх і внутрішніх потоках продукції, послуг, фінансів та інформації від джерела до споживача [1].

Сучасний рівень глобалізації та розвитку ІТ-технологій і логістики значно підняв рівень конкуренції за ресурси та ринки, що посприяло на необхідність ефективного управління ланцюгами постачання, як одними з найважливіших інструментів збільшення конкурентних переваг. Здатність створювати ефективні і стабільні відносини між постачальниками та покупцями може бути головним фактором успіху.

Не зважаючи на велику кількість досліджень у галузі теорії ланцюгів, на теперішній час існує дуже багато певних «вузьких місць», що обумовлено впливом стохастичних збурень при імовірнісному прогнозуванні якісної та кількісної оцінки моделі ланцюга постачання. Оптимізація конструкції ланцюга постачання забезпечує «ідеальне» зображення реальної ситуації, яка за побудовою не піддається звичайному математичному моделюванню [2].

Стратегія організації є важливим фактором, що впливає безпосередньо на процес планування ланцюгів постачання та їх структуру. Зазвичай стратегія формується під впливом історичних даних та бачення майбутнього організації. З точки зору ланцюга постачання, в межах стратегічного бачення процесу можливо розбити на [3]:

- *Створення «бачення» фірми* – визначає поточний та майбутній очікуваний обсяг бізнесу, ринки, географічне охоплення ділової діяльності, ключові партнери та інше.
- *Розробка керівних принципів планування ланцюгів постачання* – прагматичні керівні принципи щодо горизонтів планування ланцюгів постачання, оцінка зовнішніх факторів та зовнішнього середовища, розподіл управлінських обов'язків та визначення цілі корпоративної діяльності.
- *Формулювання стратегічних планів дій* для підтримання довгострокової конкурентної переваги, які зосереджені на визначенні основних компетенцій, потенціалі конкурентного лідерства та розподілу наявних ресурсів.
- *Оцінка успіху або невдачі стратегічних планів дій* – налаштування контролю на основі чітких вимірів ефективності.
- *Забезпечення підтримки від зацікавлених сторін*, у тому числі вищого керівництва.

Беручи до уваги взаємозалежність логістики, постачальників та маркетингу, логістичну стратегію можна сформулювати, виконавши наступні кроки [3]:

1. Огляд ланцюга постачання: опис логістичної стратегії в загальних рисах та її зв'язок із функціями постачання та збуту.

2. Заява про цілі логістики: формулювання та визначення пріоритетних довгострокових цілей, яких потрібно досягти протягом п'яти або більше років стосовно контролю витрат та обслуговування споживачів.

3. Опис тактичних та оперативних планів: детальний опис та документування стратегії перевезень, складування, обробки замовлень та інвентаризації, необхідних для підтримки загальних планів логістики.

4. Прогноз необхідних ресурсів для реалізації стратегічних планів логістики: забезпечення людських, капітальних та фінансових ресурсів, необхідних для успішного здійснення стратегічних планів логістики.

5. Оцінка нижчого результату логістичної стратегії: розробка показників, які можуть вимірювати ступінь успіху, що приносить логістична стратегія, з точки зору корпоративного прибутку, ефективності обслуговування споживачів та частки ринку.

За останні роки сфера управління ланцюгами постачання (Supply Chain Management, SCM) швидко розвивається. Ця тема цікавить менеджерів логістики та дослідників, оскільки вважається джерелом конкурентних переваг [4].

Системна модель ланцюга постачання складається з послідовно пов'язаних між собою підсистем, кожна з яких моделює окремого учасника ланцюга постачання починаючи від споживача і закінчуючи, безпосередньо, виробником,

включаючи постачальників i -го рівня. Між сусідніми підсистемами виникають інформаційний і матеріальний потоки.

Узагальнену модель ланцюгів постачання можливо представити у вигляді моделі перетворення, яка зображена на рисунку 1.



Рисунок 1 – Модель перетворення ланцюга постачання

Формула ланцюжка поставки передбачає наявність послідовного процесу: постачання необхідного виду продукції, заданої якості, в потрібній кількості, в певний момент часу, в вказане місце за встановленою ціною з мінімальними витратами. Критеріями оптимальності при вирішенні завдань управління ланцюжком постачання служать витрати на визначення і оформлення замовлень, транспортування, зберігання, а також тимчасові витрати.

Область SCM включає абстрактні поняття, такі як інтеграція, співпраця, координація, конкурентні переваги та багато інших, які можуть бути пов'язані між собою. Такі поняття можуть бути представлені прихованими змінними або факторами які не піддаються спостереженню чи вимірюванню. Зважаючи на це, необхідно мати набір мір, або показників, для врахування абстрактних понять, що представляють можливість для якісного планування. Одним з інструментів рішення задачі планування ланцюгів постачання є метод моделювання структурних рівнянь (Structural Equation Modeling, SEM) [5].

SEM - це статистична техніка, яка поєднує моделі вимірювань (підтверджуючий факторний аналіз) та структурні моделі (регресійний аналіз) в одночасний статистичний тест [6]. Той факт, що SEM може одночасно аналізувати структурні та вимірювальні моделі, робить це особливо цінним для дослідників SCM. Метод SEM вимагає, щоб дослідник розглянув базову модель, яка залежить від деяких структурних параметрів, а потім використовував коваріантності спостережуваних даних для перевірки гіпотез щодо цих параметрів.

Корисність SEM полягає у його здатності перевіряти гіпотези, які важко, а то й неможливо оцінити іншими аналітичними методами. В першу чергу це обумовлено тим, що використання методу SEM передбачає інтеграцію двох різних статистичних процесів: факторного аналізу та одночасного моделювання рівнянь системи. Загальним методом для SEM є лінійна регресія. Більш стандартні статистичні методи, такі як регресійний аналіз, часові ряди, факторний аналіз або ANOVA, можна розглядати як особливі випадки SEM. Також необхідно визначити, що для окремих випадків SEM передбачає використання нелінійних рівнянь.

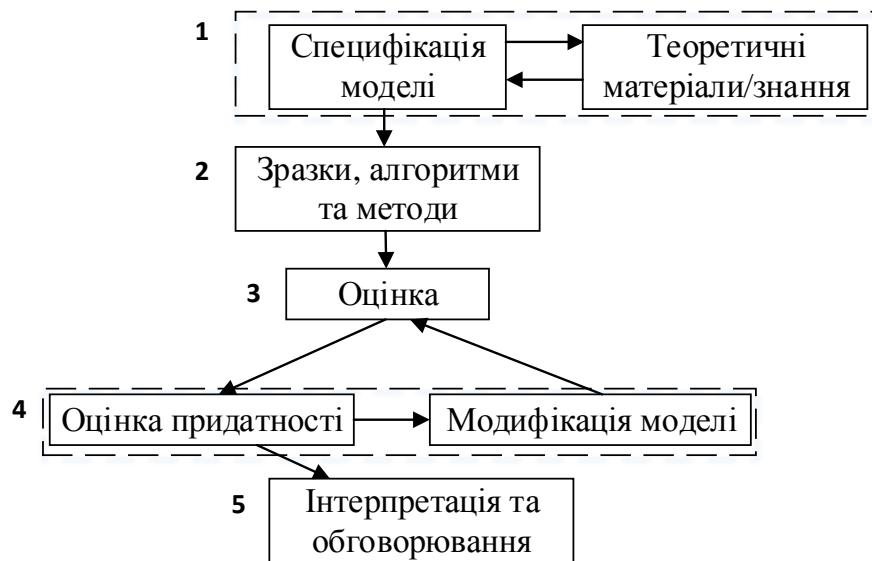


Рисунок 2 - Діаграма звичайного підходу до SEM

Як бачимо на рисунку 2, перший етап процесу складається з розробки теоретичної моделі із зазначенням змінних та причинно-наслідкових зв'язків між ними. Тут дослідники висловлюють свої гіпотези у вигляді моделі структурного рівняння. Рівняння визначають: структурні рівняння, що пов'язують конструкції (залежні незалежні змінні співвідношення), та модель вимірювання. Визначають набір матриць, що вказують на будь-яку гіпотетичну кореляцію між конструкціями [5].

На другому етапі дослідник повинен вибрати міри прихованих змінних обраної моделі та зібрати дані. Це один з найважливіших аспектів оцінки SEM. Неможливо отримати хороші оцінки параметрів моделі, якщо спостережувані змінні насправді не вимірюють те, що дослідник має намір виміряти.

Третій етап присвячений оцінці моделі. Існують різні процедури оцінки: максимальна ймовірність, метод найменших квадратів, зважені найменші квадрати тощо. Вибір дослідника повинен базуватися на його адекватності даним та моделі, що аналізуються. Важливо аналізувати різні частини моделі окремо.

Наприклад, якщо відповідність оціночної моделі погана, то необхідно мати можливість визначити, чи не була допущена помилка в специфікації структурної частини моделі або в частині вимірювання моделі.

На четвертому етапі відбувається оцінка відповідності моделі задачам аналізу. Це відбувається на двох рівнях: спочатку для загальної моделі, а потім окремо для вимірювальної та структурної моделей. Існують різні заходи для перевірки відповідності загальної моделі, такі як порівняльний індекс виправлення (Comparative Fix Index), середньоквадратична похибка регресії (Root Mean Square Residual) та інші. Після того, як загальна модель була оцінена, вимірювання кожної конструкції має бути оцінено на предмет одномірності та надійності. Це можна зробити за допомогою коефіцієнта детермінації (R^2). Якщо модель не відповідає даним, потрібно модифікувати модель і повторити оцінку, поки не буде досягнуто належної відповідності моделі.

Останній етап процесу передбачає інтерпретацію результатів. Це означає визначити, підтримуються чи ні відносини, встановлені в теоретичній моделі. З цією метою слід вивчити весь результат процесу оцінки, а не лише загальні показники відповідності. Може бути так, що деякі частини моделі не пояснюються належним чином. Ретельне вивчення тестів значимості коефіцієнтів, і особливо кореляцій між залишками оцінки, може допомогти оцінити модель.

Заснований на коваріації метод SEM не тільки дозволяє включати теоретичні конструкції як приховані змінні, але також кореляції між різними екзогенними змінними, а також причинно-наслідкові зв'язки та кореляції між різними змінними, що дозволяє всі гіпотези перевірити одночасно. Це очевидні переваги перед багатовимірний регресійним аналізом, який вимагає незалежних змінних і може включати лише одну ендогенну змінну в кожен аналіз. Ще однією перевагою є те, що придатність моделі можна оцінити за допомогою статистичних тестів та різноманітних критеріїв придатності.

Одним із значних недоліків моделі SEM є те, що він вимагає великих обсягів вибірки, які в більшості випадків перевищують 200 окремих випадків. Крім того, більшість встановлених функцій оцінки, що використовуються в процесі, вимагають метрично масштабованих показників та нормального розподілу даних.

Кількісне дослідження ланцюга поставки на основі моделей можна розділити на два різні класи:

1. Аксиоматичний дослідницький підхід. Цей підхід стосується суворого процесу теорем та логічних доказів. Використовуються математичні моделювання. Імітаційні моделі є об'єднуючим елементом для другого класу кількісних модельних досліджень [7].

2. Кількісні емпіричні дослідження. Визначається емпіричними висновками та вимірами. Тут першочерговим завданням дослідника є переконатися, що існує модель, яка відповідає спостереженню та дії в реальності. Емпіричні дослідження на основі кількісних моделей генерують моделі причинно-наслідкових зв'язків між змінними та показниками ефективності. Цей логічний емпіричний підхід ізолює явище від контексту для логічного аналізу. Потім ці моделі аналізуються або тестуються [8].

Тип досліджень, що використовується, може бути описовим або нормативним. Описове емпіричне дослідження зацікавлене у створенні моделі, яка описує причинно-наслідкові зв'язки, які можуть існувати в дійсності, і призводить до поліпшення розуміння механіки процесів, наприклад, дослідження системної динаміки процесів [9], і годинної швидкості в промислових системах [10]. У цьому сенсі моделювання - це більше, ніж лише частина аксіоматичних кількісних досліджень, і його також можна використовувати в другому класі модельних досліджень. Нормативне емпіричне кількісне дослідження, метою якого є розробка політики, стратегії та дій з метою покращення поточної ситуації, у багатьох випадках ґрунтується на аксіоматично кількісному типу досліджень.

