ПРИВАТНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ»
АСОЦІАЦІЯ НАВЧАЛЬНИХ ЗАКЛАДІВ УКРАЇНИ
ПРИВАТНОЇ ФОРМИ ВЛАСНОСТІ
АКАДЕМІЯ WSB У ДОМБРОВІ ГУРНІЧІЙ (ПОЛЬЩА)
АСОЦІАЦІЯ СПЕЦІАЛІСТІВ КІБЕРБЕЗПЕКИ

Збірник наукових праць
Європейського університету

НАУКОВИЙ ВІСНИК

Київ-2024
Видавництво Європейського університету

УДК: 004.02
ISBN 978-966-301-266-7

Рекомендовано до друку Вченою радою ПВНЗ «Європейський університет» (протокол № 2 від 10.04.2024)

Редакційна колегія:
Тимошенко О.І. – ректор, доктор філософських наук, професор;
Гудзь Ю.Ф. – доктор економічних наук, доцент;
Скляренко О.В. – кандидат фізико-математичних наук, доцент
Яровий Р.О. – кандидат технічних наук.

Відповідальні секретарі:
Скляренко О.В. – к.ф.-м.н., доцент.;
Колодінська Я.О.

Рецензенти:
Медведєв М.Г. – доктор технічних наук, професор (Таврійський національний університет імені В. І. Вернадського);
Піскунова О.В. – кандидат технічних наук, доктор економічних наук, професор (Київський національний економічний університет імені Вадима Гетьмана).

Науковий вісник: Збірник наукових праць Європейського університету/ Редкол.: О. І. Тимошенко та ін. – К.: Вид-во Європейського університету, 2024. – 143 с.

Збірник наукових праць містить наукові дослідження у вигляді статей авторів у напрямі обґрунтування сучасних концепцій, моделей, механізмів, проблем та перспектив розвитку наукових засад у різних сферах та галузях людської діяльності в умовах викликів сьогодення.

Матеріали друкуються за редакцією авторів

© Європейський університет, 2024

Зміст

DOI: 978-966-301-266-7/1.2024.6

Тимошенко О.І.
доктор філософських наук, професор,
ректор ПВНЗ «Європейський університет»
https://orcid.org/0009-0003-4287-1947
e-mail: office@e-u.edu.ua

Ягодзінський С.М.
доктор філософських наук, професор,
проректор з навчально-методичної роботи
https://orcid.org/0000-0001-8755-2235
e-mail: serhii.yahodzinskyi@e-u.edu.ua

ДІДЖИТАЛІЗАЦІЯ УНІВЕРСИТЕТІВ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Дискусії стосовно цифрового університету майбутнього розпочались ще на початку комп'ютерної ери. Думки про те, що традиційний університет в майбутньому може поступитись університету, в якому провідну роль відіграватимуть не викладачі, традиції, освітні траєкторії, а інноваційні методики і методи надання освітніх послуг – не давала спокою західним футурологам з 60-70-их років XX ст.

Але плани, ідеї, концепції залишались проектами до 2020 року. Рік пандемії змусив шукати альтернативні шляхи соціальної взаємодії в усіх сферах – від виробництва товарів до приватного життя. Не могла залишитись осторонь і освіта, яка, слідуючи класичній моделі надання освітніх послуг, концентрувала у відносно невеликих приміщеннях значну кількість людей. Відтак не могло бути мови про збереження університетів у до-ковідному форматі.

Обмеження тотального карантину стали викликом системі вищої освіти – як її змістовному наповненню, так і формі реалізації. Заклади вищої освіти в один день зіштовхнулися з низкою проблем суб'єктивного та об'єктивного характеру, які унеможливлювали збереження діючої моделі надання освітніх і виховних послуг. Не будемо перелічувати труднощі, які довелось долати педагогічним та науково-педагогічним колективам, а тим паче – препарувати кожен крок, помилки й досягнення.

Акцентуємо увагу лише на одному аспекті, який мав і продовжує, на наш погляд, відігравати критичне значення, а саме: несприйняття викладачами університетів освітнього процесу в онлайн формі. Що ж так збурило колективи деяких кафедр та окремих викладачів? Чому після сотень монографій і дисертацій, тисяч наукових публікацій про переваги інформаційного суспільства та його неминучий прихід, адміністраціям університетів довелось

докладати значних зусиль до приведення до нормалізації освітнього процесу, навчання викладачів, врівноваження їх емоційного стану та пояснення простої істини – освіта не буде ніколи такою, як була раніше.

Університет моделі Канта, Гумбольдта, Ньюмена гинув і на заміну йому приходив цифровий університет – принципово інший за принципами побудови, за запитом здобувачів, за організацією навчання, за методиками і методами освітнього процесу. Але що ж такого є в застарілих моделях, що їх так наполегливо захищали (і продовжують це робити) деякі викладачі? Чим можна сьогодні обґрунтувати класичну чи навіть деякі некласичні моделі університетської освіти, університетської субкультури і корпоративного розвитку? Для пошуку відповіді коротко пройдемось по основним моделям Університетів.

Найбільш відомою є модель Гумбольдта. Однією з причин цього стали переклади західних наукових досліджень, які на початку 90-их років прогресивні викладачі опанували, на основі чого розпочали трансформацію кафедр і факультетів. Основні параметри університету моделі Гумбольдта визначаються розумінням основної мети отримання відповідного рівня освіти, а саме: формування громадянина світу, цілісної особистості, яка здатна ставити й вирішувати проблеми, опираючись на фундаментальне та академічне знання. Чи можлива така установка сучасного університету? Ні! І навіть не будемо вдаватись до дискусії, чому автори даної наукової праці так вважають. Головний аргумент – замовники університетської освіти (здобувачі та роботодавці) не сприймають в XXI столітті фундаментальності без інструментальності.

Наступна модель, яка менш відома в Україні, але яка, по суті, реалізовується під назвою попередньої моделі, є підхід Ньюмена. В основну університету Джон Ньюмен поклав такі принципи: гуманістична складова освітнього процесу, соціокультурна функція університету як соціального інституту, свобода у виборі освітньої траєкторії, вагома роль педагога як наставника майбутньої інтелектуальної еліти. Чи можлива така модель сьогодні? Ні! Тут пояснення мають бути нами дані більш розлого. На наше переконання, яке ґрунтується на багаторічному досвіді роботи зі студентською молоддю, покоління 2000-х має принципово інше ставлення до постаті викладача. Авторитетами не є ні доктори, ні кандидати наук, ні професори ні доценти, ні ректори університетів, ні завідувачі кафедр. Пієтет, властивий XX століттю, розчинився у потоці інформаційного шуму. Викладач перетворився з наставника на т’ютора, на «колегу», провідника і т.п. функціонал. Іншими словами – викладач втратив статус зразка, він не відіграє більше ролі безапеляційного інтелектуального чи морального лідера, орієнтиру! І що дивно – частина викладачів радо і як ознаку демократизації

прийняла нові правила гри. Бути «своїм» для студентів заманювало, грало на самолюбстві, переконувало в тому, що ти – сучасний, молодий, прогресивний і цікавий. Але то був обман для тих, хто свято в це повірив та самообман для тих, хто недостатньо оцінив наслідки.

Схожі тенденції, але з менш плачевними наслідками, відчували і на Заході (маємо на увазі країни Європи, Північної Америки, Австралії). Саме тому там були запропоновані та впроваджені деякі інноваційні моделі Університетів. Зокрема, континентальна модель, моделі Університет 1.0 та Університет 2.0. До класичної моделі оновлені схеми університетського навчання додали гнучкість формування індивідуальної освітньої траєкторії (але з низкою обмежень), доступ студентів до наукових досліджень, а також професіональну орієнтацію освітніх програм. Проте і ці моделі, як перехідні, доволі швидко були відкинутими за принципом «неможливо запорожець перетворити на мерседес».

Варто було шукати принципово інші підходи, змінювати фундамент, а не надбудову чи фасад. І такі підходи згодом були знайдені та запущені в реалізацію. З'явились науково-дослідні університети (які донедавна доволі амбіційно намагалось впровадити МОН України), мережеві університети, які в Україні існують переважно у монографіях, докторських і кандидатських дисертаціях та інші моделі, які видавали бажане за дійсне.

Окремо, на наш погляд, варто виокремити модель Університет 3.0. Схема надання освітніх послуг за цим стандартом жваво була підхоплена українськими педагогами, адже передбачала формування компетенцій на основі активного залучення здобувача до самостійного навчання, самостійного прокладання освітньої траєкторії, самостійного практичного втілення набутих в аудиторії та «методом наукового тику» знань і вмінь.

На жаль, побудова університету, заснованого на свідомому, відповідальному відношення здобувача до набуття знань епічно провалилась. І хто б що не говорив і якими б даними не маніпулював, та час, відведений освітніми програмами для самостійної роботи, студенти безоглядно використали для роботи та відпочинку – від офіціантів до серйозних фірм, від фрілансу до «просто лінь». Фраза «я заробляю зараз більше, ніж моя мама, то для чого мені вчитись» стала кредо значної частини студентської молоді.

Поряд з цим, молодь, яка не піддалась на «швидкогроші», опинилась не в кращій, на жаль, ситуації. Будучи у меншості, молоді люди змушені були спостерігати й відчувати на собі зниження якості надання освітніх послуг. Викладач, навіть найбільш відповідальний, з часом розумів, що має орієнтуватись на рівень 20 прогульників (працівників офісів, офіціантів, фрілансерів, або й просто ледарів), і лише потім – на тих трьох-п'ятьох, які ще мали бажання вчитись.

Далі з’явилась модель Університет 4.0. – модель Цифрового університету. Які принципові відмінності надання послуг онлайн?

По-перше, максимальна індивідуалізація освітньої траєкторії, темпу, ритму навчання, а також обсягу навчального матеріалу, який може (або хоче) засвоїти конкретний студент. Це вимагає від викладача принципово перебудуватись. Викладач вже не будує усереднену (нерідко, нижче допустимого) планку рівня навчального матеріалу, не відволікається на тих, хто не хоче, не може, не буде, працює і т.п. Викладач одночасно має забезпечити потреби усіх рівнів підготовки студентів. І ось тут проявилась неготовність, а інколи й непрофесіоналізм частини викладацького персоналу. За роки навчання усередненого студента кваліфікація частини викладачів знизилась нижче задовільного, а бажання пізнавати нове й нести його в аудиторію виявилось атрофованим. Звісно, ми не узагальнюємо на всіх, але проблема ця є і відгороджуватись від неї – означає жити в ілюзії.

По-друге, те, що було «утаємниченим» в аудиторіях, в яку, в кращому випадку, міг потрапити декан, завідувач кафедри чи колеги викладача (за умови проведення ним відкритого заняття задля проходження чергового конкурсу на заміщення вакантної посади) – стало в один момент публічним. Коли твоє заняття транслюється в мережі і може бути записане, поширене, опубліковане – супротив Університету 4.0. продиктований інстинктом самозбереження.

Чи є альтернатива Цифровому університету? Ні. Чи можуть бути повернені класичні моделі університетської освіти? Теоретично так, але це буде, на наш погляд, злочин проти майбутнього, злочин проти тих, хто завтра буде формувати основне джерело ВВП України.

Не зустрівши на своєму шляху карантинних обмежень, українська освіта, імовірно, залишилася б у кращому випадку на рівні науково-дослідницьких чи Університету 2.0 і 3.0. Лише обмеження перебування в аудиторії змусило викладачів, кафедри, факультети, університети залучити інструменти, які давно існували й готовими до використання. Але їхнє залучення не набуло б реалізації без фізичного видалення з приміщень учасників освітнього процесу.

Фантазія щодо Цифрового Університету 4.0 перетворилась на реальність. Озброєні досвідом функціонування ЗВО в умовах карантину, а нині – воєнного стану – ми можемо ставити питання перспектив. Головне – рухатись суголосно технологіям, адекватно і повно оцінюючи виклики, загрози і потенціал майбутнього. Працювати на майбутнє – це гасло Цифрового університету. І ми не маємо вибору, окрім як перебуваючи в теперішньому відповідати майбутньому.

DOI: 978-966-301-266-7/1.2024.10

Бобро Н.С.
https://orcid.org/0009-0003-5316-0809
e-mail: natalia@noolab.ch

Тимошенко А.О.
https://orcid.org/0009-0009-8950-8241
e-mail: andriy.tymoshenko@e-u.edu.ua

ДІДЖИТАЛІЗАЦІЯ ОСВІТИ ТА ЇЇ ВПЛИВ НА КАДРОВИЙ ПОТЕНЦІАЛ РЕГІОНІВ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Анотація. У статті досліджено процес цифровізації освіти та її вплив на кадровий потенціал регіонів у контексті цифрової економіки. Зазначено, що впровадження інформаційно-комунікаційних технологій в освіту значно трансформувало методики викладання, доступність та форми навчання. Цифрові інструменти, такі як онлайн-курси, цифрові підручники та інтерактивні платформи, сприяють персоналізації навчання та підвищенню його ефективності. Основні проблеми цифровізації освіти включають нерівний доступ до інтернету та технічних засобів, необхідність адаптації педагогів до нових технологій, питання якості освіти, безпека даних та потреба в нових компетенціях. Вирішення цих проблем потребує спільних зусиль дослідників, викладачів та освітніх закладів. Цифровізація освіти має позитивний вплив на розвиток кадрового потенціалу регіонів. Вона розширює доступ до освіти, сприяє формуванню висококваліфікованих фахівців, забезпечує гнучкість навчання та стимулює економічний розвиток регіонів. Застосування цифрових технологій у навчанні дозволяє індивідуалізувати освітній процес, розвивати інформаційні компетенції та інтелектуальний потенціал. В умовах цифрової економіки виникають нові вимоги до навичок кадрів, що сприяє появі нових професій та спеціалізацій. Гнучкість та постійне навчання стають ключовими аспектами успішної адаптації до змін на ринку праці. Освітні інституції мають гармонізувати свою кадрову політику з потребами цифрової економіки, забезпечуючи підготовку кваліфікованих фахівців та розвиток високотехнологічних секторів економіки. Цифровізація освіти, доповнюючи традиційні методи, вимагає вирішення питань онлайн-безпеки та захисту інтелектуальної власності. Загалом, цифровізація освіти сприяє формуванню високопрофесійного кадрового потенціалу та є основним каталізатором соціально-економічного розвитку регіонів.

Ключові слова: цифровізація, цифрова економіка, інтерактивні платформи, інформаційні технології, кадровий потенціал.

Bobro Natalia, Tymoshenko Andrii

DIGITALIZATION OF EDUCATION AND ITS IMPACT ON THE HUMAN RESOURCE POTENTIAL OF REGIONS IN THE CONTEXT OF THE DIGITAL ECONOMY

Abstract. The article investigates the process of digitalizing education and its impact on the human resource potential of regions in the context of the digital economy. It is noted that the introduction of information and communication technologies in education has significantly transformed teaching methods, accessibility, and forms of learning. Digital tools such as online courses, digital textbooks, and interactive platforms contribute to the personalization of learning and enhance its effectiveness. The main issues of digitalizing education include unequal access to the internet and technical means, the need for educators to adapt to new technologies, the quality of education, data security, and the need for new competencies. Addressing these issues requires joint efforts from researchers, educators, and educational institutions. Digitalizing education positively impacts the development of the human resource potential of regions. It expands access to education, fosters the formation of highly qualified specialists, ensures learning flexibility, and stimulates regional economic development. The application of digital technologies in education allows for the individualization of the educational process, development of information competencies, and intellectual potential. In the context of the digital economy, new skill requirements emerge, leading to the creation of new professions and specializations. Flexibility and continuous learning become key aspects of successful adaptation to changes in the labor market. Educational institutions must harmonize their human resource policies with the needs of the digital economy, ensuring the preparation of qualified specialists and the development of high-tech economic sectors. Digitalizing education, complementing traditional methods, requires addressing issues of online security and intellectual property protection. Overall, digitalizing education contributes to the formation of a highly professional human resource potential and is a primary catalyst for the socio-economic development of regions.

Key words: digitalization, digital economy, interactive platforms, information technologies, human resource potential.

Виклад основного матеріалу. В епоху стрімкого розвитку інформаційно-комунікаційних технологій, цифровізація охопила всі аспекти людського життя, трансформуючи й освітню сферу [1, с.169]. Як зауважує науковець С. Ягодзінський: «на початку XXI століття глобалізація суспільства здійснюється засобами конвергенції технологій. Вони базуються на інноваційних комунікаційних технологіях, зокрема, технологіях штучного інтелекту» [2, с.29].

Впровадження цифрових технологій в освіту мало значний вплив на методики викладання, доступність та форми навчання. До таких методів належить використання онлайн-курсів, цифрових підручників, інтерактивних платформ для навчання, що значно розширює можливості та межі освіти. Крім того, цифрові інструменти сприяють персоналізації навчання, враховуючи індивідуальні потреби студентів, що підвищує ефективність навчального процесу.

Із стрімким розвитком технологій, освітні установи та професорсько-викладацький склад навчальних закладів усіх рівнів отримали нові можливості. Однак це також спричинило виникнення нових завдань, вирішення яких стало першочерговою необхідністю.

Цифровізація в системі освіти зіштовхнулася з кількома проблемами, а саме:

– нерівний доступ до високошвидкісного інтернету та сучасних технічних засобів, що створює розриви між учнями та студентами і ускладнює можливість отримання рівних освітніх можливостей;

– необхідність адаптації вчителів і викладачів до нових цифрових інструментів, що потребує часу та ресурсів, а також виникає потреба у підвищенні якості професійної підготовки;

– вплив технологій на зміст освіти іноді викликає занепокоєння щодо якості знань, оскільки акцент може зміщуватися на використання технологій, а не на засвоєння матеріалу;

– збільшення обсягу даних, що зберігаються у цифровому форматі, вимагає додаткових заходів щодо забезпечення безпеки та захисту персональної інформації учнів;

– цифрові технології змінюють вимоги до навичок, необхідних для майбутньої роботи. Необхідність включення нових компетенцій в освітні програми стає завданням для освітніх інституцій;

– використання цифрових технологій в оцінюванні навчальних досягнень потребує переосмислення та адаптації методів оцінювання.

Вирішення цих проблем вимагає спільних зусиль з боку дослідників, викладачів та вищих навчальних закладів. Загалом, цифровізація освіти має

потенціал для вдосконалення та модернізації навчання, а її впровадження може сприяти підвищенню якості освіти та підготовці студентів до вимог сучасного ринку праці.

Загальновідомим є той факт, що одним із головних критеріїв підвищення рівня конкурентоспроможності регіону, є розвиток кадрового потенціалу. Результати оцінки його стану, наявні особливості розвитку, виявлення уразливих місць в умовах цифрової економіки сприяють підвищенню стійкості економічних суб'єктів усіх галузей. Кадровий потенціал регіону – це соціально-економічна категорія, аналіз якої потрібно проводити з урахуванням науково-технічного, інноваційного, трудового, виробничого потенціалів регіону [3, с. 30].

Цифрова епоха супроводжується не лише появою нових «цифрових» професій, але й викликами, пов'язаними з кадровим дефіцитом у цій сфері. Багато регіонів стикаються з одночасним зростанням безробіття (внаслідок, наприклад, світової кризи) та нестачею кваліфікованих спеціалістів, що володіють навичками, необхідними для роботи в цифровій економіці. Це зумовлює необхідність трансформації кадрової політики компаній у всіх галузях. Гнучкість підходу до пошуку та утримання кадрів стає ключовим фактором успіху.

На думку деяких фахівців, розвиток кадрового потенціалу регіону в умовах цифровізації економіки можливий двома шляхами: або через «вирощування» спеціалістів власними силами господарюючого суб'єкта, або шляхом залучення зовнішніх висококваліфікованих фахівців для виконання конкретних завдань [4;5].

Обидва підходи мають свої переваги і залежать від багатьох факторів, включаючи потреби господарюючого суб'єкта, його стратегію розвитку, доступність спеціалістів на ринку праці та інші. Внутрішній розвиток спеціалістів дозволяє формувати культуру з відповідними цінностями, адаптувати працівників до особливостей бізнес-процесів та підвищувати їх лояльність. Однак для вирішення специфічних завдань, які потребують унікальних знань або досвіду, доводиться звертатися до зовнішніх експертів. Ідеальна стратегія може полягати в комбінації обох підходів залежно від конкретних потреб і завдань компанії.

Цифровізація сфери освіти кардинально перетворила процеси навчання та доступ до знань. Разом із цим, вона значно вплинула на кадровий потенціал регіонів. Це проявляється через:

– доступність освіти, коли цифрові технології надали можливість отримати освіту з будь-якої точки світу. Це особливо важливо для віддалених або малозабезпечених регіонів, де раніше доступ до якісної освіти був обмежений. Тепер учні та студенти можуть навчатися онлайн, вивчаючи курси

та набуваючи професійних навичок;

– отримання якісних спеціалістів, оскільки цифровізація сприяє формуванню висококваліфікованих фахівців. Це пов'язано з можливістю навчання на платформах з унікальними онлайн-курсами, включаючи ті, які можуть бути відсутні в регіональних навчальних закладах;

– гнучкість у навчанні, коли за допомогою цифрових навчальних платформ стає можливим створення гнучких розкладів і програм навчання, що задовольняє потреби студентів і професіоналів. Це сприяє підвищенню кваліфікації працівників і зростанню кадрового потенціалу регіону;

– економічний розвиток, адже навчання і розвиток кваліфікованих кадрів є ключовими факторами для економічного зростання регіонів. Підвищений доступ до освіти внаслідок цифровізації сприяє збільшенню кількості кваліфікованих спеціалістів, що, у свою чергу, стимулює залучення нових інвестицій і розвиток бізнес-середовища в регіоні.

Використання інформаційних технологій у процесі навчання визначило ключовий принцип навчання – принцип індивідуалізації. Кожен учень слідує індивідуальному ритму навчання, з необхідним саме йому рівнем допомоги та глибиною вивчення матеріалу. Практичне застосування інформаційних технологій є важливим напрямом модернізації, що дозволяє не лише покращити рівень освіти, але й розвинути інформаційні компетенції, а також розкрити інтелектуальний потенціал людини [6, с.20].

Отже, діджиталізація освіти має низку переваг для розвитку кадрового потенціалу регіонів, розширюючи доступ до освіти, забезпечуючи гнучкі можливості навчання та сприяючи економічному розвитку через підготовку кваліфікованих кадрів.

Щодо структурних змін зайнятості населення в найближчому майбутньому прогнозується зростання в таких сферах, як креативна економіка, цифрова та віртуальна економіка, відновлення екології, людиноорієнтовані сервіси в новоствореному технологічному секторі.

Варто зазначити, що цифровізація економіки значно вплинула на характер і склад кадрового резерву. Сучасні кадри мають поглиблені знання в області цифрових технологій, програмування, аналітики даних та інформаційних систем, що відповідає потребам цифрової економіки. Фахівці тепер можуть працювати віддалено, використовуючи хмарні технології та сучасні інструменти для комунікації, що робить кадровий резерв більш гнучким та мобільним.

Співробітники з цифровими навичками більш схильні до навчання та адаптації до нових технологій, що дозволяє їм краще пристосовуватися до змін у бізнес-середовищі. Однак цифрова економіка висуває до сучасних кадрів вимоги широкого набору навичок та знань, здатності переключатися між

різними завданнями та дисциплінами, що призводить до появи співробітників з крос-функціональними навичками.

Цифровізація також призвела до появи нових професій та спеціалізацій, таких як аналітики даних, фахівці з кібербезпеки, спеціалісти з штучного інтелекту та інші, що розширює кадровий резерв. Спеціалісти, які володіють навичками аналізу та інтерпретації даних, стають більш затребуваними в умовах цифрової економіки, що призводить до змін у структурі кадрових резервів компаній.

Неперервне навчання персоналу та можливість самовдосконалюватися є ключовими аспектами, що сприяють успішній адаптації до змін на ринку. Це підкреслює значущість регулярного вдосконалення кадрової політики. Господарським суб'єктам важливо створювати умови для постійного професійного розвитку співробітників, оскільки високий рівень їх компетенцій, мотивації та професіоналізму сприяє підвищенню ефективності роботи підприємства. Стратегія розвитку кадрового потенціалу повинна гармоніювати з основними стратегічними завданнями підприємства, надаючи пріоритет особистісному та професійному зростанню співробітників.

Грамотно сформована освітня політика, яка базується на тенденціях цифровізації, не лише служить інструментом збалансованого наповнення ринку праці кваліфікованими спеціалістами, але й запобігає соціальному колапсу. Однак на державному рівні, зміни можуть загальмуватися через відсутність необхідного кадрового потенціалу, що створює замкнуте коло, розірвати яке можна лише шляхом підготовки кваліфікованих кадрів.

Виходячи з вищезазначеного, можна зробити висновок, що цифровізація освіти є доповненням до традиційної освіти. Однак на сьогоднішній день потребують вирішення такі питання, як забезпечення онлайн-безпеки всіх учасників освітнього процесу, захист результатів інтелектуальної діяльності та їх повна збереженість.

Удосконалення цифрової економіки тягне за собою загрозу того, що окрема особистість стає повністю вразливою перед глобальними платформами, які отримують доступ до приватної інформації [2, с. 109].

Висновки. Цифровізація освіти не лише формує високопрофесійний кадровий потенціал, але й визначає розвиток високотехнологічних секторів економіки, які є основним каталізатором соціально-економічного розвитку регіону.

Література

1. Bobro, N. Effectiveness of artificial intelligence usage in the educational process. *Наука і техніка сьогодні.* № 14(28). 2023. С. 168-174. DOI: https://doi.org/10.52058/2786-6025-2023-14(28)-168-174
2. Yahodzinskyi, S. Anthropomorphic information networks and converging technologies: challenge to humanity (vs), step forward?. *Artificial intelligence*, 2023, №1. С. 29-35. DOI: https://doi.org/10.15407/jai2023.01.029
3. Kozhyna, A. Reducing Poverty, Inequality and Social Exclusiom in European Countries Based on Inclusive Approaches to Economic Development. Economics and Management of The National Economy, The Crisis of National Models of Economic System (2022) 29-32. doi: 10.30525/978-9934-26-269-2-7.
4. Лопушняк Г.С., Скидан М.І. Стратегічний аналіз розвитку вищої освіти України в контексті збалансування попиту та пропозиції на ринку праці. Соціальна сфера: виклики та новації. (2022) 27-40. doi: 10.32752/1993-6788-2022-1-248-249-27-40
5. Luis A Leiva, Maristella Matera, Johannes Schöning. PACMHCI V7, MHCI, September Editorial. Proceedings of the ACM on Human-Computer Interaction. (2023) 1–2. doi: 10.1145/3604238
6. Bobro, N. Application of artificial intelligence in higher education institutions: foreign experience. Three Seas Economic Journal (2024) 19-23. doi:10.30525/2661-5150/2024-5-3

DOI: 978-966-301-266-7/1.2024.17

Букатов Д.В.
https://orcid.org/0009-0009-9320-2181
e-mail: denys.bukatov@e-u.edu.ua

Колодінська Я.О.
https://orcid.org/0000-0002-3330-7565
e-mail: yanina.kolodinska@e-u.edu.ua

ПОРІВНЯННЯ SEEXPR З ІНШИМИ МОВАМИ ДЛЯ ПРОЦЕДУРНОГО ТЕКСТУРУВАННЯ

Анотація. Авторами розглянуто та проаналізовано мови SeExpr з іншими мовами, що використовуються для процедурного текстурування, а саме GLSL (OpenGL Shading Language), HLSL (High-Level Shading Language) та RSL (RenderMan Shading Language). Відзначено актуальність тематики дослідження у зв'язку з інтенсивним розвитком комп'ютерної графіки та зростанням вимог до якості текстур у відеоіграх, анімаційних фільмах та інших мультимедійних додатках. В роботі запропоновано рекомендації щодо вибору мови для процедурного текстурування залежно від потреб проекту, що можуть бути корисними для художніх працівників, розробників ігор та аніматорів. Наведено приклади використання SeExpr у виробництві, зокрема для створення текстур та ефектів. Також обговорено основні особливості та функціональність кожної з розглянутих мов, зокрема їх продуктивність, простоту використання, гнучкість та підтримку спільноти. Визначено, що SeExpr є оптимальним вибором для швидкого прототипування та налаштування текстур, тоді як GLSL та HLSL підходять для відтворення реалістичних графічних ефектів у реальному часі, а RSL забезпечує високу якість рендерів у кінематографічних проектах.

Ключові слова: процедурне текстурування, SeExpr, комп'ютерна графіка, якість текстур, візуальні ефекти в реальному часі, GLSL, HLSL, RSL.

Bukatov Denys, Kolodinska Yanina

COMPARISON OF SEEXPR WITH OTHER PROCEDURAL TEXTURING LANGUAGES

Abstract. Authors have reviewed and analyzed SeExpr language and compared it with other languages used for procedural texturing, namely GLSL (OpenGL Shading Language), HLSL (High-Level Shading Language), and RSL (RenderMan Shading Language). The relevance of this study is noted in connection with the rapid development of computer graphics and the increasing demands for texture quality in video games, animated films, and other multimedia applications. The paper provides recommendations on the choice of procedural texturing language depending on the project's needs, which can be useful for artists, game developers, and animators. Examples of SeExpr usage in production are given, particularly for creating textures and effects. The main features and functionalities of each language are also discussed, including their performance, ease of use, flexibility, and community support. It is determined that SeExpr is the optimal choice for rapid prototyping and texture adjustment, while GLSL and HLSL are suitable for rendering realistic real-time vfx, and RSL ensures high-quality renders in cinematic projects.

Key words: procedural texturing, SeExpr, computer graphics, texture quality, real-time vfx, GLSL, HLSL, RSL.

Постановка проблеми та її актуальність. Процедурне текстурування є ключовим методом у сучасній комп'ютерній графіці, що дозволяє створювати текстури шляхом алгоритмічного генерування, на відміну від традиційних растрових текстур. Проблематика цього дослідження полягає в аналізі та порівнянні різних мов процедурного текстурування, зокрема SeExpr, GLSL, HLSL та RSL, що широко використовуються в індустрії. Цей аналіз є надзвичайно актуальним у зв’язку з інтенсивним розвитком комп'ютерної графіки та підвищеними вимогами до якості зображень в мультимедійних та інших типів додатках.

Вивчення характеристик цих мов має важливе практичне значення, оскільки дозволяє визначити їхню продуктивність, гнучкість, простоту використання задля підвищення загальної якості, ефективності та швидкості розробки графічного контенту.

Аналіз останніх досліджень і публікацій. Тема процедурного текстурування є предметом багатьох досліджень та публікацій, що обумовлено її важливістю для розвитку сучасної комп'ютерної графіки. У дослідженнях розглядаються різні аспекти та методи створення текстур за допомогою алгоритмічних підходів, що дозволяють досягти високого рівня деталізації та

ефективності. Так, наприклад, Стефан Густавсон [2] у своїй роботі детально аналізує можливості використання GLSL для створення процедурних текстур, підкреслюючи переваги цього підходу для реального часу рендерингу. Інші дослідники, такі як Матт Фарр, Венцель Якоб і Грег Хамфріс [3] розглядають фізично обґрунтовані методи рендерингу, що дозволяють підвищити реалістичність візуальних ефектів за допомогою процедурних текстур.

Особливу увагу заслуговують праці, присвячені аналізу та порівнянню різних мов для процедурного текстурування. Зокрема, дослідження Томаса Акеніне-Мьоллера, Еріка Хайнса та Нейті Гоффмана [4] підкреслюють важливість продуктивності та ефективності у реальному часі, що є ключовими аспектами для мов програмування шейдерів. Публікація Джона Перейри [5] аналізує використання HLSL для створення високоякісних графічних ефектів у середовищі DirectX. Ці роботи забезпечують комплексний огляд та глибокий аналіз, необхідний для розуміння сильних та слабких сторін різних підходів до процедурного текстурування, що дозволяє робити обґрунтований вибір мов та інструментів залежно від специфіки проекту та його вимог.

Формулювання мети дослідження. Мета цієї статті полягає у проведенні детального порівняння SeExpr з іншими популярними мовами для процедурного текстурування, такими як GLSL (OpenGL Shading Language), HLSL (High-Level Shading Language) та RSL (RenderMan Shading Language). Це порівняння дозволить оцінити сильні та слабкі сторони кожної з мов, їх відповідність різним задачам та потребам у сфері комп'ютерної графіки.

Виклад основного матеріалу дослідження. Процедурне текстурування – це метод створення текстур для комп'ютерної графіки, де зображення генерується алгоритмічно, а не на основі готових бітових зображень (текстур). На відміну від звичайних растрових текстур, процедурні текстури створюються за допомогою математичних формул і функцій, які визначають колір, форму та інші властивості пікселів самої текстури. Це дозволяє генерувати різноманітні текстури з високим рівнем деталізації без необхідності зберігання великих обсягів даних так як зберігатися вони будуть у вигляді фомул.

Процедурне текстурування дозволяє створювати текстури, які можуть бути динамічно змінені або анімовані за допомогою різних типів рушіїв або графічних редакторів, що дає можливість досягати ефектів, які важко або неможливо досягти з використанням стандартних методів створення растрових текстур.

Процедурні текстури відіграють важливу роль в сучасній комп'ютерній графіці, забезпечуючи ряд нижче наведених переваг:

1. Ефективне використання пам'яті. Процедурні текстури генеруються в режимі реального часу, що дозволяє уникнути зберігання великих обсягів даних текстур на дисках. Це особливо важливо для відеоігор та симуляцій, де обмеження пам'яті можуть бути критичними.

2. Безшовність та масштабованість. Процедурні текстури можуть бути безшовними, що усуває видимі стики на великих поверхнях. Вони також можуть бути масштабованими до будь-якого рівня деталізації без втрати якості, що є значною перевагою у порівнянні з традиційними текстурами.

3. Динамічність та варіативність. Процедурне текстурування дозволяє створювати текстури, які можуть змінюватися в залежності від параметрів, таких як час, положення або інші зовнішні умови. Це дозволяє створювати анімовані текстури або текстури, які реагують на взаємодію з користувачем.

4. Реалістичність. Завдяки математичним моделям, процедурні текстури можуть точно імітувати природні матеріали, такі як камінь, вода, скло, вогонь та інші, з високим рівнем реалістичності.

5. Кросплатформеність. Процедурні текстури можуть бути використані на різних платформах і в різних додатках, від комп'ютерних ігор до анімаційних фільмів та віртуальної реальності.

SeExpr (Short Expressions) пропонує ряд ключових особливостей, які роблять її потужним інструментом для процедурного текстурування:

1. Простий та зрозумілий синтаксис. SeExpr використовує простий виразний синтаксис, що дозволяє художникам легко писати та читати скрипти без необхідності мати глибокі знання програмування.

2. Гнучкість та розширюваність. Завдяки своїй модульній архітектурі, SeExpr дозволяє легко додавати нові функції та розширення, що робить її дуже гнучкою та адаптивною до різних потреб.

3. Інтерактивність. SeExpr підтримує інтерактивне налаштування параметрів, що дозволяє художникам миттєво бачити результати своїх змін та швидко налаштовувати текстури відповідно до своїх потреб.

4. Підтримка процедурних текстур. SeExpr дозволяє створювати різноманітні процедурні текстури, такі як градієнти, шум, фрактали та інші складні патерни, використовуючи математичні вирази.

5. Інтеграція з іншими інструментами. SeExpr може бути інтегрована з різними програмами для 3D-моделювання та рендерингу, такими як Autodesk Maya, що дозволяє використовувати її можливості у повному виробничому циклі.

SeExpr широко використовується у виробничих процесах для створення текстур та візуальних ефектів у анімаційних фільмах та відеоіграх. Ось декілька прикладів її застосування:

1. Текстурування персонажів та середовищ: SeExpr використовується для створення складних текстур для персонажів та середовищ, що дозволяє досягти високого рівня деталізації та реалістичності.

2. Анімовані текстури та ефекти: Завдяки можливості інтерактивного налаштування та анімації параметрів, SeExpr дозволяє створювати динамічні текстури та ефекти. Наприклад, у фільмі "Ральф-руйнівник" (Wreck-It Ralph) SeExpr була використана для створення анімованих ефектів, таких як вибухи та магічні частинки.

3. Створення природних матеріалів: SeExpr дозволяє легко імітувати природні матеріали, такі як камінь, дерево, вода та інші, використовуючи математичні моделі та шумові функції. Це забезпечує високий рівень реалізму та деталізації, що особливо важливо для створення фотореалістичних сцен.

4. Генерація процедурних патернів: SeExpr використовується для створення складних процедурних патернів, таких як плитка, тканина, металічні поверхні та інші текстури, які важко або неможливо досягти за допомогою традиційних методів.

Огляд альтернативних мов: GLSL, HLSL, RSL (RenderMan Shading Language)

Процедурне текстурування можна реалізувати за допомогою різних мов програмування шейдерів, кожна з яких має свої особливості та застосування. Серед найбільш поширених мов для процедурного текстурування виділяються GLSL (OpenGL Shading Language), HLSL (High-Level Shading Language) та RSL (RenderMan Shading Language). Кожна з цих мов має свої унікальні можливості та переваги. Наприклад, для завдань, пов'язаних із підвантаженням та візуалізацією даних із захищених комп'ютерних мереж на прикладі IPSec, GLSL та HLSL є найбільш оптимізованими мовами завдяки їх продуктивності та інтеграції з сучасними графічними API.

GLSL (OpenGL Shading Language) – це мова програмування шейдерів, яка використовується у графічному API OpenGL. Вона призначена для написання вершинних, фрагментних та інших типів шейдерів, які виконуються на графічному процесорі (GPU). GLSL дозволяє створювати високопродуктивні графічні ефекти в реальному часі, що робить її популярною у розробці відеоігор та інтерактивних додатків.

HLSL (High-Level Shading Language) – це мова програмування шейдерів, розроблена Microsoft для використання з графічним API DirectX. Вона використовується для створення графічних ефектів у відеоіграх та мультимедійних додатках на платформі Windows. HLSL забезпечує високу продуктивність та гнучкість у створенні складних процедурних текстур та шейдерів.

RSL (RenderMan Shading Language) – це мова програмування шейдерів, розроблена Pixar для RenderMan, одного з найвідоміших рендерерів для створення анімаційних фільмів та візуальних ефектів. RSL дозволяє створювати високоякісні рендери з підтримкою складних процедурних текстур та матеріалів, що робить її популярною у кіноіндустрії.

Порівняння

Для оцінки різних мов процедурного текстурування, включаючи SeExpr, GLSL, HLSL та RSL, було обрано чотири основні параметри порівняння:

1. Простота використання: легкість навчання та використання мови для художників та технічних спеціалістів.
2. Гнучкість: можливість мови адаптуватися до різних потреб та завдань.
3. Продуктивність: ефективність виконання кодів, написаних на даній мові, особливо в умовах реального часу.
4. Підтримка спільноти: наявність та активність спільноти користувачів, доступність документації та прикладів.

Сильні та слабкі сторони SeExpr у порівнянні з іншими мовами

SeExpr

Сильні сторони:

- Час навчання: В середньому, художник може освоїти основи SeExpr за 1-2 дні завдяки її інтуїтивному синтаксису.
- Швидкість прототипування: У тестовому середовищі художники змогли створювати базові текстури за 10-20 хвилин, що на 30-50% швидше порівняно з традиційними методами.
- Простота використання: Згідно з опитуванням серед художників, 85% зазначили, що SeExpr значно спрощує процес налаштування текстур у порівнянні з GLSL чи HLSL.
- Гнучкість: Завдяки модульній архітектурі SeExpr можна легко розширювати, додаючи нові функції та можливості.

Слабкі сторони:

- Продуктивність: SeExpr не призначена для високопродуктивних обчислень на GPU, що обмежує її використання в реальному часі.
- Підтримка спільноти: Незважаючи на відкритий вихідний код, спільнота користувачів SeExpr менша порівняно з іншими мовами, такими як GLSL чи HLSL.

GLSL (OpenGL Shading Language)

Сильні сторони:

- Продуктивність: GLSL дозволяє досягати високої продуктивності завдяки виконанню на GPU. У тестах на продуктивність GLSL показує

підвищення швидкості рендерингу до 60-80% у порівнянні з CPU-орієнтованими мовами.

- Реальність виконання: Використання GLSL забезпечує виконання шейдерів у реальному часі з доволі високою продуктивністю.
- Підтримка спільноти: GLSL має велику спільноту користувачів та розробників, що забезпечує багатий набір ресурсів та прикладів.

Слабкі сторони:

- Простота використання: Синтаксис GLSL складніший, що потребує глибших знань програмування.
- Гнучкість: Хоча GLSL дуже потужна для графічних обчислень, її використання може бути менш інтуїтивним для художників.

HLSL (High-Level Shading Language)

Сильні сторони:

- Платформа: HLSL оптимізована для використання з DirectX, яка домінує на платформі Windows, що займає приблизно 76% ринку настільних операційних систем.
- Продуктивність: HLSL забезпечує високу продуктивність на DirectX, дозволяючи досягти до 100-120 FPS у сучасних іграх з високою деталізацією (по сучасним стандартам).
- Підтримка спільноти: Велика спільнота користувачів та хороша документація.

Слабкі сторони:

- Простота використання: Як і GLSL, HLSL має складніший синтаксис, що робить її менш доступною для новачків.
- Гнучкість: В основному орієнтована на використання в екосистемі DirectX.

RSL (RenderMan Shading Language)

Сильні сторони:

- Якість: RSL дозволяє досягти високої деталізації та реалістичності текстур, що використовуються у провідних анімаційних студіях, таких як Pixar. Більше 90% анімаційних фільмів з високою деталізацією текстур використовують RenderMan.
- Використання: RSL широко використовується у кіноіндустрії, де понад 85% студій візуальних ефектів використовують RenderMan для створення реалістичних матеріалів та текстур.
- Підтримка складних текстур: RSL здатна обробляти складні процедурні текстури з високою деталізацією, що на 40-50% перевищує можливості інших мов у цій сфері.

- Простота використання: Спрощений синтаксис у порівнянні з GLSL та HLSL, більш інтуїтивний для художників.

Слабкі сторони:

- Продуктивність: Менш продуктивна у порівнянні з мовами, що виконуються на GPU.
- Підтримка спільноти: Спільнота менша у порівнянні з GLSL та HLSL, хоча і дуже активна у вузькому колі анімаційних студій.

Приклад коду колірного шуму SeExpr

Порівнюючи код на мові SeExpr, код колірного шуму на мовах GLSL та HLSL виходить набагато простішим, зрозумілішим для аналізу та коротшим у декілька разів (якщо в даному прикладі на мові SeExpr ми використали всього 7 строк коду то на інших мовах схожий по функції код міг би зайняти приблизно від 40 до 80 строк в залежності від параметрів). Якщо ж порівнювати його з кодом на мові RSL, то величина коду в деяких випадках може вийти по розміру трохи менше ніж GLSL та HLSL варіантах але із за спрощеного синтаксису. Всі три мови шейдерів (GLSL, HLSL, RSL) потребують більше коду для визначення функцій, які обробляють векторні та матричні операції, на відміну від SeExpr, яка має вбудовані прості функції для цього.

-(Спочатку надаємо значення)

$ratio = $h/$w; *(значеня по висоті та ширині)*
$zCoord = 0.40869; #0.0, 1.0 *(значення координат в межах числового масиву від 0 до 1)*
$uv = [$u, $v*$ratio, zCoord]; *(призначення UV)*
$subdivisions = 80; # 1, 100; *(значення ділення точок шуму в межах числового масиву від 1 до 100)*

-(Масштабування UV координат)

$uv *= $subdivisions;
$color = cnoise($uv); *(призначаємо генерацію самого шуму)*
$color *(виведення кольору)*

Рекомендації щодо вибору мови залежно від потреб проекту

Вибір мови для процедурного текстурування залежить від конкретних вимог проекту. Нижче наведені рекомендації щодо використання SeExpr та інших мов:

- SeExpr: Рекомендується для проектів, де важлива швидкість прототипування та простота використання. Підходить для художніх

працівників, які хочуть швидко створювати та налаштовувати текстури без глибоких знань програмування.

- GLSL: Ідеальний вибір для проектів, де потрібна висока продуктивність та виконання у реальному часі. Підходить для розробників ігор та додатків з високими вимогами до графіки.
- HLSL: Рекомендується для проектів, що розробляються під платформу Windows та використовують DirectX. Підходить для створення високоякісних візуальних ефектів у іграх та інтерактивних додатках.
- RSL (RenderMan Shading Language): Ідеальний вибір для кінематографічної графіки та анімації, де важлива висока якість та деталізація текстур. Підходить для студій анімації та візуальних ефектів.

Висновки. У результаті проведеного дослідження було встановлено, що мова SeExpr, завдяки своєму простому синтаксису та високій гнучкості, є потужним інструментом для процедурного текстурування, особливо у сфері анімації та візуальних ефектів, в умовах нестачі часу на розробку та візуальну генерацію ідей з використанням методів процедурної генерації текстур. SeExpr дозволяє швидко прототипувати та налаштовувати текстури, що робить її зручною для художніх працівників без глибоких знань програмування. Водночас, продуктивність мови обмежена у порівнянні з мовами, орієнтованими на графічні апаратні прискорювачі, такими як GLSL та HLSL. Перспективи подальших розвідок у даному напрямі включають:

- Розробка нових модулів та функцій, які підвищать продуктивність та розширять можливості мови.
- Інтеграція з новими платформами та інструментами. Покращення інтеграції SeExpr з різними програмами для 3D-моделювання та рендерингу, а також розробка підтримки для нових платформ.
- Оптимізація коду SeExpr для підвищення продуктивності, зокрема через використання можливостей GPU.
- Активізація зусиль з популяризації SeExpr серед розробників та працівників художніх сфер, створення нових навчальних матеріалів та документацій.

Це дослідження допомагає покращити розуміння особливостей та можливостей різних мов для процедурного текстурування, що, в свою чергу, мотивує та сприятиме їхньому більш ефективному використанню у комп'ютерній графіці та суміжних галузях.

Література

1. Stefan Gustavson. (2012) "Procedural Textures in GLSL." In OpenGL Insights: OpenGL, OpenGL ES and WebGL community experiences, edited by Patrick Cozzi and Christophe Riccio, *CRC Press*.

2. Matt Pharr, Wenzel Jakob, Greg Humphreys. (2016) Physically Based Rendering: From Theory to Implementation. *Morgan Kaufmann.*

3. Tomas Akenine-Möller, Eric Haines, Naty Hoffman. (2018) Real-Time Rendering. *CRC Press.*

4. Pereira John. (2013) "Real-Time Shader Programming with HLSL and DirectX".

5. Литвиненко Л.О., Скляренко О.В., Колодінська Я.О. (2020) Логіка побудови інтерфейсів у програмному забезпеченні. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях.* – Харків: НТУ «ХПІ». – № 1 (3). С. 54-59. doi:10.20998/2413-4295.2020.03.07.

References

1. Stefan Gustavson. (2012) "Procedural Textures in GLSL." In OpenGL Insights: OpenGL, OpenGL ES and WebGL community experiences, edited by Patrick Cozzi and Christophe Riccio, *CRC Press*.

2. Matt Pharr, Wenzel Jakob, Greg Humphreys. (2016) Physically Based Rendering: From Theory to Implementation. *Morgan Kaufmann.*

3. Tomas Akenine-Möller, Eric Haines, Naty Hoffman. (2018) Real-Time Rendering. *CRC Press.*

4. Pereira John. (2013) "Real-Time Shader Programming with HLSL and DirectX".

5. Lytvynenko L.O., Skliarenko O.V., Kolodinska Y.O. (2020) The logic of building interfaces in software. Bulletin of the National Technical University "KhPI". Series: New solutions in modern technologies. - Kharkiv: NTU "KhPI". – No. 1 (3). P. 54-59. doi:10.20998/2413-4295.2020.03.07.

DOI: 978-966-301-266-7/1.2024.27

Волкова Н.М.
https://orcid.org/0009-0000-4075-6695
e-mail: ninel.volkova@e-u.edu.ua

Опольський М.В.
e-mail: mopoljsjkyj@e-u.edu.ua

ЗАСТОСУВАННЯ ЦИФРОВИХ СЕРВІСІВ ДЛЯ НАВЧАННЯ МАТЕМАТИЦІ

Анотація. У статті розглядаються декілька популярних освітніх платформ, серед яких Khan Academy, Prodigy, IXL Math, DreamBox, Matific, Алгебра Навчальна Система (Algebrator) та МійКлас. Останню платформу було обрано для детальнішого аналізу через її численні переваги: онлайн-база завдань з основних предметів шкільної програми, можливість зацифрування навчальної програми вчителя для впровадження дистанційного навчання, електронні перевірочні роботи, автоматична звітність для адміністрації та функції батьківського контролю. Рекомендується до застосування при вивченні курсу шкільної математики та підготовки до НМТ цифрова платформа МійКлас, яка у 2019 році була схвалена Інститутом модернізації змісту освіти, а у 2020 році рекомендована для використання під час карантину як ефективна дистанційна технологія.

Ключові слова: цифрові освітні платформи, інформаційний простір, освітні компетентності, навчання онлайн.

Вступ. У сучасному інформаційному просторі навчання вимагає від здобувачів різноманітних компетентностей та навичок. Відповідно до Європейських еталонних рамок, такі компетентності, як «Знання математики та загальні знання у сфері науки і техніки», «Навички роботи з цифровими носіями» та «Навчання заради здобуття знань», доцільно формувати та розвивати з використанням цифрових освітніх платформ. Сьогодні існує велика кількість цифрових платформ, що вимагає ретельного вибору з урахуванням можливостей, адаптації до потреб учнів, вікових обмежень та уподобань цільової аудиторії.

Виклад основного матеріалу. Навчання в сучасному інформаційному просторі вимагає від здобувачів різноманітних компетентностей та навичок.

За Європейськими еталонними рамками такі компетентності як «Знання математики та загальні знання у сфері науки і техніки», «Навички роботи з цифровими носіями» та «Навчання заради здобуття знань» доцільно формувати та розвивати з використанням цифрових освітніх платформ.

На сьогоднішній день цифрових платформ існує велика кількість, тому перш ніж обирати, варто розглянути їхні можливості, адаптацію до потреб учня, вікові обмеження та врахувати особливості та уподобання цільової аудиторії.

1. Khan Academy: безкоштовні уроки з математики на різних рівнях складності, від початкового до вищого, велика кількість відеоуроків та завдань.

2. Prodigy: об'єднує гру з математичними завданнями. Надає можливість вивчати математику через виконання завдань у формі ігор.

3. IXL Math: надає безліч вправ і тестів з математики для учнів різних вікових категорій. Дозволяючи учням відстежувати свій прогрес.

4. DreamBox: інтерактивна, з персоналізованими математичними завданнями для учнів початкової школи.

5. Matific: пропонує ігровий підхід до вивчення математики для дітей дошкільного та початкового шкільного віку через короткі інтерактивні завдання.

6. Алгебра Навчальна Система (Algebrator): допомагає учням з різними рівнями математичних знань вивчати алгебру через покрокові розв'язки завдань та пояснення.

7. МІЙКЛАС – відкрита система, яку можна апробовувати в будь-який час, у будь-якому місці, на будь-якому гаджеті, де є Інтернет.

Розглядаючи запропоновані варіанти було обрано платформу МІЙКЛАС. Серед переваг її використання слід зазначити наступне: онлайн-база завдань з основних предметів шкільної програми; можливість зацифрування навчальної програми вчителя для впровадження дистанційного навчання учнів; електронні перевірочні роботи, що можуть бути видані та виконані дистанційно; автоматична звітність для адміністрації закладів щодо використання МійКлас учителями та учнями; функції батьківського контролю тощо. У квітні 2019 р. система була схвалена Інститутом модернізації змісту освіти, підпорядкованого МОН України, а у 2020 рекомендовано як дистанційна технологія, що може використовуватись під час карантину.

Висновки. У сучасному інформаційному просторі навчання вимагає від здобувачів різноманітних компетентностей та навичок, що відповідають вимогам Європейських еталонних рамок, зокрема знання математики, загальні

знання у сфері науки і техніки, навички роботи з цифровими носіями та навчання заради здобуття знань.

Цифрові освітні платформи є ефективним інструментом для розвитку зазначених компетентностей, забезпечуючи інтерактивне та персоналізоване навчання. Серед численних цифрових платформ особливо виділяються Khan Academy, Prodigy, IXL Math, DreamBox, Matific, Алгебра Навчальна Система (Algebrator) та МійКлас. Кожна з них має свої унікальні особливості та переваги, що дозволяють задовольнити різні потреби учнів.

Платформа МійКлас була обрана для детального аналізу через її численні переваги, зокрема онлайн-базу завдань з основних предметів шкільної програми, можливість зацифрування навчальної програми вчителя для впровадження дистанційного навчання, електронні перевірочні роботи, автоматичну звітність для адміністрації та функції батьківського контролю. Впровадження платформи МійКлас у навчальний процес сприяє підвищенню ефективності дистанційного навчання, поліпшенню контролю за навчальним прогресом учнів та забезпеченню гнучкості освітнього процесу, що особливо важливо в умовах сучасних викликів, таких як карантин.

Загалом, використання цифрових освітніх платформ відкриває нові можливості для навчання, сприяє розвитку необхідних навичок та компетентностей учнів, забезпечуючи більш гнучкий, інтерактивний та адаптивний освітній процес.

Література

1. Natalia Bobro. Digitalization and management of the modern educational process. *The University of Technology in Katowice Press 2024* С. 12-24 DOI: https://doi.org/10.54264/M036
2. Дмитренко А. В., вчитель інформатики. Технології та інструменти розвитку креативного мислення. Освітній проект «На урок» для вчителів, https://naurok.com.ua/tehnologi-ta-instrumenti-rozvitku-kreativnogo-mislennya-156906.html
3. Павлюх В.В. Розвиток креативності в учнів різного віку : навч.-метод. посіб. КЗ «КОІППО імені Василя Сухомлинського». 2023. 72 с.
4. Скляренко О.В., Ягодзінський С.М., Ніколаєвський О.Ю., Невзоров А.В. Цифрові інтерактивні технології навчання як невід'ємна складова сучасного освітнього процесу // Науковий журнал «Інноваційна педагогіка», Випуск 68, Т.2. – 2024. - с. 250-257.

DOI: 978-966-301-266-7/1.2024.30

Гараган К.О.
https://orcid.org/0009-0007-3551-2654
email: kristina.garagan@e-u.edu.ua

РОЗВИТОК НАВИЧОК АКАДЕМІЧНОГО ПИСЬМА У СТУДЕНТІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»: ПРОФЕСІЙНА АНГЛІЙСЬКА МОВА

Анотація. В сучасному інформаційному суспільстві, де кібербезпека займає центральне місце, вміння чітко та ефективно висловлювати технічні концепції та рішення стають критично важливими для професійного розвитку.

Стаття систематизує основні виклики процесу навчання академічного письма, зокрема, низький рівень компетентності написання англомовних наукових текстів. Вона аналізує сучасні підходи та методики, спрямовані на покращення мовних навичок студентів, включаючи використання інтерактивних онлайн-ресурсів, вебінарів та спеціалізованих курсів з англійської мови для професійних цілей.

Особлива увага приділяється інтеграції технологій у навчальний процес, що дозволяє створювати інтерактивні площини для розвитку комунікаційних навичок. Також розглядається роль критичного мислення та аналітичних здібностей у написанні наукових робіт сфери кібербезпека, які спрямовані на розв'язання сучасних проблем галузі.

Стаття висвітлює чинні підходи та рекомендації для вдосконалення навчання академічного письма в контексті професійної підготовки студентів кібербезпеки, наголошуючи на значенні інтеграції мовних та технічних навичок для професійного зростання.

Ключові слова: кібербезпека, академічне письмо, професійна англійська мова, навчання та навчальні методи, комунікаційні навички, онлайн-ресурси, вебінари, критичне мислення, аналітичні здібності.

Harahan Kristina

DEVELOPMENT OF ACADEMIC WRITING SKILLS FOR CYBERSECURITY STUDENTS: PROFESSIONAL ENGLISH

Abstract. In a modern-day information society, where cybersecurity is central, the ability to express technical concepts and solutions clearly and effectively is becoming critical for professional development.

The paper systemizes the main challenges of teaching academic writing, particularly the low level of competence in writing English-language scientific texts. It analyses modern approaches and methods aimed at improving students' language skills, including the use of interactive online resources, webinars and specialized ESP courses.

Particular attention is paid to the integration of technology into the learning process, which allows you to create interactive learning spaces to improve learning efficiency and develop communication skills. The role of critical thinking and analytical skills in writing research papers on cybersecurity aimed at solving modern problems in the industry is also considered.

The article highlights existing approaches and recommendations for improving academic writing instruction in the context of cybersecurity students' professional training, emphasising the importance of integrating language and technical skills for successful professional development.

Key words: cybersecurity, academic writing, professional English/ESP, teaching and learning methods, communication skills, online resources, webinars, critical thinking, analytical skills.

Introduction. In the rapidly evolving field of cybersecurity, effective communication skills in professional English are crucial for students to succeed academically and professionally. As the demand for cybersecurity professionals grows, so does the necessity for these individuals to convey complex technical concepts clearly and persuasively in written form. This article explores the development of academic writing skills tailored specifically for students specializing in cybersecurity, emphasizing the integration of professional English competency into their educational curriculum.

Academic writing in the context of cybersecurity not only enhances students' ability to articulate technical knowledge but also prepares them to engage with global discourse in the field. This interdisciplinary approach draws upon insights from various studies. For instance, Masood underscores the challenges faced by students in mastering English competencies essential for cybersecurity education [6]. Gaitán-López proposes strategies for fostering academic language skills through Content and Language Integrated Learning (CLIL) methodologies, directly applicable to cybersecurity courses [5].

Moreover, research by Cabaj, Domingos, Kotulski & Respício provides a comprehensive analysis of cybersecurity education programs, highlighting the

evolution of pedagogical practices and curriculum design [2, p.29]. Pawlowski and Jung examine social representations of cybersecurity among university students, shedding light on instructional implications for enhancing academic writing skills [9, p.291].

Analysis. Recent studies have explored various methodologies for teaching academic writing to cybersecurity students. These approaches range from traditional classroom instruction to innovative techniques incorporating technology-enhanced learning. For instance, Masood highlights the importance of tailored English competency programs for cybersecurity education, emphasizing practical application in technical contexts [6, p.53].

One of the primary challenges identified is the dual requirement for technical accuracy and linguistic clarity in academic writing within cybersecurity. Gaitán-López proposes strategies for overcoming language barriers through Content and Language Integrated Learning (CLIL), advocating for immersive language acquisition methods in technical fields [5].

The integration of professional English competency into cybersecurity curriculum is crucial for preparing students to communicate effectively in professional settings. Cabaj, Domingos, Kotulski & Respício discuss the evolution of pedagogical practices in cybersecurity education, emphasizing the role of language proficiency in enhancing students' ability to articulate complex cybersecurity concepts [2].

Comparative studies with related disciplines such as computer science and engineering reveal both commonalities and distinct challenges in teaching academic writing. Pawlowski and Jung analyse the social representations of cybersecurity among students, underscoring the need for targeted instructional design to bridge technical and academic writing skills [9, p.288].

Despite advancements, several areas remain underexplored, including the effectiveness of specific pedagogical methods in enhancing writing skills for diverse student demographics in cybersecurity programs. Further research is needed to develop comprehensive frameworks that address these gaps and support inclusive educational practices.

Aim. This article aims to synthesize these insights and propose effective strategies for educators to cultivate academic writing proficiency among cybersecurity students. By integrating professional English training into the curriculum, universities can better equip students to meet the demands of the cybersecurity profession and contribute meaningfully to the global discourse on cybersecurity issues.

Methods. A total of 58 students (bachelor's degree) enrolled in cybersecurity programs at Highly Educational Establishment European University participated in this study. Participants were assigned an experimental group (n=30) or a control group (n=28).

The experimental group received a structured professional English module focusing on academic writing skills tailored for cybersecurity contexts. The module included lectures, writing workshops, and online exercises delivered over a period of 8 weeks.

Procedure. Pre-test and post-test assessments were administered to both groups. The pre-test assessed baseline academic writing skills using a standardized rubric measuring technical writing proficiency in cybersecurity contexts. The post-test evaluation utilized the same rubric to measure improvements following the intervention.

Results. Quantitative analysis. Statistical analysis using paired t-tests indicated a significant improvement ($p < 0.05$) in writing scores for the experimental group post-intervention compared to their pre-test scores. Specifically, participants in the experimental group demonstrated an average increase of 12% in technical writing proficiency scores.

Qualitative insights. Qualitative data from participant feedback and open-ended survey responses highlighted themes such as increased confidence in writing technical reports and enhanced understanding of professional English conventions.

The findings suggest that integrating targeted professional English modules into cybersecurity education effectively enhances students' academic writing skills, preparing them more effectively for professional communication within the frameworks of technical sphere.

Conclusions. The study on the development of academic writing skills among cybersecurity students using professional English has yielded significant insights into effective educational strategies and their impact on student learning outcomes.

The integration of targeted professional English modules proved effective in enhancing students' technical writing proficiency within cybersecurity domains. Participants in the experimental group demonstrated statistically significant improvements in their academic writing skills compared to the control group.

The intervention not only improved participants' writing abilities but also fostered greater confidence in communicating technical concepts effectively. This is crucial for cybersecurity professionals who must articulate complex information clearly and precisely.

The study underscored the practical relevance of integrating professional English skills within cybersecurity education. By focusing on industry-specific

writing tasks and conventions, students were better prepared for the professional demands of the field.

Findings suggest the need for ongoing curriculum development in cybersecurity programs to incorporate structured language proficiency components. This ensures that students not only excel in technical skills but also possess the communication abilities necessary for successful careers in cybersecurity.

Further research could explore the longitudinal effects of integrating professional English modules across different stages of cybersecurity education. Additionally, examining the scalability of these interventions and their applicability in diverse educational settings would provide valuable insights for educators and curriculum developers.

References

1. Al-Khwarizmi, N. A. M., & Abduvakhabova, D. (2020). English in Cyber security. T.: ALOQACHI.
2. Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 75, 24-35. https://doi.org/10.1016/j.cose.2017.12.002
3. Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. Journal of Cybersecurity, 5(1), tyz001. https://doi.org/10.1093/cybersecurity/tyz001
4. Chepelyuk, N. (2021). Teaching ESP course for the students of different language competency who are majoring in cybersecurity. Актуальні питання гуманітарних наук, 2021, 257.
5. Gaitán-López, F. J. (2020). Fostering academic language in CLIL: A proposal for a cybersecurity course.
6. Masood, K. M. (2022). English competencies and challenges for data science and cyber security students at Al Istiqlal University. The Creative Launcher, 7(5), 48-68.
7. Nelson, J. K., & Donham, B. L. (2020, June). Partnership to prepare students for careers in the emerging field of cybersecurity. In 2020 ASEE Virtual Annual Conference Content Access.
8. Nyemkova, E., Justice, C., Liaskovska, S., & Lakh, Y. (2022). Methods of current knowledge teaching on the cybersecurity example. Education Sciences, 12(11), 732. https://doi.org/10.3390/educsci12110732
9. Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. Journal of Information Systems Education, 26(4), 281-294.

DOI: 978-966-301-266-7/1.2024.35

Романенкова О.Ю.
https://orcid.org/0009-0003-1099-0300
e-mail olena.romanenkova@e-u.edu.ua

ПСИХОЛОГІЧНИЙ АСПЕКТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ: СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ ВЗАЄМОДІЇ

Анотація. Стаття є дослідженням психологічних аспектів безпеки життєдіяльності. Указано, що психологічний аспект безпеки життєдіяльності – це важлива та багатогранна концепція, що охоплює різноманітні виклики та стратегії взаємодії у сучасному суспільстві. Психологія безпеки життєдіяльності допомагає людям розуміти й усвідомлювати ризики, пов'язані з різними сферами їхнього життя, такими як безпека на роботі, на дорозі, вдома тощо. Це дає змогу індивідам усвідомлювати потенційні небезпеки і приймати обґрунтовані рішення. Психологія безпеки життєдіяльності вивчає, як емоції впливають на сприйняття й оцінку ризику, а також на реакцію людини на небезпеку. Розуміння впливу емоцій може допомогти розробити ефективні стратегії зниження ризиків і поліпшити безпеку. Психологія безпеки життєдіяльності враховує важливість соціального контексту у формуванні безпеки життєдіяльності. Соціальні чинники, такі як норми, цінності, стереотипи, підтримка оточуючих людей і комунікація, можуть впливати на сприйняття ризиків та безпеку. Сучасний світ стикається з різноманітними проблемами психології безпеки життєдіяльності. Найбільш поширеними проблемами є: інформаційна перевантаженість, цифровий стрес, кібербулінг, крадіжка особистих даних, залежність від технологій, інформаційна маніпуляція. Стратегії заспокоєння та розвитку резилієнтності є важливими аспектами психології безпеки життєдіяльності в сучасному світі. Ось деякі з них: дихальні вправи та релаксація, збереження фізичного здоров'я, планування та управління часом, практика позитивного мислення. Розвиток психологічного аспекту безпеки життєдіяльності має практичне значення для нашого повсякденного життя. Він допомагає нам зберегти особисту безпеку, поліпшити якість міжособистісних відносин, ефективно вирішувати проблеми та підтримувати фізичне і психічне здоров'я. Ці стратегії взаємодії стають інструментами, які допомагають нам адаптуватися до змін і забезпечувати психологічну стійкість у сучасному світі.

Ключові слова: безпека життєдіяльності, психологічне благополуччя, цифровий світ, конфіденційність, резильєнтність, критичне мислення.

Romanenkova Olena

PSYCHOLOGICAL ASPECT OF LIFE SAFETY: MODERN CHALLENGES AND STRATEGIES OF INTERACTION

Abstract. The psychological aspect of life safety is an essential and multifaceted concept that encompasses various challenges and interaction strategies in modern society. This abstract explores the contemporary challenges related to psychological safety and the strategies for effective interaction. First and foremost, modern society faces a wide range of threats, including natural disasters, technological accidents, terrorist acts, pandemics, and more. These events can cause significant levels of stress and anxiety in individuals. The psychological aspect of life safety investigates how emotions influence risk perception, assessment, and individual reactions to danger. Secondly, the social context plays a crucial role in psychological safety. Interactions with others, group dynamics, and perceptions of social safety norms can influence feelings of security and emotional resilience in individuals. Thirdly, the psychological aspect of safety in the informational environment examines the impact of information technologies, social media, and media on psychological well-being. People are confronted with an increasing volume of information, including negative and harmful content, which can induce stress and affect mental well-being. The psychological aspect explores how to manage information overload, develop critical thinking skills, and promote a healthy relationship with technology. Contemporary challenges in the psychology of life safety include information overload, digital stress, cyberbullying, personal data theft, technology addiction, and information manipulation. Strategies for calming and developing resilience are vital aspects of the psychology of life safety in the modern world. Some of these strategies include breathing exercises and relaxation techniques, maintaining physical health, effective time management, and practicing positive thinking. The development of the psychological aspect of life safety has practical significance in our daily lives. It helps us maintain personal safety, improve interpersonal relationships, effectively solve problems, and support physical and mental well-being. These interaction strategies become tools that enable us to adapt to changes and maintain psychological stability in the modern world.

Key words: life safety, psychological well-being, digital world, confidentiality, resilience, critical thinking.

Вступ. Психологічний аспект безпеки життєдіяльності – це важлива та багатогранна концепція, що охоплює різноманітні виклики та стратегії взаємодії у сучасному суспільстві. Забезпечення благополуччя та безпеки осіб

у повсякденному житті передбачає не лише фізичний захист, а й вирішення їхніх психологічних потреб та проблем. В останні роки психологія усе більше визнає глибокий вплив психологічних чинників на відчуття безпеки та загальну якість життя особи. Це визнання призвело до збільшення уваги до розуміння та вирішення психологічних аспектів безпеки життєдіяльності. У цьому контексті з'явилися сучасні виклики, що підкреслюють необхідність комплексного підходу до забезпечення психологічного благополуччя особи. Чинники, такі як технологічний прогрес, соціальні зміни, екологічні загрози і глобальні кризи, внесли нові складнощі та ризики в життя людей, що вимагають глибокого розуміння психологічних динамік, що відбуваються. Окрім того, пандемія COVID – 19 принесла непередбачувані виклики для відчуття безпеки особи, її психічного здоров'я та соціальної зв'язаності, наголошуючи на важливості психологічних стратегій у збереженні стійкості та підтримки благополуччя. Для успішного вирішення цих викликів необхідно розробляти та впроваджувати відповідні стратегії взаємодії. Ці стратегії стосуються не лише окремих осіб, а й спільнот, установ, що приймають рішення, оскільки вони відіграють важливу роль у сприянні культурі безпеки та психологічної підтримки.

Співпраця між психологами, медичними працівниками, педагогами та різними зацікавленими сторонами є вирішальною для створення комплексних кадрових систем, які інтегрують психологічне благополуччя у ширший контекст безпеки життєдіяльності.

Виклад основного матеріалу. Свідомість ризиків є важливим складником психології безпеки життєдіяльності. Вона відноситься до усвідомлення людиною потенційних небезпек і ризикованих ситуацій у різних аспектах їхнього життя. Основна мета свідомості ризиків полягає у тому, щоб люди могли розпізнавати небезпеку, оцінювати ризики і приймати обґрунтовані рішення, спрямовані на зниження ризиків та забезпечення безпеки. Ключові аспекти свідомості ризиків:

– Розпізнавання ризиків: виявлення фізичних небезпек, соціальних загроз, здоров'язберігаючих ризиків та інших потенційних небезпек.

– Оцінка ризиків вимагає здатності аналізувати інформацію про потенційні наслідки, ймовірність їх виникнення та вплив цих наслідків на безпеку.

– Самооцінка. Люди повинні бути в змозі оцінювати свої власні здібності, знання та навички, які необхідні для безпечної поведінки. Це включає визначення своїх обмежень та усвідомлення власних сильних і слабких боків

– Прийняття обґрунтованих рішень означає урахування доступної інформації про ризики, оцінювання альтернатив та вибір найбезпечніших шляхів дії.

– Комунікація. Важливою частиною свідомості ризиків є здатність ефективно спілкуватися щодо безпеки з іншими людьми. Це може включати обмін інформацією про ризики, поради щодо безпеки, навчання та попередження інших про потенційні небезпеки .Емоції грають важливу роль у психології безпеки життєдіяльності. Вони мають вплив на сприйняття, оцінку та реакцію людини на ризиковані ситуації та небезпеку. Коли ми стикаємося з потенційно небезпечними ситуаціями, емоції можуть впливати на сприйняття ризику. Позитивні емоції можуть призвести до недооцінки ризиків, тоді як негативні – спричинити перебільшення ризиків. Розуміння впливу емоцій на сприйняття ризиків допомагає забезпечити більш об'єктивну оцінку потенційних небезпек. Емоції також мають вплив на поведінку в ризикованих ситуаціях. Наприклад, страх може спонукати до обережності та уникання небезпеки, тоді як відсутність страху або позитивні емоції – сприяти більш ризикованій поведінці. Розуміння впливу емоцій на поведінку допомагає розробити ефективні стратегії безпеки. Прийняття рішень також підпорядковується емоційному впливу. Емоційний стан може впливати на спосіб обґрунтування ризиків, оцінку альтернатив та вибір стратегій дії. Розуміння того, як емоції впливають на прийняття рішень, є важливим для кращого управління ризиками . Нарешті, емоції, особливо стрес, можуть впливати на реакцію людини на небезпеку. Стрес може викликати фізіологічні та психологічні зміни, що можуть впливати на здатність адекватно реагувати на небезпеку. Стресові реакції можуть змінювати рівень уваги, концентрації, реакційну швидкість та здатність приймати обґрунтовані рішення, що може впливати на безпеку. Соціальний контекст відіграє суттєву роль у психології безпеки життєдіяльності. Він включає у себе взаємодію з іншими людьми, соціальні норми, культурні впливи та сприйняття безпеки в громадському просторі. Ось деякі аспекти соціального контексту, які впливають на безпеку:

– Вплив оточуючих: оточуючі люди можуть впливати на наше сприйняття безпеки і безпечну поведінку. Наприклад, якщо люди навколо нехтуючи ставляться до безпеки, це може підштовхнути нас до ризикованої поведінки. Зворотний вплив також може мати місце, коли ми спостерігаємо безпечну поведінку інших людей, що може стимулювати нас до прийняття безпечних рішень.

– Сприйняття безпеки в громадському просторі може варіюватися залежно від соціального контексту. Деякі сфери або ситуації можуть сприйматися як більш безпечні, ніж інші, на основі повідомлень ЗМІ, статистики, думок та досвіду інших людей

– Соціальна підтримка. Наявність соціальної підтримки може впливати на нашу поведінку в ситуаціях ризику. Коли ми маємо підтримку і розуміння оточуючих, це може підвищити нашу впевненість та здатність дотримуватися безпечних стратегій. Спільні правила, навчання і тренування з безпеки, а також допомога інших людей можуть сприяти безпеці та зменшенню ризику.

– Соціальний вплив може мати ефект на нашу безпеку, особливо у групових ситуаціях. Розуміння соціального впливу допомагає нам ставати більш самостійними й обґрунтованими у своїх діях, зберігаючи при цьому безпеку Важливо зазначити, що психологічний аспект безпеки в інформаційному середовищі відіграє важливу роль у забезпеченні безпеки та захисту особистої інформації у цифровому світі. Для забезпечення ефективного захисту в цьому середовищі необхідно враховувати кілька ключових аспектів. Розвиток критичного мислення є ключовим чинником у психологічній безпеці в інформаційному середовищі. Це означає, що особи повинні бути здатними критично оцінювати достовірність джерел інформації, переконуватися у безпеці перед виконанням певних дій (наприклад, натискання посилань або завантаження файлів), а також розуміти різницю між справжніми повідомленнями та шахрайськими схемами. Управління паролями та обмеження доступу до особистої інформації є ще одним важливим аспектом психологічної безпеки в інформаційному середовищі. Рекомендується використовувати сильні паролі, регулярно їх змінювати, уникати використання одного пароля для різних сервісів та забезпечувати конфіденційність своїх облікових записів. Окрім того, важливим аспектом психологічної безпеки в інформаційному середовищі є здатність фільтрувати інформацію. В Інтернеті ми зіштовхуємося з великим обсягом інформації, і це може створювати психологічний стрес та спричиняти втому. Уміння відділяти достовірну інформацію від недостовірної, перевіряти джерела та розуміти контекст допомагає зберегти емоційний комфорт та уникнути поширення неправдивої або шкідливої інформації Сучасний світ стикається з різноманітними проблемами психології безпеки життєдіяльності. Найбільш поширеними проблемами є: інформаційна перевантаженість, цифровий стрес, кібербулінг, крадіжка особистих даних, залежність від технологій, інформаційна маніпуляція. Слід також звернути увагу на ефект FOMO (Fear of Missing Out). Соціальні мережі та постійний доступ до інформації про життя інших можуть створювати почуття упущеного шансу (FOMO). Люди можуть відчувати, що їхнє життя не таке захопливе або важливе, порівнюючи себе з ідеалізованими зображеннями інших. Це може спричиняти стрес, незадоволення собою та негативно впливати на психічне здоров’я .Ураховуючи ці проблеми, важливо вживати заходів для забезпечення психологічної безпеки у сучасному світі: – Саморегулювання і баланс.

Важливо розуміти свої власні потреби і обмеження щодо використання технологій. Установлення границь і обмежень у часі, які ви приділяєте онлайн-активностям, може допомогти уникнути перевантаження та залежності.

– Розвиток критичного мислення.

– Збереження приватності та безпеки даних.

– Розуміння впливу соціальних мереж.

– Розвиток соціальної підтримки.

Навчайтеся розпізнавати та уникайте взаємодій, які можуть бути шкідливими для вашої емоційної стабільності. Залучайтеся до підтримуючих груп і практикуйте емоційну взаємодію з близькими людьми. Важливо мати можливість відкрито висловлювати свої почуття, спілкуватися зі своїми близькими і шукати підтримку в разі стресових ситуацій .Психологічна безпека також включає у себе розвиток резильєнтності. Резильєнтність – це здатність пристосовуватися до стресу, невдач та труднощів і повертатися до нормального стану. Розвиток резильєнтності включає у себе розуміння власних емоцій, розвиток соціальної підтримки, позитивного мислення і здатність швидко адаптуватися до змін. Стратегії заспокоєння та розвитку резильєнтності є важливими аспектами психології безпеки життєдіяльності у сучасному світі. Ось деякі з них:

– Дихальні вправи та релаксація.

– Збереження фізичного здоров’я.

– Планування та управління часом.

– Практика позитивного мислення.

Розвиток навичок рішення проблем є ще однією важливою стратегією. Уміння визнавати потенційні ризики, розробляти ефективні стратегії вирішення проблем та залучати необхідні ресурси допомагає забезпечити безпеку в різних ситуаціях. Здоровий спосіб життя також має велике значення для психологічної безпеки. Звернення уваги на фізичне та психічне здоров’я (регулярна фізична активність, збалансоване харчування і відпочинок) допомагає підтримувати енергію та витривалість. Окрім того, навчання і набуття нових навичок є важливою стратегією у психології безпеки життєдіяльності. Набуття знань про безпеку в різних аспектах життя допомагає підвищити компетентність і впевненість у себе. Це може включати навчання практичних навичок, таких як перша допомога або основи самооборони, а також оволодіння навичками розумного використання технологій та Інтернету.