Дослідження управління ланцюгами постачання стикається з проблемою, що відсутня чітко визначена методологічна база для виявлення та вимірювання відповідних характеристик реальних процесів. Об'єктивної і незалежної від ситуації та одночасно загально визнаної процедури не існує. Звичайно, кожна дослідницька робота якось вирішує цю проблему, але це завжди робиться суб'єктивно, залежно від ситуації, про що часто явно не повідомляється [11].

В контексті емпіричних досліджень, які керуються кількісними моделями, вимірювання займає важливе місце. Проблема полягає в тому, що в галузі управління ланцюгами постачання використовуються переважно заходи, які більшою чи меншою мірою походять від управління операціями. Отже, ці заходи, як правило, орієнтовані лише на одну компанію і не враховують аспекти зовнішнього оточення. Отже, слід застосовувати заходи з управління ланцюгами постачання, які вирішують ці питання [12].

ВИСНОВКИ: Розглянуті моделі мають узагальнений вигляд, та не розглядають найбільш поширену проблему при побудові ланцюгів постачання – стохастичність процесів. Даний фактор можливо розглядати в спектрі синергії динамічного та стохастичного програмування, що дозволить підвищити якість процесу планування та управління ланцюгами постачання.

1. Харрингтон Дж., Эсселинг К. С., Ван Нимвеген Х. Оптимизация бизнес-процессов. Документирование, анализ, управление, оптимизация. СПб.: Азбука, 2002.
2. Mohammadi Bidhandi et al. Development of a New Approach for Deterministic Supply Chain Network Design. October 2009. European Journal of Operational Research 198(1):121-128.
3. Hokey Min. Essentials of Supply Chain Management, The: New Business Concepts and Applications. Pearson FT Press, 2015.
4. Christopher, M. Logistics and Supply Chain Management: Strategies for Reducing Cost and Improving Service. London: Financial Times Pitman Publishing, 1998.
5. Research Methodologies in Supply Chain Management, by Herbert Kotzab, Stefan Seuring, Martin Muller and Gerald Reiner. New York: Physica-Verlag, 2005.
6. Byrne, B. M. Structural Equation Modeling with AMOS – Basic Concepts, Applications and Programming, Lawrence Erlbaum Associates, Mahwah, 2001.
7. Meredith J. R., Raturi A., Amoako-Gyampah K., Kaplan B. Alternative research paradigms in operations, in: Journal of Operations Management, 1989.
8. Bertrand J. W. M., Fransoo J. C. Modelling and simulation: Operations management research methodologies using quantitative modeling, in: International Journal of Operations & Production Management, 2002.
9. Forrester J. W. Industrial Dynamics. Cambridge: MIT Press, 1961.
10. Fine C. H. Clockspeed: Winning Industry Control in the Age of Temporary Advantage. Cambridge: Perseus Books, 1998.
11. Bertrand J. W. M., Fransoo J. C. Modelling and simulation: Operations management research methodologies using quantitative modeling, in: International Journal of Operations & Production Management, 2002.
12. Reiner, G. Supply chain performance measurement with customer satisfaction and uncertainties, in: Spengler, 2004.

**Тітова Н.В.,
Прокопович І.В.**

Одеський національний політехнічний університет (Одеса)

[*tnv.titova@gmail.com*](mailto:tnv.titova@gmail.com)

ЗАСТОСУВАННЯ 3D ДРУКУ В МЕДИЦИНІ

The development of 3D technologies, the widespread distribution and improvement of 3D printers, as well as the development and use of new materials and their combinations contributes to the widespread adoption of 3D printers in medicine.

Keywords: *3D printer, biomedicine, 3D models, bioprinting.*

Слід зазначити, що медицина стала однією з перших галузей, яка оцінила потенціал 3D принтерів. Вчені провідних дослідницьких біомедичних центрів розробляли технології та матеріали які використовували для друку макетів частин людського тіла, зубів, протезів та імплантів. Сьогодні, японськими біомедичними інженерами проходить тестування відкритого методу друку біологічним матеріалом, а саме клітин нирки.

Сьогодні можливості 3D-принтерів використовують в таких медичних напрямках, як:

Протезування. Повністю функціональні кінцівки дозволяють людям, які втратили їх, жити повноцінним і насиченим життям. Найчастіше такі протези розробляються разом з пацієнтом, з урахуванням усіх його побажань до зовнішнього вигляду пристрою. Моделі не тільки враховують індивідуальні анатомічні особливості людини, а й можуть підлаштовуватися під зміни рівня рідини в організмі завдяки еластичним внутрішнім вкладкам.

Стоматологія. Ця область стала використовувати 3D-друк однією з перших. Якщо раніше, до відкриття можливостей адитивних технологій, стоматологічні коронки виготовлялися кілька тижнів зубними техніками, то тепер лікар може прямо на місці роздрукувати коронку по 3D-знімку зуба пацієнта. Отриманий результат буде відрізнятися абсолютною точністю, на відміну від коронок, зроблених вручну.

Імплантація. За допомогою 3D-друку створюють елементи черепної коробки, суглоби, хребці, щелепи та інше. Наприклад, в 2016 році в Південній Кореї зробили пересадку роздрукованої з титану черепної коробки. Цей легкий і міцний матеріал вважається найкращим для створення імплантів, так як вкрай рідко відторгається організмом. Також відомо про множинні успішні операції по

установці серцевих клапанів, слухових кісточок і ділянок кровоносних судин. Потенційно робочі органи типу серця і легенів друкують, починаючи з 2011 року, проте, пересадка таких протезів досі не проводилася, з огляду на високий ступінь ризику для життя людини.

Біопрінтинг. Це новий перспективний напрямок, що знаходиться в стадії освієння. Це допоможе вирішити проблему очікування і відторгнення донорських органів. Передбачається, що вирощений таким чином орган буде не тільки ідеально сумісний з тілом пацієнта, але і продовжить рости разом з ним, що виключить необхідність повторних трансплантацій. Уже сьогодні вчені навчилися друкувати, наприклад, печінкові тканини, що дуже допомагає в дослідженнях впливу на печінку гепатопротекторів.

Таким чином, 3D-друк - напрямок перспективний і з великим потенціалом. Основні переваги, на мій погляд, це швидкість, універсальність, простота у використанні, низька ймовірність помилок, можливість створення штучних тканин та органів, протезів, імплантів і, навіть, створення складних біологічних продуктів харчування, що складаються з різних комплексів білків, жирів, вуглеводів і вітамінів.

ЛІТЕРАТУРА

1. 3D печать. Коротко и максимально ясно (LittleTinyH Books), 2016. 73 с.
2. Токарев Б.Е., Токарев Р.Б. Анализ рыночных перспектив технологий 3D-биопечати // Интернет-журнал «Науковедение» — 2016 — Т. 8 — №2. <https://naukovedenie.ru/PDF/33EVN216.pdf>.
3. Землянов Г. С., Ермолаева В. В. 3D-моделирование // Молодой ученый. — 2015. — №11. — С. 186-189.
4. Горбатов Р.О., Романов А.Д. Создание органов и тканей с помощью биопечати. Вестник ВГМУ. – Т.3. – с. 30-39.
5. Freedman D.H. Layer By Layer. MIT Technology Review 2011: 115 (1), 50 – 3.

¹Толюпа С.В., ²Наконечний В.С., ³Браїловський М.М., ⁴Касьянов П. П.

^{1,2,3}КНУ імені Тараса Шевченка, tolupa@i.ua, nvc2006@i.ua

⁴Національний авіаційний університет, hashltcbtc@gmail.com

ЗАСТОСУВАННЯ ПРОГРАМНОГО ПРОДУКТУ SPLUNK MACHINE LEARNING TOOLKIT В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

The material discusses the creation of tools that allow the detection of security threats in combination with elements of artificial intelligence and machine learning, which makes such tools valuable assistants to security analysts. It is recommended to use the considered Splunk software for incident management in case of small cases, and also for training and demonstration of working processes for students; or in those organizations whose budget allows you to use such a tool at full capacity, because its capabilities are really great.

Key words: *information technologies, incidents, threats, software, artificial intelligence*

Компанії можуть мати десятки, сотні, або, можливо, тисячі прикладних і веб-серверів, баз даних і мережевих пристроїв, таких як комутатори, маршрутизатори й брандмауери. Всі вони створюють файли журналів або потоки даних, які фіксують їхню діяльність і стан з плином часу. Якщо потрібно вручну усунути проблему, яка викликана будь-якою з декількох частин системи, необхідно увійти до кожної з цих машин по черзі, вручну вивантажити файл журналу, шукаючи підказки. Цей процес є досить рутинним і трудомістким. Крім того, необхідна велика кількість персоналу, щоб контролювати критичні процеси й мати впевненість, що все працює належним чином.

Проте на сьогоднішній день існують можливості для автоматизації таких процесів. Наприклад, програмні платформи, які збирають і зберігають всі дані машин в одному місці. Завдяки цьому можна легко здійснювати пошук і досліджувати ці дані. Крім того, існують інструменти для створення звітів і панелей для контролю продуктивності, надійності або інших показників у всій сукупності відповідних серверів і пристроїв. Можна навіть створювати сповіщення та налаштовувати попередження за допомогою смс-повідомлень або електронної пошти, коли щось відбувається неправильно. Можливість виявлення загроз безпеці в поєднанні з елементами штучного інтелекту та машинного навчання роблять такі інструменти цінними помічниками аналітиків безпеки [1].

Одним із таких інструментів є Splunk. Splunk – американська компанія, розробник програмного забезпечення для обробки та аналізу машинно-згенерованих даних.

Основний програмний продукт компанії – однойменна система аналізу операційної діяльності в області інформаційних технологій, що збирає й аналізує великі обсяги машинних даних з усіх фізичних, віртуальних і хмарних середовищ ІТ-інфраструктури організації. Зібрані дані індексуються та система перетворює машинні дані в формат «ключ – значення», після цього дані стають доступними для пошуку та аналізу через веб-інтерфейс. Схема обробки даних продукту орієнтована на роботу з довільними форматами з системних журналів.

Система дозволяє здійснювати пошук як за даними в режимі реального часу, так і за архівними даними. На основі результатів пошуку Splunk дає можливість: аналізувати отримані результати за допомогою засобів візуалізації (використовується бібліотека D3.js), формувати звіти і попередження, створювати систему моніторингу та повідомлень у реальному часі. Передбачена можливість розширення – можна створювати нові додатки засобами спеціалізованої платформи розробки, що поставляється зі Splunk.

Продукт застосовується для пошуку й усунення недоліків у ІТ-інфраструктурі, моніторингу порушень системи безпеки, запобігання атак, отримання інформації для бізнес-аналітики, оптимізації робочого процесу підприємства й збільшення продуктивності, для роботи з різноманітними великими масивами промислових даних і даними від IoT.

Splunk є одним з найбільш популярних і перевірених часом рішень SIEM на ринку. Він має більше 15 000 клієнтів у всьому світі. У цьому матеріалі ми розглянемо деякі функції Splunk, що забезпечують моніторинг безпеки та оповіщення, і як наслідок, можуть бути використані в процесі управління інцидентами безпеки [2].

Splunk, в більшості випадків, розбирає вхідні дані на поля і значення і надалі обробляє їх. Обробка відбувається за допомогою SPL запитів – спеціальна мова від Splunk – за допомогою якої можна будувати різні вибірки і таблиці, сортувати, фільтрувати, агрегувати, будувати звіти, створювати обчислювані поля, звертатися як до внутрішніх, так і зовнішніх довідників, створювати дашборди з широким спектром візуалізації і робити алерти (наприклад, за результатами виконання запиту відправляти тікети в Service Desk) [3].

Splunk як платформа надає цілий ряд субпродуктів, які задовольняють певні організаційні потреби [4].