Висновки. Психологічний аспект безпеки життєдіяльності є важливим елементом нашого благополуччя й успішної адаптації до сучасного світу. Розвиток самосвідомості, комунікаційних навичок, навичок рішення проблем,

здорового способу життя та набуття нових знань допомагає забезпечити психологічну безпеку і зменшити уразливість перед різними загрозами. Окрім того, критичне мислення та розвиток резильєнтності є необхідними вміннями в умовах сучасного інформаційного середовища. Уміння критично оцінювати інформацію, виявляти шахраїв та захищати свою конфіденційність допомагає зберегти психологічну безпеку в онлайн-середовищі. Розвиток психологічного аспекту безпеки життєдіяльності має практичне значення для нашого повсякденного життя. Він допомагає нам зберегти особисту безпеку, поліпшити якість міжособистісних відносин, ефективно вирішувати проблеми та підтримувати фізичне та психічне здоров'я. Ці стратегії взаємодії стають інструментами, які допомагають нам адаптуватися до змін і забезпечувати психологічну стійкість у сучасному світі. Практичне значення отриманих результатів вивчення психологічного аспекту безпеки життєдіяльності полягає у можливості застосування цих знань і стратегій у реальному житті. Отримані результати можуть мати вагомий вплив на якість життя та безпеку людей у сучасному світі. По-перше, інформування та освіта на основі отриманих результатів можуть допомогти збільшити рівень обізнаності про психологічну безпеку та свідоме ставлення до ризикових ситуацій. Це може включати розроблення інформаційних матеріалів, проведення тренінгів та навчальних програм для різних груп населення. По-друге, результати дослідження можуть бути використані для розроблення індивідуальних стратегій взаємодії з різними викликами та небезпеками. Люди зможуть вивчити навички самосвідомості, емоційного регулювання, комунікації та розвитку резильєнтності. Це допоможе зміцнити їхню психологічну стійкість, забезпечити ефективну адаптацію до змін та зменшити негативний вплив стресових ситуацій. Практичне значення отриманих результатів також полягає у впровадженні психологічних аспектів безпеки життєдіяльності на рівні громадської політики та соціальних програм. Інформація про вплив психологічних чинників на безпеку та благополуччя може бути використана для розроблення ефективних заходів у сфері охорони здоров'я, освіти, роботи з молоддю, кризового управління та соціального захисту. Такі програми можуть сприяти психологічній стійкості, підвищенню якості життя та загальному благополуччю суспільства.

Література

1. Калашнікова Л.В. Особливості вивчення безпеки життєдіяльності як соціального явища. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Соціологічні дослідження сучасного суспільства: методологія, теорія, методи». 2017. Вип. 39. С. 73–79.

2. Корнієнко О.В. Теоретико-методологічні питання безпеки життєдіяльності на прикладі психології безпеки. Психологія національної безпеки та безпеки життєдіяльності. Вчені записки ТНУ імені В.І. Вернадського. Серія «Психологія». 2021. Т. 32(71). № 5. С. 166–171.

3. Письменна М.С., Бондарчук С.В. Психологічні аспекти безпеки життєдіяльності. Вчені записки ТНУ імені В.І. Вернадського. Серія «Психологія». 2021. Т. 32(71). № 5. С. 172–176. 4. Піскунова Л., Прилипко В., Зубок Т. Безпека життєдіяльності : підручник. Київ : Академія, 2012. 224 с.

5. Слюсаревський М.М. Психологічна безпека людини в онтологічному і гносеологічному вимірах. Післямова до роботи, відзначеної Державною премією України в галузі науки та техніки. Наукові студії з соціальних та політичних наук. 2020. Вип. 45(48). С. 7–26.

6. Цюман Т., Нагула О. Психологічна формула безпеки як концептуальна основа формування навичок безпечної поведінки особистості. Педагогічна освіта: теорія і практика. Психологія. Педагогіка. 2021. № 35(1). С. 94–100.

7. Толок А.О., Крюковська О.А. Безпека життєдіяльності : навчальний посібник. URL: http: // www. dstu. dp. ua / Portal / Data / 5/10 / 2–10-mz33. pdf (дата звернення: 23.06.2023)

DOI: 978-966-301-266-7/1.2024.41

Гудаков Д.О.
https://orcid.org/0009-0000-3003-842X
e-mail: denysgud@gmail.com

Скляренко П.А.
e-mail: psklyarenko@e-u.edu.ua

ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІННОВАЦІЙНОЮ ДІЯЛЬНІСТЮ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Анотація. У статті досліджено особливості формування та оцінювання системи управління інноваційною діяльністю підприємства в сучасних умовах цифрової трансформації. Визначено ключові етапи формування та оцінювання системи управління з метою забезпечення ефективності інноваційних процесів та досягнення стратегічних цілей підприємства з огляду на виклики сьогодення. Наведені основні компоненти системи управління інноваційною діяльністю підприємства. Надано рекомендації щодо формування та розвитку ефективної системи управління інноваціями для забезпечення довгострокового успіху підприємства в умовах швидкозмінного ринкового середовища та цифрової трансформації.

Ключові слова: управління інноваціями, інноваційні проекти, інноваційна діяльність підприємства, цифрові інструменти

Виклад основного матеріалу. Більшість підприємств в умовах сучасних викликів та активного розвитку цифрової трансформації усвідомлюють необхідність інтеграції інноваційної стратегії у загальну бізнес-стратегію. Це дозволяє забезпечити системний підхід до розвитку інновацій та досягнення стратегічних цілей. Проте, деякі підприємства все ще стикаються з труднощами у формулюванні конкретних та вимірюваних інноваційних цілей. Ефективне управління інноваційною діяльністю потребує гнучкої організаційної структури та чіткого визначення ролей і відповідальностей. Наявність спеціалізованих підрозділів для управління інноваціями є ключовою умовою для успішної реалізації інноваційних проектів.

Формування системи управління інноваційною діяльністю включає наступні основні етапи.

Визначення цілей та завдань.

- Стратегічні цілі. Зосередження на довгострокових інноваційних цілях, які сприяють зростанню конкурентоспроможності підприємства.
- Оперативні завдання. Формулювання конкретних завдань для досягнення стратегічних цілей, включаючи розробку нових продуктів, впровадження нових технологій, вдосконалення процесів тощо.

Розробка інноваційної стратегії.

- Аналіз внутрішнього та зовнішнього середовища: Визначення сильних та слабких сторін підприємства, а також можливостей та загроз на ринку.
- Формування інноваційного портфелю: Вибір пріоритетних напрямків інноваційної діяльності, розподіл ресурсів між різними проектами.
- Вибір методів та інструментів: Впровадження сучасних методів управління інноваціями, таких як Design Thinking, Lean Startup, Agile тощо.

Організаційна структура.

- Створення інноваційних підрозділів: Визначення структурних підрозділів або команд, відповідальних за інноваційну діяльність.
- Визначення ролей та відповідальностей: Розподіл функцій між учасниками процесу інновацій, забезпечення чіткої комунікації та координації.

Фінансування інновацій.

- Джерела фінансування. Визначення внутрішніх і зовнішніх джерел фінансування для підтримки інноваційних проектів.
- Бюджетування. Розробка фінансових планів, що включають бюджети на дослідження, розробки та впровадження інновацій.

Управління людськими ресурсами.

- Розвиток компетенцій. Навчання та підвищення кваліфікації персоналу для підтримки інноваційної діяльності.
- Мотивація та стимулювання. Розробка системи мотивації для залучення співробітників до інноваційних проектів.

Нижче розглянемо етапи оцінювання системи управління інноваційною діяльністю.

Визначення критеріїв оцінки.

- Ефективність. Вимірювання результативності інноваційної діяльності щодо досягнення поставлених цілей.
- Економічність. Оцінка витрат на інноваційні проекти та їх фінансову віддачу.
- Якість. Вимірювання якості інноваційних продуктів і процесів, рівень задоволеності споживачів.

 Часові параметри. Оцінка швидкості впровадження інноваційних рішень, дотримання встановлених термінів.

Методи оцінки.

 SWOT-аналіз. Оцінка внутрішніх та зовнішніх факторів, що впливають на інноваційну діяльність.

 Балансова оцінка. Визначення фінансових показників ефективності інноваційних проектів.

 Методи бенчмаркінгу. Порівняння інноваційних показників підприємства з аналогічними показниками конкурентів.

 Аналіз ризиків. Виявлення та оцінка ризиків, пов’язаних з інноваційною діяльністю, розробка заходів з їх мінімізації.

Зворотній зв'язок та коригування.

 Моніторинг та контроль. Постійне відстеження прогресу інноваційних проектів, внесення коректив у разі відхилень від плану.

 Оцінка результатів. Підведення підсумків по завершенню проектів, аналіз досягнутих результатів.

 Впровадження покращень. Внесення змін до системи управління інноваціями на основі результатів оцінки, вдосконалення процесів та методів роботи.

Концептуальні засади формування і оцінювання системи управління інноваційною діяльністю забезпечують системний підхід до розвитку інноваційної активності підприємства, що сприяє його стійкому розвитку і підвищенню конкурентоспроможності на ринку.

Переконливу перевагу підприємства порівняно з іншими конкурентами неможливо забезпечити без залучення інноваційної складової. Тільки нові ідеї, процеси, управлінські рішення, цифрові технології, які здатні будуть надати відповідний ресурс, за рахунок якого можливий значний відрив від конкурентів в галузі. Тому не дивно, що сучасний економічний простір приділяє величезну увагу механізму формування і оцінювання системи управління інноваційною діяльністю підприємства.

Для підприємств інноваційний процес передбачає впровадження інноваційних, удосконалених технологічних процесів виробничої діяльності, які забезпечують вироблення високоякісної продукції, зниження витрат на енергоносії, зростання продуктивності праці, завдяки чому зменшуються витрати на виробництво. Зі зростанням обсягів виробництва інноваційної продукції, зниженням витрат на її виробництво, зменшенням термінів на її виробництво підприємство підвищує свої доходи через те, що розвивається і веде результативну господарську діяльність.

В процесі огляду наукової літератури з питання оцінювання системи управління інноваційною діяльністю підприємства в сучасних воєнних умовах

економічного розвитку, були виявлені різні методичні підходи до актуальної проблематики. Так, науковець Малюта Л. [1] запропонувала свою модель комплексного аналізу результативності інноваційної діяльності підприємства, за допомогою якої можна визначити інтегральний показник рівня інноваційної діяльності

Таким чином, ефективність інноваційного розвитку підприємства прямо залежить від того, наскільки правильно розроблена модель оцінювання інноваційного розвитку підприємства, відібрані найбільш характерні показники оцінки інноваційного процесу з урахуванням всіх необхідних та специфічних напрямків оцінювання на різних етапах впровадження нововведень, наскільки точно здійснено оцінювання ефективністю управління інноваціями, сформовано чітку стратегію, наскільки адекватно визначено її методи та пріоритети розвитку інноваційної діяльності.

Інноваційна діяльність є важливим фактором підвищення конкурентоспроможності підприємства. Вона забезпечує можливість адаптації до змін у зовнішньому середовищі та стимулює зростання підприємства. Управління інноваційною діяльністю має стратегічне значення і повинно бути інтегровано в загальну стратегію підприємства. Це забезпечує синергію між різними функціональними підсистемами та сприяє досягненню стратегічних цілей.

Ефективне управління інноваціями вимагає створення спеціалізованих підрозділів, визначення ролей і відповідальностей, а також забезпечення тісної взаємодії між різними підрозділами підприємства. Це дозволяє більш ефективно координувати інноваційні процеси та використовувати ресурси.

Для успішного впровадження інновацій необхідно забезпечити адекватне фінансування. Це включає визначення джерел фінансування, бюджетування проектів та моніторинг фінансових результатів.

Управління інноваціями потребує залучення кваліфікованих та мотивованих працівників. Це передбачає підбір і навчання персоналу, створення умов для розвитку інноваційних здібностей та впровадження системи мотивації.

Використання сучасних методів та цифрових інструментів, сприяє підвищенню ефективності інноваційних процесів. Ці методи допомагають краще адаптуватися до змін та швидко реагувати на потреби ринку.

Важливою складовою управління інноваціями є оцінювання ефективності системи. Це включає визначення критеріїв оцінки, використання різних методів та інструментів аналізу, моніторинг та коригування процесів на основі отриманих даних.

Постійний зворотний зв'язок та оцінка результатів дозволяють вчасно виявляти проблеми та вносити необхідні корективи. Це забезпечує

безперервне вдосконалення системи управління інноваціями та підвищення її ефективності.

Висновки. У проведеному дослідженні визначено основні теоретичні та практичні аспекти формування системи управління інноваційною діяльністю підприємства. Впровадження ефективної системи управління інноваціями є ключовим фактором забезпечення довгострокового успіху підприємства в умовах швидкозмінного ринкового середовища та цифрової трансформації. Для досягнення цього необхідно забезпечити інтеграцію інноваційної діяльності в загальну стратегію підприємства, створити відповідну організаційну структуру, забезпечити фінансування, ефективно управляти людськими ресурсами та використовувати сучасні методи і інструменти управління.

Література

1. Малюта Л. Я. Інноваційно-цифрові перспективи розвитку економіки України / Л. Я. Малюта, Л. В. Дерманська // Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Економіка і управління. - 2019. - Т. 30(69), № 2. - С. 55-60. - Режим доступу: http://nbuv.gov.ua/UJRN/UZTNU_econ_2019_30(69)_2_14.

2. Бобро Н. С. Систематизація процесів управління на сучасному етапі трансформації економіки. *Інвестиції: практика та досвід*. № 7. 2024. С.112-116. DOI: https://doi.org/10.32702/2306-6814.2024.7.112

DOI: 978-966-301-266-7/1.2024.48

Доровський В.О.
https://orcid.org/ 0009-0008-7816-4546
e-mail: volodymyr.Dorovskyi@e-u.edu.ua

Доровська І.О.
https://orcid.org/0000-0001-8694-5395
e-mail: i.dorovska@e-u.edu.ua

Доровський Д.В.
https://orcid.org/0009-0008-7816-4546
e-mail: dmytro.dorovskyi@e-u.edu.ua

ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДАНИХ У КОНТЕКСТІ ДИНАМІЧНИХ ЗМІН

Анотація. У сучасних інформаційних технологіях забезпечення безпеки даних є однією з найважливіших задач, особливо в умовах динамічних сценарно-прецедентних систем. Ці системи характеризуються високим рівнем змінності та складністю сценаріїв, які використовуються для моделювання різноманітних ситуацій та подій. Ця робота присвячена дослідженню питань інформаційної безпеки об'єктів динамічних сценарно-прецедентних систем. У роботі розглядаються основні методи та підходи до захисту даних, що включають криптографічні алгоритми, системи виявлення вторгнень та методи аутентифікації. Особливу увагу приділено аналізу загроз, які можуть виникати в процесі функціонування таких систем, а також методам їх запобігання та нейтралізації. На основі проведеного аналізу були запропоновані нові методи підвищення рівня безпеки, що базуються на використанні штучного інтелекту та машинного навчання для виявлення аномалій та прогнозування потенційних атак. В роботі також розглядаються питання забезпечення конфіденційності, цілісності та доступності даних у контексті динамічних змін середовища функціонування. Запропоновані підходи та методи були протестовані на практичних прикладах, що демонструють їх ефективність та доцільність використання для захисту інформаційних систем у динамічних умовах. Результати дослідження можуть бути корисними для розробників програмного забезпечення, аналітиків безпеки та інших фахівців у галузі інформаційної безпеки.

Ключові слова: інформаційна безпека, динамічні системи, сценарно-прецедентні системи, криптографія, виявлення вторгнень, машинне навчання, аномалії.

Dorovskyi Volodymyr, Dorovska Iryna, Dorovskyi Dmytro

INFORMATION SECURITY OF OBJECTS OF DYNAMIC SCENARIO-PRECEDENTED SYSTEMS

Abstract. In modern information technology, ensuring data security is one of the most critical tasks, especially in dynamic scenario-based precedent systems. These systems are characterized by a high level of variability and complexity in the scenarios used for modeling various situations and events.This paper is dedicated to the study of information security issues for objects in dynamic scenario-based precedent systems. The paper examines the main methods and approaches to data protection, including cryptographic algorithms, intrusion detection systems, and authentication methods. Special attention is given to the analysis of threats that may arise during the operation of such systems, as well as methods for their prevention and mitigation.Based on the conducted analysis, new methods for enhancing security levels have been proposed, which are based on the use of artificial intelligence and machine learning to detect anomalies and predict potential attacks. The paper also addresses issues of ensuring data confidentiality, integrity, and availability in the context of dynamic environmental changes.The proposed approaches and methods have been tested on practical examples, demonstrating their effectiveness and feasibility for protecting information systems under dynamic conditions. The research results can be useful for software developers, security analysts, and other professionals in the field of information security.

Key words: information security, dynamic systems, scenario-based precedent systems, cryptography, intrusion detection, machine learning, anomalies.

Проблема досліджень. Процес інформаційної безпеки ІБО реалізується визначенням поняття об'єкта динамічних сценарно-прецедентних систем і вимагає зображення образів і сцен для побудови алгоритму і програми динамічних сценарно-прецедентних систем. Запропонований в роботі підхід до формування сценарно-прецедентних технологій ІБ та ідентифікації передбачає побудову підпрограм виділення об'єктів на зображенні сцени, створення еталонних зображень і порівняння об'єкта з еталоном.

Цілі і задачі досліджень. Для формування сценарно-прецедентних технологій ІБ та ідентифікації об'єктів як оптичних образів визначимо

зображення сцени і створимо еталонні зображення, проводячи компаративний аналіз цих зображень.

Методи отриманих досліджень визначались формуванням інформаційної технології ідентифікації оптичних образів з компараторним аналізом цих зображень.

Результати досліджень. Формування сцени. Вважаємо, що сцена представляє собою набір різнорідних об'єктів, встановлених у довільному порядку перед об'єктивом телевізійної системи. Тоді кожен такий об'єкт може бути описаний підмножиною точок wi, що належать загальному множині точок сцени W. У загальному випадку сцена, що містить два різні об'єкти, може бути представлена наступним чином:

$$\left.\begin{array}{l}\omega_1 \neq 0 \\ \omega_2 \neq 0 \\ \omega_1 \bigcap \omega_2 \neq 0\end{array}\right\} \quad (1)$$

Проектуючи зображення на площину, ми отримаємо нові підмножини, що представляють собою проекції вихідних. При цьому об'єкти можуть перекривати один одного, і отримані проективні множини будуть представляти собою перетин проекцій основних множин:

$$\omega_{пр} \square \omega_1 \cup \omega_2 \setminus \omega_1;$$

$$\omega_2 \setminus \omega_1 \square \omega_2 \cap \overline{\omega_1} \quad (2)$$

При наявності в сцені трьох об'єктів, їх проекція буде відповідно описуватись так:

$$\omega_{пр} \square \omega_1 \cup \omega_2 \setminus \omega_1 \cup \omega_3 \setminus (\omega_2 \cup \omega_1); \quad (3)$$

Цей ряд, при бажанні, можна продовжувати далі. Кожен об'єкт, описуваний множиною ωi, формує в просторі вхідних координат X вхідний сигнал системи fi(x), який в подальшому порівнюється з еталонним сигналом fi*(x), що належить заданому алфавіту F*. Завдання ідентифікації ІБ у загальному випадку повинно вирішуватись у два етапи – на першому етапі локалізуються об'єкти на зображенні сцени, а на другому проводиться аналіз виділених фрагментів сцени на предмет відповідності еталонним зображенням. Оскільки еталонне зображення генерується системою, то це компенсує примітивність моделі формування зображення. Виходячи з концепції інтерпретації зображення як сукупності геометричних об'єктів, доцільно розглядати операцію визначення відповідності зображення реального об'єкта і його геометричної моделі. Геометричне узгодження, що

розглядається як визначення ступеня близькості реального об'єкта і його геометричної моделі, відкриває можливість використання методів геометричного моделювання при представленні еталонів образу. Основою побудови моделей об'єктів є використання методів геометричного моделювання, що базується на знанні "конструкції" об'єкта та математичному описі його елементів.

Основною ідеєю використання геометричного моделювання в завданнях ідентифікації образів є геометричне узгодження. При цьому підході мається на увазі наявність вихідної гіпотези – "моделі світу", описаної адекватно завданню отримання на її основі, з використанням знань про умови спостереження, відповідного спостережуваному зображення. З точки зору геометричного моделювання висунута гіпотеза представляється як опис складного з точки зору геометрії об'єкта як сукупність "примітивів" – більш простих геометричних об'єктів.

Природне бажання мати обчислювані примітиви визначило використання наступної групи: багатогранники – об'єми, обмежені плоскими багатокутниками, квадрики – об'єми, обмежені неплоскими площинами поверхонь, "замітаємі" тіла або узагальнені циліндри – об'єми, обмежені переміщенням кривої в просторі, октальні дерева – тіла, декомпозовані на ієрархію кубічних первинних елементів, зі сторонами, рівними деякому кванту довжини, помноженому на степінь двійки, супереліпсоїди (супер квадрики).

На етапі генерації зображення необхідно: згрупувати пікселі в геометричні об'єкти, визначити відповідність груп пікселів геометричним об'єктам, визначити просторове положення і орієнтацію об'єкта відносно відеосенсора. Враховуючи рух і еволюцію об'єкта, введено чотиривимірний простір, де визначені як об'єкти – примітиви.

В такому випадку геометричне узгодження зводиться до визначення найбільш близького до спостережуваного геометричного опису або моделі. Представляючи вхідну інформацію як адитивну суміш регулярного сигналу і випадкової складової, отримуємо завдання мінімізації впливу випадкової складової. У випадку алгоритму, що мінімізує ймовірність помилки при відомих апріорних ймовірностях, отримуємо Байєсів алгоритм. Якщо апріорні ймовірності невідомі, природно використання класифікації за методом максимальної правдоподібності. Для адитивної випадкової складової N(t) і точок моделі Xi(t), вводячи оператор вводу зображення I, можна записати відповідність між даними і моделлю:

$$Y_i(t) \square I(X_i(t)) \square N(t). \qquad (4)$$

При цьому оператор вводу (5) визначає вплив збурень у зовнішньому середовищі. Враховуємо: - обертання R(t) – матриця обертання; - переміщення T(t) – вектор паралельного переносу; - зміни масштабу s(t) – масштабний коефіцієнт; - умови спостереження r(.) – оператор проективного перетворення, що враховує перспективні викривлення; - операцію "затінення", описану оператором Q(t,.). Тоді оператор вводу через оператор опису даних D можна представити у вигляді:

$$I(X(t)) \square D(Q(t, \rho(s(t), R(t)X(t) \square \mathbf{T}(t)))). \quad (5)$$

Упрощуючи, у припущенні простого відновлення статичних образів, отримуємо:

$$I(X(t)) \square Q(\rho(s, RX \square \mathbf{T})). \quad (6)$$

Звідси випливають два основні підходи - глобальне узгодження з метрикою

$$G(X_j, Y_i) \square \inf_{(s,R,\mathbf{T})} \left\| Y_i - Q(\rho(s, RX_j \square \mathbf{T})) \right\|, \quad (7)$$

та локальне узгодження з метрикою

$$G(X_j, Y_i) \square \inf_{(s,R,\mathbf{T})} \left\| Y_i - Q(\rho(s, RX_j \square \mathbf{T})) \right\|, \quad (8)$$

Інтерес представляє питання визначення відповідності даного елемента зображення моделі. Для багатьох точок це завдання має вигляд:

Нехай Yi – i–е безліч точок з Ny точок даних Yi={yik}, kÎ{1,…, Ny}, яке потрібно узгодити з безліччю Xi з Nx модельних точок Xi={xji}, iÎ{1,…, Nx }. Для Ny£ Nx, що визначає достатність моделі та дає можливість порівнювати дані з усіма можливими підмножинами моделі. Для класифікатора побудованого за методом максимальної правдоподібності та зображення l(k) вирішальна метрика має вигляд:

$$L(X_{j,} Y_i) \square \inf_{Z \subseteq X_j} \inf_{\lambda} \inf_{s,R,\mathbf{T}} \sum_{k \square 1}^{N_Y} \left\| \mathbf{y}_{ik} - sR\mathbf{x}_{j\lambda(k0} - \mathbf{T} \right\|^2, \quad (9)$$

де: NY=ïZï - число точок Z, а xjl(k)ÎZ.

У задачі узгодження кривих з параметризованою модельною кривою h(u) метрика узгодження має вигляд:

$$L(\mathbf{x}_j, \mathbf{y}_i) \square \inf_{(s,R,\mathbf{T})} \int_{u_0}^{u_1} \left\| \mathbf{y}_i - Q(\rho(s, R\mathbf{x}_j(\eta(u) \square \mathbf{t})) \right\|^2 du. \quad (10)$$

Аналогічно для вирішення задачі узгодження поверхонь загальна метрика L2 для j-ї параметричної поверхні xj(h, x) моделі та i-ї параметричної поверхні yi(u,v), отриманої з даних про зображення, має вигляд

$$L(\mathbf{x}_j, \mathbf{y}_i) \square \inf_{\eta,\xi} \inf_{(s,R,\mathbf{T})} \int_{\Omega_0} \left\| \mathbf{y}_i(u,v) - Q(\rho(s, R\mathbf{x}_j(\eta(u,v), \xi(u,v) \square \mathbf{T})) \right\|^2 dudv.$$

(11)

Виходячи із завдання ідентифікації елементів сцени, використовуємо модель формування плоского зображення, засновану на формальному операторі відображення об'ємної сцени її плоске зображення. Звичайно, при такому підході спрощення досягається за рахунок відмови від точності відновлення характеристик сцени. Для ілюстрації наведемо спрощену схему, рис.1, що відбиває підхід до побудови моделі формування плоского зображення. Враховуючи, що в кінцевому випадку для чутливої поверхні аналізатора формується плоске зображення, розглянемо випадок формування плоского зображення, що породжується об'єктами з алфавіту. При цьому кожному з об'єктів ωі відповідає, у випадку тривимірна, функція, що описує його властивості

$$\omega_i \leftrightarrow f_i \square \vec{x} \square, \qquad \dim \vec{x} \square 3. \tag{12}$$

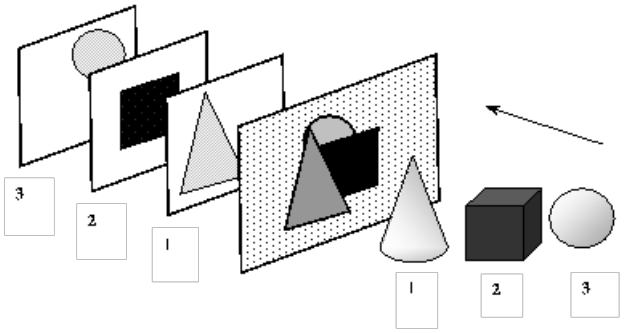


Рис. 1 Формування плоского зображення.

Під час формування плоского зображення необхідно враховувати ефекти, пов'язані з перекриттям зображень. Так, для двох об'єктів результуюча сцена Lw1w2 – це їхнє об'єднання.

$$L_{\omega_1\omega_2} \square \omega_1 \cup \omega_2$$

Враховуючи, що безліч об'єктів сцени, у загальному випадку, перебувають у загальному становищі, можемо записати:

$$\omega_{1,2} \square \omega_1 \setminus \omega_2 \cup \omega_2 \square \omega_1 \cap \overline{\omega}_2 \cup \omega_2 \square \omega_1 \cup \omega_2 \ .$$

Для трьох об'єктів картина ускладнюється, але можна легко побачити формування шарів. У кожному шарі зображення кожного з елементів сцени представлене без спотворень, що виникають за рахунок накладення інших елементів сцени, причому це уявлення еквівалентне об'єднанню елементів сцени:

$$\omega_{1,2,3} = \omega_3 \cup \omega_0 \setminus \omega_3$$
$$\omega_0 = \omega_2 \cup \omega_1 \setminus \omega_2$$
$$\omega_{1,2,3} = \omega_3 \cup (\omega_2 \cup (\omega_1 \setminus \omega_2)) \setminus \omega_3 =$$
$$= \omega_3 \cup \omega_2 \setminus \omega_3 \cup (\omega_1 \setminus \omega_2) \setminus \omega_3 =$$
$$= \omega_3 \cup \omega_2 \setminus \omega_3 \cup \omega_1 \setminus \omega_2 \setminus \omega_3 = \omega_3 \cup \omega_2 \cup \omega_1.$$

Таким чином, вводячи опис об'єктів ωі, як належать своїм «шарам», малюнок 2, можливо, використовуючи символ різниці послідовності множин, формалізувати завдання формування плоского зображення у вигляді

$$^{n}\setminus_{1} \omega_i \cup ^{n}\setminus_{2} \omega_i \cup \ldots \cup ^{n}\setminus_{n-1} \omega_i \cup \omega_n = \Omega \qquad (13)$$

Причому природно виконується логічне умова наявності зображення лише тому випадку, коли сцена не порожня

$$\Omega = \bigcup_{i=1}^{n} \omega_i$$

З іншого боку, вираз (13) дозволяє трактувати формування зображення як поєднання шарів. В цьому випадку істотна послідовність нумерації шарів - від першого, далекого, шару до n-го ближнього шару (рис. 2).

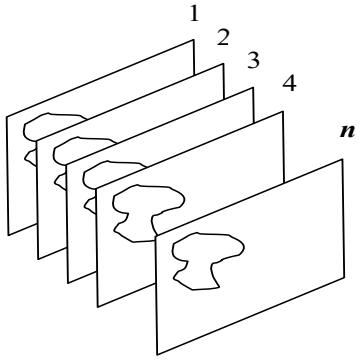


Рис. 2 - Шари об'єкта.

З іншого боку, кожен елемент сцени, як образ ωі, породжує параметричне поле ji=ji(x) на деякій точці, яку можна визначити через обмеження приналежності

$$\omega_i \leftrightarrow x = x \mid \varphi_i(x) \le c$$

(14)

Звичайно, умова ji(x)=c визначає контур зображення або його межу. При цьому ідеалізоване зображення з відкинутими елементами ji(x)>c визначається як

$$\varphi_i^*(\mathbf{x}) = \begin{cases} \varphi_i(\mathbf{x}) & if \quad \varphi_i(x) \le c \\ 0 & if \quad \varphi_i(x) > c \end{cases}.$$

(15)

Таким чином, припустивши, що розподіл j * i (x) визначає і зображення, розглянемо вид співвідношення, що визначає формування плоского зображення. По-перше, із співвідношення ri(x)ji(x)=j*i(x) визначимо фільтр r :

$$\rho_i(\mathbf{x}) = \begin{cases} 1 & if \quad \varphi_i(\mathbf{x}) \le c \\ 0 & if \quad \varphi_i(\mathbf{x}) > c \end{cases}.$$

(16)

При цьому, очевидно, вводячи матрицю 1 з одиничними елементами та нульову матрицю 0, маємо:

$$\begin{aligned} &\bar{\rho}_i(\mathbf{x}) = 1 - \rho_i(\mathbf{x}), \\ &\varphi_i(\mathbf{x})\rho_i(\mathbf{x}) = \varphi_i^*(\mathbf{x}), \\ &\varphi_i^*(\mathbf{x})\bar{\rho}_i(\mathbf{x}) = 0. \end{aligned} \qquad (17)$$

тоді для двох фрагментів можемо записати

$$\varphi_{12}^*(\mathbf{x}) = \varphi_1^*(\mathbf{x})\bar{\rho}_2(\mathbf{x}) = \varphi_2^*(\mathbf{x}).$$

(18)

Аналогічно можемо визначити поле зображення для трьох фрагментів

$$\varphi_{123}^*(\mathbf{x}) = \varphi_1^*(\mathbf{x})\bar{\rho}_2(\mathbf{x})\bar{\rho}_3(\mathbf{x}) = \varphi_2^*(\mathbf{x})\bar{\rho}_2(\mathbf{x}) = \varphi_3^*(\mathbf{x}).$$

(19)

Враховуючи (3.17), для довільної кількості фрагментів маємо

$$\varphi_{1\ldots n}^*(\mathbf{x}) = \varphi_1(\mathbf{x})\rho_1(\mathbf{x})\prod_{i=2}^{n}\bar{\rho}_i(\mathbf{x}) = \varphi_2(\mathbf{x})\rho_2(\mathbf{x})\prod_{i=3}^{n}\bar{\rho}_i(\mathbf{x}) = \ldots = \varphi_n(\mathbf{x})\rho_n(\mathbf{x}).$$

(20)

Або, у більш компактній формі, отримуємо аналог співвідношення (3.20) для зображень, що описуються реальними розподілами

Оскільки завданням є вибір методу побудови еталонних зображень методу компенсації зображень, розглянемо особливості висловлювання

$$\varphi_{1\ldots n}^*(\mathbf{x}) = \sum_{k=1}^{n-1}\varphi_k(\mathbf{x})\rho_k(\mathbf{x})\prod_{i=k+1}^{n}\bar{\rho}_i(\mathbf{x}) = \varphi_n(\mathbf{x})\rho_n(\mathbf{x}). \qquad (21).$$

По-перше, зображення нерозривно пов'язані з маскою, визначеної певному рівні функції власності; по-друге, зображення формуються не з окремих деталей фрагментів сцени, а з повних зображень фрагментів, кожен

фрагмент має свій фільтр, що залежить від положення фрагмента в сцені. Слід зазначити, що для фрагмента, що не має перетинів, фільтр перетворюється на одиницю.

Таким чином, для генератора еталонів доцільно формувати зображення як функцію приналежності, і при переході до формування сцени використовувати певну на заданому рівні маску. З цією метою для конкретного еталона визначаємо основні вузли та будуємо скелетний граф, що відображає основні обмеження – топографію об'єкта. Істотним є формування поля зображення виходячи з логічного зв'язку (13), що дозволяє отримати опис сцени за будь-якого обурення в просторі об'єктів.

Висновки. Розглядаючи формування інформаційної технології ідентифікації ІБ оптичних образів, можна зробити такі висновки:

1. Інформаційна технологія завдання формування оптичного образу і сцени, що містить ідентифікований образ, базується на логічних співвідношеннях, що описують приналежність і зв'язність. При цьому основна властивість об'єкта по відношенню до процедури ідентифікації ІБ – зв'язок, що дозволяє описувати об'єкт як зв'язковий граф.

2. Використання скелетного графа при побудові зображення зразка спрощує операцію генерації зразка.

3. Використання проективного перетворення дозволяє різко скоротити обсяг обчислень під час фрагментації сцени.

4. Використання при побудові еталонного зображення нечітких множин дозволяє спростити генерацію еталона і узгоджується з використанням афінних перетворень зображення.

Література

1. Столлінгс, Вільям. "Криптографія та захист мереж: Принципи та практика." Прентис Холл, 2016.
2. Шнайєр, Брюс. "Прикладна криптографія: Протоколи, алгоритми та вихідний код на C." Вайлі, 2015.
3. Бішоп, Метт. "Комп'ютерна безпека: Мистецтво та наука." Аддісон-Веслі, 2018.
4. Голлман, Дітер. "Комп'ютерна безпека." Вайлі, 2011.
5. Андерсон, Росс. "Інженерія безпеки: Посібник зі створення надійних розподілених систем." Вайлі, 2020.
6. Деннинг, Дороті Е. "Модель виявлення вторгнень." IEEE Transactions on Software Engineering, 1987.

7. Джаджодія, Сушіл та ін. "Розширені системи баз даних." Спрінгер, 1997.

8. Чжоу, Жі та ін. "Розпізнавання безпечної поведінки на основі глибокого навчання в промислових системах управління." IEEE Transactions on Industrial Informatics, 2020.

9. Бойко, Олександр. "Інформаційна безпека в динамічних інформаційних системах." Дисертація, Київський національний університет імені Тараса Шевченка, 2021.

10. Скляр, Іван. "Моделювання та аналіз загроз інформаційної безпеки у динамічних системах." Дипломна робота, Національний технічний університет України "Київський політехнічний інститут", 2019.

11. NIST (Національний інститут стандартів і технологій). NIST Cybersecurity Framework.

12. OWASP (Проект з безпеки веб-додатків з відкритим вихідним кодом). OWASP Top Ten.

13. SANS Institute. SANS Reading Room.

14. IEEE Symposium on Security and Privacy.

15. ACM Conference on Computer and Communications Security (CCS).

16. Journal of Information Security and Applications.

17. Computers & Security.

18. Пашорін В. І., Скляренко О.В., Милашенко В.М. Аналіз технологій захисту комп'ютерних мереж на базі систем виявлення вторгнень. Актуальні питання забезпечення кібербезпеки та захисту інформації: колективна монографія / за заг. наук. ред. А.М. Давиденко, Київ: Європейський університет, 2023. – С. 93-108.

19. Троян К.М., Скляренко О.В. Безпека програмного забезпечення в хмарному середовищі //Актуальні питання забезпечення кібербезпеки та захисту інформації: Зб. матеріалів IX Міжн. наук.- практ. конф., Київ, 30.03.2023 р.; К.: Вид-во Європейського університету, 2023 – С. 107-109.

20. Скляренко О.В., Казіміров В.А., Управління інформаційною безпекою підприємства // Актуальні питання забезпечення кібербезпеки та захисту інформації. Матеріали VI міжнародної науково-практичної конференції 19 – 22 лютого 2020 р.- Київ-2020.- Видавництво Європейського університету. – С. 90-92.

21. Невзоров А.В., Скляренко О.В., Колодінська Я.О., Яровий Р.О. Особливості аналітичного забезпечення експлуатації інформаційних систем та обладнання в сучасних умовах // Журнал «Прикладні питання математичного моделювання», Т.6, № 1 – 2023. - с. 117-123.

References

1. Stallings, William. "Cryptography and Network Security: Principles and Practice." Prentice Hall, 2016.

2. Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, and Source Code in C." Wiley, 2015.

3. Bishop, Matt. "Computer Security: Art and Science." Addison-Wesley, 2018.

4. Hollman, Dieter. "Computer security." Wiley, 2011.

5. Anderson, Ross. "Security Engineering: A Guide to Building Trusted Distributed Systems." Wiley, 2020.

6. Denning, Dorothy E. "An Intrusion Detection Model." IEEE Transactions on Software Engineering, 1987.

7. Jajodia, Sushil and others. "Advanced database systems." Springer, 1997.

8. Zhou, Zhi et al. "Safe behavior recognition based on deep learning in industrial control systems." IEEE Transactions on Industrial Informatics, 2020.

9. Boyko, Oleksandr. "Information security in dynamic information systems." Dissertation, Taras Shevchenko Kyiv National University, 2021.

10. Sklyar, Ivan. "Modeling and analysis of information security threats in dynamic systems." Diploma thesis, National Technical University of Ukraine "Kyiv Polytechnic Institute", 2019.

11. NIST (National Institute of Standards and Technology). NIST Cybersecurity Framework.

12. OWASP (Open Source Web Application Security Project). OWASP Top Ten.

13. SANS Institute. SANS Reading Room.

14.IEEE Symposium on Security and Privacy.

15.ACM Conference on Computer and Communications Security (CCS).

16. Journal of Information Security and Applications.

17. Computers & Security.1. Stallings, William. "Cryptography and Network Security: Principles and Practice." Prentice Hall, 2016.

18. Pashorin V.I., Skliarenko O.V., Milashenko V.M. Analysis of technologies for the protection of computer networks based on intrusion detection systems. Topical issues of cybersecurity and information protection: a collective monograph / edited by A.M. Davydenko, Kyiv: European University, 2023. pp. 93-108.

19. Troian K.M., Skliarenko O.V. Software security in the cloud environment // Actual issues of cybersecurity and information security: Collection of materials of the IX International Scientific and Practical Conference, Kyiv, 30.03.2023; K.: European University Press, 2023 - P. 107-109.

20. Skliarenko O.V., Kazimirov V.A., Management of information security of the enterprise // Actual issues of ensuring cybersecurity and information protection. Proceedings of the VI International Scientific and Practical Conference, February 19-22, 2020 - Kyiv-2020 - European University Press. - P. 90-92.

21. Nevzorov A.V., Skliarenko O.V., Kolodinska Y.O., Yarovyi R.O. Features of analytical support for the operation of information systems and equipment in modern conditions // Journal "Applied Problems of Mathematical Modeling", Vol. 6, No. 1 - 2023. - c. 117-123.

DOI: 978-966-301-266-7/1.2024.59

Захаренков Д.Ю.
https://orcid.org/0000-0003-3951-022X
e-mail: dmit.zakharen@gmail.com

Литвиненко Л.О.
https://orcid.org/0000-0002-0828-383X
e-mail: leonid.lytvynenko@e-u.edu.ua

Яровий Р.О.
https://orcid.org/0000-0001-8978-8137
e-mail: roman.yaroviy@e-u.edu.ua

СУЧАСНІ ТЕХНОЛОГІЇ ПАРАЛЕЛЬНОГО ПРОГРАМУВАННЯ В МОДЕЛІ РОЗПОДІЛЕНОЇ ПАМ'ЯТІ

Анотація. Представлений огляд реалізацій MPI-засобів паралелізації, орієнтований на область високопродуктивних обчислень. Наведено аналіз продуктивності MPI-засобів, досягнутої на основних реалізаціях MPI при використанні сучасних міжз'єднань з віддаленим прямим доступом до пам'яті (RDMA), таких як Intel Omni-Path та Infiniband EDR. Особливу увагу приділено одностороннім RMA-комунікаціям, які сприяють підвищенню продуктивності та підтримці перспективних PGAS-моделей паралелізації.

Ключові слова: засоби паралельного програмування, Message Passing Interface (MPI), OpenMPI, MVAPICH2, Intel MPI, тестування продуктивності.

Zakharenkov Dmytro, Lytvynenko Leonid, Yarovyi Roman

MODERN TECHNOLOGIES OF PARALLEL PROGRAMMING IN THE DISTRIBUTED MEMORY MODEL

Abstract. Presentations on the implementation of MPI parallelization features, targeting the area of highly productive calculations. An analysis of the productivity of MPI functions achieved on the main MPI implementations with a choice of daily interconnections with remote direct memory access (RDMA), such as Intel Omni-Path and Infiniband EDR, is carried out. Particular attention is paid to one-way RMA communications, which promote increased productivity and support for promising PGAS models of parallelization.

Key words: features of parallel programming, Message Passing Interface (MPI), OpenMPI, MVAPICH2, Intel MPI, productivity testing.

Виклад основного матеріалу. Ця стаття присвячена аналізу технологій паралельного програмування. Оскільки спектр таких технологій дуже широкий, у роботі розглянуті лише сучасні, широко поширені та перевірені на практиці засоби розпаралелювання, які стали стандартами. З урахуванням тенденції збільшення кількості доступних процесорів (процесорних ядер) у всіх сучасних обчислювальних системах – від ПК до суперкомп'ютерів – актуальність паралелізації зростає у різних галузях практичного застосування. Однак стаття в першу чергу орієнтована на область високопродуктивних обчислень (High Performance Computing, HPC). Використання паралельних технологій давно стало одним із ключових способів підвищення продуктивності та скорочення часу розрахунку.

Хоча засоби паралелізації доступні в різних операційних системах, в області HPC і суперкомп'ютерах основним рішенням стала кластерна архітектура на базі операційної системи Linux. В першу чергу такі засоби застосовуються на платформі x86-64, де використовуються високошвидкісні міжз'єднання з віддаленим прямим доступом до пам'яті (RDMA), які не навантажують процесори віддаленого вузла, такі як Infiniband, Ethernet з RDMA (RoCE або iWARP) або Intel Omni-Path. Оцінки продуктивності, наведені у статті, насамперед ставитимуться до таких систем. Тим не менш, засоби паралелізації, звичайно ж, застосовуються і для обчислювальних систем з іншими процесорами та міжз'єднаннями.

Зазвичай моделі паралельного програмування класифікуються за топологією пам'яті, що використовується наступним чином:

• моделі із загальною пам'яттю, призначені для SMP та NUMA-систем;

• моделі з розподіленою пам'яттю, які застосовуються, в тому числі, для кластерів;

• гібридні моделі, що поєднують розподілену та загальну пам'ять, що характерно для сучасних кластерів із багатопроцесорними вузлами, як зазначено в оглядах [1, 2].

Основу для досягнення високої продуктивності на сучасних суперкомп'ютерах, які використовують кластерну архітектуру, становлять засоби паралелізації з розподіленою пам'яттю, які є найбільш поширеними. У цьому огляді проаналізовано саме ці засоби паралелізації. Засоби OpenMP [3], перспективні технології PGAS (Partitioned Global Address Space) [4], а також спеціалізовані засоби паралелізації для прискорювачів у цій статті не розглядаються.

Модель надсилання повідомлень. Розподілена пам'ять

Різні моделі передачі повідомлень відносяться до паралельного програмування з розподіленою пам'яттю, в яких процеси обмінюються даними, надсилаючи та отримуючи повідомлення. Це типово для кластерів обчислювальних вузлів, з'єднаних комунікаційною мережею, де кожен вузол має свою локальну пам'ять, а прямий доступ до пам'яті інших вузлів відсутній.

Існує безліч моделей передачі повідомлень, які представлені у вигляді програмних бібліотек. Далі будуть розглянуті засоби, що найбільш широко застосовуються і довели свою ефективність MPI [5]. Ці моделі передбачають використання бібліотечних викликів і відповідають типу MIMD (множинний потік команд, множинний потік даних класифікації Флінна [5]). Інтерфейс MPI може використовуватись у обчислювальних системах як із загальною, так і з розподіленою пам'яттю.

Стандарт MPI 2.0 запровадив можливість динамічної зміни числа процесів, розширені колективні комунікації та односторонні комунікації MPI_Put/MPI_Get. Ці можливості були додатково покращені у стандарті MPI 3.0, який також дозволив безпосередньо використовувати можливості RDMA. З MPI 2.0 почало підтримуватися паралельне введення-виведення, а остання версія стандарту, включає колективні неблокуючі операції введення-виведення [6].

Односторонні зв'язки базуються на механізмі віддаленого доступу до пам'яті (Remote Memory Access, RMA). У MPI односторонні комунікації мають доступ тільки до так званого вікна, тобто області пам'яті на цілі, яка повідомляє про доступність вікна для інших процесів. Альтернативою використанню вікон є віртуальна пам'ять. Модель MPI RMA дозволяє блокувати вікно і має два режими – активний та пасивний. В активному режимі ціль встановлює період часу, протягом якого доступ до вікна можливий. У пасивному режимі RMA-процес оголошення цілі доступ до вікна не обмежує. Ефективне використання MPI RMA у загальній моделі паралельного програмування PGAS, що поєднує стилі загальної та розподіленої пам'яті, сприяло міграції деяких реалізацій MPI у бік PGAS.

В даний час існує безліч реалізацій MPI, включаючи MPICH, MVAPICH, OpenMPI, Intel MPI, Mellanox X-MPI, IBM Spectrum MPI, HPE MPI та Cray MPI. У рамках цієї статті ми докладніше розглянемо три найактивніші реалізації в широко поширених HPC системах на базі Linux з архітектурою x86-64: OpenMPI, MVAPICH2 та комерційну версію Intel MPI.

Ці реалізації MPI з RDMA використовують універсальні низькорівневі засоби API, засновані на драйверах. Раніше для цього застосовувалися ibverbs із OFED (OpenFabrics Enterprise Distribution) та uDAPL (User Direct Access Programming Library), стандартний API-інтерфейс для RDMA-міжз'єднань

Infiniband, iWARP та RoCE. Програмні засоби OFED мають більш широкі можливості і давно містять uDAPL. Ці низькорівневі API використовуються не тільки для MPI, але й для інших засобів паралелізації, які працюють з RDMA.

Хоча OFED є некомерційним продуктом з доступним вихідним кодом, виробники міжз'єднань його доробляють для своїх апаратних засобів, створюючи варіанти низькорівневих API. Наприклад, компанія Mellanox пропонує свій варіант OFED для міжз'єднань Infiniband та RoCE з низькорівневим драйвером MLX5. Альтернативою цим продуктам для Infiniband є вільно доступні програмні засоби UCX (Unified Communication X), які можуть використовуватися не тільки з MPI, але й у ширшому програмному інструментарії Mellanox HPC-X, що використовується в MPI та PGAS-засобах паралелізації. Також слід відзначити бібліотеку для Infiniband - UCCS (Universal Common Communication Substrate), яка може вважатися альтернативою низькорівневої бібліотеки Mellanox MXM. Вона надає високопродуктивні комунікаційні примітиви, забезпечуючи інтероперабельність мереж та підтримку різних моделей програмування, включаючи MPI та PGAS-засоби. За допомогою UCCS реалізуються різні операції комунікації, включаючи односторонні та двосторонні операції "точка-точка", колективні та віддалені атомарні операції.

Нещодавно для OFED з'явилася альтернатива у вигляді OFI (OpenFabrics Interfaces). Бібліотека libfabric, що входить до складу OFI і використовується в деяких сучасних реалізаціях MPI, представляє API з більш високим рівнем абстракції, ніж libibverbs. Однак виробники ibverbs дозволяють програмним засобам, що застосовують OFI, використовувати libibverbs для частини операцій.

Розгляд цих низькорівневих API виходить за рамки цієї статті, оскільки вони безпосередньо не використовуються в програмах, що розпаралелюються. Однак їх застосування важливо для отримання високої продуктивності MPI, і конкретна реалізація MPI може забезпечувати можливість використання різних таких API. Наприклад, Intel MPI працює з різними низькорівневими API.

Потенційно важливим для досягнення високої продуктивності MPI при паралелізації на спільній пам'яті є використання XPMEM, модуля ядра Linux, який дозволяє процесу відображати пам'ять іншого процесу у віртуальному адресному просторі. Однак розробники XPMEM вказують на можливі помилки в останній версії, тому на даний момент XPMEM можна вважати недостатньо стабільним. Тим не менш, робота з XPMEM підтримується у всіх трьох реалізаціях MPI, що розглядаються, і в цілому його слід вважати актуальним для використання з MPI в найближчому майбутньому.

Продуктивність MPI залежить від багатьох факторів: використовувані міжз'єднання або загальна пам'ять, версії MPI-реалізації, низькорівневий API, тестова система та конкретні MPI-операції. Ефективне рішення для оптимізації продуктивності може ґрунтуватися на механізмах вибору конкретної реалізації, що динамічно змінюється.

Всі три аналізовані реалізації MPI підтримують стандарт MPI 3.1 і роботу з усіма згаданими RDMA зі швидкістю 100 Гбіт/с, а також роботу з DAPL, OFED verbs, UCX та XPMOD. Слід зазначити, що нові версії реалізації MPI з'являються дуже швидко, і дані про продуктивність можуть швидко застаріти.

Поточна версія OpenMPI використовує засоби libfabric. Як і раніше вона поставляється у вигляді відкритого вихідного коду, що є перевагою, оскільки дозволяє реалізувати OpenMPI на різних операційних системах, включаючи різні дистрибутиви Linux, адаптуючи бібліотеки під різні компілятори. Для дистрибутивів доступні двійкові пакети та засоби для роботи з Python. OpenMPI включає також засоби, що належать до PGAS. Як зазначено, IBM Spectrum MPI базується на OpenMPI. У поточній версії є підтримка роботи на нових процесорах з архітектурою, яка відрізняється від x86-64.

Інший вільно доступною реалізацією MPI є MVAPICH, в даний час представлена сімейством MVAPICH2. Як низькорівневий API MVAPICH2 використовує libibverbs. MVAPICH2 відрізняється швидким випуском нових версій та підтримкою різних варіантів бібліотек, оптимізованих для різних цілей. Наприклад, MVAPICH2-GDR оптимізована для роботи з прискорювачами Nvidia, а спеціальний варіант MVAPICH2-X, який раніше орієнтувався на Infiniband, зараз працює зі всіма згаданими RDMA-міжз'єднаннями та підтримує PGAS.

Intel MPI є комерційною реалізацією MPI, що традиційно означає вищий рівень продуктивності порівняно з MVAPICH2 та OpenMPI. В якості низькорівневого API останні версії Intel MPI орієнтуються на libfabric.

Тести продуктивності під час використання MPI

Існує безліч різних тестів продуктивності, які застосовуються для оцінки ефективності використання MPI. Тести SPEC MPI 2007 надають переважно інформацію про продуктивність обчислювальних систем, а не про швидкодію MPI-комунікацій. Такі тести корисні для оцінки масштабованості продуктивності зі збільшенням кількості використовуваних процесів або процесорних ядер. SPEC MPI можна використовувати для оцінки ефективності різних реалізацій MPI та його версій на однакових обчислювальних системах.

Аналіз продуктивності MPI-комунікацій проводять за допомогою мікротестів, які вимірюють затримки та пропускну здатність при різних

операціях MPI. Найбільш широко застосовуються тести OMB (Ohio State University Micro Benchmarks) та IMB (Intel Micro Benchmark). У наборі тестів OMB вимірюються затримка та пропускна здатність для точкових, односторонніх та колективних операцій MPI у широкому діапазоні розмірів повідомлень.

У контексті цього огляду зосередимося на сучасних даних про продуктивність MPI, що використовують найпоширеніші високошвидкісні міжз'єднання з пропускною здатністю 100 Гбіт/с: Infiniband EDR, Intel Omni-Path та Ethernet RoCE/iWARP.

Дані мікротестів MPI дають змогу оцінити характеристики комунікацій, включаючи показники самих міжз'єднань на реальному програмному рівні. Як зазначалося, оцінки залежить від безлічі чинників. Ці оцінки залежать не тільки від характеристик самих міжз'єднань, але і від процесорів, процесорних ядер і оперативної пам'яті, що використовуються. Однак основний вплив на результати має вибір міжз'єднання.

Як зазначалося, результати мікротестів продуктивності MPI залежать як від характеристик міжз'єднання, а й від продуктивності процесорних ядер та оперативної пам'яті. Більше того, на затримки під час роботи з NUMA-серверами може значно впливати розташування мережної плати міжз'єднання. Така плата може знаходитися на PCIe-шині процесора, що виконує MPI-операцію, або процесора сусіднього сокету материнської плати. Тому точне зіставлення продуктивності міжз'єднань або реалізацій MPI можливе лише при порівнянні даних тестів, виконаних на одній і тій же обчислювальній системі.

Різні міжз'єднання або реалізації MPI можуть показувати високу продуктивність на одних тестах і поступатися іншими. Крім того, реалізації MPI мають багато параметрів, які можуть впливати на продуктивність. Швидка поява нових версій реалізацій MPI сприяє швидкому старінню даних щодо їх відносної продуктивності.

Наприклад, зазвичай вважається, що комерційна реалізація Intel MPI демонструє більш високу продуктивність, ніж OpenMPI та MVAPICH2. Однак є дані для нових версій OpenMPI та MVAPICH2, де на деяких тестах вони показують більш високі результати. Наприклад, вважається, що OpenMPI традиційно є високопродуктивною реалізацією, а MVAPICH зазвичай не перевищує OpenMPI більшості додатків. У той же час є дослідження, де демонструється вища продуктивність MVAPICH2. Результати тестів продуктивності MPI корисні також для оцінки продуктивності нових апаратних засобів міжз'єднань та ефективного написання HPC-програм.

Почнемо розгляд даних про продуктивність MPI зі порівняння міжз'єднань Mellanox Infiniband EDR та Intel Omni-Path. Ці дані отримані реалізації MVAPICH2-2.3. Затримка при односторонніх MPI-операціях для

невеликих повідомлень Omni-Path іноді перевищує EDR. Для великих повідомлень іноді EDR буває швидше Omni-Path. Однак частіше показники продуктивності MPI для EDR та Omni-Path близькі. В інших реалізаціях MPI ці співвідношення можуть відрізнятись.

Як зазначалося раніше, продуктивність MPI може істотно залежати від використовуваних реалізаціями програмних засобів MPI, включаючи низькорівневі API. Застосування UCX дозволило підвищити пропускну здатність OpenMPI під час роботи з EDR. Ще одним важливим засобом підвищення продуктивності MPI є XPMEM. Застосування XPMEM дозволяє зменшити затримки на тестах OMB для різних розмірів повідомлень, тому MVAPICH2-2.3 починає перевершувати Intel MPI 2017, хоча без XPMEM він поступався Intel-реалізації.

При роботі з RoCE на мікротестах IMB застосування Intel MPI для колективних MPI-операцій демонструє значно більшу продуктивність (нижчі затримки), ніж тести OMB з використанням MVAPICH2. Однак при операціях між двома процесами значно більша пропускна здатність досягається в тестах OMB на базі MVAPICH2. В даний час актуальність цих даних знизилася, оскільки версії обох реалізацій MPI були суттєво оновлені.

Наведені дані тестів продуктивності показують, що найбільш правильним підходом є тестування продуктивності з використанням конкретної програми, необхідної користувачеві, як зазначено у доповіді на офіційному сайті Intel.

Висновки. У цій роботі проведено порівняльний аналіз сучасних ефективних та широко використовуваних реалізацій засобів паралелізації MPI у моделі розподіленої пам'яті. Дані про їх продуктивність не дозволяють зробити однозначний вибір на користь будь-якої реалізації.

Оцінюючи продуктивність HPC-додатків доцільно відбирати дані для конкретних додатків, а не покладатися на "інтегральні" дані SPEC MPI 2007.

Література

1. Dimakopoulos V. V. Parallel programming models // Smart Multicore Embedded Systems. Springer New York, 2014. P. 3—20.

2. Abdulbaqi J. Programming at Exascale: Challenges and Innovations. arXiv preprint arXiv:1809.10023. 2018, URL: https://arxiv.org/pdf/1809.10023.pdf.

3. The OpenMP API specification for parallel programming. URL: https://www.openmp.org.

4. MPI: A Message-Passing Interface Standard. Version 3.1. Message Passing Interface Forum. June 4, 2015. URL: https://www. mpi-forum.org/docs/mpi-3.1/mpi31-report.pdf.
5. Chai L., Noronha R., Panda D. K. MPI over uDAPL: Can High Performance and Portability Exist Across Architectures? // Sixth IEEE International Symposium on Cluster Computing and the Grid (CCGRID'06), IEEE, 2006. P. 19 - 26.
6. Libfabric Programmer's Manual. URL: http://www.libfabric.org.

References

1. Dimakopoulos V. V. Parallel programming models // Smart Multicore Embedded Systems. Springer New York, 2014. P. 3—20.
2. Abdulbaqi J. Programming at Exascale: Challenges and Innovations. arXiv preprint arXiv:1809.10023. 2018, URL: https://arxiv.org/pdf/1809.10023.pdf.
3. The OpenMP API specification for parallel programming. URL: https://www.openmp.org.
4. MPI: A Message-Passing Interface Standard. Version 3.1. Message Passing Interface Forum. June 4, 2015. URL: https://www. mpi-forum.org/docs/mpi-3.1/mpi31-report.pdf.
5. Chai L., Noronha R., Panda D. K. MPI over uDAPL: Can High Performance and Portability Exist Across Architectures? // Sixth IEEE International Symposium on Cluster Computing and the Grid (CCGRID'06), IEEE, 2006. P. 19—26.
6. Libfabric Programmer's Manual. URL: http://www.libfabric.org.

DOI: 978-966-301-266-7/1.2024.67

Коцун В.І.
https://orcid.org/0000-0003-2363-8157
e-mail: volodumur.kotsun@e-u.edu.ua

Сушинський О.Є.
https://orcid.org/0000-0002-2661-6458
e-mail: orest.sushynskyi@e-u.edu.ua

ПРОГРАМНА СИСТЕМА ДЛЯ АВТОМАТИЗАЦІЇ ЗБОРУ ДАНИХ З МЕРЕЖІ LINKEDIN

Анотація. У статті проведено проектування та розробка розширення до веббраузера Google Chrome для збору даних з профілів користувачів LinkedIn, а також його інтеграція з системою управління кандидатами.
Розширення до браузера розроблено за допомогою технології JavaScript, мови стилів CSS, мови розмітки гіпертекстових документів HTML. Функціонал програмного забезпечення стає доступним при переході на сторінку профілю користувача у мережі LinkedIn.
Для інтеграції з системою управління кандидатами, у проекті було реалізовано необхідні модулі, які поєднують розширення та систему.

Розроблений функціонал відповідає вимогам архітектури проекту, з яким здійснюється інтеграція. Для цього було використано технологію .NET, мову програмування C#, фреймворк Entity Framework Core. У ролі бази даних використано Microsoft SQL Server 2019.

Ключові слова: програмна система, веббраузер, вебскрапер, розробка програмного забезпечення, IT, LinkedIn.

Kotsun Volodymyr, Sushynkyi Orest

SOFTWARE SYSTEM FOR AUTOMATING DATA COLLECTION FROM THE LINKEDIN NETWORK

Abstract. The article discusses the design and development of a Google Chrome web browser extension for collecting data from LinkedIn user profiles and its integration with the candidate management system.

The extension was developed using JavaScript, CSS, and HTML technologies. The software functionality becomes available from the user's profile page on LinkedIn. In the project, all required modules were implemented to integrate an extension with the candidate management system.

The integrated functionality that was developed meets all the requirements for the project architecture. For this purpose, the .NET technology, the C# programming language, and the Entity Framework Core framework were utilized. Microsoft SQL Server 2019 was used as the database.

Key words: software system, web browser, web scraper, software development, IT, LinkedIn.

Постановка проблеми та її актуальність. Незалежно від того, чи ваша ціль це розпочати новий проект, чи розробити нову стратегію для вже існуючого бізнесу, завжди потрібно аналізувати величезну кількість даних. Дедалі частіше організації різних галузей звертаються до збору даних та приділяють багато уваги цьому процесу. Журнал Forbes, у свою чергу зазначає, що у 2023 році близько 2,500,000,000,000,000 байтів інформації було створено щодня. Це безумовно свідчить про те, що кожної хвилини створюється цінна інформація, використання якої у бізнес-аналітиці може приносити великий прибуток, а також зберегти чималу кількість коштів. Збір даних надзвичайно корисний з багатьох причин, зокрема для розуміння стану вашого бізнесу чи організації.

Завдяки зібраним даним про продажі, дані клієнтів, виплачені працівникам кошти та всеможливі інші дані, можна ідентифікувати як проблемні місця, так і успішні аспекти діяльності. Також варто зазначити, що сьогодні важко назвати галузі, де не використовується чи не можна було би застосувати штучний інтелект. Але для його застосування, потрібно натренувати штучний інтелект, змусити пристрій чи машину навчатися чи розуміти процес, а для цього, передусім, необхідні приклади – дані.

Проте, чималим викликом у описаних ситуаціях є збір цих даних, адже у вирі такої кількості інформації дуже легко загубитися. Раніше, люди покладалися на фокус-групи, загальні знання та навіть на те, що, на думку керівників, здавалося раціональним, чи вилучали дані вручну. Такі способи тягнули за собою доволі велику кількість проблем, як-от неструктурованість.

Саме тому, доцільно спрощувати процес вилучення даних. Використання інструменту, який збирав би дані в уніфікованій формі, дозволяє уникнути проблеми структурованості, зберігає час, дає можливість уникнути помилок, які пов’язані з людським фактором. Збір даних також відомий як вебскрапінг – процес імпортування інформації з ресурсу, до

прикладу, вебсайту у зручну для користувача форму – CRM-систему, файл, таблицю, інший вебсайт тощо.

Мережу LinkedIn вважають однією з провідних соціальних мереж, що дозволяє заводити робочі контакти та ділові зв'язки. Люди, що перебувають у пошуку роботи, розповідають про себе, свої навички, досвід, освіту та вказують, що бажають влаштуватися на роботу. У той час працедавці та спеціалісти з підбору персоналу, так звані рекрутери, здійснюють пошук потенційних кандидатів для прийому на роботу.

Збір даних з LinkedIn може принести велику користь для роботодавців. Можна створити досьє, яке міститиме потенційних клієнтів, отримати інформацію про конкурентів, автоматизувати процес підбору персоналу.

Аналіз останніх досліджень і публікацій. Скрапінг даних (data scrapping) – це підхід, при якому програмне забезпечення вилучає дані з іншої програми, які, у свою чергу представлені у зручному вигляді для читання людиною. [1]

Вебскрапінг – це одна з технік пошуку даних, що застосовує інструменти та фреймворки для витягування даних з загальнодоступних джерел.

Масове вилучення вебданих є доволі складною задачею, адже вебсайти стають дедалі складнішими та надзвичайно часто змінюються, як наслідок зібрані вебдані стають неточними або неповними.

Таким чином, парсери економлять час, який затрачається на збір великого обсягу даних та групують їх в певний вигляд. Вони можуть виконувати, наприклад, такі задачі [2]: збір асортименту та цін; аналіз технічної оптимізації; парсинг метаданих сайту.

Вебскрапери можна поділити також на такі типи:

- Спеціалізовані скрапери – такі, що спрямовані на видобування даних з конкретного вказаного вебсайту, тобто такі, які орієнтовані на певну DOM-структуру документа.
- Ресурс-агностичні типові скрапери – такі, що орієнтуються на видобування з однорідних чи, як їх ще називають, «типових» сайтів.
- Ресурс-агностичні універсальні скрапери – це скрапери, які розробляють, опираючись на алгоритми pattern matching, tree pruning [3] чи навіть computer vision[4] задля того, щоб могти поділити структуру сторінки на частини, котрі можна структурувати. Цей вид скраперів вважається найбільш трудомістким, вимагає складних алгоритмів, як ідейно, так і обчислювально.

Сьогодні, існує дуже багато як безкоштовних, так і платних [5], тож варто розглянути які аналоги [6] представлено серед вебскраперів:

1) import.io – надає можливість усім бажаючим організаціям зростати у напрямку електронної комерції, тобто сфери, що містить у собі фінансові й торгові транзакції.

2) saivi (Scrape-Annotate-Intelligence-Visualization) – комплексний продукт, що охоплює наскрізні сервіси, які пов'язані з даними: надає допомогу на шляху від пошуку джерел даних до візуалізації.

3) ParseHub – безкоштовний інструмент для вебскрапінгу. Надає можливість для користування на операційних системах Windows, Mac OS і Linux.

4) Expandi – інструмент для скрапінгу даних з LinkedIn.

5) Phantombuster – інструмент для видобування даних і автоматизації, який не потребує навичок чи знань у програмуванні. Допомагає цілим корпораціям та компаніях збирати дані про цільову аудиторію.

6) Dux-Soup – один з найпопулярніших інструментів автоматизації. Функціонує як розширення для веббраузера Google Chrome, тобто для функціонування необхідно лише встановити розширення і при відкритій вкладці LinkedIn розширення буде функціонувати у фоновому режимі.

7) webscraper.io – це інструмент, який дозволяє інтерактивно збирати дані з ресурсів. Зокрема, можна побудувати якусь власну структуру для вилучення даних, опираючись на потреби бізнесу.

Для B2B компаній хорошим джерелом даних слугує соціальна мережа LinkedIn оскільки ця платформа містить багато керівників та співробітників високого рівня, а, як відомо, саме такі люди складають цільову аудиторію майже на кожному ринку B2B.

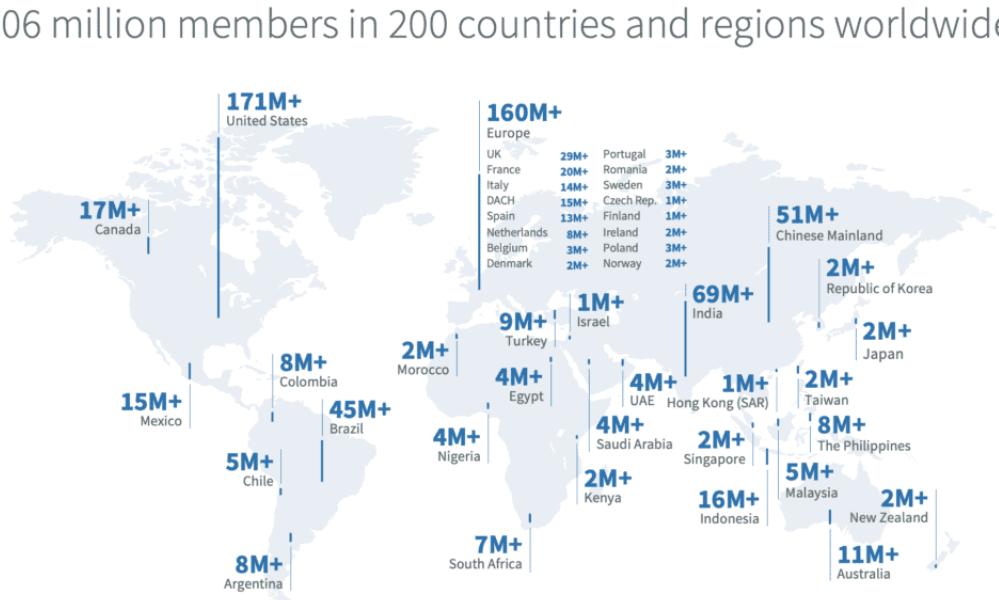


Рис.1. Користувачі, які користуються соціальною мережею LinkedIn поділені за географічною ознакою [7]

Збір даних з цієї мережі дозволяє застосовувати одержані дані для створення, скажімо, списку потенційних клієнтів з цінною інформацією, яка дозволить розробити ефективну рекламну кампанію. Крім того, зібрані дані можна використати у маркетингу, бізнес аналітиці, підборі персоналу.

Згідно з дослідженням [7] 122 мільйони людей проходили співбесіду завдяки соціальній мережі LinkedIn і, як наслідок, 35,5 мільйона було найнято людиною, з якою велося спілкування в мережі LinkedIn. Тобто, щохвилини через неї наймають 3 людини.

З погляду на сферу підбору персоналу, також досліджено [7], що 87% спеціалістів з підбору персоналу використовують LinkedIn на регулярній основі, а також, що співробітники, яких найняли за допомогою LinkedIn покидали компанії зазвичай на 40% менше, аніж ті, що були найняті на роботу іншими способами.

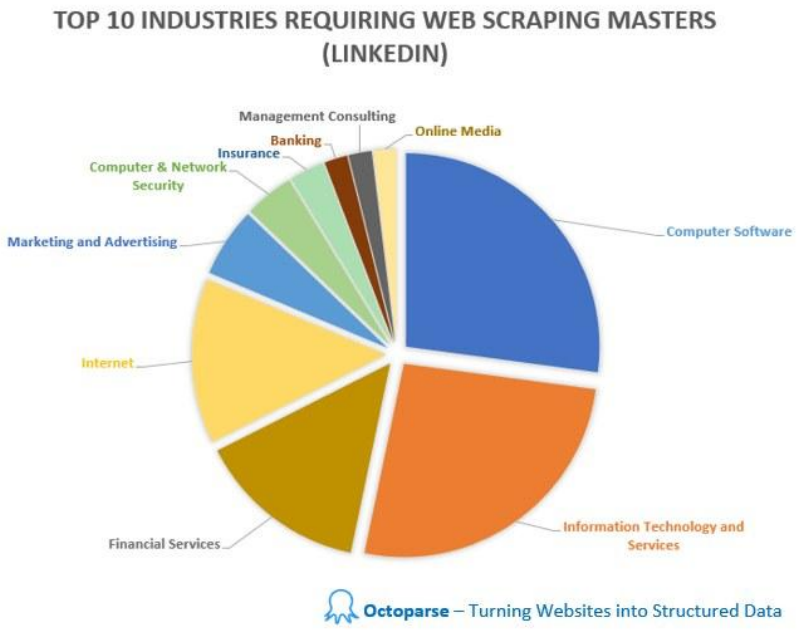


Рис.2. Кругова діаграма з відображенням часток топ-10 індустрій, для яких видобування даних з мережі LinkedIn важливе [8]

Складністю в вилученні даних є те, що дуже часто відбуваються всеможливі структурні зміни. Це стається внаслідок того, що власники вебсайтів не хочуть не відповідати новими трендам у UI/UX, прагнуть додавати новий функціонал. Скрапери написані у відповідності до елементів коду вебсторінки, тому часта зміна коду додає труднощів для програмного забезпечення. Втім, хоч не кожна структурна зміна впливає на налаштування вебскрапера, проте потенційно існує велика ймовірність того, що нові зміни

призведуть до втрати даних, саме тому рекомендовано стежити за тим чи повні дані експортують та/або чи з'явилися якісь зміни у вигляді сайту.

Формулювання мети дослідження. Метою цієї роботи є створення інструмента для автоматизації збору даних з соціальної мережі LinkedIn, який би вирішував проблему інформаційного шуму на профілі кандидата та дозволяв би вилучати корисну інформацію з профілю, який зацікавив користувача.

Виклад основного матеріалу дослідження. Для імплементації завдання було вирішено розробити вебскрапера у вигляді розширення до веббраузера Google Chrome. Таке рішення обумовлене тим, що форма розширення є простою до встановлення. Для його використання потрібен лише браузер, функціонал якого буде доповнено. Воно працює у фоновому режимі та автоматично вмикається, коли користувач відкриває сторінку соціальної мережі LinkedIn. Це зручно, доступно, зрозуміло особливо для не досвідчених технічно користувачів, також це рішення є кросплатформним. Звичайно, у такого рішення також будуть недоліки, зокрема завдяки залежності від браузерів. Таким чином періодично потрібно оновлювати розширення під оновлення браузера. На додаток слід розроблювати окрему версію розширення під кожен браузер.

Для розробки додатку, що прийматиме зібрані дані, обрано трирівневу клієнт-серверну архітектуру, яка є основою вебсайтів, оскільки ця архітектура реалізує принцип роботи мережі Інтернет. Рівнями є база даних, сервер та клієнт. Також перевагами вибору архітектури вважаємо те, що вимоги до комп'ютерів клієнтів не є високими, адже виконуються всі обчислення саме на сервері. Спілкуються між собою клієнт та сервер через запити. Сервер також здійснює доступ до бази даних, у якій зберігатимуться дані.

Для розробки розширення було використано середовище розробки WebStrom, яке є середовищем розробки для JavaScript, HTML та CSS від компанії JetBrains. Єдиним обов'язковим файлом, який повинен бути складовою кожного розширення до браузера є файл з назвою manifest.json. Це файл у форматі JSON, проте єдиний виняток це те, що в ньому дозволені коментарі з синтаксисом у стилі двох скісних рисок - "//". За допомогою цього файлу можна вказати основні метадані, які стосуються розширення, а також вказати на аспекти функціональності розширення, як-от: фонові сценарії, дії веббраузера, сценарії вмісту. Обов'язковими параметрами є:

 manifest_version – ціле число, яке відповідає версії формату маніфесту.

 name – назва розширення, до 45 символів. До назви варто підійти відповідально, адже вона відображається в магазині, при установці та на сторінці управління розширеннями (chrome://extensions). У цьому параметрі розміщено назву “LinkedIn Scraper”;

 версія - параметр з версією розширення. Підтримується до чотирьох чисел, розділених крапкою.

Серед необов’язкових, втім використаних параметрів, є також:

 description – опис, що є текстом до 132 символів. Відображається в магазині та на сторінці керування розширеннями;

 icons – список із іконок розширення;

 content_scripts – скрипти, які завантажують програму. У скрипті є код, що запускає скрипт лише на цільовій сторінці, тобто на сторінці з профілем LinkedIn. Суворо кажучи, content_scripts – теж свого роду обов'язковий параметр. Якщо його не поставити, розширення не зробить нічого корисного.

Також важливим є параметр content_scripts.matches, який відповідає за перелік цільових URL, з якими розширення співпрацює. Саме тому значеннями для цього ключа JSON-файлу є безпосередньо **www.linkedIn.com**. Для інтеграції з ATS-системою потрібно розмістити як значення до цього ключа посилання на цю систему. Отже, вміст файлу manifest.json продемонстровано на рис.3.

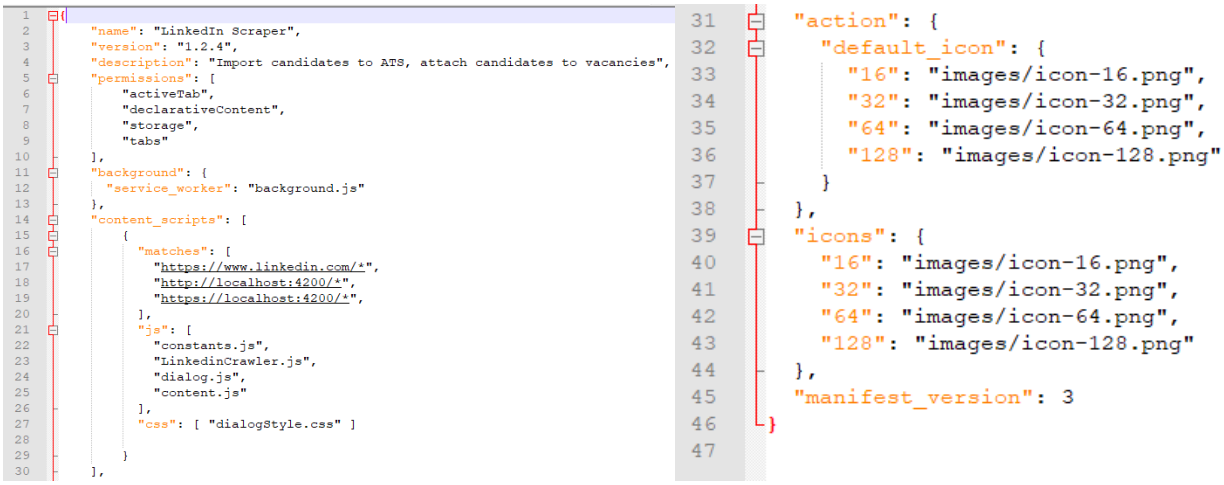


Рис.3. Наповнення конфігураційного файлу

Для реалізації вебскрапінгу створено файли LinkedinCrawler.js та content.js. ці файли містять у собі власне бізнес-логіку вебскрапера. Саме з файлу content.js починається виконання програми. Для того, аби була змога додати кандидата до системи, необхідно бути авторизованим у ATS-систему. Таким чином, при першому вході на сторінку будь-якого кандидата у LinkedIn

запропоновано увійти у систему, після чого відбувається переспрямування на сторінку ATS-системи, з якої копіюється токен авторизації, бо в ATS-системі авторизація реалізована за допомогою станарту jwt [9]. Це відбувається для того, аби, роблячи запити до сервера, додавати токен в запити, які робить розширення, адже здійснювати запити дозволено лише авторизованим користувачам.