Крім того, що Splunk може збирати логи практично з будь-яких джерел і будувати аналітичні звіти, дашборди та алерти на основі вбудованої мови пошукових запитів SPL, Splunk ще має дуже велику базу безкоштовних аддонів і додатків.

Розглянемо один з найпопулярніших, з точки зору користувачів, додаток – Splunk Machine Learning Toolkit. Варто зазначити, що Splunk Machine Learning Toolkit вузькоспеціалізований. Він підтримує тільки алгоритми навчання без учителя, і має дуже конкретне застосування.

Так як Splunk в першу чергу орієнтований на машинні дані, то і кейси, реалізовані в Machine Learning Toolkit, спрямовані на цю специфіку. Сам додаток безкоштовно доступний для скачування на Splunkbase, але так як всі алгоритми штучного інтелекту й машинного навчання застосовують Python, то перед завантаженням потрібно встановити Python for Scientific Computing Add-on.

Додаток містить шість модулів з базовими статистичними алгоритмами, кожен з яких має особливості застосування та окреме призначення [5]:

1. Predict Numeric Fields. Цей модуль робить прогнозування значень числових полів на основі комбінації значень інших полів у цій події.

Для прогнозування числових значень використовується алгоритми регресії. Такі моделі корисні для визначення того, наскільки певні периферійні фактори сприяють певному результату метрики. Після того, як інструмент обчислить модель регресії, можна використовувати ці периферійні значення, щоб зробити прогноз результату метрики [6].

Рисунок 1.1 ілюструє діаграму розсіювання фактичних і прогнозованих результатів. Ця візуалізація є прикладом демонстрації енергоспоживання сервера.

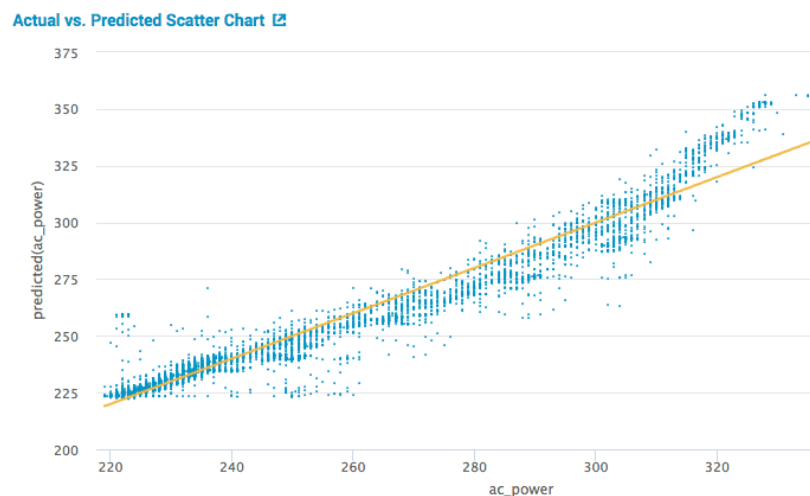


Рисунок 4.1 – Діаграма розсіювання фактичних і прогнозованих результатів енергоспоживання сервера

2. Detect Numeric Outliers. Даний модуль виявляє аномальні значення на основі попередніх даних по цьому полю.

Виявлення числових відхилень полягає у визначення значень, які здаються надзвичайно вищими або нижчими, ніж інші дані. Ідентифіковані відхилення свідчать про цікаві, незвичайні та, можливо, небезпечні події [7].

На рисунку 4.2 жовті точки вказують на відхилення.

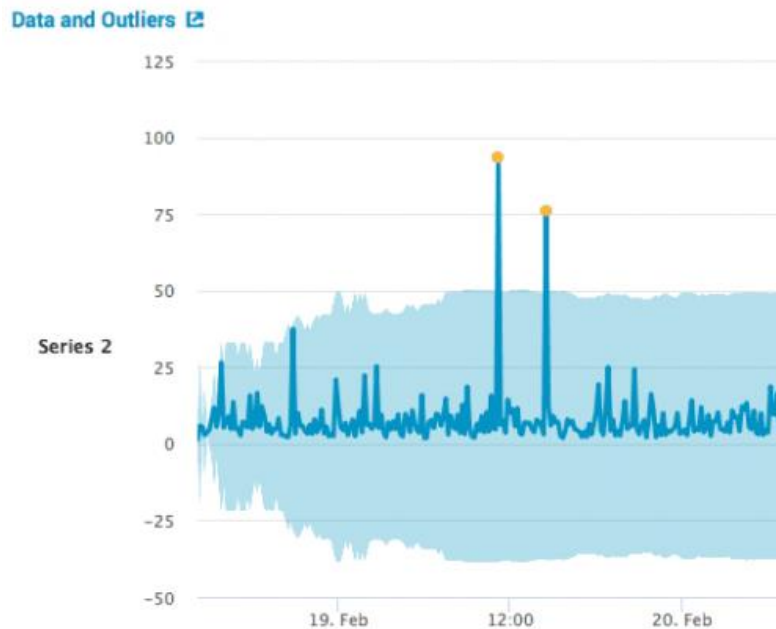


Рисунок 4.2 – Виявлення числових відхилень модулем Detect Numeric Outliers

3. Forecast Time Series. Даний модуль призначений для прогнозування часових рядів, тобто на основі минулих даних може спрогнозувати майбутні. Модуль прогнозує наступне значення в послідовності даних часових рядів. Результат включає як прогнозовану величину, так і міру невизначеності цього прогнозу. Прогнозування відбувається на основі даних часових рядів з минулого [30].

4. Predict Categorical Fields. Даний модуль призначений для прогнозування категоріальної, тобто якісної змінної на основі інших полів у цій події. Алгоритм класифікації вивчає тенденцію, чи належать дані до однієї категорії або іншої на основі пов'язаних даних [8].

5. Detect Categorical Outliers. Модуль призначений для пошуку аномалій на основі аналізу значень полів у події.

Модуль ідентифікує дані, які вказують на цікаві або незвичайні події. Він працює з нечисловими та багатовимірними даними, такими як ідентифікатори рядків та IP-адреси. Якщо декілька полів у сукупності мають рідкісні значення, результатом є відхилення [9].

6. Cluster Numeric Events. Модуль, що дозволяє виробляти кластеризацію подій. Розділяє події з кількома числовими полями на групи на основі значень цих полів [10].

Усі модулі мають керований інтерфейс користувача.

Під час розгляду роботи Splunk machine learning toolkit, було виявлено наступні переваги даного програмного забезпечення:

- Splunk створює таблиці та моделі з величезної кількості даних з різних систем, що насправді є трудомістким процесом (він їх збирає, зберігає і робить первинну обробку).

- Забезпечується можливість швидкого статистичного аналізу.
- У Splunk відкритий API і якщо вбудованих алгоритмів виявиться недостатньо, то можна їх довантажити з відкритих Python бібліотек.

Програма дозволяє вирішувати завдання пошуку, моніторингу, аналізу та профілактики у всіх областях ІТ, проте найбільшу віддачу для бізнесу приносить її застосування в таких областях як:

- Забезпечення інформаційної безпеки, що допомагає відповідати вимогам чинного законодавства.
- Управління інфраструктурою ІТ.
- Управління ІТ-додатками.
- Управління комп'ютерними мережами і їх безпекою.
- Бізнес-аналітика.

Враховуючи наведені вище плюси даної програми, рекомендується використовувати її на підприємствах як для виявлення інцидентів ІБ, так і для аналізу ризиків, побудови звітів та прогнозів.

Таким чином, рекомендується використовувати розглянуте ПЗ у будь-яких організаціях для управління інцидентами у випадку невеликих кейсів (коли вистачатиме 500 Мб безкоштовного простору на день), а також для навчання та демонстрації робочих процесів для студентів; або у тих організаціях, бюджет яких дозволяє використовувати такий інструмент на повну потужність, адже його можливості є дійсно великими.

Наостанок, варто врахувати, що Splunk – дуже потужний інструмент, але основа його могутності – це люди, які зможуть їм правильно скористатися. Навіть

впровадження і підтримка Splunk вимагає ресурсів. Тому наявність такого ПЗ потребує відповідної кількості кваліфікованого персоналу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. James H. Baxter. Splunk 7.x Quick Start Guide [Електронний ресурс] / James H. Baxter // Packt Publishing. – 2018. – Режим доступу: <https://learning.oreilly.com/library/view/splunk-7x-quick/9781789531091/>
2. Splunk [Електронний ресурс] // Википедія – Режим доступу: <https://ru.wikipedia.org/wiki/Splunk>
3. Manish Kumar. Artificial Intelligence for Big Data [Електронний ресурс] / Manish Kumar, Anand Deshpande // Packt Publishing. – 2018. – Режим доступу: <https://learning.oreilly.com/library/view/artificial-intelligence-for/9781788472173/>
4. Alex Kulakov. Splunk — общее описание платформы, базовые особенности установки и архитектуры [Електронний ресурс] / Alex Kulakov // сайт tssolution.ru. – 2017. – Режим доступу: <https://habr.com/ru/company/tssolution/blog/323814/>
5. Alex Kulakov. Обзор Splunk Machine Learning Toolkit [Електронний ресурс] / Alex Kulakov// сайт tssolution.ru. – 2017. – Режим доступу: <https://habr.com/ru/company/tssolution/blog/327943/>
6. Predict Numeric Fields Classic Assistant [Електронний ресурс] – Режим доступу: <https://docs.splunk.com/Documentation/MLEApp/4.2.0/User/PNFlegacyassist>
7. Detect Numeric Outliers Classic Assistant [Електронний ресурс] – Режим доступу: <https://docs.splunk.com/Documentation/MLEApp/4.2.0/User/DNOlegacyassist>
8. Forecast Time Series Classic Assistant [Електронний ресурс] – Режим доступу: <https://docs.splunk.com/Documentation/MLEApp/4.2.0/User/FTSlegacyassist>
9. Predict Categorical Fields Classic Assistant [Електронний ресурс] – Режим доступу: <https://docs.splunk.com/Documentation/MLEApp/4.2.0/User/PCFlegacyassist>
10. Detect Categorical Outliers Classic Assistant [Електронний ресурс] – Режим доступу: <https://docs.splunk.com/Documentation/MLEApp/4.2.0/User/DCOlegacyassist>

¹Толюпа С.В., ²Шестак Я.В., ³Кулько А.А., ⁴Чечуга А.М.
^{1,2,3}*КНУ імені Тараса Шевченка, tolupa@i.ua, yaninashestak@gmail.com*
⁴*Національний авіаційний університет, ccg.barbour@gmail.com*

АВТОМАТИЗАЦІЯ ПРОЦЕСУ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

With the right automated incident response tools, you can set up automated systems to protect the most critical data. Automated incident response capabilities can speed up response processes and reduce the proportion of manual work. Most importantly, it can help minimize the potential damage that an incident can cause to the organization and customers. Automation makes the whole incident response process faster and more efficient.

Keywords: incidents, security, threats, automation, cloud technologies, Internet of Things.

Протягом довгого часу інформаційна безпека була війною між людьми. Механізм захисту в значній мірі був кордоном через брандмауери, проксі, антивірусне програмне забезпечення, засоби контролю доступу, динамічні паролі тощо. Однак ці старі методи починають здаватися невідповідними сьогодні, оскільки поле бою змінилося на людину проти машини. Зі збільшенням кількості точок входу в корпоративні системи та кількості підключених пристроїв як кінцевих точок, новини про порушення безпеки з'являються частіше, ніж раніше.

Хмарні технології, Інтернет речей, і BYOD (Bring Your Own Device – принеси свій власний пристрій на роботу) дають початок мікросередовищам, які містять багато чутливих даних про користувача. Якщо ці пристрої потраплять в чужі руки, це, звичайно, може призвести до серйозних наслідків. Ситуація є ще більш небезпечною, коли мова йде про нові типи атак, які в основному розробляються машиною. Наприклад, адаптивна шкідлива програма створюється за допомогою техніки машинного навчання. Цей тип шкідливого програмного забезпечення може проникнути в систему, зібрати та передати дані про цю систему і залишатися непоміченими протягом декількох днів.