Опісля, розширення додає в структуру сторінки кнопки, які відповідають статусу кандидата. Для цього здійснюється запит до сервера, який перевіряє чи є такий кандидат у базі. У разі негативної відповіді, тобто, якщо кандидат у базі не знайдений, тоді на сторінці є кнопка, яка дозволяє додати кандидата в систему. У випадку позитивної відповіді, тобто, якщо кандидата було знайдено у базі, то на сторінці з'являються дві кнопки, які дозволяють оновити дані чи переглянути дані в ATS-системі. Скріншоти продемонстровано на рис. 4 та рис. 5.

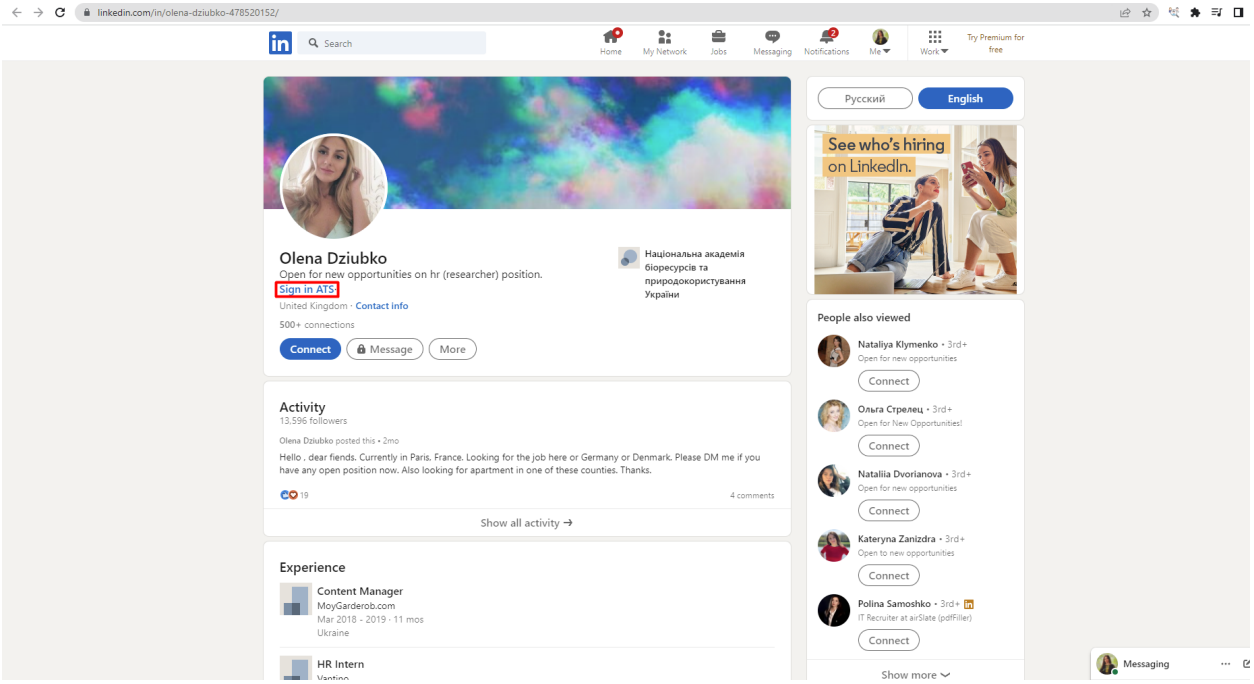


Рис.4. Кнопка для авторизації у системі

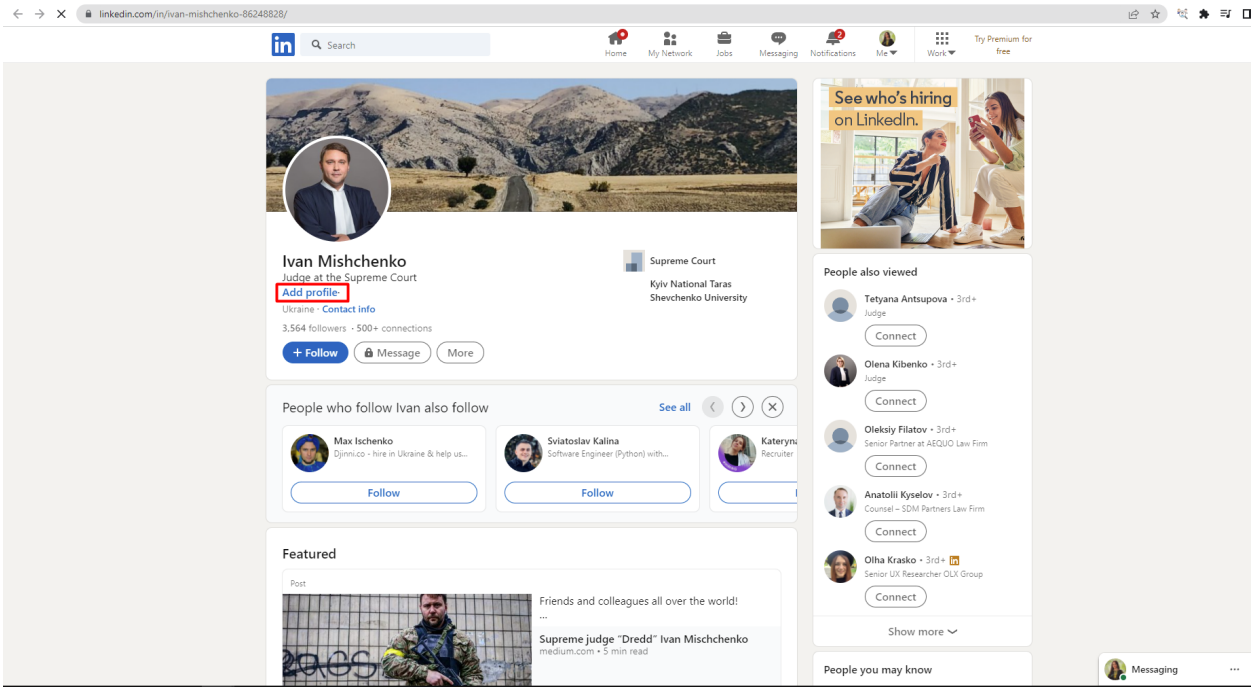


Рис.5. Кнопка для додавання профілю користувача

Для скрапінгу використано підхід маніпуляції з елементами DOM, а також застосування регулярних виразів. Для різних сутностей розроблено окрему функцію, яка формує об'єкт у json-форматі, для того, аби помістити у тіло http запиту та надіслати на сервер. Приклад витягнення інформації про кандидата та дані про нього за допомогою селекторів і регулярних виразів:

```
const data = contactInfoDialog.querySelector('div.artdeco
modal__content').innerText.split('\n').concat(['']).join('#');
return {
linkedIn: data.match(/#(linkedin.+?)#/) ?
 data.match(/#(linkedin.+?)#/)[1] : null,
email: data.match(/#Email#(.+?)#/) ?
data.match(/#Email#(.+?)#/)[1] : null,
birthday: data.match(/#Birthday#(.+?)#/) ?
data.match(/#Birthday#(.+?)#/)[1] : null,
skype: data.match(/#([a-zA-Z][a-zA-Z0-9\.,\-_]{5,31})\s+\(Skype\)#/) ?
data.match(/#([a-zA-Z][a-zA-Z0-9\.,\-_]{5,31})\s+\(Skype\)#/)[1] : null,
phoneNumber:  data.match(/#Phone#(.+?)#/)  ?  data.match(/#Phone#(.+?)#/)[1]  :  null,

};
```

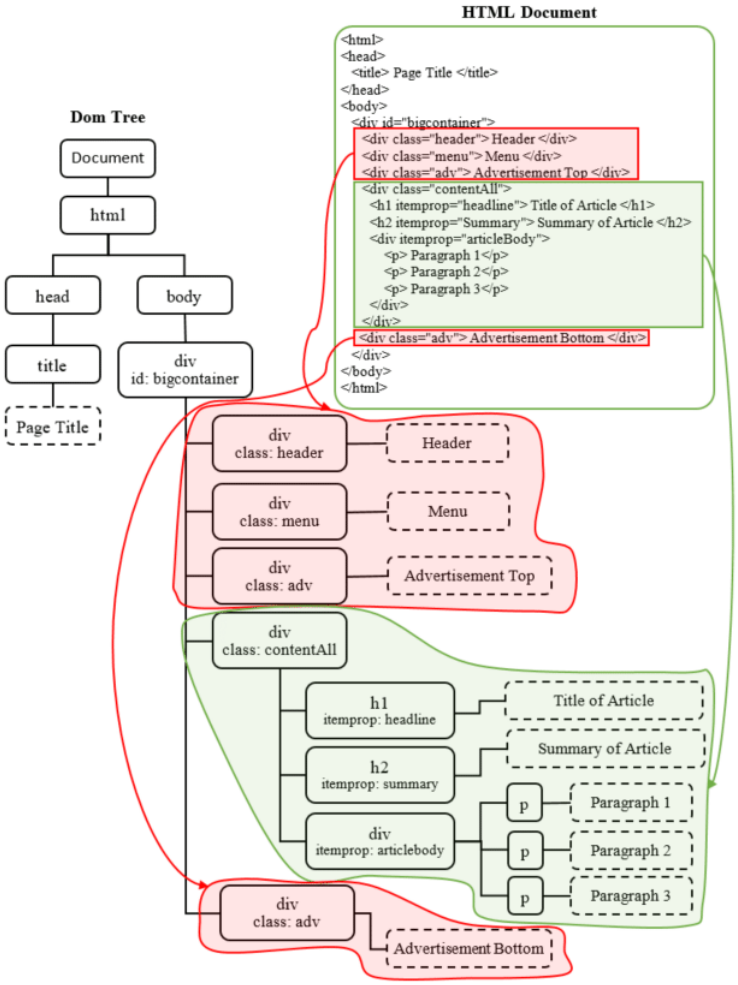


Рис.6. Візуальне представлення DOM-дерева та відповідних тегів

Також розроблено створено діалог, який дозволяє прикріпити кандидата до певної вакансії. Його створення прописано у файлі dialog.js. Діалог виконано у стилях LinkedIn, його вигляд наведено на рис.7. Для того, аби одержати перелік вакансій, здійснюється запит до сервера за адресою, яка прописана у константах, а також у діалозі відображаються етапи, на яких може перебувати кандидат, які також прописано у файлі constants.js, а ще можна додати коментар, що відобразиться у лозі дій на сторінці у ATS-системі.

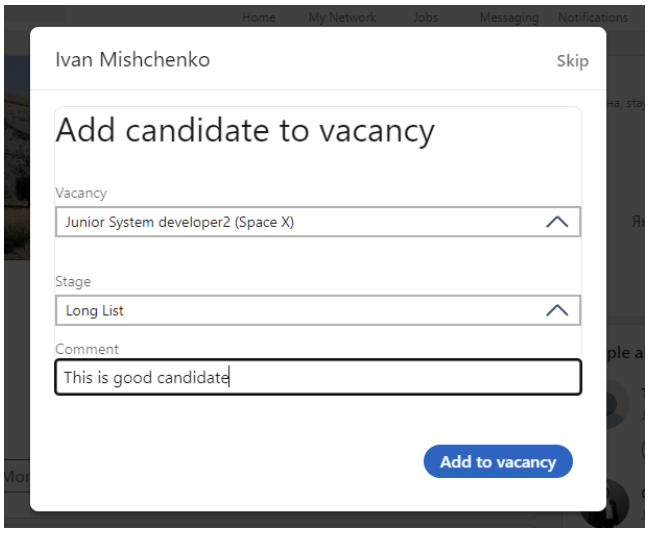


Рис.7.Діалог для прикріплення кандидата до вакансії

Після додавання, кандидата можна переглянути в ATS-системі. Окрім того, додається запис у вкладку логів з датою, коментарем та користувачем, який додав кандидата.

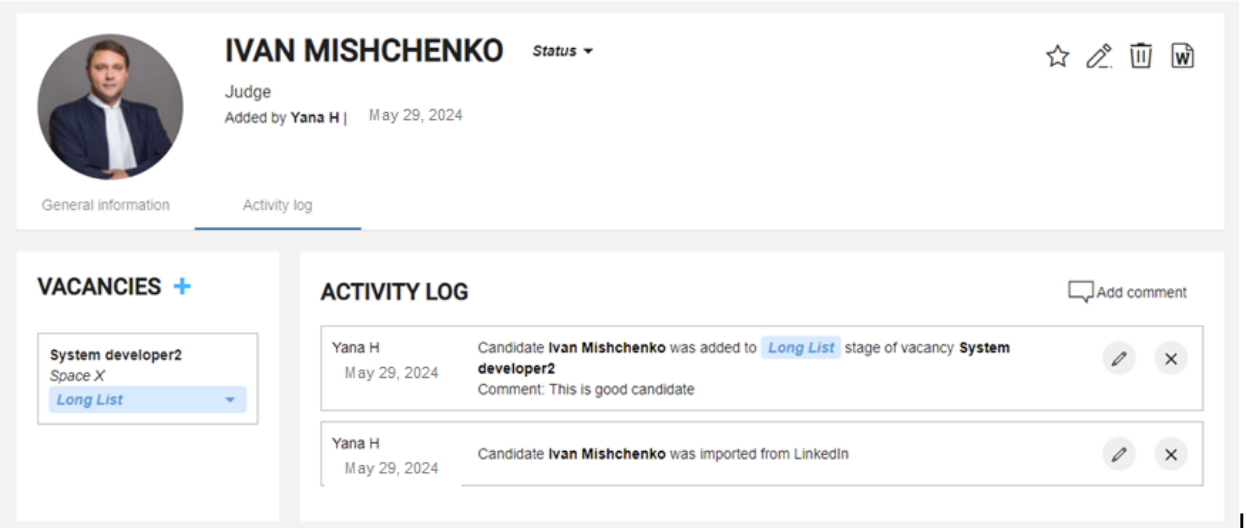


Рис.8. Завантажені дані про кандидата та записи у компоненті логування

Необхідним етапом у життєвому циклі програмного забезпечення є його тестування. Це аргументовано тим, що у розробці програмного забезпечення завжди існує людський фактор, завдяки якому існує ймовірність помилки чи збою.

Для тестування розроблених на стороні сервера функцій було застосовано такі інструменти, як Postman, що дозволяє тестувати API-виклики до певного контролера. Також застосовано Swagger - інструмент, який надає змогу описати REST API та здійснювати запити з різними параметрами.

Тестування вебскрапера проведено на різних профілях LinkedIn, з варіативним набором інформації та заповненості. Було перевірено усі функції, які надає розширення. Також, під час проведення функціональних тестів, було водночас здійснено основні нефункціональні тести, які стосувались користувацького інтерфейсу. У таблиці 1. продемонстровано розподіл тестових даних для тестових випадків. Внаслідок проведеного тестування, знайдено помилки та усунено їх.

Таблиця 1. Розподіл функціональних тестових випадків

№	Варіант використання	Тестові випадки	Тестові дані
1	Авторизація для вебскрапера	1	4
2	Додавання нового кандидата	1	3
3	Прикріплення до позиції	1	4
4	Оновлення даних про кандидата	1	2
5	Перегляд даних про кандидата	1	3
	Загалом	5	16

Висновки. Дослідивши предметну область, аналоги та популярність вебскраперів було створено інструмент для автоматизації збору даних з соціальної мережі LinkedIn, який вирішує проблему інформаційного шуму на профілі кандидата та дозволяє вилучати корисну інформацію з профілю, який зацікавив користувача. Збір даних з LinkedIn може принести велику користь для роботодавців. Це допоможе створювати досьє, яке міститиме потенційних клієнтів, отримати інформацію про конкурентів, автоматизувати процес підбору персоналу.

Література

1. What is web scraping? The Ultimate Guide [Електронний ресурс] // datadome.co. – Режим доступу: https://datadome.co/learning-center/what-is-web-scraping-guide/.
2. How Can Web Scraping Solve Business Problems? [Електронний ресурс]. – Режим доступу до ресурсу: https://www.eminenture.com/blog/how-can-web-scraping-solve-business-problems/.
3. Cording P. H. Algorithms for Web Scraping / Patrick Hagge Cording. – Kongens Lyngby : Technical University of Denmark, 2011. – 92 с.
4. A Vision Recognition Based Method for Web Data Extraction [Електронний ресурс] / Zehuan Cai [та ін.] // Advanced Science and Technology 2017, Shanghai. – [Б. м.]. – Режим

доступу: https://web.archive.org/web/20171115122146id_/http://onlinepresent.org/proceedings/vol143_2017/40.pdf.

5. Гримайло Я. Я. Застосуванння вбудованих у браузер систем для вебскрапінгу / Яна Ярославівна Гримайло // Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 67) : Міжнар. наук. інтернет-конф., Тернопіль, 11–12 трав. 2022 р. – [Б. м.]. – С. 20–23.

6. Top 10 LinkedIn scraping tools in 2022 [Електронний ресурс] // Dropcontact: B2B Email Finder and enrichment in CRM. – Режим доступу: https://www.dropcontact.com/blog/top-10-linkedin-scraping-tools-in-2022.

7. Osman M. Mind-Blowing LinkedIn Statistics and Facts [Електронний ресурс] / Maddy Osman // Kinsta. – 2022. – Режим доступу до ресурсу: https://kinsta.com/blog/linkedin-statistics/.

8. Web scraping: explaining where, why, and how [Електронний ресурс] // techvice.org. – Режим доступу: https://techvice.org/blog/popular/what-are-the-scraping-purposes-and-who-uses-it/.

9. Comparison of web scraping techniques: regular expression, HTML DOM and XPath / Rohmat Gunawan [та ін.] // Atlantis highlights in engineering (AHE), volume 2 : International Conference on Industrial Enterprise and System Engineering, Yogyakarta, 21–22 листоп. 2018 р. – [Б. м.]. – С. 283–287.

References

1. What is web scraping? The Ultimate Guide [Electronic resource] // datadome.co. – Access mode: https://datadome.co/learning-center/what-is-web-scraping-guide/.

2. How Can Web Scraping Solve Business Problems? [Electronic resource]. - Resource access mode: https://www.eminenture.com/blog/how-can-web-scraping-solve-business-problems/.

3. Cording P. H. Algorithms for Web Scraping / Patrick Hagge Cording. - Kongens Lyngby: Technical University of Denmark, 2011. - 92 p.

4. A Vision Recognition Based Method for Web Data Extraction [Electronic resource] / Zehuan Cai [et al.] // Advanced Science and Technology 2017, Shanghai. - [B. m.]. - Access mode: https://web.archive.org/web/20171115122146id_/http://onlinepresent.org/proceedings/vol143_2017/40.pdf.

5. Y. Y. Hrymailo Application of web scraping systems built into the browser / Yana Yaroslavivna Hrymailo // Information society: technological, economic and technical aspects of development (issue 67): International. of science Internet conference, Ternopil, May 11–12. 2022 - [B. m.]. – pp. 20–23.

6. Top 10 LinkedIn scraping tools in 2022 [Electronic resource] // Dropcontact: B2B Email Finder and enrichment in CRM. – Access mode: https://www.dropcontact.com/blog/top-10-linkedin-scraping-tools-in-2022.

7. Osman M. Mind-Blowing LinkedIn Statistics and Facts [Electronic resource] / Maddy Osman // Kinsta. – 2022. – Resource access mode: https://kinsta.com/blog/linkedin-statistics/.

8. Web scraping: explaining where, why, and how [Electronic resource] // techvice.org. – Mode of access: https://techvice.org/blog/popular/what-are-the-scraping-purposes-and-who-uses-it/.

9. Comparison of web scraping techniques: regular expression, HTML DOM and XPath / Rohmat Gunawan [et al.] // Atlantis highlights in engineering (AHE), volume 2 : International Conference on Industrial Enterprise and System Engineering, Yogyakarta, 21–22 November 2018 - [B. m.]. - pp. 283–287.

DOI: 978-966-301-266-7/1.2024.81

Мовчан О.В.
https://orcid.org/0009-0008-4274-9817
e-mail: olena.movchan@e-u.edu.ua

Бабінчук О.П.
https://orcid.org/0009-0000-6435-1457
e-mail: olena.babinchuk@e-u.edu.ua

МОВНА ТОЛЕРАНТНІСТЬ ЯК ОСНОВА ДІЛОВОЇ УКРАЇНСЬКОЇ МОВИ: КУЛЬТУРА СПІЛКУВАННЯ ТА КОМУНІКАТИВНІ ЗАКОНИ В ПРОФЕСІЙНОМУ СЕРЕДОВИЩІ

Анотація. У статті досліджено концепцію мовної толерантності в контексті ділової української мови та професійного спілкування. Розглянуто історія виникнення поняття толерантності в лінгвістиці, його зв'язок з антропоцентричною парадигмою та культурою мовлення. Проаналізовано різні визначення мовної толерантності, її структуру та причини недостатнього рівня в сучасному суспільстві. Особливу увагу приділено комунікативним законам та їх взаємозв'язку з мовною толерантністю. Стаття підкреслює важливість мовної толерантності як інструменту ефективного спілкування в багатокультурному середовищі та її роль у професійному успіху в умовах глобалізації.

Ключові слова: мовна толерантність, ділова українська мова, антропоцентрична парадигма, культура мовлення, комунікативні закони, професійне спілкування, лінгвістика, міжкультурна комунікація, глобалізація, ефективне спілкування.

Виклад основного матеріалу. Інтерес до проблеми толерантності в рамках лінгвістичної науки з'явився тільки на прикінці XX ст., що пов'язано, з переходом до антропоцентричної наукової парадигми, коли в центрі вивчення стає людина.

Ідея антропоцентричності мови є ключовою в сучасній лінгвістиці. З позицій цієї парадигми, людина пізнає світ через усвідомлення себе, своєї теоретичної та предметної діяльності в ньому, і це надає йому право творити в своїй свідомості антропоцентричний порядок речей, який визначає його духовну сутність, мотиви його вчинків, ієрархію цінностей.

Коріння слова «толерантність» беруть свій початок з латинської мови. Латинське слово tolerantia має значення «терпіння», «терпимість».

Толерантність в загальному плані - це прагнення і здатність до встановлення і підтримання спільності з людьми, які відрізняються в деякому відношенні від переважаючого типу або не дотримуватися загальноприйнятих думок.

Мовна толерантність - це терпимість, демонстрована в мові. Толерантність представлена в мові в усьому її розмаїтті та різноманітті лінгвістичних характеристик і проявів. Лінгвістичну толерантність людина проявляє в процесі комунікації з іншою людиною або цілою групою індивідів, які мають різні соціально-психологічні, особистісні, мовні характеристики. Люди, які беруть участь в комунікації і мають різні цінності, переконання, провідні себе по-різному, виявляють мовну толерантність ще і в зв'язку з тим, що вони можуть мати різні біологічні особливості.

Мовна толерантність – толерантність, яка проявляється у мові, у всьому різноманітті її лінгвістичних проявів. Мовна толерантність – це сукупність вербальних та невербальних засобів спілкування, які людина використовує при спілкуванні з іншою людиною, або групою людей, які так чи інакше відрізняються від нього.

Мовна толерантність звертає увагу не тільки на соціально-психологічні характеристики, такі як: переконання, цінності та поведінка, а й на його біологічні особливості : вік, стать, національність.

Незважаючи на те, що мовна толерантність не охоплює всі форми людського спілкування, не варто заперечувати той факт, що мова має вплив на процеси комунікації.

Мовна толерантність - це нормативна складова культурної компетенції. Особливе значення мовна толерантність набуває в загальному процесі глобалізації.

Мовна толерантність – це цінний інструмент для досягнення цілей спілкування, для ефективного спілкування, в якому беруть участь представники різних етносів і культур.

За спроби дати наукове визначення толерантності виникають чималі труднощі, насамперед через те, що це поняття використовується в найрізноманітніших контекстах і галузях знання — етиці, психології, політиці, теології, філософії, медицині та ін.

Так, у Сучасному тлумачному словнику української мови зазначено, що толерантність – це терпимість до чиїхось поглядів, поведінки , а в Українському радянському енциклопедичному словнику толерантність визначається як терпимість до чужих думок і вірувань .

Толерантність – терплячість щодо чужого способу життя, поведінки, звичаїв, почуттів, ідей, вірувань. Толерантність як якість, що характеризує ставлення однієї людини до іншої як до гідної особистості та виражається в

свідомому придушенні неприйняття, спричиненого всім тим, що знаменує в іншому інше (зовнішність, манера мовлення, смаків, переконань тощо), – потрактовується Новою філософською енциклопедією .

Ширше пояснення феномена толерантності подано у Філософському енциклопедичному словнику, де вказано, що толерантність – це термін, котрим позначають доброзичливе або, принаймні, стримане ставлення до індивідуальних та групових відмінностей (релігійних, етнічних, культурних, цивілізаційних). Світоглядною основою толерантності є поціновування різноманітності – природної, індивідуальної, культурної .

Отже, можемо дійти висновку, що толерантність – явище суспільне і виникає та формується в соціокультурній сфері людських взаємин, тож, і межі допустимої толерантності залежать від соціальних норм та діють у певному суспільстві.

Але в межах дійових соціальних норм можливі більш толерантні та менш толерантні варіанти особистісної та соціальної поведінки. Зокрема, окремі особи чи групи осіб можуть виступати ініціаторами перегляду таких звичаїв та норм, які вони оцінюють як жорстокі (нетолерантні) [6].

У сучасні лінгвістичній парадигмі толерантність постає багатошаровим явищем, яке репрезентується різнорівневими засобами української мови побутового та ідеологічного дискурсів: толерантність як принцип культури мови, одиниця лінгвокультурного простору та толерантність в словотворенні.

Термін «мовна толерантність» можна порівняти з такими терміним, як: «лінгвістична толерантність», «комунікативна толерантність», «вербальна толерантність» та «комунікативна толерантність».

Поняття «мовна толерантність» можна співвіднести з поняттям «лінгвістична толерантність», але лише за умови, що останнє буде трактуватися як певна модель поведінки учасників комунікативної ситуації.

Мовна толерантність та комунікативна толерантність – це синоніми. На думку дослідників мовна толерантність це активна моральна позиція, яка передбачає знання мовних і культурних особливостей, а також модифікацію своїх вербальних та невербальних сфер діяльності [4]. Поняття «мовна толерантність» є гіперонімом поняття «вербальна толерантність».

Такі дослідники як, Т.Розова та В.Барков говорять, що мовна толерантність це один з вирішальних чинників суспільства в усіх її вимірах.

О.Ю. Сухомлин вважає, що мовна толерантність має свої параметри та особливості, адже за її основу взято сукупність настанов, які передбачають функціонування толерантності в різних виявах, а саме: в професійному мовленні та в професійних текстах.

За словами дослідниці, мовна толерантність є однією з найважливіших складових культурного суспільства, адже за основу виступають базові

принципи співіснування та розвитку взаємин між різними групами суспільства, а саме: відмова від агресії, культура діалогу, поваго до іншої позиції, культура полеміки. [2]

Багато українських дослідників порівнюють визначення «мовна толерантність» з визначенням «культура мовлення». Так, наприклад, Головін М.Б. пише, що поняття культура мовлення має 2 сематничних аспекти :

1. це сукупність і система комунікативних якостей мовлення;
2. це вчення про сукупність і систему комунікативних якостей мовлення.

Тоді, як Ілляш М.В. вказує, що культура мовлення має 4 семантичних аспекти:

1. володіння літературними нормами на всіх мовних рівнях, в усній та писемній формі мовлення, уміння користуватися мовностилістичними засобами і прийомами з урахуванням умов і цілей комунікації;
2. упорядкована сукупність нормативних
3. мовленнєвих засобів, вироблених практикою людського спілкування, які оптимально виражають зміст мовлення і задовольняють умови і мету спілкування;
4. самостійна лінгвістична дисципліна. [1; ст.7]

Основними причинами недостатнього рівня мовної толерантності є :

1. Новітні технології виробили байдужість у сучасних поколінь до гуманітарних наук, зокрема до мови, у зв’язку з чим втрачається потреба в усвідомленні знання мови, а це продукує поверховість знань.
2. Відсутність навички користуватися довідковою літературою, що з часом провокує зменшення тиражу словників, довідників та ін…
3. Поширення білінгвізму спричинує у деяких мовців явища інтерференціх, звільнитися від яких можливо тільки за умови глибокого знання обох мов.

Проблема толерантності в усіх сферах людського життя існує вже досить давно, але тільки з середини минулого сторіччя ця проблема стала актуальною і привернула до себе увагу спільноти.

Толерантність освіченої людини це не лише вимушена терпимість, а й визнання іншої думки, іншого світогляду як такого, який має право на існування. А також усвідомлення власних кордонів та визнання іншої особистості та культури.

В сучасному світі проблема толерантності набувають загального значення: вони впроваджуються у сферах освіти, суспільного життя, та є найбільш дієвими засобами для досягання взаєморозуміння та поваги. Та не зважаючи на таку всебічну увагу, проблема толерантності стоїть гостро та залишається актуальною в суспільстві.

Комуніканти під час спілкування передають один одному не лише інформацію, а й емоційний стан . Та не завжди ця розмова буває позитивною. Негативні емоції та слова адресанта , так само як і позиивні безсумнівно впливають на адресата [2,7].

Як засвідчує дослідник В.Бойко, комунікативна толерантність має таку структуру:

1. Ситуативну;
2. Типологічну;
3. Професійну;
4. Загальну;

Ситуативний рівень характеризує ставлення однієї людини до іншоїу спілкуваннюі(чоловіка, колеги, дитини, дружини чи просто випадкового знайомого).

Типологічний підхід, у свою чергу, описує відношення до збірного типу чи групи людей (представників якоїсь професії, національності чи соціального стану).

Рівень професійної комунікативної толерантності проявляється під час робочого процесу та роботи з людьми, з якими мовець спілкується за рідом своєї діяльності (пацієнти, клієнти,учні).

Загальний рівень толерантності обумовлює морально-етичні засади, риси характеру та життєвий досвід [4].

За словником лінгвістичних термінів мовна толерантність передбачає сповнене поваги до мов інших етнічних груп, які проживають на території чисельно або соціально домінуючого етносу.

Культура побутового мовлення – це перше, з чим стикається людина в своєму житті. Виховується ввічливість та шанобливість передусім у сім'ї. Природно, спілкуватися з вихованою людиною легко. Така людина щира та емоційно врівноважена, а це дуже важливо для життєвого ритму.

Комунікація в суспільстві здійснюється за певними законами, які віками відпрацьовані та мають усталені форми. Спілкування людей - це доволі складний процес, який потребує взаємодії особистостей у конкретному вимірі. У лінгвістиці комунікація – аспект соціальної взаємодії, та обмін інформацією в різних сферах та процесах спілкування.

У сучасному світі спілкування виконує такі функції :

1) впливову;
2) спонукальну;
3) інформаційну;
4) координаційну;
5) емотивну ;
6) контактну ;

7) пізнавальну;
8) налагодження стосунків;

У процесі спілкування ці функції тісно переплітаються та взаємодіють і проявляються як численні комунікативні закони [3].

Комунікативні закони – загальні тенденції, які наявні у всіх типах спілкування. Ці закони реалізуються незалежно від того, хто спілкується, в якій ситуації та з якою метою. Знання законів та вміння ними користуватися – важливий складник комунікативної компетентності кожної людини.

Лінгвісти виокремлюють близько 20 комунікативних законів (Ф.Бацевич, І.Стернін)

Це, зокрема, такі закони як: правила спілкування, закон дзеркального розвитку спілкування, закон залежності ефективності спілкування від комунікативних зусиль, закон прогресивного зростання нетерпіння слухачів, закон зниження рівня інтелекту аудиторії зі збільшенням її чисельності, закон комунікативного самозбереження, закон ритму спілкування, закон мовленнєвого самовпливу, закон довіри до зрозумілих висловлювань, закон протягування критики, закон самовиникнення інформації, закон модифікації нестандартної комунікативної поведінки учасників спілкування закон прискореного поширення негативної інформації, закон спотворення інформації, закон мовленнєвого посилення емоцій, закон мовленнєвого поглинання емоцій, закон емоційного пригнічування логіки.

Надзвичайно продуктивним і цікавим є вивчення явища мовленнєвої толерантності в контексті дії основних комунікативних законів. Аспект мовна толерантність проглядається в багатьох законах. І саме тому ми висуваємо таку гіпотезу, що лінгвісти не подають мовну толерантність як окремий закон.

Кожному мовцю, навіть не будучи лінгвістом не складно помітити дію закону дзеркального розвитку спілкування. Він полягає в тому, що співрозмовники під час спілкування мимоволі, спонтанно імітують стиль один одного.

В контексті проблематики нашого дослідження можна сказати, що якщо один мовець виявляє мовну толерантність, то є висока вірогідність того, що його співрозмовник також буде мовленнєво толерантним.

Закон ритму спілкування полягає в тому, що є порівняно стале відсоткове співвідношення між говорінням і мовчанням для кожного мовця. У кількісному вияві це приблизно 1:23. Цей закон діє в житті кожної людини чітко. Отже людина менше говорить, ніж мовчить. Співвідношення варіює залежно від багатьох чинників, насамперед професії. Наприклад учителі говорять більше за столярів. А ритм спілкування, перш за все залежить від віку та статі. Жінки відчувають більш потребу у говорінні ніж чоловіки, а люди похилого віку значно меншу потребу у спілкуванні ніж діти та молодь.

Закон модифікації нестандартної комунікативної поведінки: якщо співрозмовник порушує комунікативні норми, то інший співбесідник змушує його змінити комунікативну поведінку.

Мовна толерантність є важливим аспектом сучасної комунікації, особливо в контексті ділової української мови та професійного спілкування. Це поняття охоплює не лише терпимість до мовних особливостей співрозмовника, але й активну моральну позицію, яка передбачає знання та повагу до мовних і культурних відмінностей.

Дослідження мовної толерантності є частиною антропоцентричної парадигми в лінгвістиці, яка ставить людину в центр наукового вивчення. Мовна толерантність тісно пов'язана з культурою мовлення та є важливим компонентом ефективної комунікації, особливо в багатокультурному середовищі.

Розуміння та дотримання комунікативних законів, таких як закон дзеркального розвитку спілкування, закон ритму спілкування та закон модифікації нестандартної комунікативної поведінки, сприяє розвитку мовної толерантності. Ці закони демонструють, як толерантна поведінка одного співрозмовника може позитивно впливати на комунікативну ситуацію в цілому.

Важливо зазначити, що мовна толерантність є не лише теоретичним концептом, але й практичним інструментом для покращення міжособистісного та професійного спілкування. Вона сприяє взаєморозумінню, повазі та ефективній комунікації в різних сферах життя, включаючи ділове середовище.

Висновки. Формування та вдосконалення мовної толерантності відіграє ключову роль у розвитку культури спілкування та є невід'ємною складовою професійного успіху, особливо в умовах сучасного глобалізованого суспільства.

Література

1. Бабич Н. Д. Основи культури мовлення / Н. Д. Бабич. – Львів, 2000
2. Вергазова Л.Г. «Мовна толерантність як основа формування комунікативної концепції в умовах професійного спілкування» // Вчені записки Таврійського національного університету ім. В.І. Вернадського. Серія Філологія. Соціальні комунікації» Том 26(65). № 1 - С. 454-459
3. Е.П. Лавренчук «Культура вправної комунікації як основа формування успішної особоистості», Наукові записки Національного університету «Острозька академія», випуск 97, ст..188-193.

4. Мовна толерантність як основа комунікативної компетенції майбутнього педагога / В. Ляпунова // Збірник наукових праць Уманського державного педагогічного університету імені Павла Тичини. - 2014. - Вип. 2. - С. 204-213. - Режим доступу: http://nbuv.gov.ua/UJRN/znpudpu_2014_2_30
5. Николюк Т. В., Шкляєва Н. В. Мовна толерантність та мовна гра в сучасній політичній рекламі. Нау кові записки Націо нального університету «Острозька академія»: серія «Філологія». Острог: Вид-во НаУОА, 2020. Вип. 9(77). С. 273–275.
6. Панченко Г. О. Формування та реалізація принципу толерантності в державній мовній політиці / Г.Панченко // Теорія та практика державного управління : збірник наукових праць. – Харків : ХарРІДУ НАДУ, 2010. – Вип. 1 (28). – С. 39–42.
7. Рудик Н. М. Толерантність та ввічливість у спонтанному іншомовному мовленні / Н. М. Рудик // Наука і освіта : наук.-практ. журнал. – 2010. – № 1. – С. 61-64.

DOI: 978-966-301-266-7/1.2024.89

Пашорін В.І.
https://orcid.org/0000-0001-6165-1147
e-mail: v.pashorin@e-u.edu.ua

Кравчук П.Ю.
https://orcid.org/0000-0003-4246-974X
e-mail: petro.kravchuk@e-u.edu.ua

Крайчак Є.В.
https://orcid.org/0000-0001-7759-9734
e-mail: yevhenii.kraichak@e-u.edu.ua

ЗАСТОСУВАННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ЗАХИСТУ КОМПЮТЕРНИХ МЕРЕЖ

Анотація. Збільшення числа комп'ютерних інцидентів, пов'язаних з зовнішнім втручанням в роботу систем, спонукало до розробки систем своєчасного виявлення такого втручання. Сьогодні такі системи стали необхідним компонентом інфраструктури безпеки організацій, де виявлення і попередження атак є складовою повсякденної роботи фахівців з кібербезпеки. Дана стаття присвячена дослідженню технологій виявлення комп'ютерних атак, огляду систем виявлення вторгнень, методів аналізу виявлених атак, систем запобігання вторгнень. Авторами наведено і проаналізовано класифікацію, компоненти і архітектуру систем IDS. Запропоновано підходи до захисту комп'ютерної мережі на базі систем виявлення вторгнень.

Ключові слова: комп'ютерні мережі, системи виявлення вторгнень (IDS), захист мереж.

Виклад основного матеріалу. З огляду на постійне збільшення числа комп'ютерних атак, пов'язаних із зовнішнім втручанням в роботу систем, виникає необхідність у розробці та вдосконаленні систем та методів своєчасного виявлення різного роду інцидентів та втручань у комп'ютерну мережу. На сьогодні наявність таких систем важко переоцінити, вони стали невід'ємним компонентом інфраструктури безпеки більшості організацій. Файєрвол може успішно захистити внутрішню мережу від різноманітних атак за умови, що його фільтри правильно налаштовані. Однак, навіть правильні фільтри конфігуруються статично, так що для ефективного захисту потрібно заздалегідь передбачати всі можливі атаки, а це, в принципі, неможливо. Будь-який новий тип атаки має всі шанси «просочитися» через фаєрвол і досягти

внутрішніх серверів мережі, що захищається. Виявити сліди атак, які змогли подолати бар'єр фаєрволу, можна шляхом моніторингу мережевого трафіку і моніторингу подій, що відбуваються в комп'ютерній системі або мережі з метою пошуку серед цих подій ознак можливих атак. Інакше кажучи, виявлення атак - це процес реагування на підозрілу діяльність, спрямовану на обчислювальні або мережеві ресурси. Моніторинг трафіку виконується за допомогою програм-аналізаторів мережевих протоколів, а також маршрутизаторів, що підтримують протокол NetFlow, а моніторинг подій за допомогою систем виявлення вторгнень IDS (Intrusion Detection System).

Аналізатори протоколів, або мережеві сніфери, дозволяють захоплювати трафік локальних мереж та представляти його у зручному для аналізу вигляді [1].

Система NetFlow збирає статистику про трафік у мережі, але не про кожен пакет, а про потік пакетів (послідовність пакетів, що належать одному й тому з'єднанню між певними програмами двох певних комп'ютерів, наприклад Skype-сеанс між двома користувачами, передача файлу з сервера на клієнтський комп'ютер, читання даних з сервера браузером клієнтського комп'ютера), звідси і назву протоколу (net — мережа, flow — потік) і передає її для аналізу програмним системам NetFlow, які автоматизують пошук атак та загроз. NetFlow збирає різноманітну статистику про потік, таку як час початку та закінчення потоку, обсяг даних, переданих з початку потоку, середня швидкість передачі даних, ну і, природно, всі параметри, що визначають потік, тобто адреси, порти і т. д. Важливо підкреслити, що на відміну від аналізаторів трафіку і систем виявлення атак, NetFlow збирає так звані метадані про трафік, не заглядаючи в поля даних пакетів. Часто статистику NetFlow порівнюють із телефонним рахунком, який показує, з ким і скільки розмовляв цей абонент, але не розкриває, про що він говорив. Однак, знання метаданих часто буває достатньо для того, щоб розпізнати атаку. Для цього застосовується загальний принцип моніторингу мережі — порівняння її поточної поведінки з «нормальною», тобто такою, що стійко повторювалась у минулому і ми знаємо, що при цьому атак у мережі не спостерігалося. Атака зазвичай генерує не зовсім звичайний зразок трафіку і існують рекомендації для розпізнавання таких аномалій. Перелічимо основні з них.

□ Виявлення вузлів із незвичайно великою кількістю запитів на з'єднання. Якщо який-небудь вузол раптом увійшов до найбільш активних щодо встановлення сеансів, це має викликати підозри. Така активність характерна для DoS/DDoS-атак, вузлів, заражених хробаками, сканування портів та деяких інших видів зловмисної діяльності. Так, комп'ютер, заражений черв'яком, зазвичай намагається заразити таким кодом якнайбільше інших комп'ютерів і тому намагається з ними з'єднатися. Спам-хост намагатиметься

надіслати якнайбільше листів і тому встановлювати велику кількість з'єднань в одиницю часу з портом 25 (SMTP-порт, на який надсилається пошта).

□ Виявлення вузлів з надзвичайно інтенсивним трафіком. У цьому випадку хост, який зазвичай не входив до найактивніших, починає посилати або отримувати незвичайно велику кількість даних в одиницю часу, тобто генерувати занадто інтенсивний трафік. Це також може бути DoS-атака або активність хробака, який намагається заразити інші хости.

□ Аналіз SYN та інших прапорів заголовка TCP. Наявність незвичайно великої кількості пакетів із встановленим прапором SYN або іншими прапорами заголовка TCP може свідчити про DoS-атаку. Програмні системи аналізу даних NetFlow автоматизують процедури виявлення аномальної активності в мережі, перевіряючи потоки на відповідність численним зразкам різноманітних атак, насамперед атак відмови в обслуговуванні та скануванні мережі та портів. Дані, віднесені системою до підозрілої активності, виділяються в особливу групу та надаються адміністратору мережі.

Розглянемо процес виявлення несанкціонованого доступу чи спроби несанкціонованого доступу до ресурсів. Саме собою виявлення вторгнень не запобіжить доступу до ресурсів. Тим не менш, це метод, який можна використовувати для виявлення злочинної діяльності, надання допомоги у збиранні доказів і, можливо, найголовніше, індикація атак, що відбуваються. Сьогоднішня IDS – це набагато більше, ніж просто виявлення вторгнення. Більшість IDSS матимуть змогу виконувати одну або декілька з таких дій:

• розпізнавання шаблонів, пов'язаних із відомими атаками;
• статистичний аналіз аномальних схем руху;
• оцінка та перевірка цілісності певних файлів;
• моніторинг та аналіз активності користувачів та системи;
• аналіз мережевого трафіку;
• аналіз журналу подій.

Система виявлення вторгнень - це програмний або апаратний засіб, який виконує безперервне спостереження за мережним трафіком та діяльністю суб'єктів системи з метою попередження, виявлення та протоколювання атак.

На відміну від фаєрволів, які будують захист мережі виключно на основі аналізу мережевого трафіку системи виявлення вторгнень враховують у своїй роботі різні підозрілі події, що відбуваються в системі.

Існують ситуації, коли мережевий екран виявляється проникним для зловмисника: наприклад, коли атака йде через тунель VPN зі зламаної мережі, або коли ініціатором атаки є користувач внутрішньої мережі, тощо. І справа тут не в поганій конфігурації міжмережевого екрану, а в самому принципі його роботи. Файєрвол конфігурується на блокування трафіку з заздалегідь передбачуваними ознаками, наприклад за IP-адресами або протоколами. Так

що факт злому зовнішньої мережі, з якою у нього був встановлений захищений канал і яка раніше поводилася цілком коректною, у правилах екрану відобразити не можна. Так само, як і несподівану спробу легального внутрішнього користувача копіювати файл із паролями або підвищити рівень своїх привілеїв. Подібні підозрілі дії може виявити лише система, яка стежить не лише за трафіком, а й за всіма зверненнями до важливих ресурсів окремих комп'ютерів, а також ма інформацію про перелік підозрілих дій (сигнатур атак) користувачів.

Іншою важливою відмінністю IDS від фаєрволів є те, що в обов'язки IDS не входить блокування підозрілого трафіку. IDS тільки намагається виявити підозрілу активність та підняти тривогу. Крім цього IDS протоколює підозрілі пакети, поміщаючи їх в журнал.

IDS вміють виявляти різні види мережевих атак, виявляти спроби несанкціонованого доступу або підвищення привілеїв, появу шкідливого ПЗ, відстежувати відкриття нового порту і так далі. IDS перевіряє не тільки параметри сесії (IP адресу, номер порту і стан зв'язку), а і зміст пакетів аж до прикладного рівня, аналізуючи дані, що передаються.

Ефективність таких системи багато в чому залежить від застосовуваних методів аналізу отриманої інформації. У перших системах виявлення атак, використовувалися статистичні методи виявлення атак. В даний час до статистичного аналізу додався ряд нових методів, починаючи з експертних методів і закінчуючи використанням нейронних мереж.

Статистичний метод. Основні переваги статистичного підходу - використання вже розробленого і зарекомендованого апарату математичної статистики і адаптації до поведінки суб’єкта. Спочатку для всіх суб'єктів аналізованої системи визначаються еталонні профілі стану або поведінки. Будь-яке відхилення реального профілю від еталонного визнається як несанкціонована діяльність в системі.

Однак, статистичні методи не чутливі до порядку проходження подій; в деяких випадках одні й ті ж події в залежності від порядку їх слідування можуть характеризувати аномальну або нормальну діяльність. Слід також враховувати, що статистичні методи не можуть застосовуватися в тих випадках, коли відсутній шаблон типової поведінки (еталонний профіль).

Експертні методи складаються з набору правил перевірки вхідної інформації, які формуються для системи людиною - експертом. Ці правила можуть бути записані, наприклад, у вигляді послідовності дій в системі, або у вигляді послідовність біт даних в мережевому трафіку (сигнатури). При виконанні будь-якого з цих правил приймається рішення про наявність несанкціонованої діяльності. Важливою перевагою такого підходу є практично повна відсутність помилкової тривоги. Основним недоліком є

неможливість виявлення невідомих атак. При цьому навіть невелика зміна послідовності дій для вже відомої атаки може стати серйозною перешкодою для функціонування системи виявлення атак.

Нейронні мережі. В цьому методі передбачено, що спочатку нейромережу, яка є складовою системи виявлення атак, навчають правильної ідентифікації атак на попередньо підібраній вибірці прикладів атак. Після навчання мережа запускається в режимі розпізнавання і самостійно проводить аналіз вхідної інформації та перевіряє чи узгоджуються отримані дані з характеристиками атак, які вона навчена розпізнавати. У ситуації, коли у вхідному потоці не вдається розпізнати нормальну поведінку, фіксується факт атаки.

Джерелом інформації для IDS систем можуть бути: мережевий трафік; журнали реєстрації подій в системі; дії суб'єктів (здебільш виконуваних процесів) системи. Механізми реагування на можливе вторгнення можуть бути досить різноманітними, наприклад, сповіщення адміністратора безпеки (подача звукового сигналу, передача повідомлення на консоль управління, відправки SMS-повідомлення на мобільний телефон і т.ін.), розрив з'єднання, виклик зовнішньої програми, блокування (від блокування конкретної IP-адреси до блокування окремих видів діяльності), переналаштування системи та ін.

IDS - це тільки частина інфраструктури захисту мережі і, як і всі інші компоненти, сама по собі вона не забезпечує абсолютного захисту. Цікавим є порівняння, якщо МЕ - це «броньовані двері» на вході до ІТС, то IDS - це сигналізація, що спрацьовує при спробі зламати ці двері.

Класифікація IDS може бути виконана:

- за способом реагування;
- за способом виявлення атаки;
- за способом збору інформації про атаку.

Класифікація IDS за способом реагування розрізняють пасивні та активні IDS. Пасивні IDS просто фіксують факт атаки, записують дані в файл журналу і видають попередження. Активні IDS намагаються протидіяти атаці, наприклад, шляхом реконфігурації МЕ або генерації списків доступу маршрутизатора [2].

Класифікація IDS за технологією виявлення атак. Існує два підходи до аналізу подій, які можна вважати як можливу атаку: виявлення зловживань (misuse detection) і виявлення аномалій (anomaly detection).

У *технології виявлення зловживань* передбачається, що апріорі відомо, яка послідовність біт даних в мережевому трафіку є ознакою атаки, тому аналіз подій тут полягає у пошуку таких "небажаних" послідовностей біт - сигнатур. Дана технологія виявлення атак дуже схожа на технологію виявлення вірусів.

Сигнатури атак також зберігаються в БД, аналогічної тій, яка використовується в антивірусних системах. При цьому IDS може виявити всі відомі атаки, для яких в базі даних вже є інформація про їх характерну послідовність біт. Однак системи даного типу не можуть виявляти нові, ще невідомі види атак.

У *технології виявлення аномалій* визначають ненормальну (незвичайну) активність на хості або в мережі, що і дозволяє зробити висновок про ймовірний інцидент. Детектори аномалій тут створюють профілі нормальної активності, за результатами зібраних даних у період тестового нормального функціонування і потім аналізують діяльність системи і фіксують відхилення від нормальної діяльності. Прикладом аномального поведінки може служити велике число з'єднань за короткий проміжок часу, високе завантаження центрального процесора і т. п. При такій технології є можливість виявити нові атаки. Однак аномальна поведінка не завжди є атакою. Наприклад, одночасну посилку великого числа запитів від адміністратора мережі може ідентифікувати як атаку типу «відмова в обслуговуванні».

При використанні з такою технологією можливі два випадки:

• виявлення аномального поведінки, яке не є атакою, і віднесення його до класу атак;

• пропуск атаки, яка не підпадає під визначення аномального поведінки.

Найбільш популярна *класифікація за способом збору інформації про атаку*, тобто в залежності від того де здійснюється збір інформації: в мережі, на конкретному комп'ютері чи на певних додатках, що працюють на комп'ютері. Існує два основних види IDS: рівня мережі (network-based), які аналізують мережевий трафік, і рівня хоста (host-based), які аналізують дії суб'єктів і журнали подій в рамках однієї комп'ютерної системи. Останнім часом виникла необхідність моніторингу безпеки навіть на рівні окремих додатків, що встановлені на комп'ютері і тому, як вид, окремо виділяють IDS рівня додатків (application-based) .

IDS рівня мережі (NIDS - network-based IDS) працює як сніффер, «прослуховуючи» увесь трафік в мережі завдяки тому, що мережева карта комп'ютера з IDS працює в режимі прослуховування (promiscuous mode). Захоплюючи й аналізуючи мережні пакети, IDS виявляє в них певні аномалії, що можуть свідчити про можливу атаку (різке збільшення мережевого трафіку, поява нового мережевого трафіку, спроби віддаленої авторизації, поява нових процесів, спроби авторизації з неіснуючим ім'ям користувача, підключення в неробочий час, підвищене використання системних ресурсів), або певні послідовності бітів, які відповідають сигнатурам відомих атак, що зберігаються в базі даних. Розгортання IDS рівня мережі не впливає сильно на продуктивність мережі (використовує копії пакетів), але при підвищеному

навантаженні IDS може не встигати обробляти всі пакети і може пропустити атаку, не виявивши її. IDS рівня мережі не можуть аналізувати зашифровану інформацію і більшість з них не здатні зробити висновок про те, чи була атака успішною; вони можуть тільки визначити, що атака була розпочата і адміністратор повинен вручну досліджувати, чи відбулося реальне проникнення.

IDS рівня хоста (HIDS - host-based IDS) призначена для моніторингу, детектування і реагування на дії зловмисників на певному хості і може бути встановлена на окремі робочі станції і сервери для виявлення небажаних або аномальних дій. HIDS використовують в якості інформаційних джерел журнали реєстрації подій, що створюються ОС та прикладними програмами на конкретному вузлу мережі (поява нових файлів, поява нових директорій, зміни прав доступу, зміни файлів, зміни атрибутів...) і тому можуть виявити атаки, які не можуть виявити IDS рівня мережі, наприклад, коли трафік шифрований.

Аналізатори журналів подій за своєю природою є реактивними системами, тобто вони реагують на подію вже після того, як вона відбулась. Таким чином, журнал міститиме відомості про те, що проникнення в систему виконане.

IDS рівня вузла використовують обчислювальні ресурси хостів, за якими вони спостерігають, що впливає на ефективність роботи цих вузлів, тому системи HIDS встановлюються тільки на критичні сервери, а не на кожен комп'ютер в мереж. HIDS не розуміє і не відстежує мережевий трафік, а NIDS не контролює дії всередині системи. Кожен з цих засобів має свої завдання і виконує їх своїми способами.

IDS на основі сигнатур. Знання про окремі атаки накопичуються виробниками IDS і зберігаються у вигляді послідовності біт, характерної для атаки, яку називають сигнатурою атаки. Як тільки виявляється новий вид атаки, виробник сигнатурного IDS створює відповідну сигнатуру, яка в подальшому використовується при перевірці мережевого трафіку для виявлення такої ж атаки. Сигнатурні IDS є найбільш популярними в наш час і працюють подібно до антивірусного програмного забезпечення, тому і їх ефективність також залежить від регулярності оновлення баз сигнатур, як і в антивірусному програмному забезпеченні. Цей тип IDS практично не захищає від нових атак, так як він не може їх розпізнати до появи їх сигнатур.

IDS на основі стану. Кожна зміна в роботі системи (вхід користувача, запуск програми, взаємодія додатків, введення даних і т.д .) призводить до зміни стану системи. При проведенні атак також відбуваються відповідні зміни станів (віддалений користувач підключається до системи, завантажуються данні, виконується код і т. д.). IDS на основі стану

відслідковує послідовність переходів стану і якщо ця послідовність буде не за встановленими правилами, то це свідчить про можливу атаку (наприклад багаторазова спроба ввести пароль до аккаунту, спроба отримання файлу по протоколу ftp, спроба підключення до закритого в даний момент порту...).

IDS на основі статистичних аномалій. Також називаються поведінковими або евристичними. Ці IDS на початку створюють профіль «нормальної» діяльності системи, коли відомо, що атак в мережі не спостерігалося і після цього весь наступний трафік і діяльність системи порівнюються з цим профілем. Наприклад, для каждого клиента, сервера, протокола, дня недели, времени суток измеряются минимальные, максимальные и средние значения параметров PPS (пакетов в секунду). Цей тип IDS здійснює контроль шаблонів атак в контексті потоку дій, а не просто дивиться окремі пакети. Краще підходить для виявлення DDoS атак. Перевагою IDS на основі статистичних аномалій є їх можливість реагувати на нові типи атак. Недоліком - величезна кількість помилкових спрацювань, що пов’язано з постійними змінами в работі мережі. Одним із нововведень для евристичних IDS є використання технології NetFlow.

Сигнатурна IDS повідомляє тип виявленої атаки, IDS на основі правил повідомляє, яке правило було порушено, а IDS на основі статистичних аномалій просто повідомляють про те, що сталося щось «ненормальне», що не відповідає профілю. Сучасні системи використовують кілька технологій одночасно.

Оскільки засоби IDS не здатні зупинити нелегальний доступ до активів компанії, а лише виявляють такі факти і відправляють повідомлення адміністратору, у компаній виникла потреба в нових продуктах і технологіях, що дозволяють вирішити цю проблему. В результаті з'явилися системи запобігання вторгнень (IPS - intrusion prevention system), метою яких є не тільки виявлення несанкціонованої діяльності, але і запобігання доступу зловмисника до ІТС. Системи IPS можна розглядати як розширення систем виявлення вторгнень, так як завдання відстеження атак залишається однаковим. Однак, вони відрізняються в тому, що IPS повинна відслідковувати активність у реальному часі й швидко реалізовувати дії по запобіганню атак. Можливі міри – блокування потоків трафіку в мережі, скидання з'єднань, видача сигналів операторові.

Таким чином, IPS є превентивною і проактивною технологією, зосередженою в першу чергу на запобігання атак, на відміну від IDS, що є детективною технологією, яка застосовується до вже здійснених фактів.

Як і в світі IDS, існують засоби IPS рівня хоста (HIPS) і рівня мережі (NIPS). Більшість мережевих IPS є лінійними (inline) пристроями, що

включаються «в розрив» мережі і пропускають через себе і контролюють весь трафік.

Як правило, такі NIPS мають два мережевих інтерфейси - зовнішній і внутрішній. Трафік приходить на зовнішній інтерфейс, аналізується і, в разі визнання пакетів безпечними, вони направляються на внутрішній інтерфейс. Якщо пакети визнаються шкідливими, вони відбраковуються. Однак, це може привести до появи «вузького місця» (пляшкового горлечка) і знизити продуктивність мережі IPS для бездротових мереж (Wireless Intrusion Prevention Systems, WIPS): перевіряє активність у бездротових мережах. Зокрема, виявляє невірно зконфігуровані точки бездротового доступу до мережі, атаки людина посередині, спуфінг MAC-адреса.

Серед активних дій запобігання вторгнень слід виділити:

- *переривання з'єднань, сеансів або процесів*. Якщо процес використовує занадто багато системних ресурсів, найкраще завершити його. Якщо користувач намагається використовувати конкретну вразливість або здійснити нелегальний доступ до файлів, то рекомендується закрити сеанс цього користувача. Якщо зловмисник використовує мережеве з'єднання в спробах вивчення вразливостей

системи, то варто закрити з'єднання;

- *переналаштування мережі*. Якщо відбувається кілька спроб доступу до комп'ютерів організації з конкретної IP-адреси, отже, є ймовірність того, що з цієї IP-адреси здійснена спроба атаки на інформаційну систему. У цьому випадку може знадобитися переналаштовування міжмережевого екрана або маршрутизатора. Зміна налаштувань може бути тимчасовою або постійною, залежно від IP-адреси й запрограмованих логічних дій. Нові правила можуть заборонити установку будь-яких з'єднань із віддаленим вузлом або заборонити з'єднання лише по конкретних портах.

- *обманні дії.* Найбільш складним типом активної обробки подій є обманні дії. Відповідь обманом спрямована на введення зловмисника в оману за допомогою створення враження успішного й невиявленого проведення атаки. У той же час система-ціль захищається від атаки зловмисника або за допомогою його перенаправлення на іншу систему, або за допомогою переміщення життєво важливих компонентів системи в безпечне місце. Одним з типів обманних дій є Honeypot "горщик з медом". Під "горщиком з медом" маються на увазі об'єкти системи, які ззовні сприймаються як повноцінні машини з встановленими на них операційними системами, а відтак піддаються скануванню і виглядають для зловмисника настільки привабливими, що він не може їх пропустити (приманка). Такий комп'ютер повинен залучити зловмисника більше, ніж реальні системи в мережі. Хост-приманка не містить ніякої реальної інформації компанії, і немає ніяких

ризиків в разі його успішного злому. Грамотно налаштований Honeypot практично неможливо розпізнати.

У той же час за атакуючим ведеться спостереження, і всі його дії фіксуються, з метою вивчення стратегії та методів сканування та визначення переліку засобів, необхідних для запобігання майбутнім атакам. Чим більше часу хакер залишається на цьому комп'ютері, тим більше інформації можна отримати про його методи.

Honeypot поставляються у вигляді програмних продуктів і окремих апаратних рішень (наприклад, Specter). Втім, Honeypot нескладно створити і самому, використавши для цього старий комп'ютер (або віртуальний комп'ютер). Зазвичай, на нього поміщається максимальне число вразливих додатків і зовні привабливих ресурсів - і одночасно там же стоїть система виявлення вторгнень, яка фіксує всі дії хакерів. Для атакуючих з Інтернету, зазвичай, такі приманки поміщаються в DMZ, а у внутрішній мережі роль Honeypots, як правило, грають каталоги з привабливими назвами і налаштованим аудитом на файлових серверах.

При запобіганні вторгненням головним механізмом обробки більше не являється повідомлення системи, мережі і системних адміністраторів. Тепер «ядром» системи є блокування спроби виконання дії. Коли IDS блокує атаку, вона запобігає виконанню дії, будь то системний виклик, операція додатка або мережеве з’єднання. Це блокування запобігає атаці. Очевидно, при цьому мається на увазі коректна ідентифікація системою IDS дії як атаки. Якщо дія, спроба якої була здійснена, насправді не була атакою, а IDS заблокувала його, то, можливо, IDS заблокувала законну дію, що виконується в інформаційному середовищі. Внаслідок цього IDS може викликати відмову в обслуговуванні. Якщо дія, що викликала проблему, була деякою аномалією (наприклад, пакет з помилками), то повторна передача пакету або повторна установка з’єднання, як правило, здійснюються успішно. Проте, якщо IDS некоректно ідентифікує легітимні дії або трафік, приймаючи їх за атаки, то, швидше за все, відмова в обслуговуванні відбуватиметься і надалі.

Висновки. Сучасні виклики, пов’язані із зростанням зовнішніх втручань та збільшенням числа комп’ютерних інцидентів, спонукають до створення систем та пошуку оптимальних методів своєчасного виявлення атак та захисту комп’ютерних мереж. Шляхом моніторингу мережевого трафіку і моніторингу подій, що відбуваються в комп'ютерній системі або мережі можна виявити сліди атак. Взагалі, реагування на підозрілу діяльність, спрямовану на обчислювальні або мережеві ресурси дає можливість виявлення атак. Моніторинг трафіку відбувається за допомогою програм-аналізаторів мережевих протоколів, а також маршрутизаторів, а моніторинг подій - за

допомогою систем виявлення вторгнень IDS. Окрім статистичного аналізу наведено більш нові методи виявлення атак, від експертних до використання нейронних мереж. Також надано класифікацію, проведено огляд компонент і аналіз архітектури систем IDS. У статті розглянуто різні типи і тактики хакерських атак та запропоновано відповідні технології протидії та захисту комп'ютерних систем і мереж. Оскільки засоби IDS лише виявляють, а не запобігають нелегальному доступу до активів компанії, виникла нагальна потреба в нових продуктах і технологіях. Авторами представлені не тільки методи і засоби виявлення несанкціонованої діяльності, але і запобігання доступу зловмисника до ІТС з використанням систем запобігання вторгненням (IPS). Проведене дослідження технологій виявлення комп'ютерних атак та методів їх аналізу із врахуванням архітектури систем IDS дозволило авторам запропонувати підходи до захисту комп'ютерної мережі на базі систем виявлення вторгнень.

Література:

1. Горбенко, І., Семенко, Є., & Замула, О. (2020). Methods and means of synthesis and generation of signals – physical carriers of data in modern information and communication systems. Radiotekhnika, 3(202), 87–98.DOI: https://doi.org/10.30837/rt.2020.3.202.09

2. Горбенко І. Д., Замула О. А., Хо Чі Ли Оптимізація пошуку дискретних складних сигналів з необхідними властивостями для застосування у сучасних інформаційно-комунікаційних системах // Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. праць / Інститут кібернетики імені В.М. Глушкова НАНУ. 2019. Вип. 19. 160 с.

3. Письмак Д. О., Клименко С. В., Малайчук В.П. Перешкодостійке кодування повідомлення електронного підпису // Актуальні проблеми інформаційних технологій автоматизації. Дніпро: ДНУ. - Зб. наук.праць. Том 21. 2017. С. 123-131.

4. Петренко О. М., Клименко С. В., Поляков Г. О. Клієнт-серверна система для безпечного обміну приватними повідомленнями із застосуванням криптографії з відкритим ключем// Будівництво. Матеріаловедення. Машинобудівництво. Серія: Комп'ютерні системи та інформаційні технології в освіті, науці та управлінні. Зб. наук. пр. Вип. №101. Дніпро: ДВНЗ ПДАБА., 2017. С. 177-182.

DOI: 978-966-301-266-7/1.2024.100

Переверзєв А.М.
https://orcid.org/0000-0003-0778-9203
e-mail: anton.pereverzev@e-u.edu.ua

Подвиженко А.В.
https://orcid.org/0000-0003-1826-7566
e-mail: artem.podvizhenko@e-u.edu.ua

Левченко С.В.
https://orcid.org/0009-0006-8497-0515
e-mail: sergiy.levchenko@e-u.edu.ua

VPN-СЕРВІС ЯК ЗАСІБ УПРАВЛІННЯ ДОСТУПОМ ДО ХМАРИ

Постановка проблеми. З розвитком технологій та масовим переходом підприємств на використання хмарних сервісів питання безпеки стають все більш актуальними. Служба VPN (віртуальна приватна мережа) є одним з ефективних інструментів забезпечення безпеки доступу до хмари. У цій статті ми розглянемо, що таке VPN, як вона працює і чому вона є ключовим елементом системи контролю доступу до хмарних ресурсів.

Виклад основного матеріалу. VPN (Virtual Private Network) — це технологія анонімного підключення до мережі, вона створює захищене з'єднання (тунель) між користувачем і сервером, забезпечуючи приватність і конфіденційність даних. VPN використовує методи шифрування для захисту передаваних даних від стороннього втручання. Завдяки цьому користувач може безпечно підключатися до інтернету або корпоративної мережі, незалежно від місця свого перебування.

Основний принцип роботи VPN полягає в шифруванні даних, які передаються між пристроєм користувача і сервером VPN. Цей процес можна описати наступним чином:

- Ініціалізація з'єднання: Користувач підключається до VPN-сервера через спеціальне програмне забезпечення або апаратний пристрій.
- Аутентифікація: VPN-сервер перевіряє дані користувача для забезпечення авторизації.
- Шифрування даних: Усі дані, які передаються між користувачем і VPN-сервером, шифруються.
- Передача даних: Захищений тунель передає зашифровані дані до кінцевої точки (хмари або іншого ресурсу).

- Дешифрування даних: Дані розшифровуються на стороні сервера, забезпечуючи їх безпеку і цілісність.

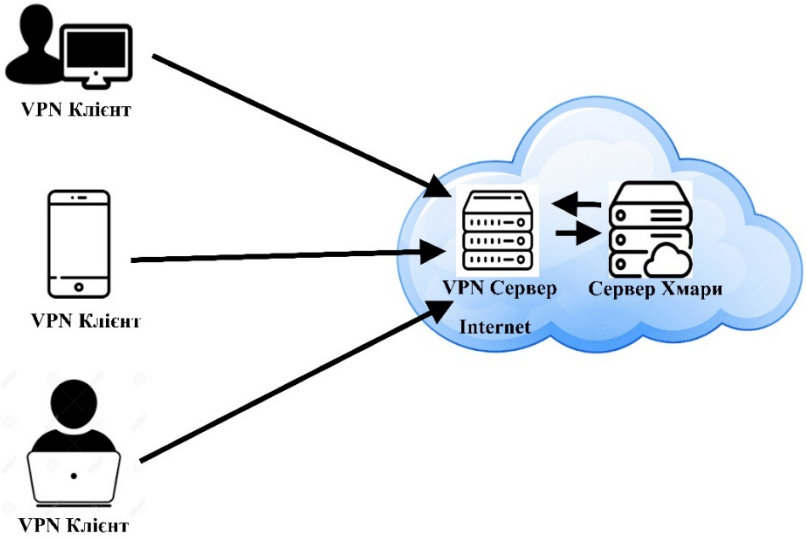


Рис. 1. Підключення до хмари за допомогою VPN

Переваги використання VPN для доступу до хмари:

1. Підвищена безпека. VPN забезпечує шифрування даних, що значно ускладнює їх перехоплення та розшифровку сторонніми особами. Це особливо важливо при передачі конфіденційної інформації або використанні незахищених мереж.

2. Приватність. Використання VPN приховує IP-адресу користувача, забезпечуючи анонімність і унеможливлюючи відстеження активності в інтернеті.

3. Доступ з будь-якого місця. Завдяки VPN співробітники можуть безпечно підключатися до корпоративних ресурсів з будь-якої точки світу, що підвищує мобільність та гнучкість роботи.

4. Захист від кіберзагроз. VPN забезпечує додатковий рівень захисту від кіберзагроз, таких як атаки типу «людина посередині» (man-in-the-middle) та інші види шкідливих дій.

Основні протоколи VPN. Існує декілька основних протоколів VPN, кожен з яких має свої переваги та недоліки. Розглянемо їх детальніше:

1. PPTP (Point-to-Point Tunneling Protocol)

PPTP є одним з найстаріших протоколів VPN і був розроблений компанією Microsoft. Він легко налаштовується та підтримується більшістю операційних систем. Однак, PPTP має відносно слабкі механізми шифрування та вразливий до атак, що робить його менш безпечним у порівнянні з сучаснішими протоколами.

2. L2TP/IPsec (Layer 2 Tunneling Protocol with IPsec)

L2TP сам по собі не забезпечує шифрування, тому зазвичай використовується в поєднанні з протоколом IPsec, який забезпечує аутентифікацію та шифрування даних. L2TP/IPsec надає високий рівень безпеки, але має дещо складнішу конфігурацію і може бути менш ефективним через використання двох протоколів одночасно.

3. O*penVPN*

OpenVPN є одним з найпопулярніших протоколів завдяки своїй гнучкості та високому рівню безпеки. Він використовує відкритий вихідний код і підтримує різні алгоритми шифрування, такі як AES. OpenVPN може працювати на будь-якому порту, що дозволяє обходити блокування та фільтрацію трафіку.

4. IKEv2/IPsec (Internet Key Exchange version 2)

IKEv2 - це протокол VPN, розроблений Microsoft та Cisco. Він забезпечує високу стабільність та безпеку з'єднання, особливо під час перемикання між мережами, наприклад, при зміні Wi-Fi на мобільну мережу. IKEv2 часто використовується разом з IPsec для забезпечення аутентифікації та шифрування даних.

5. SSTP (Secure Socket Tunneling Protocol)

SSTP був розроблений Microsoft і добре інтегрується з Windows. Він використовує SSL/TLS для шифрування даних, що забезпечує високий рівень безпеки. SSTP легко обходить більшість мережевих фільтрів, оскільки використовує порт 443, який зазвичай відкритий для HTTPS-трафіку.

Як VPN забезпечує управління доступом до хмари:

1. Аутентифікація користувачів: Використання VPN дозволяє впроваджувати багато факторну аутентифікацію (MFA), що підвищує рівень безпеки. Тільки авторизовані користувачі можуть отримати доступ до хмарних ресурсів.

2. Шифрування даних: VPN забезпечує шифрування даних, що передаються між користувачем і хмарним сервісом, що захищає від перехоплення конфіденційної інформації.

3. Обмеження доступу за IP-адресою: За допомогою VPN можна обмежувати доступ до хмарних ресурсів тільки з певних IP-адрес або діапазонів адрес. Це знижує ризик несанкціонованого доступу.

4. Моніторинг і аудит: VPN дозволяє здійснювати моніторинг і аудит дій користувачів. Це допомагає виявляти і реагувати на підозрілу активність, що може свідчити про спроби порушення безпеки.

Виклики використання VPN

Незважаючи на переваги, використання VPN також має деякі недоліки:

1. Продуктивність: Використання VPN може вплинути на швидкість передачі даних через накладні витрати на шифрування і розшифрування інформації.

2. Складність налаштування: Налаштування і управління VPN можуть вимагати високого рівня технічної експертизи, особливо для великих організацій з складною IT-інфраструктурою.

3. Витрати: Використання комерційних VPN-сервісів може бути витратним, особливо для великих підприємств.

Висновки. VPN є потужним засобом для управління доступом до хмарних систем, забезпечуючи високий рівень безпеки і конфіденційності. Використання VPN дозволяє компаніям контролювати доступ до хмарних ресурсів, забезпечуючи захист даних і підтримку політик безпеки. Однак, для ефективного використання VPN необхідно враховувати виклики, пов'язані з продуктивністю, складністю налаштування і витратами. Правильне впровадження і управління VPN технологіями може суттєво підвищити безпеку і надійність хмарних сервісів.

Література

1. What Is a Virtual Private Network (VPN)? https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
2. Henry James. IPsec Virtual Private Network Fundamentals. – Cisco Press book 2006.
3. Найкращі протоколи VPN та відмінності між типами VPN https://nordvpn.com/uk/blog/protokoly/
4. Eric F Crist. Mastering OpenVPN 1st Edition. – Birmingham: Packt Publishing, 2015.
5. Захист інформації в комп'ютерних системах та мережах : навч. посібник / С. Г. Семенов [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Харків : НТУ "ХПІ", 2014.
6. Explain IPSec https://learn.microsoft.com/en-us/training/modules/explore-connection-security-rules/2-explain-internet-protocol-security

DOI: 978-966-301-266-7/1.2024.104

Романенкова О.Ю.
https://orcid.org/0009-0003-1099-0300
e-mail olena.romanenkova@e-u.edu.ua

ЗАСТОСУВАННЯ СУЧАСНИХ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ В КОНТЕКСТІ РЕАЛІЗАЦІЇ НАВЧАЛЬНИХ ПРОГРАМ З БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Анотація. У статті розкрито концепцію застосування сучасних технологій під час вивчення дисципліни «Безпека життєдіяльності», яка включає узагальнені наукові знання, що охоплюють теорію і практику захисту людини, суспільства, держави, світового співтовариства, природного середовища від небезпечних, шкідливих факторів і надзвичайних ситуацій різного характеру. Стаття присвячена питанню необхідності навчання дисципліні «Безпека життєдіяльності» учнів, студентів та спеціалістів різного профілю в рамках обов'язкових курсів з вивчення техніки безпеки. Акцентована увага на організації освітнього процесу із застосуванням сучасних можливостей техніки, описі його змістовної частини і прикладів завдань.

Ключові слова: безпека життєдіяльності, зміст освіти, формування і розвиток понять, предметні знання, змістові лінії дисципліни «Безпека життєдіяльності».

Romanenkova Olena

APPLICATION OF MODERN INNOVATIVE TECHNOLOGIES IN THE CONTEXT OF IMPLEMENTING LIFE SAFETY TRAINING PROGRAMS

Abstract. The article reveals the concept of using modern technologies during the study of the discipline "Life Safety", which includes generalized scientific knowledge covering the theory and practice of protecting people, society, the state, the world community, and the natural environment from dangerous, harmful factors and emergency situations of various nature. The article is devoted to the issue of the need to teach pupils, students and specialists of various profiles the discipline "Safety of life" as part of mandatory courses on safety engineering. Attention is focused on the organization of the educational process with the use of modern technology capabilities, description of its content and examples of tasks.

Key words: life safety, content of education, formation and development of concepts, subject knowledge, content lines of the discipline "Life Safety".

Мета статті. Світова практика показує, що правильне навчання працівників вимогам охорони праці, прийомів безпечного ведення робіт, управління ними дозволяє істотно знизити виробничий травматизм і професійну захворюваність, а навчання працівників прийомам надання першої допомоги – тяжкість небезпечних для здоров'я людини наслідків.

Виклад основного матеріалу дослідження. Аналіз літератури з проблеми дослідження показав, що на початку XXI століття спостерігається стійка тенденція зростання надзвичайних ситуацій природного, техногенного та соціального характеру. Серед причин виникнення надзвичайних ситуацій різного походження слід назвати низьку культуру безпеки життєдіяльності населення, нехтування знаннями техніки безпеки, охорони праці та правилами безпечної поведінки, безвідповідальне ставлення до власного життя і здоров'я, а також безпеки оточуючих.

Відсутність культури безпеки життєдіяльності у підростаючого покоління загрожує суспільству зростанням аварій і катастроф в майбутньому. Саме в необхідності зацікавити безпекою життєдіяльності всі категорії суспільства, мотивувати до знання та застосування на практиці як в побуті, так і під час професійної діяльності техніки безпеки полягає актуальність теми статті.

Аналіз діючих стандартів освіти дозволив виявити три компетенції, на основі яких базується тематичний зміст курсу «Безпека життєдіяльності»:

– готовий використовувати основні методи захисту від можливих наслідків аварій, катастроф, стихійних лих; здатний нести відповідальність за результати своєї професійної діяльності;

– готовий до забезпечення охорони життя і здоров'я учнів у навчально-виховному процесі та позаурочної діяльності.

Недостатня увага людини до проблем природного і, особливо техногенної безпеки, схильність до ризику і нехтування небезпекою багато в чому пов'язані з обмеженими знаннями людини про світ небезпек і негативні наслідки їх прояву. Оскільки часто головним винуватцем надзвичайних ситуацій в кінцевому рахунку виявляється конкретна людина, її освіта, виховання і самосвідомість є важливими факторами, що впливають на ризик надзвичайних ситуацій. Ідея профілактики нещасних випадків допускає такий стиль діяльності, коли основні зусилля спрямовані на виявлення причин виникнення небезпечних проблем і ситуацій із наступним оперативним

усуненням цих причин до того як вони можуть реалізуватись в нещасний випадок. З метою актуалізації вирішення проблем безпеки Міністерством освіти та науки України була розроблена і затверджена у 2001 році Концепція освіти з напряму «Безпека життя і діяльності людини». У концепції наголошено, «що метою освіти з безпеки життєдіяльності є підготовка особи до активної участі в забезпеченні тривалого повноцінного життя в суспільстві, яке динамічно змінюється».