Застосування старого підходу до збору інформації про порушення даних, типи шкідливих програм та фішинг-діяльність вже не є достатньо потужним для роботи з новим поколінням кібератак. Стандартні автоматизовані системи виявлення загроз, хоч і вдосконалюються, не завжди можуть швидко реагувати на непередбачені або новоутворені загрози.

Новий підхід вимагає постійного моніторингу великої кількості факторів і виявлення того, що являє собою аномальну активність. Машини повинні застосовувати методи самонавчання, щоб визначити, що може бути зловмисною діяльністю, не знаючи, що саме шукати. Цей новий підхід можна порівняти з діяльністю організму людини, де білі клітини й антитіла безперервно сканують і нейтралізують будь-який організм, який не відповідає нормальному функціонуванню. Таку роль може виконувати штучний інтелект. Алгоритми машинного навчання можуть розпізнавати потенційні порушення безпеки або атаки шляхом постійного спостереження за ненормальною поведінкою, і якщо їм надано повноваження і права, вони можуть автоматично вимикати системи під сприйнятою загрозою, зменшуючи або ізолюючи ризики для всього підприємства [1].

Компанії в усьому світі інвестують у штучний інтелект і автоматизацію, щоб поліпшити свої бізнес-процеси, підвищити продуктивність і ефективність роботи. Банки вивчають нові способи виявлення шахрайства у банкоматних мережах, страхові компанії вивчають, як використовувати штучний інтелект для прогнозування прибутковості своїх послуг, а брокери почали застосовувати штучний інтелект для прогнозування руху на фондових ринках [2].

Автоматизація визначається як техніка, метод або система управління або контролю процесу високоавтоматичними засобами, що зводить до мінімуму втручання людини. Автоматизація насправді являє собою ручні правила та процеси, які повторюються автоматично. Ніякі нові знання у процесі автоматизації не здобувають, на відміну від діяльності штучного інтелекту чи машинного навчання. Автоматизація часто є кінцевим результатом систем штучного інтелекту й машинного навчання в організації. Наприклад, організація може використовувати штучний інтелект і машинне навчання для виявлення підозрілої діяльності, а потім застосовувати автоматизацію для автоматичного надання сповіщень про цю діяльність або навіть вживати заходів для її припинення. Іншими словами, автоматизація може бути видимим результатом систем застосування штучного інтелекту, наприклад [3].

При автоматизації процесів управління інцидентами в першу чергу необхідно приділяти увагу автоматизованій обробці подій інформаційної безпеки – основі практично будь-якого інциденту. Події від різних технічних засобів захисту є найважливішим джерелом інформації про процеси, що відбуваються в системі управління інформаційною безпекою (далі – СУІБ), порушення та ризики. На підставі подій проводяться коригувальні дії, оцінка поточної захищеності системи, ефективності функціонування СУІБ. Тільки маючи повний і достовірний перелік

подій, можна провести належне розслідування інцидентів, отримати уявлення про динаміку розвитку СУІБ. Можна сказати, що події – основний канал зворотного зв'язку для керуючих впливів у рамках СУІБ. Важливим є і те, що події легко документовані та відтворювані.

Організація процесу обробки подій без використання засобів автоматизації являє собою складну і трудомістку задачу. Необхідно збирати й консолідувати велику кількість даних у різних форматах, вести центральний архів. Для ручної обробки подій потрібна велика кількість висококваліфікованих фахівців-аналітиків.

Через наявність великого обсягу рутинної ручної роботи обробка подій часто буває неповною та не відбиває реальний стан поточної ситуації. При цьому можлива ситуація, коли події, критичні для надійного і захищеного функціонування бізнес-систем, виявляться поза увагою аналітиків, і що до них не будуть приймаються відповідні превентивні заходи.

Для підтримки процесу обробки подій на рівні, відповідному сучасним вимогам, можливо застосування різних автоматизованих систем обробки подій (далі – СОП).

СОП повинні забезпечувати наступний функціонал:

- дозволяти збирати події від всіх технічних засобів забезпечення захисту, використовуваних в рамках СУІБ, виробляти нормалізацію подій, приводячи їх до єдиного формату; здійснювати фіксацію подій способом, що дозволяє зберігати необхідні обсяги даних;
 - надавати інструментарій для пошуку в сховище даних;
 - надавати механізми формування звітів різного роду;
 - бути здатними до розширення і масштабування;
 - опціонально здійснювати кореляцію зібраних подій.

Процес обробки подій автоматизованими системами включає наступні основні кроки: нормалізація (приведення до єдиного формату) даних, агрегування (накопичення), кореляція та візуалізація.

На перших двох стадіях інформація про події безпеки збирається практично з усіх використовуваних у рамках СУІБ засобів захисту: міжмережевих екранів, систем виявлення атак, антивірусних систем, операційних систем і додатків різних виробників, а також засобів контролю фізичного доступу. Зібрана інформація перетворюється в єдиний, зручний для розуміння формат, піддається кореляції і виводиться на консоль оператора системи. Розвинені засоби пошуку дозволяють проводити оперативне та всебічне розслідування інцидентів, забезпечувати

свідчення наявності і функціонування засобів захисту в рамках СУІБ при проведенні різних аудитів [4].

Розглянемо деякі приклади автоматизації реагування на інциденти, порівнюючи їх з тим, що потрібно для обробки вручну. Спробуємо зрозуміти, які автоматизовані можливості реагування на інциденти матимуть найбільший вплив на процеси та часові рамки.

1. Взаємодія користувача зі шкідливою IP-адресою. Необхідно оновити брандмауер, щоб заблокувати IP-адресу.

Брандмауери допомагають захиститися від зловмисників шляхом фільтрації мережевого трафіку. Тим не менш, вони мають межі. Більшість брандмауерів не підключено до інших інструментів безпеки, а їх правила нечасто оновлюються, тобто вони можуть не бути актуальними для протидії останнім загрозам. Вирішення цієї ситуації тягне за собою виявлення проблеми за допомогою іншого програмного забезпечення, визначення пріоритетів події та ручне оновлення брандмауера за допомогою нового правила для блокування шкідливої IP-адреси.

Завдяки автоматизованому реагуванню на інцидент можна автоматично оновлювати брандмауер, щоб блокувати шкідливі IP-адреси, коли вони з'являються. Наприклад, програми такого типу можуть виявляти трафік із зовнішньої IP-адреси, який через інтегрований інтелект розпізнається, як шкідливий. Брандмауери нового покоління можуть блокувати або ізолювати IP-адресу, використовуючи автоматичну або ручну реакцію на інцидент.

2. Зараження системи шкідливим програмним забезпеченням. Потрібно мінімізувати збитки й дізнатися, скільки систем вразливі до того, як пошириться шкідлива програма.

Спираючись на ручні процеси, щоб впоратися зі шкідливим програмним забезпеченням, існує довгий алгоритм: ідентифікувати всі заражені системи, проаналізувати загрози, зібрати журнали подій з різних місць тощо.

Автоматизовані інструменти реагування на інциденти можуть скоротити список справ. За допомогою спеціальних інструментів, можна автоматизувати дії, такі як отримання додаткових даних для розслідування, вимкнення мереж на інфікованій системі, автоматичне сканування вразливостей для виявлення інших систем, які знаходяться в зоні ризику, а також їх ізоляцію до можливості виправити інцидент. Завдяки автоматизації заходів реагування на інциденти можна працювати швидше та ефективніше.

3. Визначення обсягу шкідливих наслідків інциденту.

Розслідування порушення допоможе отримати критичну інформацію про те, що сталося, і як інцидент впливає на організацію. Якщо порушено властивості

конфіденційної інформації клієнтів, потрібно знати відразу. Однак, щоб отримати потрібну інформацію, часто потрібно мати справу з повторюваними, ручними діями, такими як перехід до кожної системи, щоб переглянути події та журнали, щоб спробувати зрозуміти, як відбулося порушення та що було скомпрометовано.

Наявність рішення з можливостями управління журналами дозволить працівникам шукати відповідні сигнали та події, а не переглядати й аналізувати їх вручну. Наприклад, можна налаштувати програму на об'єднання подій та журналів з усіх систем і мереж та отримати потрібну інформацію відразу за допомогою потужних можливостей пошуку та фільтрації. Можна здійснювати пошук подій або нагадувань на основі критеріїв, наприклад типу події, назви джерела, імені користувача та групи активів, а також можна ознайомитися з детальною інформацією про кожну подію.

4. Взаємодія однієї з систем із сервером Command&Control для засобу віддаленого адміністрування – remote administration tools (далі – RAT). Необхідно заблокувати будь-яке подальше спілкування зі зловмисним доменом.

Якщо інструмент IDS виявляє трафік з відомого зловмисного домену, наприклад, сервера C2, потрібно виконати низку дій, щоб розібратися з ситуацією та дослідити область потенційного вторгнення. Однією з таких дій є блокування відомого зловмисного домену, щоб запобігти подальшому спілкуванню. Можна вручну записати домен до списку заблокованих.

Завдяки можливостям автоматизації можна негайно перейти від виявлення до відповіді, автоматично блокуючи домен, коли система виявлення вторгнення знаходить загрозу.

5. Поява нового експлойту, який використовує вразливість у використовуваній операційній системі. Потрібно виявити, чи є вразливими системи організації, і якщо так, то вжити заходів.

Коли план безпеки спирається на велику кількість ручної роботи, вивчення нових варіантів атак і способів захисту активів можуть викликати навіть паніку. Потрібно не лише переконатися, що організація залишається у безпеці, а також заспокоїти інших зацікавлених сторін [5].

У цьому випадку автоматизація може допомогти до того, як інцидент навіть виникне. Продукт, який додає актуальні результати розвідки загроз у план безпеки організації, може гарантувати, що відбувається оновлення нових уразливостей та загрози без необхідності робити власні дослідження та створювати правила виявлення загроз. Завдяки автоматичному скануванню вразливостей, запланованому для регулярних інтервалів часу, ви можете бути в курсі ризиків, які виникають у вашій інфраструктурі, коли з'являються нові уразливості, що

дозволяє вам або виправити їх, або обмежити їх вплив на решту мережі. Коли ви дізнаєтеся про нові зловмисні програми в новинах, ви можете бути впевнені, що знаєте рівень ризику вашої організації.

6. Реагування команди на інцидент. Необхідно стежити за діями команди людей, які займаються розслідуванням.

Навіть з інструментами автоматизації, реакція на інцидент може включати багато різних дій для команди аналітиків з безпеки (або для однієї відповідальної особи). Без можливості відстежувати діяльність з IP, легко втратити ключові пріоритети або зосередитися на неправильних завданнях. Наприклад, двоє членів команди можуть із запізненням дізнатися, що вони працювали над тим самим питанням, витрачаючи час, який не може дозволити собі втратити команда, обмежена ресурсами.

На щастя, деякі рішення містять інструменти, які допоможуть відстежувати зусилля команди.

7. Виявлення підозрілої активності на сервері, на якому зберігаються важливі дані клієнта.

Кожна організація має свої унікальні інфраструктурні потреби та пріоритети, що робить універсальну автоматизацію безпеки непрактичною та потенційно руйнівною. Недоцільно вимикати критично важливі для бізнесу системи щоразу, коли в одному з середовищ виникає помилково-позитивний сигнал. Однак для певних ситуацій негайне реагування на інцидент може перешкодити виникненню значних збитків.

За допомогою правильних інструментів автоматизованого реагування на інциденти можна налаштувати автоматизовані відповіді для захисту найбільш критичних даних. Наприклад, якщо на певному сервері з'являються ознаки вторгнення, можна налаштувати правило для автоматичного вимикання мережі з метою захисту даних. Для критично важливого для бізнесу сервера, який не можна вимкнути, можна налаштувати відправку автоматичних сповіщень електронною поштою або SMS-повідомленням на мобільний телефон. Правила можна налаштувати у відповідності з конкретними потребами безпеки організації.