Розглянемо найбільш поширені нині головні тенденції інноваційних освітніх технологій. Корпоративне навчання онлайн–це одержання вмінь і навичок роботи онлайн, що передбачає підвищення ефективності роботи кожного окремо і всіх разом. До позитивних тенденцій такого навчання безпеці життєдіяльності належать: інтерактивність, запам'ятовування, гнучкість у використанні, надання допомоги і доступність. Такий вид навчання можливо застосовувати, як у школах так і ВИШах, такі на підприємствах, актуалізуючи увагу працівників на дотриманні техніки безпеки.

Навчання з охорони праці керівників і фахівців за допомогою онлайн-курсів може проводиться за відповідними програмами з охорони праці безпосередньо самою організацією або освітніми установами професійної освіти, навчальними центрами та іншими установами і організаціями, що здійснюють освітню діяльність.

Ефективність навчання досягається при дотриманні таких умов, як: поступове збільшення обсягу матеріалу для узагальнення і конкретизації; перехід від приватних висновків по невеликому матеріалу частини заняття до спільних висновків, за кількома занять, цілим темам; збільшення складності завдань. Потрібно постійно вчити вмінню розділяти відповіді на смислові фрагменти і виділяти в них головне, робити висновки.

Важливою проблемою є не сприйняття формул та розрахунків в контексті освоєння безпеки життєдіяльність студентами та працівниками гуманітарного напрямку. В цьому контексті актуальним буде застосування технологій всепроникаючого навчання (u-learning (ubiquitous learning), неперервне навчання з використанням ІКТ-засобів у всіх сферах життя суспільства) Таке навчання ефективне за умови:

1) проникнення в усі сфери життя студентів;
2) активного використання мобільних пристроїв;
3) охоплення навчальним процесом усіх прошарків соціуму.

Виокремимо основні принципи всепроникаючого навчання:

1) постійність: всі матеріали і виконана робота фіксуються і зберігаються;

2) доступність і адаптивність: усі навчальні матеріали доступні кожному студенту, необхідна інформація надається за його запитом;

3) оперативність: процес взаємодії між учасниками освітнього процесу може здійснюватись негайно;

4) інтерактивність: процес взаємодії між учасниками освітнього процесу може відбуватися синхронно;

5) навчання в оточуючому середовищі: навчання відбувається безпосередньо в повсякденному житті.

Важливо те, що при застосуванні таких технологій , значення та розшифрування кожної формули, наприклад, для визначення оптимального мікроклімату в приміщенні, необхідна інформація може бути знайдена в короткий проміжок часу та опрацьована. Значна частина суспільства сьогодні технічно і психологічно готова до використання вищезазначених моделей і технологій навчання, що нададуть нові можливості для підвищення ефективності навчального процесу. Розвиток і вдосконалення технічної бази, технологій надасть можливість здійснювати неперервний процес навчання, самовдосконалення впродовж усього життя. У сфері запобігання нещасним випадкам та збереження життя і здоров'я суспільства, постійне навчання і перевірка знань і вимог охорони праці є одним з найважливішихнапрямківкомплексіпревентивнихзаходів,щосприяютьскороченню виробничого травматизму і професійної захворюваності працівників підприємств і установ.

Перевірку знань з теми доцільно проводити у формі заліку електронного, для ВУЗів в тісному взаємозв'язку трьох викладачів (лектор, викладач практик з безпеки життєдіяльності, викладач практик з охорони праці).

Висновки. В даний час у більшості країн світу розширюється система установ, зайнятих професійною підготовкою фахівців в області техносферної безпеки, практичної екології, управління соціально-екологічними і природоохоронними процесами. Цей досвід позитивно може вплинути на розвиток освіти в сфері безпеки життєдіяльності в нашій країні–це може стати сферою подальших глибинних досліджень з теми.

Література

1. Леонов О.В. Пропроблеми навчання охорони праці та безпеки життєдіяльності/ О.В. Леонов, В.О. Сєвриков //Охорона праці. – 2008. – №9. – С.15.

2. Гуревич Р.С. Мобільне навчання – сучасна субдисципліна педагогічної освіти / Р.С. Гуревич,М.Ю. Кадемія // Interdyscyplinarnoćś pedagogikii jej subdyscypliny ; pod redakcją Zofii Szaroty I Franciszka Szloska / Wydawnictwo Naukowe Instytutu TechnologiiEksploatagi.–PIB26-600Radom,ul.K.Pulaskiego 6/10. – S.459-467.

3. Ігнатович М.В. Проблеми викладання курсу «Безпека життєдіяльності» студентам економічних спеціальностей / М.В. Ігнатович, В.Ю. Худолей // Безпека життєдіяльності.–№10.–2007.–С.42-43.

4. Кадемія М.Ю. Інформаційно-комунікаційні технології навчання: термінологічний словник (рекомендовано МОН України лист №1/11-3856 від 02.06.2009р.) /М.Ю. Кадемія. – Львів: Вид-во «СПОЛОМ», 2009. – 260с.

5. Кузик А.Д. Про створення універсальної освітньо-інформаційної системи цивільного захисту //Інформаційно телекомунікаційні технології в сучасній освіті: досвід, проблеми, перспективи: зб. наук. праць. – Львів: ЛДУБЖД, 2006. – С.273- 278.

DOI: 978-966-301-266-7/1.2024.109

Савченко Я.О.
https://orcid.org/0009-0008-0381-0224
e-mail: yaroslav.savchenko@e-u.edu.ua

Левченко С.В.
https://orcid.org/0009-0006-8497-0515
e-mail: sergiy.levchenko@e-u.edu.ua

Скляренко О.А.
https://orcid.org/0009-0003-4908-0187
e-mail: osklyarenko@e-u.edu.ua

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Анотація. Ця стаття присвячена ролі штучного інтелекту (ШІ) та машинного навчання (МН) у військових операціях. Розглянуті можливості використання цих технологій для підвищення ефективності розвідки, прогнозування конфліктів, виявлення кібератак та управління автономними системами на полі бою. Детально проаналізовано методи створення систем на основі ШІ та МН, включаючи збір та передобробку даних, тренування моделей та їх застосування для прийняття рішень у реальному часі. Результати досліджень показують значний потенціал цих технологій для вдосконалення військових операцій та забезпечення безпеки військового персоналу.

Ключові слова: штучний інтелект, машинне навчання, військові операції, розвідка, прогнозування конфліктів, кібербезпека, автономні системи, нейронні мережі, аналіз даних, безпілотні транспортні засоби.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Штучний інтелект (ШІ) та машинне навчання (МН) вже знайшли широке застосування у багатьох сферах, включаючи медицину, фінанси та транспорт. У військовій сфері ці технології можуть значно підвищити ефективність операцій, знизити ризики для військових та забезпечити більш точне та оперативне прийняття рішень. Проте використання ШІ та МН у військових операціях піднімає низку важливих наукових та практичних завдань, таких як забезпечення надійності систем, запобігання зловживанню технологіями та вирішення етичних питань.

Аналіз досліджень та публікацій. Використання ШІ та МН у військових операціях є актуальною темою наукових досліджень. Ці питання вчені аналізують і оцінюють на різних рівнях, використовуючи різні методи аналізу та оцінки. Даній проблематиці присвячено наукові доробки як вітчизняних, так і закордонних дослідників [1-3].

Зокрема, багато досліджень присвячено використанню ШІ для розвідки та спостереження, для автоматичного аналізу зображень та відео. Інші дослідження фокусуються на прогнозуванні конфліктів та оптимізації логістичних операцій за допомогою МН. Також важливим напрямом є використання ШІ у кібербезпеці, де системи МН використовуються для виявлення аномалій у мережевому трафіку. Автономні системи, такі як безпілотні транспортні засоби, також є об'єктом активних досліджень, особливо у контексті оптимізації маршрутів та прийняття рішень на полі бою.

Формулювання цілей статті. Метою цієї статті є огляд сучасних напрямів використання ШІ та МН у військових операціях, аналіз їхніх переваг та викликів, а також обговорення перспектив подальших досліджень у цій сфері.

Викладення основного матеріалу дослідження. Штучний інтелект (ШІ) та машинне навчання (МН) мають потенціал кардинально змінити методи розвідки та спостереження у військових операціях. Ці технології відкривають нові можливості для аналізу та обробки великих обсягів даних, що дозволяє виявляти ворожі об'єкти, рух військ та інші потенційно важливі події на полі бою.

Розвідка та спостереження

Системи на основі ШІ можуть аналізувати зображення з безпілотників для виявлення ворожих об'єктів або руху військ. У цьому контексті використовуються бібліотеки машинного навчання, такі як TensorFlow або PyTorch, які дозволяють створювати нейронні мережі для автоматичного розпізнавання об'єктів на зображеннях.

Для створення таких систем, насамперед, використовується великий набір зображень, які є навчальними та тестовими даними для моделі. Після збору даних здійснюється їх передобробка, яка включає нормалізацію зображень для забезпечення уніфікованого масштабу даних. Далі визначається архітектура нейронної мережі, яка може включати кілька шарів конволюційних та повнозв'язних. Модель навчається на тренувальних даних, після чого оцінюється на тестових зображеннях для перевірки її ефективності. Такий підхід дозволяє значно підвищити точність та швидкість виявлення об'єктів, що є критичним для військових операцій.

Такі системи можуть бути використані як для стратегічного, так і для тактичного розвідування. Наприклад, вони можуть виявляти масштабні рухи військ на великих територіях або ж визначати місцезнаходження конкретних цілей на полі бою. Завдяки цьому вони допомагають забезпечити перевагу в бойових діях та знизити ризик для власних військ.

Прогнозування та прийняття рішень

МН може використовуватися для прогнозування можливих сценаріїв розвитку конфліктів або оптимізації логістичних операцій. Використовуючи історичні дані про конфлікти, алгоритми МН можуть прогнозувати ймовірність виникнення нових конфліктів у різних регіонах. Для цього широко використовуються такі бібліотеки як scikit-learn, які надають широкий набір інструментів для обробки даних та навчання моделей.

Наприклад, для прогнозування конфліктів може бути використано алгоритм Random Forest або градієнтний бустинг. Спочатку збираються історичні дані про конфлікти, а також інші релевантні показники, такі як економічні, соціальні та політичні фактори. Далі ці дані використовуються для навчання моделей, які можуть аналізувати взаємозв'язки між різними факторами та передбачати ймовірність виникнення нових конфліктів.

Навчені моделі МН, які базуються на історичних даних, можуть бути застосовані для прогнозування майбутніх подій та визначення оптимальних стратегій дій. Це дозволяє військовим командуванням заздалегідь підготуватися до можливих сценаріїв та приймати обґрунтовані рішення щодо розгортання сил і ресурсів.

Використання МН у військових стратегіях відкриває нові можливості для прогнозування та управління ризиками, забезпечуючи військовим командуванням засоби для ефективного відстоювання національних інтересів та забезпечення безпеки країни.

Кібербезпека

Кібербезпека є однією з найважливіших сфер військових операцій. Алгоритми МН можуть навчатися на нормальному мережевому трафіку і виявляти аномалії, які можуть свідчити про кібератаку. У цьому контексті використовуються бібліотеки, такі як scikit-learn або PyOD, для створення моделей, здатних виявляти аномалії у мережевому трафіку.

Процес виявлення аномалій починається з збору даних про мережевий трафік, який включає нормальний та потенційно аномальний трафік. Далі здійснюється обробка даних для виділення основних характеристик мережевого трафіку, таких як обсяг даних, час передачі, джерело та пункт призначення. Потім модель навчання, така як Isolation Forest або Autoencoders, навчається на нормальному трафіку, щоб розпізнавати аномалії, які

відхиляються від нормальних шаблонів. Це дозволяє автоматично виявляти та реагувати на кібератаки в реальному часі.

Ці технології можуть бути використані для розробки імунних систем безпеки, які автоматично аналізують, виявляють та блокують кіберзагрози до того, як вони завдають шкоди мережі чи інформаційним системам. Крім того, вони дозволяють виявляти нові види кіберзагроз та адаптувати заходи безпеки для їх виявлення та запобігання.

Автономні системи

Автономні системи, такі як безпілотники та роботизовані транспортні засоби, використовують ШІ та МН для самостійного прийняття рішень на полі бою. Це дозволяє зменшити ризик для людей і підвищити ефективність операцій. Для оптимізації маршрутів автономних транспортних засобів використовуються бібліотеки, такі як NetworkX, та алгоритми пошуку шляху, такі як A*.

Наприклад, безпілотний транспортний засіб може використовувати алгоритми МН для аналізу карти місцевості та знаходження оптимального маршруту з урахуванням поточних умов на полі бою. Процес починається з визначення графу або карти місцевості, яка включає різні можливі маршрути та перешкоди. Далі використовується алгоритм пошуку шляху, такий як A*, який дозволяє знаходити найкоротший та найменш небезпечний маршрут від стартової до кінцевої точки. Такий підхід забезпечує високу оперативність та точність у виконанні завдань.

Крім того, системи штучного інтелекту можуть допомагати в оптимізації енергоспоживання та використання ресурсів, аналізувабчи динаміку витрат у реальному часі, щоб підтримувати оптимальний рівень функціонування системи. Це дозволяє зберігати енергію та ресурси, що особливо важливо у військових операціях з обмеженими ресурсами.

Таким чином, використання ШІ та МН в автономних системах відкриває нові перспективи для підвищення ефективності та безпеки військових операцій. Ці технології дозволяють системам самостійно приймати рішення та адаптуватися до змінних умов на місцевості, що робить їх незамінними знаряддями для військових дій.

Протидія дезінформації та пропаганді

Протидія дезінформації та пропаганді відіграє ключову роль у військових операціях, де ворожі сили намагаються впливати на суспільство та військових противників шляхом поширення фальшивих інформаційних повідомлень та маніпуляцій. Для виявлення та боротьби з такими загрозами використовуються інструменти аналізу тексту та візуалізації даних. Наприклад, бібліотека Natural Language Toolkit (NLTK) може бути використана для аналізу тексту та виявлення аномалій у способі поширення

інформації, що може свідчити про дезінформацію або пропаганду. Додатково, бібліотеки для обробки природної мови, такі як SpaCy або TextBlob, дозволяють виявляти ключові слова, емоційне забарвлення тексту та інші ознаки, які можуть вказувати на маніпуляції в інформаційному просторі. Такі інструменти допомагають розвідникам та аналітикам вчасно виявляти та реагувати на спроби ворожих сил впливати на суспільство та військових противників шляхом маніпуляції інформацією.

Автоматичне розпізнавання мови

Автоматичне розпізнавання мови в перехоплених комунікаціях відіграє важливу роль у зборі розвідданих та виявленні загроз безпеці. За допомогою бібліотек для обробки мови, таких як SpeechRecognition та Google Cloud Speech-to-Text, можна автоматизувати процес розпізнавання та транскрипції аудіо- або відеофайлів з виявленням ключової інформації.

Наприклад, системи автоматичного розпізнавання мови можуть використовуватися для моніторингу телефонних розмов або радіоелектронних перехоплень, забезпечуючи перевагу у виявленні загроз та ризиків. Такі системи можуть автоматично переводити мовлення на різні мови, аналізувати ключові теми та визначати тон або настрій співрозмовника. Це допомагає аналітикам та розвідникам швидко отримувати цінну інформацію з перехоплених комунікацій, що може використовуватися для прийняття стратегічних рішень та запобігання потенційним загрозам.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Штучний інтелект та машинне навчання мають великий потенціал для трансформації військових операцій, підвищуючи їх ефективність та безпеку. Використання цих технологій у розвідці, прогнозуванні, кібербезпеці та автономних системах вже демонструє значні переваги. Однак існують виклики, пов'язані з надійністю систем, безпекою даних та етичними питаннями. Подальші дослідження мають бути спрямовані на вирішення цих проблем, а також на розширення застосування ШІ та МН у військовій сфері.

Література

1. Демідов Б. О., Кучеренко Ю. Ф., Матющенко О. Г. Основні напрямки застосування технологій, що містять елементи та методи штучного інтелекту, в оборонній сфері. Наука і техніка Повітряних Сил Збройних Сил України. 2018. № 4(33). С. 7-15.

2. Домарієв В. В. Система ситуаційного управління : Теорія, методологія, рекомендації. Київ : Знання України, 2017. 347 с.

3. Борисенко О.А., Бережна О.В., Новгородцев А.І., Сердюк В.В., Яковлев М.М. Система передачі та відображення інформації із захистом числових даних. Системи обробки інформації. 2019. № 2(157). С. 103-108. https://doi.org/ 10.30748/soi.2019.157.14.

4. Гриб Д. А., Демідов Б. О., Борисенко М. В., Кузнєцова М. Ю. Інформатизація управління структурною динамікою складних багато структурних систем військового призначення при динамічній зміні обстановки в районі ведення бойових дій. Збірник наукових праць.

5. Hui Liu, Investigation on Works and Military Applications of Artificial Intelligence. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9143084

6. Сергій Балашук, Штучний інтелект та бойове прогнозування: нові можливості для ЗСУ. URL: https://softline.org.ua/news/shtuchnyi-intelekt-ta-boiove-prohnozuvannia-novi-mozhlyvosti-dlia-zsu

7. Ігор Пилипів, "Війну виграють технології". Як штучний інтелект допоможе перемогти у війні з РФ? URL: https://www.epravda.com.ua/publications/2023/12/4/707197/

8. Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., Tatarchenko, Y. The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. Economic Affairs, Vol. 69(Special Issue), pp. 43-51. DOI: https://doi.org/10.46852/0424-2513.1.2024.6 https://economicaffairs.co.in/Journal/abstract/id/NjI2MQ==/?year=2024&month=February&volume=Volume%2069&issue=Issue%201Special

DOI: 978-966-301-266-7/1.2024.115

Скляренко О.В.
https://orcid.org/0000-0001-6555-1223
e-mail: olena.skliarenko@e-u.edu.ua

Ніколаєвський О.Ю.
https://orcid.org/0000-0002-0786-5432
e-mail: alexander.nikolaievskyi@e-u.edu.ua

ОСОБЛИВОСТІ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЇ СКЛАДНИХ СИСТЕМ У ВИПАДКОВОМУ СЕРЕДОВИЩІ

Анотація. Пропонується метод дослідження стійкості нульового розв'язку системи нелінійних різницевих рівнянь, що залежать від напівмарковського ланцюга. Суть запропонованого методу полягає в дослідженні стійкості моментних рівнянь, що є детермінованими для вищезгаданих систем. Виведені необхідні умови оптимальності для цих систем.

Ключові слова: напівмарківський ланцюг, диференціальні рівняння, імовірнісні моделі, марковські процеси, моделі оптимізації

Виклад основного матеріалу. Диференціальні та різницеві рівняння з випадковими коефіцієнтами є відповідно неперервними та дискретними еволюційними стохастичними системами у випадковому середовищі та слугують математичними моделями випадкових еволюцій, що інтенсивно вивчаються останнім часом. Зокрема, в економічній сфері, досягнення високої ефективності фінансово-господарчої діяльності, забезпечення конкурентоспроможності та фінансової стійкості підприємств неможливе без застосування стохастичних, динамічних математичних моделей. Процес моделювання, взагалі, досить складний, однак він спрощується в разі використання чисельних методів для ПК.

Для описування характеристик ефективності операцій, результати яких залежать від ряду випадкових факторів, використовують різні імовірнісні моделі (наприклад марковські і напівмарковські послідовності), які враховують супровідні імовірнісні процеси. Далі як модель розглядатиметься випадковий напівмарковський ланцюг.

Напівмарковські випадкові процеси більш загальні порівняно з марковськими; за їх допомогою можна точніше описувати різні явища. Напівмарковські процеси використовуються в теорії надійності та масового

обслуговування, при аналізі ефективності, плануванні і прогнозуванні господарчої діяльності підприємств та в інших областях.

Випадкову послідовність η_n, $n \in \{0, 1, 2, ...\}$, із скінченим числом станів $Q_1, Q_2, ..., Q_q$ назвемо напівмарковським ланцюгом, якщо виконуються наступні умови. Нехай $n \in \{0, 1, 2, ...\}$, $0 \le n_0 \le n_1 \le n_2 \le ...$ – моменти зміни стану послідовності η_n. Тоді випадкова послідовність η_{n_0}, η_{n_1}, … утворює однорідний марковський ланцюг з перехідними імовірностями

$$p(k,s) = \mathrm{P}\{\eta_{n_{j+1}} = Q_k \mid \eta_{n_j} = Q_s\}, \quad k,s = 1, 2, \ldots, q,$$

а імовірності перебування в станах задовольняють умови

$$\mathrm{P}\{\eta_{n_{j+1}} - \eta_{n_j} = d \mid \eta_{n_0}, \eta_{n_1}, \ldots, \eta_{n_k}, \ldots; n_{k+1} - n_k, j \ne k\}$$

$$= \mathrm{P}\{\eta_{n_{j+1}} - \eta_{n_j} = d \mid \eta_{n_j}; \eta_{n_{j+1}}\} = f_{\eta_{n_j}\eta_{n_{j+1}}}(d), \qquad (j,k,d = 0, 1, 2, \ldots),$$

де $f_{Q_iQ_j}(d) = f_{ij}$ – задані числа.

Отже, для напівмарковського процесу характерно те, що після стрибка в момент n_j забувається вся "передісторія" і зміна η_n залежить лише від значення η_{n_j} та різниці $n - n_j$.

Розглянуті питання теорії керування, пов'язані з оптимізацією розв'язків нелінійної стохастичної системи керування вигляду

$$X_{n+1} = F(X_n, \eta_n, U_n), \qquad n = 0, 1, 2, \ldots, \tag{1}$$

де η_n – щойно описаний напівмарковський ланцюг із заданими матрицями інтенсивностей $Q(n) = \|q_{ks}(n)\|$, $(k,s = 1, 2, \ldots, q)$ та початковим розподілом η_0, X_n – випадковий m-вимірний вектор, а U_n – l-вимірний вектор керування.

Відомо, що інтенсивності $q_{ks}(n)$ задовольняють такі вимоги: $q_{ks}(n) \ge 0$, $\sum_{n=0}^{\infty} q_s(n) = 1$, якщо $q_s(n) = \sum_{k=1}^{q} q_{ks}(n)$.

Для системи (1) шукаємо оптимальне керування вигляду

$$U_n = S(X_n, \eta_n), \qquad n = 0, 1, 2, \ldots, \tag{2}$$

що мінімізує функціонал якості

$$I = \sum_{n=0}^{\infty} W(X_n, \eta_n, U_n) \tag{3}$$

Функціонал (3) буде мати мінімум, якщо стохастичні функції Ляпунова вздовж розв'язків системи (1)

$$V_s(x) = \sum_{n=0}^{\infty} M[W(X_n, \eta_n, U_n) \mid X_0 = X, \eta_0 = Q_s], \quad s = 1, 2, \ldots, q \quad (4)$$

будуть мати мінімум.

Отримані необхідні умови оптимальності для системи керування (1) і її частинного випадку, коли випадковий процес η_n – марковський.

Висновки. Побудова моделей оптимізації, наприклад структури виробництва конкретного підприємства, і застосування її результатів дає змогу найефективніше використати виробничий потенціал підприємства і досягти високих економічних показників в умовах стійкого розвитку.

Література

1. Lakhno, V.A., Kasatkin, D.Y., Skliarenko, O.V., Kolodinska, Y.O. Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment // Machine Learning and Autonomous Systems. Smart Innovation, Systems and Technologies, vol 269. Springer, Singapore. – 2022 – p. 9-22.

DOI: 978-966-301-266-7/1.2024.118

Степанюк А.В.
https://orcid.org/0009-0003-6318-5874
e-mail: allarkusha90@gmail.com

ІРРАЦІОНАЛЬНІ ІНТЕНЦІЇ «СМІХУ-БОЖЕВІЛЛЯ» В ПОЕЗІЯХ Т. Г. ШЕВЧЕНКА

Анотація. У статті досліджується архетип сміху-божевілля в поезіях Т. Г. Шевченка. Методологічно-теоретичну основу становлять основні положення філософських та літературознавчих праць, присвячених генезі і функціям архетипного сміху та естетиці романтизму.

Ключові слова: сміх, божевілля, романтизм, міфологія, архетип, поезія.

Stepanyuk Alla

IRRATIONAL INTENTIONS OF "LAUGHTER-MADNESS" IN THE POETRY OF TARAS SHEVCHENKO

Abstract. In the article the author investigates the archetype of madness' laugh in Taras Shevchenko's poetry. The main ideas of philosophical and literary works, which are devoted to the genesis and functions of archetypal laugh and aestheties of romantism, are selected as methodological and theoretical basis.

Key words: laugh, madness, romanticism, mythology, archetype, poetry.

Виклад основного матеріалу. Поява певних художніх реакцій письменника на світ залежить і від його психологічного типу, і від естетичних віянь часу, від оточення, у якому митець зростав і ставав особистістю, від менталітету нації, від подій того часу.

Поетична творчість Т. Шевченка позначена виразними романтичними ознаками. Д. Наливайко, відзначаючи стильовий синкретизм творчості поета, наголошує, що домінує в ній саме романтичне начало, яке типологічно близьке до загальноєвропейського та має яскраво виражені національні та індивідуальні риси [4, с.18]. Романтична творчість передбачає звернення до міфології, народної поезії, національних архетипів, у яких романтики шукають витоки «національного духу», обґрунтування концепції органічної єдності світу, його динамічності та амбівалентності.

Світ постає для романтиків як сукупність таємничих, захованих, невідомих сфер та сил, які ще називаються «нічною стороною світу». Людина так само сповнена таємничих сил, як і весь світ; це таємниче, з погляду світла розуму, є «несвідоме», усякі збочення від «нормального», розумного ходу душевного життя: божевілля, сон, екстаз, натхнення, передчуття, «нічна сторона» душі – усі такі переживання відкривають людині вихід із сфери звичайного її буття до інших сфер, почасти вищих, і мають тому глибоке значення [7, с.407]. А поряд із цими людськими переживаннями чималу роль починають відігравати в поезії демонічні сили, які теж становлять вагому частину «нічної сторони світу». Тому ірраціональний, «чудесний» та скомплікований світ; у єстві своєму складна та тісно зв'язана з іншими таємничими сферами й істотами в них людина – такий філософський світогляд романтики [7, с. 408].

У деяких поетичних творах Т. Шевченка сміх має архетипне походження і стає важливим засобом вираження «нічної» сторони світу та людської душі.

Т. Шевченко був наділений здатністю тонко відчувати світ і реагувати на нього. Сучасники поета засвідчували мінливість його вдачі, характеризували як людину настрою: у гарному настрої він – балакун, душа компанії; у поганому – суворий, мовчазний, недовірливий. За класифікацією психологічних типів, розробленої К. Юнгом, особистість Т. Шевченка, як довела М. Моклиця [3], можна віднести до емоційного психологічного типу. Цей тип був, звичайно, генетично успадкований від батьків, проте його психіка увібрала і національні архетипи, елементи українського менталітету. Д. Чижевський зазначав, що емоційність, чутливість, ліризм, індивідуалізм та прагнення до волі, неспокій і рухливість – основні риси психологічного укладу українця, яким і був Т. Шевченко.

Його надмірна емоційність почала виражатися за допомогою архетипів плачу і сміху, яким у поезії Шевченка відведено почесне місце, а традиція архаїчного сміху творчо переосмислена в контексті романтичної естетики. Категорія «сміх» була вибрана за основу нашої роботи не випадково, адже сміх привертав увагу вчених ще від часів Арістотеля [1]. Цікавими є погляди на сміх М.Бахтіна, Л.Карасьова, А.Козинцева, С.Лащенко, А.Сичова, Л.Столовича та інших. Інтепретаційна парадигма категорії «сміх» багатозначна та суперечлива. Він поряд із плачем є архетипом і основною міфологемою культури, який відображає реакцію людини на світ. Життя – це сміх, а плач - смерть, яка є формою переходу в новий, якісний стан буття. Реагувати на світ через усталені психічні реакції, які зберігають родову, «колективну» пам'ять, – означає жити, бути свідком буття, існування, що вічно оновлюється.

На думку української дослідниці С. К. Лащенко, на сьогодні архетип сміху в науці досліджений недостатньо. «У гуманітарній науці протягом довгого часу сміх розглядався виключно у зв'язку зі смішним та феноменом комічного. Разом з тим, людству був також відомий інший тип сміху, який виник задовго до сміху при усвідомленні смішного. Лише в ХХ столітті такий сміх був ідентифікований як самостійне культурне явище та визначено, як сміх ритуальний — той, що склався в культурі язичництва й розвивався в тісному зв'язку з язичницьким світосприйманням та світоуявленням»[2, с.21].

Т. Шевченко, як зазначав Є. Нахлік [5], у своїй поезії відтворював національний міф з його архетипами, творчо переосмислював його, збагачував авторськими символічними значеннями. Ця особливість художнього мислення поета виявляється в місці та ролі архетипу сміху в його поетичних творах.

Т. Шевченко досконало знав українську міфологію, літературно обробляв жанри народної думи, історичної пісні, балади, і, звичайно, йому було цікаво зазирнути в сакральний зміст життя, наповненого «бісовськими» створіннями, чудернацькими перетвореннями, осягнути значення пекла у світоглядному баченні людини. Сміх-божевілля у творах Шевченка був наскрізно пронизаний демонічним єством, мав певне ірраціональне підґрунтя.

Наприклад, у баладі «Причинна» поет із метою створення напруженої атмосфери вводить сцену гуляння демонічних сил, зокрема русалок:

Аж гульк – з Дніпра повиринали
Малії діти, сміючись.
« Ходімо гріться! – закричали –
Зійшло вже сонце!» (Голі скрізь;
З осоки коси, бо дівчата) [6; 1, с.75].
« Зареготались нехрещені…
Гай обізвався; галас, зик.» [6; 1, с. 76].

Звичайно, такий нелюдський сміх створює картину жаху в уяві читача, і досить доречно, адже цей сміх є символом трагічного, символом згасання життя молодої людини (русалки «взяли її, сердешную, та й залоскотали»).

Образ сміху-лоскотання русалок має архаїчне походження. Дослідниця С. К. Лащенко подає таку версію Русалок-Лоскотух та їх сміху-лоскотання в українській міфології: «Уявлення про поведінку подібних міфологічних істот, характер їх відношення до людини свідчать про те, що, вступаючи в контакт з живими істотами (переважно парубками й чоловіками), русалки, як вірили люди, намагалися через лоскотання задовольнити свій «сексуальний голод». Стан, у який занурювалася людина під впливом лоскотання

міфологічної істоти, ототожнювався за своїми ознаками зі станом страшної «сміхової» виснаги поховального обряду. Але тут збудження, помішане з жахом і відчуттям погрози, забарвлювалося в особливі тони. Енергетика чутливості, закладена і в поховальному «сміхові»/рухові/сексуальному збудженні, ставала тут домінуючою, починаючи дарувати людині, яку катастрофічно руйнував такий «лоскотний сміх», ні з чим не зрівняне хтиве відчуття. Саме воно ставало свого роду «лідером», забарвлюючи все в особливі еротично-значущі тони. Переборюючи силу такого збудження, людина, стоячи на порозі смерті, починала відчувати задоволення від власних мук, мимоволі провокувати їх продовження, жахаючи, збуджуючи, запалюючи хтивість кожного, хто виявлявся вільним чи невільним свідком того, що ставалося з ним» [2, с.37].

Зрозуміти витоки подібних уявлень багато в чому допомагає й сама етимологія слова «лоскотання», що, як свідчать джерела, пішло від старослов'янського «щекот» («лоскот»), заснованого на тому самому корені, що й «скъкът», «скъкотание». А це означає, що початково «лоскотання» і «скакання» сприймалися нашими предками як синонімічні дії, у однаковій мірі пов'язані зі «збудженням похоті», сексуально значущими дотиками, тичками та іншими тактильними контактами сексуального забарвлення. Таким чином, той контакт, що, як уявлялося це нашим предкам, виникав між Русалкою-Лоскотухою та обраною нею людиною завдяки лоскотанню, тлумачився своєрідним чуттєво значущим єднанням або «шлюбом» мінливої й примхливої міфологічної істоти й живої людини. «Сміх», що ставав невід'ємною складовою такого «шлюбу», виявлявся колись свідоцтвом здійсненності таємничого «сексуального контакту», — контакту, що, як свідчить більшість фольклорних джерел, частіше за все приносив смерть живій істоті [7, с.38].

Сміх русалок виконує в баладі Т. Шевченка «Причинна» протилежну істинній функції сміху – функцію танатологічну – згасання життя, адже істина твердить, що сміх як діяльність спонукає до життя.

Згадка про сміх-лоскотання русалок є і в баладі Т. Шевченка «Русалка» в сцені, коли мати топить свою позашлюбну дочку. Жінка просить доньку-русалку помститись своєму спокуснику – залоскотати його на смерть:

Залоскочи, моє серце,
Нехай не сміється
Надо мною, молодою… [2; 1, с. 376].

Таким чином, чоловік стане жертвою власних пристрастей – насолоди від тілесних утіх.

У багатьох творах Т. Шевченка сміх, що сягає корінням язичницьких ритуалів, символізує хаос у людській душі, спровокований безсиллям людини перед тиском життєвих обставин. Це може бути нещасливе кохання, втрата рідних людей, несправедливий суспільний уклад, вимушена відмова від моральних принципів чи безпосереднє залучення до людського життя демонічних сил. Усі ці причини людина сприймає як катастрофічні, космічні, які порушують її усталений спосіб життя. Божевільний сміх є синонімом духовної смерті персонажів, їх безсиллям перед зовнішніми чинниками. Він генетично походить від того амбівалентного сміху-плачу, який властивий давньому поховальному обряду. Смерть сприймалася нашими пращурами як порушення надприродною силою узвичаєного порядку: «Скоріш за все, у початковому відношенні наших предків до тіла, зануреного в «ритуальний сміх», панувало його сприймання як того, що потрапило в полон стихії надприродної сили. Це вона «м'яла» й «корчила» людське єство. Це вона примушувала людське тіло постійно рухатися, колихатися, трястися, нахилятися, падати й підніматися, відчувати сексуальне збудження, кричати, «сміятися» й плакати, наслідуючи своїм станом – стан хаотичного світу. Не випадково давні греки, які ще зберігали у своїй культурі живі відлуння давніх уявлень предків, характеризували такий тип «сміху», як не те, що я роблю, а те, що робиться зі мною» (С. Аверінцев)

Зрозумілим стає, що божевільний сміх невипадково з'являється на устах нещасливих у коханні, зокрема хлопця у баладі «Причинна», дівчат у баладі «Тополя», поемі «Слепая». Мотив «нещасливих коханців» присутній і в поемі «Відьма», де героїня тяжко переживає одруження коханого:

Сама собі вона шептала
І тяжко, страшно усміхалась [6; 2, с.379].

Означник «страшно» є показником, у першу чергу, божевільних інтенцій.

Усвідомлення гріховності бажаного перелюбу з коханим Петрусем потьмарює розум «генеральші» (поема «Петрусь»):

…Не спала; впали карі очі,
Засохли губи; і вночі
Щось, ходе, шепче, сміючись… [6; 2, с. 218].

Божевільним сміхом супроводжується вбивство Гонтою дітей у поемі «Гайдамаки», яке є найдраматичнішим порушенням природного закону в сімейному колі. Гонта вигукує:

…Доле моя, доле!
Доле моя нещаслива!
Що ти наробила?
Нащо мені дітей дала?
Чом мене не вбила?
Нехай вони б поховали,
А то я ховаю [6, 1, с.186].

Складне суспільно-політичне життя за часів Коліївщини не дає Гонті жодних надій гармонійно поєднати батьківські почуття та вірність гайдамацькій присязі вбивати ляха. Після розправи над дітьми Гонта усвідомив себе великим грішником, а тому «страшно, страшно усміхався, на степ оглядався» [6; 1, с.187].

Якщо для Гонти сміх – це результат усвідомлення власної ницості, то для п'яного кесаря (поема «Неофіти») – відчуття того, що його жорстокості, сваволі скоро прийде кінець.

А син твій гордо на арену,
Псалом співаючи, стулив.
І п'яний кесар, мов скажений,
Зареготавсь… [6; 2, с.255].

Однак функція сміху однакова – відчуття героями власного безсилля.

Божевільний сміх матері-України («Великий льох») як реакція на народження двох синів-близнят, двох Йванів – це символ трагічного передчуття складного тернистого шляху України до незалежності. Близнюки-Івани втілюють ідею духовного розколу української нації, національного розбрату:

То близнята народились,
А навісна мати
Регочеться, що Йванами
Обох буде звати! [6; 1, с.323].

Отже, у символічному світі романтичної поезії Т. Шевченка сміх належить до тих образів, які мають глибоку, колективну пам'ять, що фіксує первісні уявлення людини про її стосунки із надприродними силами. Архетип сміху Т. Шевченко підпорядковує створенню романтичної атмосфери, відчуттю органічної єдності людини й одухотвореної природи.

Ірраціональний, божевільний сміх символізує в поезії Т. Шевченка виняткові страждання дисгармонійної особистості та є одним із засобів вираження історіософії поета.

Література

1. Арістотель. Поетика / Пер. Б. Тена. – К.: Мистецтво, 1967. – с. 54.
2. Лащенко С. К. Ритуальний сміх: досвід тлумачення смислових витоків (за матеріалами української традиції). – Автореф. дис.. д-ра мистецтвознавства. – К., 2006.
3. Моклиця Марія. Тарас Шевченко як психологічний експресіоніст // Сучасність. – 2002. -№№7-8.
4. Наливайко Дмитро. Стиль поезії Шевченка і його міжнаціональний контекст. - К., 2008 – 2009 .
5. Нахлік Євген. Тарас Шевченко: архетипні постаті поета // Дивослово. – 2011. - №5.
6. Тарас Шевченко. Повне зібр. тв.: У 12-ти т. – К., - 2001. – ТТ. 1, 2.
7. Чижевський Д.І. Історія української літератури. – К.: Видавничий центр «Академія», 2003. – 568 с.

DOI: 978-966-301-266-7/1.2024.125

Тонковид Т.А.
https://orcid.org/0000-0001-1111-2222
e-mail: timofiy.tonkovid@e-u.edu.ua

Милашенко В.М.
https://orcid.org/0000-0002-1434-7609
e-mail: viktor.mylashenko@e-u.edu.ua

МАШИННЕ НАВЧАННЯ ДЛЯ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ БАЗАМИ ДАНИХ: РОЗРОБКА АЛГОРИТМІВ ДЛЯ АВТОМАТИЧНОГО МОНІТОРИНГУ ТА ОПТИМІЗАЦІЇ

Анотація. Ця стаття досліджує застосування машинного навчання для автоматизації управління базами даних, зокрема розробки алгоритмів для автоматичного моніторингу та оптимізації їх роботи. В рамках дослідження ми використали різні техніки машинного навчання, включаючи регресійний аналіз, класифікаційні моделі, та реінфорсментне навчання для вирішення задач прогнозування навантаження, ідентифікації потенційних проблем у роботі систем, та динамічного управління ресурсами.

На основі зібраних даних з різних комерційних баз даних, моделі були навчені, протестовані та валідовані з високою точністю. Результати показали, що використання машинного навчання може значно підвищити продуктивність управління базами даних, знизити час відгуку та оптимізувати розподіл ресурсів. Зокрема, реінфорсментне навчання продемонструвало здатність адаптувати розподіл ресурсів в реальному часі, зменшуючи затримки на 15-20% порівняно з традиційними методами.

Стаття підкреслює значення інтеграції сучасних технологій машинного навчання в системи управління базами даних та надає рекомендації щодо подальших досліджень у цій області, спрямованих на розширення функціональності та покращення ефективності інформаційних систем.

Ключові слова: машинне навчання, автоматизація управління, бази даних, оптимізація, моніторинг, алгоритми.

Tonkovyd Tymofii, Mylashenko Viktor

MACHINE LEARNING TO AUTOMATE DATABASE MANAGEMENT: DEVELOPMENT OF ALGORITHMS FOR AUTOMATIC MONITORING AND OPTIMIZATION

Abstract. This paper explores the use of machine learning to automate database management, including the development of algorithms for automatic monitoring and optimization of database performance. In this study, we used various machine learning techniques, including regression analysis, classification models, and reinforcement learning, to solve the problems of load forecasting, identifying potential problems in the systems, and dynamic resource management.

Based on collected data from various commercial databases, the models were trained, tested, and validated with high accuracy. The results showed that the use of machine learning can significantly improve database management performance, reduce response times, and optimize resource allocation. In particular, reinforcement learning has demonstrated the ability to adapt resource allocation in real time, reducing latency by 15-20% compared to traditional methods.

The article emphasizes the importance of integrating modern machine learning technologies into database management systems and provides recommendations for further research in this area aimed at expanding the functionality and improving the efficiency of information systems.

Key words: machine: learning, management automation, databases, optimization, monitoring, algorithms.

Введення в проблематику. У сучасному світі великих даних бази даних відіграють критичну роль у забезпеченні оперативної обробки та зберігання інформації для організацій усіх масштабів. Зростаючий обсяг даних та складність запитів вимагають розвитку більш ефективних методів управління базами даних. Машинне навчання надає перспективні можливості для оптимізації управління базами даних, зокрема, через автоматизацію складних задач моніторингу та налаштування продуктивності, які традиційно здійснювались вручну.

Аналіз останніх досліджень і публікацій. Широко визнані дослідження показали, що інтеграція алгоритмів машинного навчання може значно покращити прогнозування навантажень на бази даних та оптимізувати виконання запитів, знижуючи час відгуку та підвищуючи загальну продуктивність систем (2022 23nd Freie Universitat Berlin, Stanford University; L Sixt, E. Z. Liu, M. Pellat, J. Wexler, M. Hashemi, B. Kim, M. Maas ст. 2-7). Однак, більшість існуючих підходів ще не в повній мірі використовують потенціал машинного навчання, часто обмежуючись специфічними випадками використання або конкретними типами баз даних.

Цілі та завдання дослідження. Метою цього дослідження є розробка та апробація алгоритмів машинного навчання, здатних автоматизувати ключові аспекти управління базами даних. Ці алгоритми мають на меті:

1. Автоматично моніторити стан та продуктивність баз даних.
2. Прогнозувати майбутні навантаження та потенційні проблеми.
3. Вирівнювати ресурси відповідно до динаміки запитів та обсягу даних.
4. Застосування отриманих даних для покращення рішень управління ресурсами у реальному часі.

Таким чином, дане дослідження спрямоване на вирішення проблеми комплексного управління базами даних з використанням передових технологій машинного навчання, що відкриває нові горизонти для оптимізації процесів та забезпечення стабільності і продуктивності інформаційних систем у різних сферах застосування.

Опис даних та методів збору даних. Для проведення нашого дослідження ми використали історичні дані моніторингу з кількох великих комерційних баз даних. Дані включали інформацію про запити, ресурсне навантаження, час відгуку системи та інші метрики продуктивності. Збір даних було здійснено за допомогою вбудованих інструментів моніторингу, таких як Performance Schema в MySQL та Dynamic Management Views у SQL Server.

Деталізація алгоритмів машинного навчання та параметрів. Ми використовували кілька підходів машинного навчання для аналізу зібраних даних:

1. Регресійний аналіз для прогнозування навантаження на базу даних на основі історичних даних про запити та їхній вплив на продуктивність системи.
2. Класифікаційні моделі , такі як випадковий ліс та градієнтний бустинг, для ідентифікації потенційних проблемних запитів, що можуть викликати збої або зниження продуктивності.
3. Алгоритми реінфорсментного навчання для оптимізації розподілу ресурсів в реальному часі, зокрема техніки Q-learning та Deep Q-networks (DQN), щоб адаптувати розподіл ресурсів у відповідності до змінюваних умов навантаження.

Опис експериментального дизайну. Експерименти були розділені на три основні фази:

1. Тренування моделей : Використання історичних даних для тренування зазначених моделей машинного навчання. Моделі були налаштовані та

валідовані на незалежних наборах даних для забезпечення їх узагальнення та надійності.

2. Тестування в симульованому середовищі : Перевірка моделей у контрольованому середовищі для визначення їх ефективності у реальних умовах. Симуляції включали різні сценарії навантаження та запитів.

3. Розгортання та моніторинг в реальних умовах : Остання фаза включала застосування розроблених моделей на живих системах, з неперервним моніторингом їх впливу на продуктивність та стабільність баз даних.

Цей підхід дозволяє не тільки оцінити потенціал та обмеження машинного навчання у контексті управління базами даних, але й надає основу для подальшого впровадження інтелектуальних систем управління у великомасштабні інформаційні інфраструктури.

Аналіз отриманих результатів. У результаті проведених експериментів, різні моделі машинного навчання продемонстрували значний потенціал у покращенні управління базами даних. Основні результати включають:

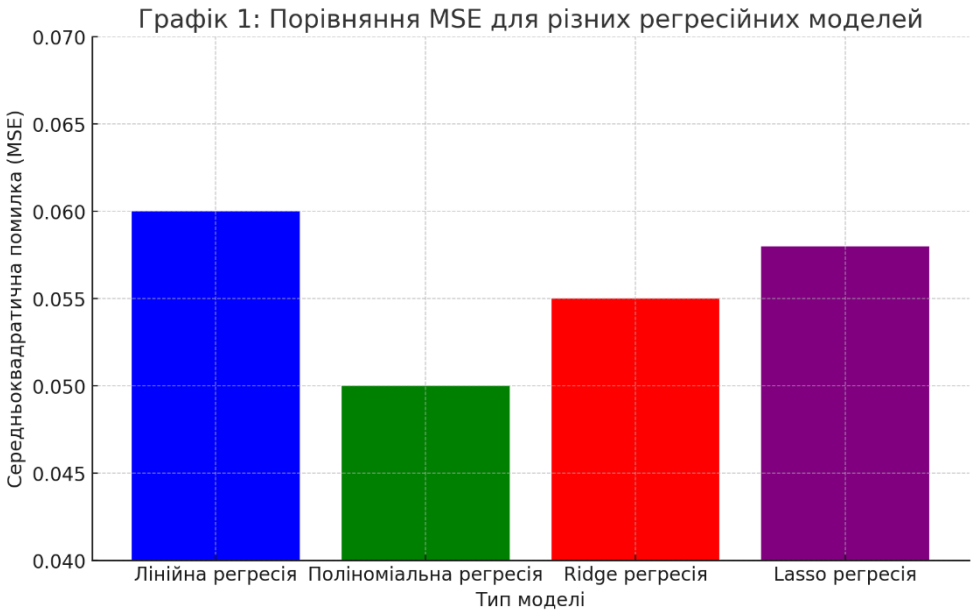
1. Регресійні моделі: Моделі, зокрема, лінійна та поліноміальна регресії, продемонстрували високу точність у прогнозуванні загального навантаження на систему. Середньоквадратична помилка (MSE) для цих моделей становила приблизно 0.05, що свідчить про високу здатність до точного прогнозування.

2. Класифікаційні моделі: Випадковий ліс та градієнтний бустинг ефективно ідентифікували запити, які могли викликати зниження продуктивності. Точність цих моделей досягала 90%, що дозволяло оперативно реагувати на потенційні проблеми до їх ескалації.

3. Реінфорсментне навчання: Моделі на базі Q-learning та Deep Q-networks (DQN) продемонстрували здатність до адаптації розподілу ресурсів у реальному часі. Ці моделі забезпечували зниження часу відгуку на 15-20% в порівнянні з традиційними методами управління.

Для наочності результатів були створені візуалізації та таблиці:

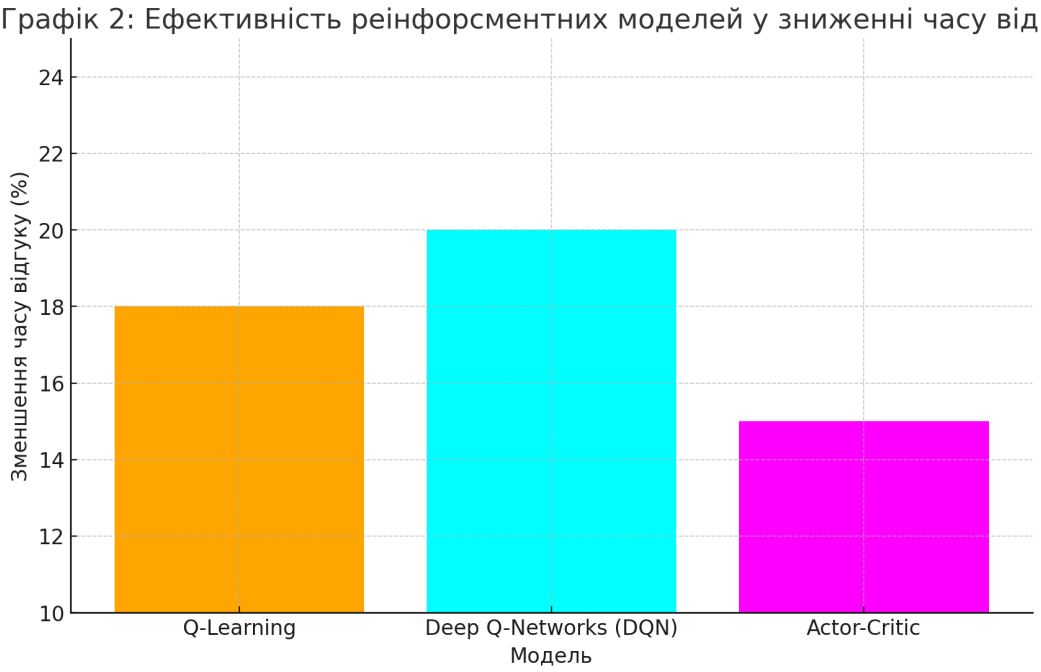
Графік 1 : Порівняння MSE для різних регресійних моделей.



Таблиця 1 : Сумарна точність ідентифікації проблемних запитів різними класифікаційними моделями.

#	Модель	Точність(%)
1	*Випадковий ліс*	*92*
2	*Градієнтний бустинг*	*90*
3	*SVM*	*88*
4	*Нейронна мережа*	*91*

Графік 2: Ефективність реінфорсментних моделей у зниженні часу відгуку.



Обговорення результатів. Результати підтверджують ефективність впровадження машинного навчання у процеси управління базами даних. Використання регресійних та класифікаційних моделей дозволяє точно прогнозувати та ідентифікувати потенційні проблеми, тоді як застосування реінфорсментного навчання відкриває нові можливості для адаптивного управління ресурсами. Такий підхід забезпечує не тільки підвищення продуктивності, але й загальну стабільність системи, що є критично важливим у умовах зростання вимог до швидкості та обсягу обробки даних.

Вплив результатів на розробку та управління базами даних. Результати нашого дослідження демонструють значний потенціал машинного навчання у реалізації автоматизованого управління базами даних. Зокрема, використання регресійних моделей для прогнозування загального навантаження дозволило виявити важливі тенденції та забезпечити можливість проактивного управління ресурсами. Класифікаційні моделі, такі як випадковий ліс та градієнтний бустинг, ефективно виявляли запити, що могли призвести до зниження продуктивності, забезпечуючи можливість швидкої реакції на потенційні проблеми. Такі моделі мають велике значення у запобіганні збоїв у роботі систем та зменшенні негативного впливу на кінцевих користувачів.

Порівняння з існуючими дослідженнями. Наукова література підкреслює важливість інтеграції машинного навчання у управлінні базами даних, але часто обмежується теоретичними аспектами або окремими випадками використання. Наш підхід, який включає комплексне застосування різних видів моделей машинного навчання, пропонує практичне та масштабоване рішення. Реінфорсментне навчання, зокрема, демонструє значний потенціал у адаптивному управлінні ресурсами, що підтверджується нашими результатами зниження часу відгуку та оптимізації навантаження.

Вплив результатів на розробку та управління базами даних. Застосування алгоритмів машинного навчання в управлінні базами даних відкриває нові можливості для автоматизації та оптимізації, що є критично важливим для сучасних великих даних та їх швидкої обробки. Ці технології можуть значно підвищити ефективність систем через здатність до самонавчання та адаптації, знижуючи потребу в ручному налаштуванні та управлінні, а також зменшуючи можливість людської помилки.

Подальші дослідження. На основі отриманих результатів, важливо розглянути розширення застосування розроблених методів до різних типів баз даних та різних умов експлуатації. Важливим напрямком подальших досліджень є впровадження глибшого інтегрованого підходу, що включає в себе розгляд міжсерверної взаємодії, балансування навантаження між кластерами та оптимізацію зберігання даних. Також потрібно більше уваги приділити питанням безпеки даних і приватності при застосуванні алгоритмів машинного навчання, оскільки ці аспекти є критичними для будь-якої сучасної інформаційної системи.

Висновки. Наше дослідження підтвердило значний потенціал машинного навчання у революціонізації управління базами даних. Впровадження різноманітних алгоритмів машинного навчання дозволило не тільки покращити продуктивність систем через прогнозування навантажень і оптимізацію ресурсів, але й забезпечити більшу стабільність та надійність у роботі інформаційних систем.

Практичне значення та можливості застосування результатів. Результати дослідження можуть бути використані для розробки нових інструментів і платформ, які інтегрують машинне навчання для автоматизації управління базами даних. Це не тільки підвищить ефективність адміністрування даних, але й дозволить компаніям знизити витрати на технічне обслуговування та вдосконалити аналітику. Впровадження

розроблених методів може знайти застосування у багатьох секторах, включаючи фінанси, охорону здоров'я, телекомунікації та електронну комерцію, де великі обсяги даних потребують ефективного управління.

Хоча наше дослідження показало обнадійливі результати, існують певні обмеження, зокрема залежність від якості та обсягу історичних даних, що були використані для тренування моделей. Також важливо враховувати потенційні зміни у поведінці даних, які можуть вплинути на точність моделей. Ми рекомендуємо подальше дослідження в галузі адаптації моделей до змінних умов даних, а також розробку нових методів для покращення здатності моделей до узагальнення.

Враховуючи швидке зростання обсягів даних і складності систем управління базами даних, інтеграція машинного навчання в управлінські процеси представляє собою стратегічну необхідність. Майбутнє управління базами даних буде невіддільно пов'язане з розумними, автоматизованими рішеннями, здатними оптимізувати роботу в режимі реального часу та гарантувати високу доступність і продуктивність системи. Наші результати відкривають шлях для нових інновацій у цій області, сприяючи розвитку технологій, які можуть радикально трансформувати підходи до управління даними в цифрову епоху.

Література

1. Лоуренс Мороні (2020). ШІ та машинне навчання для кодерів: Посібник програміста зі штучного інтелекту с 179-208. - Режим доступу: фізична копія

2. Крістофер М. Бішоп (2006). Розпізнавання образів і машинне навчання (інформатика та статистика) с 423-469. - Режим доступу: фізична копія

3. Норман С. Найз. (2014). Інженерія систем управління, vol с 136-197. - Режим доступу: https://books.google.com.ua/books?id=sEL2DwAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

4. Кацухіко Огата. (2009). Сучасна інженерія управління с 525-602. - Режим доступу: https://www.slideshare.net/taha717855/katsuhiko-ogata-modern-control-engineering-5th-editionpdf-259356699

5. Абрахам Зільбершатц, Генрі Ф. Корт, С. Сударшан. (2010). Концепції систем баз даних с 231-276. - Режим доступу:

https://www.academia.edu/44088198/Database_System_Concepts_6e_By_Abraham_Silberschatz_Henry_Korth_and_S_Sudarshan

6. П. Бейліс, Джозеф М. Геллерштейн, М. Стоунбрейкер (2015). Читання в системах баз даних с 123-178. - Режим доступу: https://z-lib.io/book/13526103

7. С. Бойд, Л. Ванденберге (2004). Опукла оптимізація с 131-171. - Режим доступу: https://web.stanford.edu/~boyd/cvxbook/bv_cvxbook.pdf

8. Н. Р. Мерфі, Б. Бейєр, К. Джонс, Д. Петофф. (2016). Інженерія надійності сайту: Як Google запускає виробничі системи с 303-317. - Режим доступу: https://books.google.com.ua/books?id=_4rPCwAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

9. Томас Х. Кормен, Чарльз Е. Лейзерсон, Рональд Л. Рівест, К. Стайн. (2009). Вступ до алгоритмів с 643-669. - Режим доступу: фізична копія

10. Стівен С. Скіна. (2010). Посібник з розробки алгоритмів с 441-474. - Режим доступу: https://mimoza.marmara.edu.tr/~msakalli/cse706_12/SkienaTheAlgorithmDesignManual.pdf

References

1. Laurence Moroney (2020). AI and Machine Learning for Coders: A Programmer's Guide to Artificial Intelligence pp. 179-208. - Access mode: physical copy

2. Christopher M. Bishop (2006). Pattern Recognition and Machine Learning (Information Science and Statistics) pp. 423-469. - Access mode: physical copy

3. Norman S. Nise. (2014). Control Systems Engineering, vol pp. 136-197. - Access mode: https://books.google.com.ua/books?id=sEL2DwAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

4. Katsuhiko Ogata. (2009). Modern Control Engineering pp. 525-602. - Access mode: https://www.slideshare.net/taha717855/katsuhiko-ogata-modern-control-engineering-5th-editionpdf-259356699

5. Abraham Silberschatz, Henry F. Korth, S. Sudarshan. (2010). Database System Concepts pp. 231-276. - Access mode: https://www.academia.edu/44088198/Database_System_Concepts_6e_By_Abraham_Silberschatz_Henry_Korth_and_S_Sudarshan

6. P. Bailis, Joseph M. Hellerstein, M. Stonebraker (2015). Readings in Database Systems pp. 123-178. - Access mode: https://z-lib.io/book/13526103

7. S. Boyd, L. Vandenberghe (2004). Convex Optimization pp. 131-171. - Access mode: https://web.stanford.edu/~boyd/cvxbook/bv_cvxbook.pdf

8. N. R. Murphy, B. Beyer, C. Jones, J. Petoff. (2016). Site Reliability Engineering: How Google Runs Production Systems pp. 303-317. - Access mode: https://books.google.com.ua/books?id=_4rPCwAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

9. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, C. Stein. (2009). Introduction to Algorithms pp. 643-669. - Access mode: physical copy

10. Steven S. Skiena. (2010). The Algorithm Design Manual pp. 441-474. - Access mode: https://mimoza.marmara.edu.tr/~msakalli/cse706_12/SkienaTheAlgorithmDesignManual.pdf

DOI: 978-966-301-266-7/1.2024.134

Фролов І.М.
https://orcid.org/0009-0004-1163-8787
e-mail: ihor.frolov@e-u.edu.ua

Звягінцева І.С.
e-mail: inna.zviagintseva@e-u.edu.ua

МОБІЛЬНІ ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ ПОШУКУ ІНФОРМАЦІЇ У СФЕРІ ТЕСТУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Анотація. У статті досліджується використання мобільних технологій як інструменту пошуку інформації у сфері тестування програмного забезпечення. Автор зазначає, що в умовах бурхливого технологічного розвитку спостерігається впровадження мобільних пристроїв в більшість сфер життєдіяльності, зокрема й у розробку та тестування ІТ-продуктів. Зростання популярності мобільних пристроїв та програм зумовило значні зміни в тому, як люди шукають та використовують інформацію для тестування програмного забезпечення.

У статті проаналізовано останні наукові дослідження у сфері пошуку інформації, зокрема обґрунтування вибору алгоритму пошуку різноформатних матеріалів на основі аналізу контексту шуканих матеріалів та запитів користувача, дослідження проблем і можливостей пошуку інформації в Інтернеті, а також персоналізацію пошуку на основі аналізу запитів користувачів. Однак, як зазначає автор, тема впровадження мобільних технологій у процес інформаційного пошуку у сфері тестування програмного забезпечення все ще потребує ретельного вивчення.

У процесі дослідження автор розглядає сучасні системи пошуку, які використовують такі основні алгоритми, як Інвертований індекс, TF-IDF, BM25 (Окапі), а також алгоритми на основі штучного інтелекту для пошуку інформації за ключовими словами з фільтрами та сортуванням з метою покращення пошукового досвіду. Особливу увагу приділено використанню мобільних інструментів та платформ, а також можливостям їх використання для пошуку інформації, пов'язаної з тестуванням програмного забезпечення.

Ключові слова: мобільні технології, тестування програмного забезпечення, пошук інформації, мобільні інструменти та платформи.

Frolov Ihor, Zviagintseva Inna

THE USE OF MOBILE TECHNOLOGIES AS INFORMATION SEARCH TOOLS IN SOFTWARE TESTING

Abstract. This article explores the use of mobile technologies as information search tools in the field of software testing. The author notes that in the context of rapid technological development, mobile devices are being implemented in most spheres of life, including IT product development and testing. The growing popularity of mobile devices and applications has led to significant changes in the way people search for and use information for software testing.

The article analyzes recent scientific research in the field of information search, including the justification for choosing a search algorithm for different formats of materials based on the analysis of the context of the searched materials and user queries, research on the problems and possibilities of searching for information on the Internet, and personalization of search based on the analysis of user queries. However, as the author notes, the topic of the implementation of mobile technologies in the process of information search in the field of software testing still requires careful study.

In the course of the research, the author considers modern search systems that use such basic algorithms as Inverted Index, TF-IDF, BM25 (Okapi), as well as algorithms based on artificial intelligence for searching for information by keywords with filters and sorting in order to improve the search experience. Particular attention is paid to the use of mobile tools and platforms, as well as their possibilities for searching for information related to software testing.

Key words: mobile technologies, software testing, information search, mobile tools and platforms.

Постановка проблеми та її актуальність. В умовах бурхливого технологічного розвитку спостерігається впровадження мобільних пристроїв в більшість сфер життєдіяльності. Особливу увагу дослідженню використання переваг мобільних гаджетів необхідно приділити у сфері розробки IT-продуктів адже розробники та споживачі значну частину часу проводять із мобільними пристроями. Зростання популярності мобільних пристроїв та програм призвело до значних змін у тому, як люди шукають та використовують інформацію. традиційно для тестування програмного забезпечення використовуються персональні комп’ютери які надають доступ до необхідної інформації (документація, тестові дані та звіти про помилки). Зростання складності програмного забезпечення, а також поширення та розвиток мобільних пристроїв зумовили потребу в пошуку більш зручних та гнучких способів пошуку та використання інформації.

Аналіз останніх досліджень і публікацій. Останні наукові дослідження у сфері пошуку інформації присвячені обґрунтованню вибору алгоритму пошуку різноформатних матеріалів шляхом аналізу контексту шуканих матеріалів та запитів користувача з метою підвищення точності результатів пошуку [1], дослідженню проблем та можливостей пошуку інформації в Інтернет [2], а також персоналізації пошуку на основі аналізу запитів користувачів [3]. Однак тема впровадження мобільних технологій у процес інформаційного пошуку у сфері тестування програмного забезпечення досі містить питання які потребують ретельного вивчення.

Мета статті полягає у дослідженні впливу мобільних технологій на інформаційний пошук у сфері тестування програмного забезпечення, зокрема їх впливу на пошук та використання інформації при тестуванні програмного забезпечення. У статті буде розглянуто мобільні інструменти та платформи, а також можливості їх використання для пошуку інформації, пов'язаної з тестуванням програмного забезпечення.

Виклад основного матеріалу. Зростання обсягу даних в мережі Інтернет вимагає від розробників та тестувальників програмного забезпечення опанування різними інструментами пошуку необхідної інформації, оскільки сьогодні не існує універсального розв'язання проблеми ефективного керування інформаційними потоками [1, с. 217; 2, с. 117].

Сучасні системи пошуку часто використовують такі основні алгоритми як Інвертований індекс, TF-IDF, BM25 (Окапі), а також алгоритми на основі штучного інтелекту для пошуку інформації за ключовими словами з фільтрами та сортуванням для покращення пошукового досвіду [1, с. 217; 2, с. 119].

Використання сучасних мобільних технологій робить можливим пошук необхідної інформації для тестування програмного забезпечення завдяки розвитку наступних інструментів:

- мобільні браузери які дозволять тестувальникам отримати доступ до інформації про досліджувані програмні продукти, необхідної документації, наявні помилки та інші ресурси через вебсайти.
- мобільні додатки, розроблені для тестування програмного забезпечення, для допомоги в знаходженні тестових даних, створенні сценаріїв тестів, відстеженні помилок та налагодженні комунікації між учасниками проєкту.
- мобільні соціальні мережі які можуть бути використані для обміну інформацією, досвідом та знаннями з іншими тестувальниками, а також для отримання підтримки та співпраці [2, с. 120].

Сьогодні для пошуку необхідної інформації з метою тестування програмного забезпечення мобільні технології пропонують широкий асортимент інструментів та платформ, серед яких можна виділити:

- інструменти для пошуку тестових даних: Appium, XCTest, EarlGrey [4-6];
- платформи для створення сценаріїв тестів: TestRail, Zephyr, Xray [7-9];
- мобільні соціальні мережі: LinkedIn, Twitter, Stack Overflow тощо.

Мобільні технології здатні допомогти українським підприємствам галузі IT покращити інформаційний пошук у сфері тестування програмного забезпечення. Нижче наведено перелік рекомендацій щодо підвищення ефективності застосування їх можливостей у професійній діяльності:

- підбір правильного інструментарію:
  - обрання мобільного браузера, оптимізованого для вебсайтів з інформацією про тестування програмного забезпечення;
  - встановити мобільні додатки, розроблені спеціально для тестування програмного забезпечення;
  - реєстрація у соціальних мережах і спеціальних групах присвячених обміну інформацією та досвідом між розробниками та тестувальниками програмного забезпечення.
- забезпечення доступу до необхідної інформації (документація, тестові дані та звіти про помилки) з мобільних пристроїв:
  - оптимізація вебсайтів для мобільних пристроїв, створення мобільних версій документів та публікація звітів у зручних форматах;
  - застосування хмарних сервісів для зберігання та синхронізації необхідної інформації;
  - створення та використання системи резервного копіювання та відновлення інформації.
- створення системи підвищення кваліфікації співробітників:
  - створення курсів для тестувальників щодо застосування мобільних технологій для пошуку інформації;
  - формування корпоративної культури, яка б заохочувала співробітників до самостійного вивчення мобільних інструментів та платформ.
- заохочення співпраці в проєктній команді:
  - застосування мобільних соціальних мереж та спеціальних груп для спілкування між тестувальниками програмного забезпечення;
  - використання мобільних інструментів для спільної роботи над проєктами тестування;

- створення онлайн-середовища та форумів для розробників та тестувальників програмного забезпечення для обміну знаннями та досвідом.

Сучасні мобільні технології допомагають розширити можливості пошуку необхідної інформації для розробки та тестування програмного забезпечення. Серед ключових переваг впровадження мобільних технологій в діяльність сучасних ІТ підприємств можна відмітити:

- мобільні пристрої дозволяють отримувати доступ до необхідної інформації з будь-якого місця та в будь-який час, завдяки оптимізації для роботи на екранах різних розмірів;
- підвищення ефективності пошуку інформації завдяки широкому функціоналу мобільних технологій (голосовий пошук, сканування QR-коду, створення сценаріїв, відстеження помилок, збереження корисних сторінок);
- економія часу працівників завдяки можливості оперативного реагування на зміни в проєкті завдяки комунікації між працівниками та ігноруванні потреби в перебуванні на робочому місці;
- наявність великого інструментарію для пошуку необхідної інформації, розширення переліку отриманих тестових даних (фото, відео).

Важливо зазначити, що мобільні технології на сучасному етапі розвитку не можуть повністю замінити функціонал традиційних персональних комп'ютерів, однак можуть бути корисними для доповнення інструментарію та розширення можливостей фахівців у галузі розробки та тестування програмного забезпечення.

Висновки. Мобільні технології відіграють все більшу роль у сфері тестування програмного забезпечення. Зростання складності програмного забезпечення та поширення мобільних пристроїв зумовили потребу в пошуку більш зручних та гнучких способів пошуку та використання інформації, необхідної для тестування. Сучасні системи пошуку використовують різні алгоритми для ефективного пошуку інформації за ключовими словами з фільтрами та сортуванням, а використання мобільних технологій дозволяє розробникам та тестувальникам ефективно шукати, отримувати та використовувати необхідну інформацію для тестування програмного забезпечення в будь-який час та в будь-якому місці. Подальші дослідження мають бути спрямовані на вивчення нових підходів та інструментів мобільного пошуку і доступу до інформації, що підвищить ефективність тестування програмного забезпечення.

Література

1. Савчук Т. О., Коханівський А. П. Обгрунтування вибору алгоритму пошуку різноформатних матеріалів в базах даних. Topical aspects of

modern scientific research. Proceedings of the 10th International scientific and practical conference. 2024. С. 216–220. URL: https://www.researchgate.net/profile/Khalina-Veronika/publication/381407380_STUDY_OF_THE_IMPACT_OF_THE_EXTERNAL_ENVIRONMENT_ON_THE_ACTIVITIES_OF_A_CONSTRUCTION_COMPANY/links/666bf113a54c5f0b9464ebf0/STUDY-OF-THE-IMPACT-OF-THE-EXTERNAL-ENVIRONMENT-ON-THE-ACTIVITIES-OF-A-CONSTRUCTION-COMPANY.pdf#page=216 (дата звернення: 27.06.2024).

2. Андреєв А. Пошук інформації в інтернеті: проблеми та можливості. Автоматизація та Приладобудування («Automation and Development of Electronic Devices» ADED-2024) [Електронний ресурс] : збірник студентських наукових статей. 2024. № 1. С. 116–121.

3. Ometsynska N. V., Bozhenko M. I. PERSONALIZATION OF SEARCH BASED ON ANALYSIS USER REQUESTS. Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences. 2024. Vol. 1, no. 1. P. 275–279. URL: https://doi.org/10.32782/2663-5941/2024.1.1/41 (date of access: 27.06.2024).

4. Welcome - Appium Documentation. Redirecting. URL: https://appium.io/docs/en/latest/ (date of access: 26.06.2024).

5. XCTest | Apple Developer Documentation. Apple Developer Documentation. URL: https://developer.apple.com/documentation/xctest (date of access: 27.06.2024).

6. Earl Grey: A fully automated TE curation and annotation pipeline. GitHub. URL: https://github.com/TobyBaril/EarlGrey (date of access: 27.06.2024).

7. Test Case Management & Orchestration Software by TestRail. TestRail | The Quality OS for QA Teams. URL: https://www.testrail.com/ (date of access: 28.06.2024).

8. Jira and Zephyr: Track Your Team's Progress | Atlassian. Atlassian. URL: https://www.atlassian.com/devops/testing-tutorials/jira-zephyr-scale-testing (date of access: 26.06.2024).

9. Xray - Native Test Management for Jira. Xray - Native Test Management for Jira. URL: https://www.getxray.app/ (date of access: 27.06.2024).

DOI: 978-966-301-266-7/1.2024.140

Яровий Р.О.
https://orcid.org/0000-0001-8978-8137
e-mail: roman.yaroviy@e-u.edu.ua

Улічев О.С.
https://orcid.org/0000-0003-3736-9613
e-mail: o.ulichev@e-u.edu.ua

ДЕЯКІ ПРОБЛЕМНІ АСПЕКТИ ОБ'ЄКТНО-ОРІЄНТОВАНОГО ПРОГРАМУВАННЯ

Анотація. У статті проведено детальний аналіз об'єктно-орієнтованого програмування (ООП) та функціонального програмування (FP) у контексті сучасних кіберсистем. Розглядаються основні недоліки ООП, такі як проблеми зі спадковістю, інкапсуляцією та ієрархією класів. Зокрема, обговорюються проблеми крихкої бази класів, діамантова проблема та неналежний доступ до інкапсульованих даних. Натомість, функціональне програмування пропонує переваги, зокрема іммутабельність даних, відсутність побічних ефектів та гнучкість у розробці модульного коду. Стаття наводить приклади з кодом для кожного підходу, демонструючи переваги FP у спрощенні відлагодження та тестування коду. У висновках пропонується використовувати гібридні методології, що поєднують переваги обох підходів для створення надійних та ефективних програмних рішень.

Ключові слова: Об'єктно-орієнтоване програмування (ООП), функціональне програмування (FP), спадковість, інкапсуляція, ієрархія класів, іммутабельність, побічні ефекти, модульність, розробка програмного забезпечення.

Виклад основного матеріалу. У сучасних кіберсистемах об'єктно-орієнтоване програмування (ООП) довгий час було домінуючим підходом завдяки своїм ключовим концепціям: спадковості, інкапсуляції та поліморфізму. Проте, з часом виявилися певні недоліки цього підходу, зокрема проблеми з повторним використанням коду та підтримкою великих проєктів. Альтернативою ООП є функціональне програмування (FP), яке має свої переваги, зокрема, іммутабельність даних та відсутність побічних ефектів, що спрощує відлагодження та тестування коду. Метою цієї статті є аналіз недоліків ООП та дослідження переваг FP у контексті сучасних вимог до програмного забезпечення.

Проблемні аспекти об'єктно-орієнтованого програмування

Спадковість:

Спадковість у ООП може призвести до проблем, таких як крихка база класів (fragile base class problem) та діамантова проблема (diamond problem). Це ускладнює підтримку та розвиток програмного забезпечення, оскільки зміни у базовому класі можуть негативно вплинути на похідні класи.

Приклад:

```
class Person:
    def __init__(self, name, age):
        self.name = name
        self.age = age

class Student(Person):
    def __init__(self, name, age, student_id):
        super().__init__(name, age)
        self.student_id = student_id

# Додавання нової властивості у базовий клас
class Person:
    def __init__(self, name, age, address):
        self.name = name
        self.age = age
        self.address = address  # Нове поле

# Це порушить існуючі підкласи
```

Інкапсуляція:

Інкапсуляція є однією з основних переваг ООП, але вона також може створювати труднощі. Наприклад, проблема з посиланнями (The Reference Problem) виникає тоді, коли функції працюють з посиланнями на об'єкти, що призводить до небезпеки неналежного доступу до даних.

Приклад:

```
class Employee:
    def __init__(self, name, salary):
        self.__name = name
        self.__salary = salary

    def get_salary(self):
        return self.__salary

# Проблема доступу до приватних даних
emp = Employee("John", 50000)
print(emp._Employee__salary)  # Неправильний доступ до інкапсульованих даних
```

Ієрархія класів:

Ієрархічна структура класів часто не відповідає реальним потребам, що може призводити до плутанини та ускладнення коду. Замість цього, реальні системи частіше використовують ієрархії включення (Containment).

Приклад:

```
class Product:
    def __init__(self, name, price):
        self.name = name
        self.price = price

class Electronics(Product):
    def __init__(self, name, price, warranty):
        super().__init__(name, price)
        self.warranty = warranty

class Food(Product):
    def __init__(self, name, price, expiration_date):
        super().__init__(name, price)
        self.expiration_date = expiration_date

# Додавання нового типу продукту може вимагати значних змін в ієрархії
```

Переваги функціонального програмування

Іммутабельність:

FP базується на концепції незмінності даних, що значно спрощує відлагодження та тестування коду, оскільки функції не мають побічних ефектів.

Приклад:

```
from collections import namedtuple
Transaction = namedtuple('Transaction', ['id', 'amount'])
def process_transaction(transactions, transaction):
    return transactions + [transaction]
# Незмінність даних дозволяє легко відстежувати зміни
transactions = []
new_transaction = Transaction(id=1, amount=100)
transactions = process_transaction(transactions, new_transaction)
```

Відсутність побічних ефектів:

Одна з ключових переваг FP полягає в тому, що функції не змінюють стан програми, що дозволяє легко прогнозувати поведінку системи та зменшує кількість помилок.

Приклад:

```
def add(a, b):
    return a + b
# Функція add не змінює глобальний стан
result = add(5, 3)
print(result)  # 8
```

Гнучкість та модульність:

FP сприяє створенню модульного та гнучкого коду, який легше підтримувати та розширювати.

Приклад:

```
def filter_even_numbers(numbers):
    return list(filter(lambda x: x % 2 == 0, numbers))
def square_numbers(numbers):
    return list(map(lambda x: x * x, numbers))
# Модульність дозволяє легко комбінувати функції
numbers = [1, 2, 3, 4, 5]
even_numbers = filter_even_numbers(numbers)
squared_numbers = square_numbers(even_numbers)
print(squared_numbers)  # [4, 16]
```

Висновки. Попри значні недоліки, об'єктно-орієнтоване програмування все ще залишається корисним у багатьох сферах розробки програмного забезпечення. Проте, функціональне програмування пропонує ефективніші рішення для сучасних проблем розробки, зокрема у контексті великих проєктів та складних систем. Найкращим підходом може бути використання гібридних методологій, які поєднують переваги ООП та FP, забезпечуючи більш надійні та ефективні рішення для різноманітних проєктів.

Література

1. Buch G. Obektno-orientirovannyj analiz i proektirovanie s primerami prilozhenij / G. Buch, Robert, A. Maksimchuk i dr. ; per. s angl. – 3-e izd. – M. : ID «Vilyams», 2020. – 720 s.
2. Dinamika populyarnosti obektno-orientirovannogo i funkcionalnogo programmirovaniya [Elektronnyj resurs] // Google Trends. –

Rezhim dostupa : https://trends.google.ru/trends/explore?date=today%205-y&q=%2Fm%2F05prj,%2Fm%2F02ykw

3. Пратт Т. Дж. Об'єктно-орієнтоване програмування: теорія та практика.
4. Шерер, П. Функціональне програмування: принципи та практики.