Таким чином, у наведених вище прикладах відповідні автоматизовані можливості реагування на інциденти можуть прискорити процеси реагування та зменшити частку ручної роботи. Найголовніше, це може допомогти мінімізувати потенційний збиток, який інцидент може спричинити для організації та клієнтів.

Автоматизація робить весь процес реагування на інциденти більш швидким і ефективним. Основні процеси, які можуть бути автоматизовані, включають: виявлення активів, сканування вразливостей, виявлення вторгнень, моніторинг

поведінки, інструменти керування інцидентами та подіями безпеки – Security information and event management (далі – SIEM) та управління журналами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

11. Мелехин И. Управление инцидентами [Електронний ресурс] / Мелехин// JetInfo. –2008. – Режим доступу: <http://www.jetinfo.ru/stati/upravlenie-intsidentami/>

12. Sachin Vyas. How to Compete in the Age of Artificial Intelligence: Implementing a Collaborative Human-Machine Strategy for Your Business [Електронний ресурс] / Sachin Vyas, Soumendra Mohanty // Apress. – 2018. – Режим доступу: <https://learning.oreilly.com/library/view/how-to-compete/9781484238080/>

13. Milad Aslaner. Hands-On Cybersecurity for Finance [Електронний ресурс] / Milad Aslaner, Dr. Erdal Ozkaya // Packt Publishing. – 2019. – Режим доступу: <https://learning.oreilly.com/library/view/hands-on-cybersecurity-for/9781788836296/>

14. Laurent Gil. Security with AI and Machine Learning [Електронний ресурс] / Laurent Gil, Allan Liska // O'Reilly Media, Inc. – 2019. – Режим доступу: <https://learning.oreilly.com/library/view/security-with-ai/97814/>

15. Julia Kisielius. Automated Incident Response in Action: 7 Killer Use Cases” [Електронний ресурс] / Julia Kisielius // AT&T Business. – 2017. – Режим доступу: <https://www.alienvault.com/blogs/security-essentials/>.

Хижняк А.О, Толюпа С.В., Пархоменко І.І.

Київський національний університет імені Тараса Шевченка

vetrafiar@gmail.com

ОСНОВНІ КРИТЕРІЇ ГОТОВНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ НЕПЕРЕРВНОСТІ РОБОТИ БІЗНЕСУ

The main criteria for the readiness of information and communication technology for business continuity is presented. These criteria should be based on the requirements of information and communication technology readiness to ensure business continuity, as well as on common goals in terms of incident response and continuity requirements.

Key words: *information and communication technology; business continuity.*

Інформаційні технології (ІТ) стали складовою частиною багатьох видів діяльності, які є елементами критичних інфраструктур у всіх секторах: державному, приватному чи громадському.

Для багатьох організацій готовність ІТ є найважливішою складовою в реалізації менеджменту безперервності бізнесу і менеджменту інформаційної безпеки.

В результаті ефективність менеджменту безперервності бізнесу часто залежить від фактичної готовності ІТ, що забезпечує впевненість у тому, що в період порушення продовжують виконуватися мети організації. Це особливо важливо у зв'язку з тим, що наслідки порушень ІТ часто мають додаткові ускладнення, будучи прихованими і (або) важко виявляються.

Готовність ІТ до забезпечення безперервності бізнесу ґрунтується на наступних ключових принципах:

- попередження інцидентів - захист послуг ІТ від таких загроз, як несприятливий вплив зовнішнього середовища і апаратні збої, операційні помилки, зловмисні атаки і природні лиха, є вкрай важливим для підтримки бажаних рівнів доступності систем в організації;

- виявлення інцидентів - найшвидше виявлення інцидентів буде зводити до мінімуму їх вплив на послуги, скорочувати роботи по відновленню і зберігати якість послуг;

- реагування - реагування на інцидент найбільш підходящим способом призведе до більш ефективного відновлення і зменшить будь-які простой. Невдале

реагування може привести до переростання незначного інциденту в щось більш серйозне;

- відновлення - визначення і реалізація відповідної стратегії відновлення забезпечуватиме впевненість у своєчасному відновленні послуг і підтримки цілісності даних. Розуміння пріоритетів відновлення дозволить відновлювати в першу чергу найкритичніші послуги. Послуги, що носять менш критичний характер, можуть відновлюватися пізніше або, за деяких умов, взагалі не відновлюватися;

- вдосконалення - уроки, засвоєні з реагування на дрібні і великі інциденти, повинні документуватися, аналізуватися і переглядатися. Розуміння цих уроків дасть можливість організації краще готуватися, контролювати і уникати інцидентів і порушень [1].

Рисунок 1 ілюструє, яким чином відповідний елемент готовності ІТ до забезпечення безперервності бізнесу підтримує типову тимчасову послідовність відновлення ІТ після лиха і, в свою чергу, підтримує діяльність щодо забезпечення безперервності бізнесу. Реалізація готовності ІТ до забезпечення безперервності бізнесу дає можливість організації ефективно реагувати на нові й виникаючі загрози, а також реагувати на порушення і відновлюватися після них.

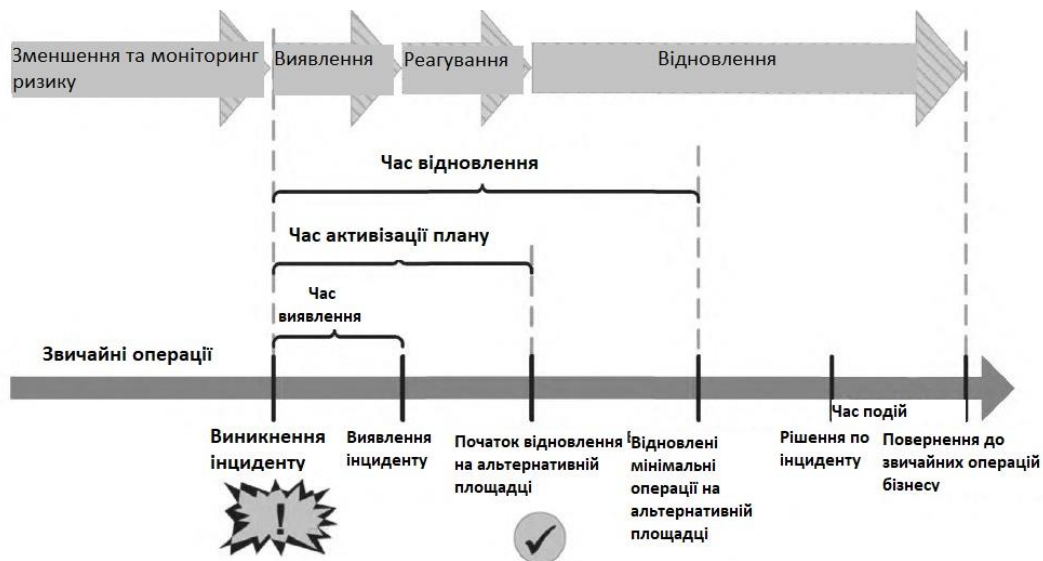


Рисунок 1. Відповідність елементу готовності ІТ до забезпечення безперервності бізнесу

Ключові елементи готовності ІТ до забезпечення безперервності бізнесу можна узагальнити наступним чином:

- кадри: фахівці, що володіють відповідними навичками та знаннями, і компетентний резервний персонал;
- споруди: фізичне середовище, в якому розташовані ресурси ІТ;
- технічне оснащення:
 - апаратні засоби (сервери, дискові масиви, накопичувачі на магнітній стрічці і прилади);
 - мережі (включаючи послуги передачі даних і голосу), комутатори та маршрутизатори;
 - програмні засоби, включаючи операційну систему і прикладні програми, зв'язок або інтерфейси між прикладними програмами і підпрограми пакетної обробки даних;
 - дані: дані прикладних програм, голосові дані та інші види даних;
 - процеси: відновлення і підтримки послуг ІТ, включаючи підтримуючу документацію для опису конфігурації ресурсів ІТ і створення можливості ефективного функціонування;
 - постачальники: компоненти ланцюжка постачання послуг, де надання послуг ІТ залежить від зовнішнього постачальника послуг або іншої організації, що беруть участь в ланцюжку поставок, наприклад, постачальник даних з фінансових ринків, постачальник телекомунікаційних послуг або постачальник Інтернет-послуг.

Готовність ІТ до забезпечення безперервності бізнесу, ймовірно, буде більш ефективною і рентабельною, коли вона спроектована і вбудована в послуги ІТ з самого початку, як частина стратегії готовності ІТ до забезпечення безперервності бізнесу, що підтримує цілі забезпечення безперервності бізнесу організації. Це забезпечить впевненість в тому, що послуги ІТ будуть краще створені, краще зрозумілі і більш стійкі. Зміна готовності ІТ до забезпечення безперервності бізнесу може бути складною та дорогою задачею, що викликає порушення [2].

Організація повинна розробляти, реалізовувати, підтримувати і постійно удосконалювати сукупність документально оформлених процесів, які будуть підтримувати готовність ІТ до забезпечення безперервності бізнесу.

Ці процеси повинні забезпечувати впевненість в тому, що цілі готовності ІТ до забезпечення безперервності бізнесу чітко викладені, зрозумілі і доведені до відома, а також демонструвати зацікавленість вищого керівництва в готовності ІТ до забезпечення безперервності бізнесу [3].

Рисунок 2 графічно показує види діяльності, що відбуваються на різних етапах забезпечення готовності ІТ до забезпечення безперервності бізнесу. Готовність ІТ до забезпечення безперервності бізнесу передбачає створення в

організації процесів розробки і вдосконалення ключових елементів готовності ІТ до забезпечення безперервності бізнесу, щоб підвищити їх здатність реагувати на порушення будь-якого виду, включаючи мінливі ситуації ризику, за допомогою використання підходу «Планування-Здійснення-Перевірка-Дія».

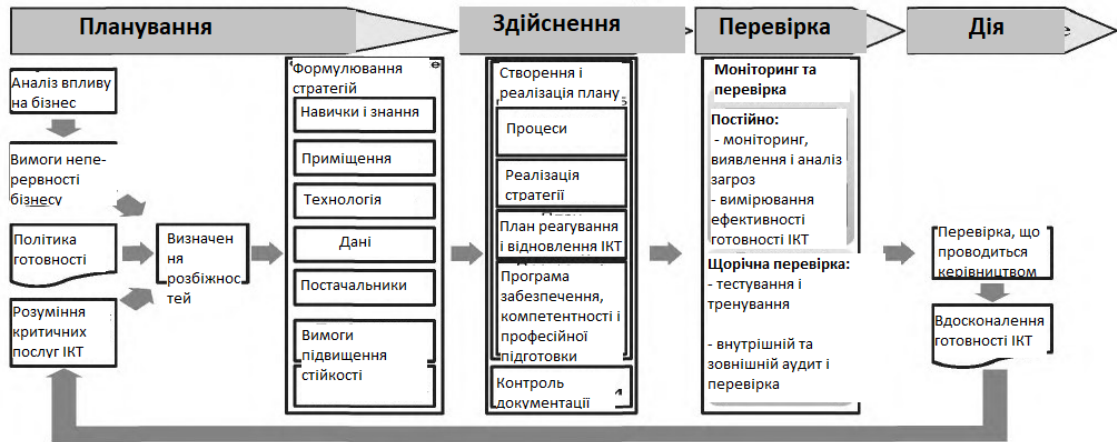


Рисунок 2. Види діяльності, що відбуваються на різних етапах забезпечення готовності ІТ до забезпечення безперервності бізнесу

Оскільки ефективність готовності ІТ до забезпечення безперервності бізнесу різниться в різних організаціях, кожна організація повинна розробити власні критерії ефективності готовності ІТ до забезпечення безперервності бізнесу і підтримувати їх як частину процесу постійного вдосконалення [4].

Основний підхід полягає у використанні відомих сценаріїв інцидентів і взаємопов'язаних подій, щоб встановити базовий рівень реагування для кожної категорії інцидентів і пов'язаних з ними подій наступним чином:

- встановлення в рамках процесів СМІБ відомих інцидентів і індикаторів подій в якості вхідних даних для подальших етапів;
- встановлення сукупності відомих інцидентів (наприклад, атака злому пароля, відмова сервера через нестачу місця на жорсткому диску);
- визначення подій, що ведуть до цих інцидентів (наприклад, невдала спроба входу в систему, використання жорсткого диска);
- визначення відповідного часу виявлення (наприклад, граничне значення для подій, про які повинні бути повідомлені та попереджені система / адміністратор);
- визначення відповідного часу реагування (наприклад, період часу для прийняття адміністратором заходів з метою запобігання реалізації інциденту);

- розподіл подій по групах, виходячи з необхідного часу реагування та видів заходів реагування;
- уточнення матриць і значень за допомогою тестування сценаріїв і навчань / тренувань;
- проведення тестування для визначення того, чи є заходи реагування здійсненними, а цілі досяжними;
- уточнення груп очікуваного часу реагування на подію і очікуваних заходів реагування на події (наприклад, пошук альтернативного методу моніторингу, виявлення та дій);
- вдосконалення шляхом збору інформації про нові інциденти і сценаріях відмови і повторення процесу [5].

Таким чином, можна зробити висновки, що організація повинна визначити критерії для вимірювання ефективності готовності її ІТ. Такі критерії можуть використовуватися для визначення бажаної якості реагування на порушення, як в термінах ефективності, так і в термінах результативності.

Критерії ефективності готовності ІТ до забезпечення безперервності бізнесу повинні бути засновані на вимогах готовності ІТ до забезпечення безперервності бізнесу, а також на спільних цілях з точки зору реагування на інциденти і вимог забезпечення безперервності.

ЛІТЕРАТУРА

1. Корченко О.Г., Гнатюк С.О., Казмірчук С.В. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. - К. : Центр навч.-наук, та наук.-пр. видань НА СБ України, 2014. - 190 с.
2. А. К. Гринь, О. Д. Довгань, В. І. Журавель Менеджмент інформаційної безпеки. підручник. -К. : Наук.-вид. центр НА СБ України, 2013. – Ч. 1. `456 с.
3. Гладиш С.В., Кононович В.Г., Тардаскін М.Ф. Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – № 15. – с. 31–39.
4. Гладиш С.В. Реагування та обробка інцидентів інформаційної безпеки в мережі GSM // Вісник Державного університету інформаційно- комунікаційних технологій. – 2008. – № 1. – с. 58-72.
5. ДСТУ ISO/IEC 27031:2015 Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=81330

Чаплінський Ю.П., Субботіна О.В.

Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ, Україна,

syuriy60@hotmail.com

olenas2011@gmail.com

КОНТЕКСТ ТА ЙОГО ПРЕДСТАВЛЕННЯ ПРИ РОЗВ'ЯЗАННІ ПРИКЛАДНИХ ЗАДАЧ ПРИЙНЯТТЯ РІШЕНЬ

Actuality of usage of context to the implementation of the decision making process is shown. Some known approaches to describe and establish a context in different information environments are analyzed. Contextual concepts and domains are defined. The features of the context model and context constraints are presented. The types of contexts used for decision support are presented.

Key words: *context, decision support system, knowledge management.*

Сучасні підходи до прийняття рішень вимагають використовувати не тільки особливості дійсності, які є найважливішими для конкретної ситуації прийняття рішень або задачі прийняття рішень, а розглядати різні аспекти прийняття рішень, які можуть бути змодельовані та досліджені один незалежно від одного та можуть базуватися не тільки на знаннях окремої предметної області, а на деякій сукупності проблемних областей. З іншої боку прийняття рішень в багатьох систем управління описуються взаємозв'язаними задачами. При цьому необхідно враховувати поведінковий аспект, організаційний аспект, інформаційний аспект. Для цього всі знання, що використовуються, розглядаються в розрізі знань, що описують контекст, та знань, що описують контент.

Поняття контексту грає важливу роль в багатьох дисциплінах, зокрема, у формальній логіці, представленні знань та міркувань, комп'ютерній лінгвістиці, при розв'язанні прикладних задач, в організаційній теорії, інформаційних систем тощо. Поняття контексту досліджене в різних областях інформаційних технологій, але не існує загального визначення контексту. Визначення контексту варіюються в залежності від області його застосування. Існує більше 150 визначень [1]. Контекст розглядають як набір обмежень, які впливають на поведінку системи (користувача або комп'ютера), як інформацію, яка може бути представлена в комп'ютерній системі з передбачуваним обсягом та виникненням, як інформацію, що характеризує взаємодію між людьми, додатками і середовищем, як будь-яку інформацію, яка може використовуватися, щоб характеризувати та інтерпретувати ситуації, в яких користувач взаємодіє із додатком в певний часі т.д..

Будемо розуміти під контекстом будь-яку інформацію, яка може бути використана або характеризує відповідну складову процесу розв'язання проблемних задач.

Модель контексту передбачає суб'єктивний погляд на розв'язання певної ситуації. На відміну від існуючих підходів, де контекст описується в монолітному сенсі або як об'єктивно певної ситуації, ми вважаємо, що будь-який вибір контекстних параметрів і їх питома вага в описі ситуації повинні бути предметом використання практики. Моделі контексту мають допомагати розв'язувати наступні проблеми з даними, що використовуються для визначення контекстно-обґрунтованих ситуацій: • неоднорідність та мобільність; • відносини та залежності; • своєчасність; • недосконалість; • міркування; • відповідність формалізму прийняття рішень; • ефективне контекстне забезпечення. Обмеження контексту має важливе значення, інакше проблема створення контекстної моделі буде незрозумілою та зменшує складність часу обчислення потенційних рішень для діяльності. Ми використовуємо такі обмежувальні критерії: наявність даних; повнота; набори включення / виключення; часові межі; просторові межі; область діяльності. Представлення контексту базується на наступних контекстних областях [2]: область мети/результату, область актора (людина, програмне забезпечення, технічна система), область процесу/дії, область об'єкту, область середовища, область можливостей, область засобів, область представлення, область розташування та область часу. Контекстні поняття взаємозв'язані між собою через контекстні відношення, включаючи внутрішньобласні, міжобласні та міжконтекстні відношення.

В рамках запропонованого підходу використовується трьохрівневе представлення складових прийняття рішень засобами моделі контексту. Будемо використовувати три типи контексту: абстрактний, конкретний та контекст реалізації. Абстрактний контекст будується на підставі інтеграції знань проблемних областей, що розглядаються при прийнятті рішень. Основним призначенням абстрактного контексту є формалізація складових прийняття рішень, які будуть використовуватися при розв'язання конкретної задачі. Абстрактний контекст визначається в результаті витягання з відповідних проблемних онтологій знань, релевантних конкретній задачі, та їх подальшої інтеграції. Основним призначенням абстрактного контексту є формалізація задач, які мають бути вирішені в конкретній ситуації прийняття рішень. Конкретний контекст є екстенсіоналом абстрактного контексту (конкретизацією абстрактного контексту) для реальних умов, що визначаються через інформаційні ресурси. Контекст реалізації є конкретизацію конкретного контексту для реальних умов програмної платформи, програмних засобів, в яких функціонує система підтримки прийняття рішень, та компетенції користувачів.

Результати представленого розгляду контексту використано в рамках науково-дослідної роботи “Розробити контекстно-орієнтовані онтологокеровані алгоритми системної оптимізації на прикладі безпеки продуктів харчування”.

ЛІТЕРАТУРА

1. Bettini C. A survey of context modelling and reasoning techniques / Bettini C., Brdiczka O., Henricksen K., Indulska, J., Nicklas, D., Ranganathan A., Riboni D. // *Pervasive and Mobile Computing*, 2010, 6, pp. 161-180.

2. Чаплінський Ю.П. Онтологія та контекст при розв’язанні прикладних задач прийняття рішень / Чаплінський Ю.П., Субботіна О.В. // *Штучний інтелект.* — 2016. — № 2. — С. 147-155.

Шолохов О. В.

Київський національний університет імені Тараса Шевченка, м. Київ
gyroalex@ukr.net

Терентьєв О. М., Присянкіна-Жарова Т. І.

Інститут телекомунікацій і глобального інформаційного простору НАН України,
м. Київ

o.terentiev@gmail.com

t.pruman@gmail.com

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СОЦІАЛЬНИХ КОМУНІКАЦІЙ НА ОСНОВІ АНАЛІЗУ ІНТЕРНЕТ-ДЖЕРЕЛ ЗАСОБАМИ TEXT MINING

A promising area for improving the quality of territorial community management is to receive feedback from the public on the response to the effectiveness and focus of ongoing reforms. One of the ways to solve this problem is to use content monitoring and analysis of the information space of the population of a certain area. The paper proposes the use of SAS text mining tools for the analysis of event and thematic sections of information flows of the Internet in the information-analytical systems of local governments and public administration.

Keywords: *text analytics, social communications, Internet information flows, text analysis, text key*

Не зважаючи на стрімкий розвиток інформаційних технологій, на даний час практично відсутня дієва, науковообгрунтована інформаційно-аналітична підтримка триваючих реформ. Важливим питанням, що потребує вирішення є забезпечення зворотного зв'язку між владою та населенням, виявлення настроїв щодо результативності реформ «на місцях», оцінки дієвості зусиль місцевої влади щодо забезпечення розвитку територіальних громад.

При цьому, дослідження не повинно обмежуватися лише аналізом суспільної думки. Адже контент-моніторинг не може в повній мірі забезпечити репрезентативність вибірки та об'єктивність опрацювання результатів.

Створення аналітичного інструментарію для підсистеми моніторингу інформаційного простору пов'язане з необхідністю відбору значної кількості кількісних та якісних факторів, призначених для формування інформативних тематичних зрізів, опрацюванням великих масивів структурованих та не структурованих даних, отримуваних з різних джерел (переважно мережі Інтернет). Перш за все це стосується дослідження особливостей життєвого циклу різних соціально-економічних систем, структури, зв'язків, суспільно-політичні чинників, екологічних факторів, зовнішніх та внутрішніх впливів різного характеру, тощо. Питанням використання засобів текстової аналітики для автоматизації аналізу даних, розташованих на Інтернет-ресурсах присвячено роботи як закордонних, так і вітчизняних дослідників [1-10].

Враховуючи предметної області, необхідність поєднання обробки текстових документів, представлених у різних форматах, з базами даних, web-документами, тощо, пропонується об'єднати всі етапи аналітичного процесу загальною формалізованою методологією, реалізованою у вигляді алгоритмів запрограмованих у пакеті прикладних програм для багатоплатформного середовища аналізу даних. А в основу інформаційної технології – хмарне середовище SAS Viya Text Analytics, яке надає змогу виконувати складні обчислення, обробляючи велику кількість даних, практично з будь-якої операційної системи, встановивши тільки браузер.

Перевагами даної інформаційної технології є можливість пошуку, категоризації та аналізу тональності інформації у різних колекціях документів значного обсягу. Дану систему можна застосовувати не лише для опрацювання Інтернет-джерел, а й для інших текстуальних даних, попередньо налаштувавши основні компоненти системи.

У системі передбачене сховище даних, де зберігаються документи, повідомлення, тощо, які можуть бути використані в подальшому для аналізу та категоризації у програмному середовищі SAS.

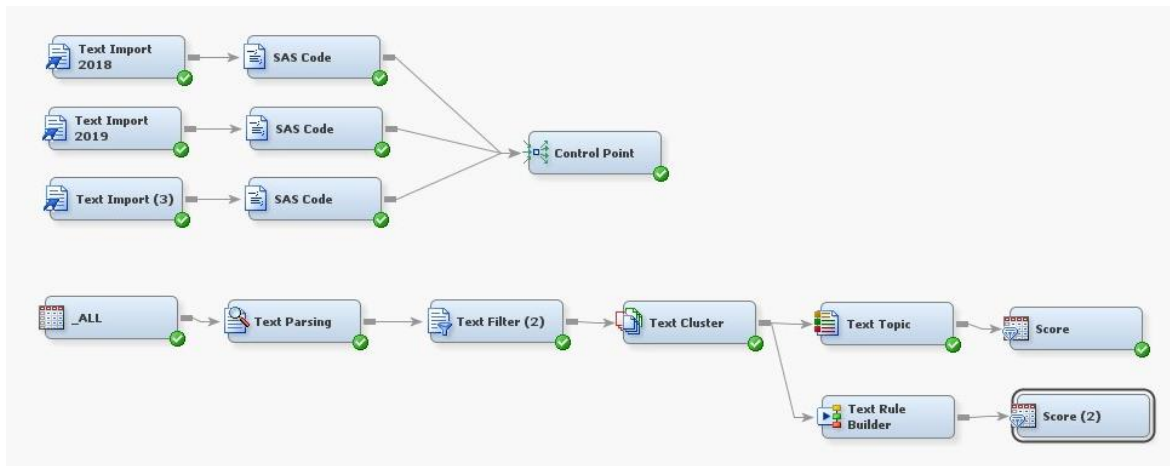


Рис. 1 Схема технологічного процесу аналізу текстових повідомлень у системі SAS Text Miner

Дослідження працездатності системи виконано на матеріалах груп повідомлень 20 територіальних громад (близько 10000 повідомлень). Для формування семантичного простору використані лексеми, сформовані з іменників та комбінацій іменників і дієслів. В результаті були сформовані пропозиції щодо першочергових проектів, які необхідно включити до бюджету об'єднаних територіальних громад на наступний бюджетний рік.

Впровадження комп'ютерних інформаційних систем, оснований на створеному інструментарії, у роботу органів державного управління, місцевого самоврядування, дорадчих структур стане в нагоді при ідентифікації об'єктів критичної інфраструктури, коротко- та середньостроковому прогнозуванні, формуванні перспективних планів, отриманні стратегічних екологічних оцінок щодо природокористування при реалізації складних інфраструктурних проектів, транспортної інфраструктури, виробничої логістики, уточненні оцінок впливу на довкілля потенційно небезпечних для довкілля проектів, а також можуть бути використані і органами місцевого самоврядування для оцінювання тенденцій розвитку певних громад та оцінюванні результативності урядування.

Дані пропозиції дозволять підвищити ефективність роботи органів державного управління та місцевого самоврядування щодо формування та реалізації державної політики розвитку всіх рівнів національної економіки, забезпечення соціальних стандартів, формуванні інвестиційної політики, будуть корисними для підприємств та бізнесу при визначення стратегії розвитку, раціонального використання наявних виробничих ресурсів, розташування

виробництва, інфраструктури, забезпечувати раціональне природокористування та продовольчу і техногенну безпеку.

ЛІТЕРАТУРА

1. Гладун, Анатолій Я. Data mining: пошук знань в даних [Текст] : [підруч. для студентів, інженерів і фахівців у сфера інтелект. аналізу даних] / Гладун А. Я., Рогущина Ю. В. - Київ : АДЕФ-Україна, 2016. 451 с.
2. Аналіз та обробка потоків даних засобами обчислювального інтелекту [Текст] : монографія / [Є. В. Бодянський та ін.] ; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2016. 235 с.
3. Ланде, Д. В. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки [Текст] : навч. посіб. / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова ; Ін-т спец. зв'язку та захисту інформації Нац. техн. ун-ту України "Київ. політехн. ін-т ім. Ігоря Сікорського". - Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 300 с.
4. Шкурко, Олена Василівна. Види лінгвістичного аналізу тексту [Текст] : навч. посіб. / О. В. Шкурко ; Ун-т ім. Альфреда Нобеля. - Дніпро : Ун-т ім. Альфреда Нобеля, 2018. 119 с.
5. Перебийніс В. І. Статистичні методи для лінгвістів : посібник. Вінниця : Нова Книга, 2013 — 176 с.
6. Литвин В.В. Аналіз даних та знань: Навчальний посібник / Литвин В.В., Пасічник В.В., Нікольський Ю.В. — Львів : Магнолія 2006 , 2017 — 276 с.
7. Батура Т.В. Математическая лингвистика и автоматическая обработка текстов: учеб. пособие /Т. В. Батура; Новосиб. гос. ун-т.–Новосибирск:РИЦ НГУ,2016. – 166 с.
8. Автоматическая обработка текстов на естественном языке и компьютерная лингвистика: учеб. пособие / Большакова Е. И., Клышинский Э. С., Ландэ Д. В., Носков А. А., Пескова О. В., Ягунова Е. В. - М.: МИЭМ, 2011. – 272 с.
9. Ланде Д. В. Елементи комп'ютерної лінгвістики в правовій інформатиці.- К.: НДПП НАПрН України, 2014. – 168 с.
10. Калиновский Я. А., Ландэ Д. В., Бояринова Ю. Е., Хицко Я. В. Гиперкомплексные числовые системы и быстрые алгоритмы цифровой обработки информации.- К.: ИПРИ НАН Украины, 2013. - 125 с.
11. Додонов А. Г., Ландэ Д. В., Путятин В. Г. Компьютерные сети и аналитические исследования. - К.: ИПРИ НАН Украины, 2014. - 486 с
12. Барсегян, А. А. Анализ данных и процессов: учеб. пособие / А. А. Барсегян, М. С. Куприянов, И. И. Холод, М. Д. Тесс, С. И. Елизаров. — 3-е изд.,

перераб. и доп. — СПб.: БХВ-Петербург, 2009. — 512 с.: ил. + CD-ROM — (Учебная литература для вузов) ISBN 978-5-9775-0368-6

13. Survey of Text Mining I: Clustering, Classification, and Retrieval / Ed. by M. W. Berry. — 2004. — Springer, 2003. — 261 p. — ISBN 0387955631.

14. Aggarwal C. C. Mining Text Data./ C. C. Aggarwal, C. Zhai — Springer, 2012. — 527 p. — ISBN 9781461432234.

15. Do Prado H. A. Emerging Technologies of Text Mining: Techniques and Applications /Ed. by H.A. Do Prado, E.Ferneda.—Idea Group Reference,2007.— 358 p. — ISBN 1599043734.

16. Text analytics using SAS Text Miner: course notes. –NC.: SAS Institute,2014. –218 p.

17. Андреев А. М., Берёзкин Д. В., Симаков К. В. Модель извлечения фактов из естественно-языковых текстов и метод её обучения [Электронный ресурс] – Режим доступа http://www.ixlab.ru/pub/docs/RCDL_2006_1.pdf

18. Терентьев А. Н. SAS BASE: Основы программирования / Терентьев А. Н., Домрачев В. Н., Костецкий Р. И. - Киев : Эдельвейс, 2014. - 303 с–ISBN 978-966-2748-49-9.

Шумейко О.А., Литвин І.С.

Національний транспортний університет (Київ)

shumeyko.ntu.edu.ua@gmail.com

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОПТИЧНОГО РОЗПІЗНАВАННЯ МОВИ ЖЕСТІВ

Information technology for optical recognition of sign language by tracking key points of joints and tips on human fingers, followed by conversion of gestures into plain text.

Keywords: *Python, neural network, TensorFlow, OpenCV, gesture recognition.*

Розпізнавання жестів є рук є важливою темою комп'ютерного зору до широкого спектру застосувань у взаємодії людина-комп'ютер, розширена/ віртуальна реальність та ігри. Такі програми часто вимагають сегментації руки, оцінки суглобової пози в руці і відстеження. Останні методи оцінки стану тіла використовуються для виявлення та сегментації рук за допомогою суглоба рук людського тіла особливості. Зчленована оцінка позиції руки із зображень у форматі RGB, як і раніше є в основному

невирішеною проблемою в декількох аспектах [1, 3]. Це тому що у кожної людини руки дуже різноманітні, з позою людської руки, що має понад 20 степенів свободи. Руки менше, ніж тіло, і тому вони займають невелику частину зображення, у порівнянні коли видно повне тіло. Крім того, ключові точки рук часто закриваються іншими частинами тієї ж руки, з іншого руки, або решта тіла.

Наразі глибокі методи навчання досягають найсучаснішого рівня ефективності розпізнавання пози тіла — суглобова проблема оцінки положення тіла, подібна до оцінки жестів рук. Однак розпізнавання пози тіла простіша, завдяки орієнтації тіла, а також через оклюзії є менш частою і менш гострою проблемою для повного зображення тіла, порівняно із зображеннями рук. Досліджуються методи, засновані на глибокому навчанні для розпізнавання пози рук, які виконують цілісну артикульоване виявлення жестів [2, 4, 5].

Виявлення ключових точок на руці та оцінка позицій мають чимало застосувань у комп'ютерному зорі, але це все ще невирішена проблема у багатьох аспектах. Застосовується програма виявлення ключових точок рук, виконання пізнавальних оцінок суб'єкта шляхом дотримання виконання цього предмета у фізичних завданнях із залученням швидкого руху пальців. У рамках цієї роботи використовую набір даних для тестування ключових точок руки, який складається із записаних жестів рукою спеціально для контролю когнітивної поведінки. Досліджую сучасні методи для виявлення ключових точок на руці та пропоную кількісні оцінки ефективності цих методів на використаному наборі даних. Надалі ці результати та даний набір даних можуть слугувати як корисний орієнтир для розпізнавання ключових точок руки для швидкого руху пальців.

Отже, завданням розробки є створення додатку для розпізнавання мови жестів шляхом відстежування 21 ключову точку суглобів та кінчиків на пальцях людини із наступним перетворенням жестів у звичайний текст, застосовуючи вибрані мною технології, які мають певні переваги для розробки програми розпізнавання мови жестів. І мати вискоефективне рішення, яке повинно мати можливість працювати в режимі реального часу, також мати високу точність при прогнозуванні.

Об'єктом дослідження є розпізнавання та оцінка відстежування ключових точок суглобів та кінчиків на пальцях людини.

Предметом дослідження є модель нейронної мережі та алгоритм відстежування об'єктів, що призначена для відстежування та розпізнавання пози рук та виявлення жестів.

ЛІТЕРАТУРА

1. Valentin Bazarevsky, Fan Zhang; Google AI Blog: On-Device, Real-Time Hand Tracking with MediaPipe (2019). <https://ai.googleblog.com/2019/08/on-device-real-time-hand-tracking-with.html>
2. Rokade, R., et al.: Hand Gesture Recognition by Thinning Method. In: International Conference on Digital Image Processing, IEEE (2009).
3. Futane, P.R., Dharaskar, R.V.: “Hasta Mudra” An Interpretation Of Indian Sign Hand Gestures. In: 2011 3rd International Conference on Electronics Computer Technology (ICECT 2011).
4. Bhuyan, M.K., Neog, D.R., Kar, M.K.: Hand Pose recognition using geometric features. IEEE (2011).
5. Mitra, S.: Gesture Recognition: A survey. IEEE Transactions on Systems, Man, And Cybernetics — Part C: Applications And Reviews (2007).

Ярмоленко Ю. А., Черноус Г. О.

Київський національний університет імені Тараса Шевченка

м. Київ

yu.yarmolenko@gmail.com

gach.2012@gmail.com

МУЛЬТИАГЕНТНА ІНФОРМАЦІЙНА СИСТЕМА ПІДТРИМКИ ТРАНЗАКЦІЙНОГО ЦІНОУТВОРЕННЯ

This work explains the architectural concept of a multi-agent information system for supporting transactional pricing. This architecture is a universal approach to implementing an automated system of transactional pricing, which uses a wide range of information sources in order to evaluate consumer demand with high precision. The use of multi-agent system can help to increase the competitiveness of an enterprise in the information economy.

Keywords: *process automation, e-commerce, e-business, multi-agent systems, distributed information systems, transactional pricing.*

Величезна кількість джерел даних з інформаційного простору спонукають теоретиків та практиків шукати нових шляхів для ціноутворення на підприємствах

електронної комерції з метою більш ефективного оцінювання попиту споживачів. З іншого боку, бажання підприємств підтримувати високий рівень лояльності клієнтів та існуюча соціальна відповідальність вимагають дотримання норм етичності стосовно клієнтів компаній. Такі цілі підприємства вимагають використання автоматизованого інструменту ціноутворення, що має можливість залучення якомога більшої кількості знань при встановленні оптимальної ціни на товари та послуги.

За визначенням авторів, під транзакційним ціноутворенням слід розуміти процес встановлення ціни на одиницю товару або послугу у рамках транзакції, що полягає у врахуванні прямих та опосередкованих ознак транзакції, з метою досягнення цілей підприємства електронної комерції [6]. Транзакційне ціноутворення стосується купівлі та продажу на ринку електронної комерції. Процес встановлення транзакційних цін на основі економіко-математичних та інформаційних методів називається моделюванням транзакційного ціноутворення. Моделювання дозволяє вирішити оптимізаційну задачу, що має на меті знаходження оптимальної ціни за певних обмежень. Під оптимальністю у контексті транзакційного ціноутворення слід розуміти одну, або декілька цілей підприємства: максимізація прибутку, максимізація рівня лояльності клієнтів, максимізація суспільного блага клієнтів тощо.

Автоматизація транзакційного ціноутворення є нетривіальною задачею в силу того, що інформаційна системи, яка займається його підтримкою, має виконувати низку функцій:

1. На основі інформаційних трендів ринку та «досвіду» системи встановлювати оптимальні ціни купівлі та продажу товарів;

2. робити оцінку поточної кон'юнктури ринку та стану інформаційного простору, необхідним чином досліджувати вплив персональних характеристик клієнтів з метою встановлення цін, що відповідають індивідуальним цінам попиту та пропозиції;

3. встановлювати закономірності процесів торгівлі на основі внутрішньої інформації про історію купівель та продажів з метою визначення найбільш ефективної стратегії торгівлі.

Такі вимоги до системи підтримки транзакційного ціноутворення вимагають використання мультиагентного підходу при створенні інформаційної системи [1, 7, 5, 2]. Агентом у системі є певна обчислювальна програма, що «автономно діє у складному динамічному середовищі з метою реалізації цілей, для яких його спроектовано» [4]. Окремі задачі при моделюванні транзакційного ціноутворення мають виконувати когнітивні та реактивні агенти. У своєму найширшому

функціоналі, схема архітектури мультиагентної інформаційної системи (МАІС) підтримки транзакційного ціноутворення виглядає наступним чином (рис. 1). Далі описано функції кожної з компонент запропонованого архітектурного рішення та їх зв'язок із інформаційним простором компанії.

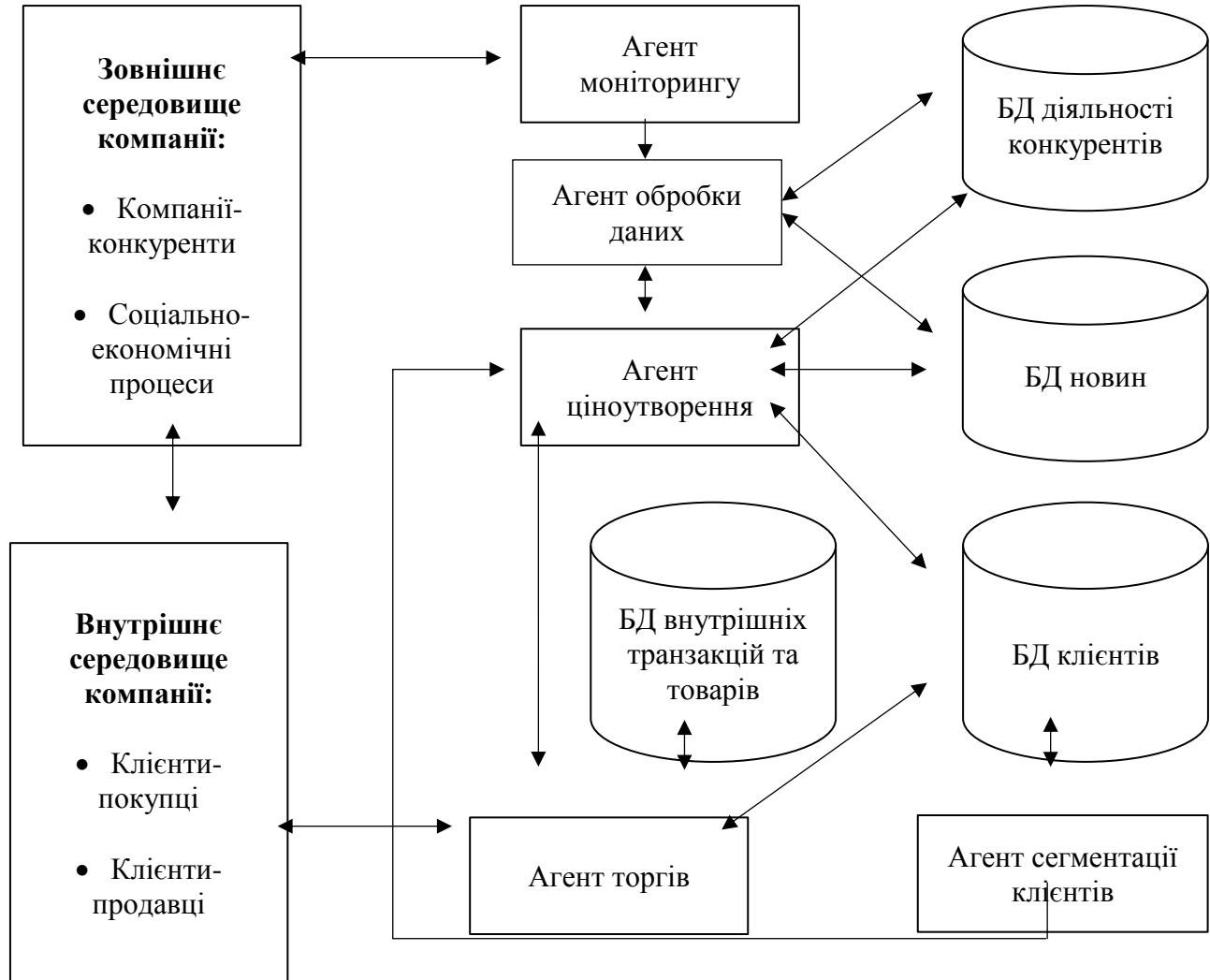


Рис. 1. Архітектура мультиагентної інформаційної системи підтримки транзакційного ціноутворення

Джерело: складено авторкою

Зовнішнє середовище компанії є складною та динамічною системою, що включає в себе підприємства-конкурентів, потенційних клієнтів компанії, організації та інформаційні джерела, які впливають на діяльність компанії, та, відповідно, зв'язки між усіма цими компонентами. Разом вони утворюють інформаційний простір довкола підприємства електронної комерції [3], що впливає на усі торговельні процеси.

Реактивний агент моніторингу має на меті постійний контроль стану інформаційного простору, що проявляється у новинах галузі та інших джерелах даних, таких як соціальні мережі, сайти-агрегатори інформації про товари та компанії, зміни у процесах компаній-конкурентів тощо. Оскільки усі ці фактори мають вплив на споживацький попит, вчасна реакція МАІС на зміни стану інформаційного простору є дуже важливою.

Когнітивний агент обробки даних структурує інформацію, зібрану агентом моніторингу, у знання про інформаційні тренди, попит на ринку, та стан ринку загалом. Використовуючи методи штучного інтелекту, агент виконує функції Entity Linking, Natural Language Processing, Sentiment Analysis, Automatic Summarization тощо.

База даних діяльності конкурентів є сховищем даних, що містить структуровані знання у вигляді даних про торговельні стратегії конкуруючих економічних суб'єктів.

База даних новин містить знання стосовно стану інформаційного простору у вигляді трендів, рейтингів, відгуків. Ці дані дають уявлення про зміну відношення клієнтів до товарів та компанії в цілому.

Внутрішнє середовище компанії складають клієнти компанії, які вступили у торговельні зв'язки із підприємством електронної комерції. Завдяки засобам PR та маркетингу, частина потенційних клієнтів із зовнішнього середовища може мігрувати до внутрішнього.

База даних клієнтів містить знання про усіх існуючих клієнтів компанії. Можливі два сценарії у роботі компанії. Перший – компанія обирає етичну стратегію при ціноутворенні та прозоро інформує про використання клієнтських даних та використання алгоритмів з метою ціноутворення. Другий – неетична стратегія, за якої існує асиметрія інформації між підприємством та клієнтами.

База даних транзакцій та товарів містить інформацію про транзакції та їх атрибути, а також товари (продані та на складах). Ця база є найважливішим джерелом даних для моделей ціноутворення.

Когнітивний агент сегментації клієнтів використовується за умови неетичної стратегії торгівлі, його основна функція полягає у поділі усіх клієнтів на основі особистих характеристик на певні кластери, до яких можуть застосовуватися різні підходи при ціноутворенні.

Когнітивний агент ціноутворення є ключовим обов'язковим компонентом для усієї системи. Застосовуючи економіко-математичні методи та інформаційні технології до відповідних даних системи, агент встановлює оптимальну ціну на товари і послуги у рамках кожної транзакції, та використовує набуті у процесі навчання знання для корекції моделей та стратегії торгівлі.

Реактивний агент торгів встановлює зв'язок клієнтів компанії із підприємством шляхом контролю процесів торгів та визначення ефективних умов кожної угоди.

Частина архітектурних компонент МАІС є опціональними (наприклад, агент моніторингу та агент сегментації клієнтів), а релевантність їх використання залежить від економічної ефективності (співвідношення між вартістю розробки компоненти та підвищенням прибутковості від використання) та етичних принципів компанії (використання персональних даних чи відмова від їх використання).

Таким чином, моделювання транзакційного ціноутворення є складною нетривіальною задачею, що потребує врахування багатьох факторів інформаційного простору компанії, а його реалізація пов'язана із використанням мультиагентного підходу до побудови інформаційної системи. Така інформаційна система дає змогу підвищити конкурентоспроможність підприємства електронної комерції шляхом його вчасної реакції на зміни стану інформаційного простору.

ЛІТЕРАТУРА

1. Плескач В. Л. Онтологічний підхід для представлення знань у мультиагентних системах інформаційних послуг суспільству / В. Л. Плескач // Вісник Київського національного університету імені Тараса Шевченка. – 2007. – 138-147.
2. Чорноус Г. О. Агентна модель інтелектуальної інформаційної системи управління в економіці/ Г. О. Чорноус // Вісник Київського національного університету. Економіка. – 2016. – Вип. 178. – С. 41-47.
3. Чорноус Г. О. Інформаційна модель ціноутворення на електронних ринках / Г. О. Чорноус, В. С. Саженок, Ю. А. Ярмоленко // Кібернетика і системний аналіз. – 2020. – Том 56(4). – С. 160-171.
4. Чорноус Г. О. Моделювання процесу прийняття управлінських рішень в соціально-економічних системах на основі інтелектуального аналізу даних: дисертація доктора екон. наук / Галина Олександрівна Чорноус. – Київ, 2015. – 485 с.
5. Чорноус Г. О. Оптимізація ціноутворення на основі моделей інтелектуального аналізу даних/ Г. О. Чорноус, С. А. Рибальченко // Вісник Київського національного університету. Економіка. – 2015. – Вип. 172. – С. 52-58.
6. Ярмоленко Ю. А. Співвідношення між різновидами ціноутворення в інформаційній економіці / Г. О. Чорноус, Ю. А. Ярмоленко // В кн.: Инструментальные средства моделирования систем в информационной экономике

/ Под ред. В.С. Пономаренко, Т. С. Клебановой. – Харьков, ВШЭМ – ХНЭУ им. С. Кузнеця, 2019. – С. 120-135.

7. Pleskach V. Information Security Management System in Distributed Information Systems / V. Pleskach, M. Pleskach, O. Zelikovska // Proceedings of the 2019 IEEE International Conference on Advanced Trends in Information Theory. – Kyiv, 2019. – P. 300-303.

Наукове видання

ПРИКЛАДНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ – 2020

Збірник тез

IV Міжнародної науково-практичної конференції
30 вересня 2020 року

м. Київ

Відповідальні за випуск:

В.Л. Плєскач,

В.Л. Міронова,

І.І.Гарко