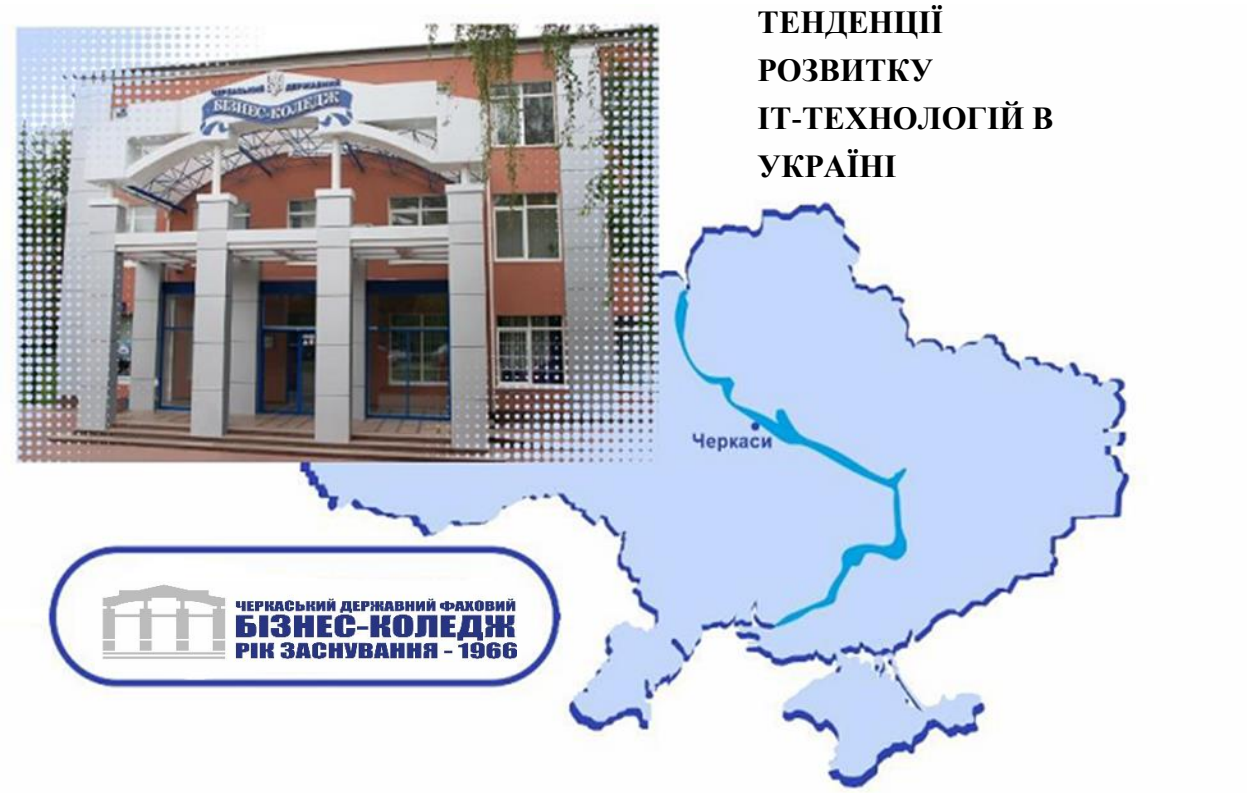

МАТЕРІАЛИ

XVII Студентської

науково-практичної конференції

студентів, аспірантів та молодих вчених

за тематикою
«Тенденції розвитку
ІТ-технологій в Україні»

26-27 березня 2025 р.
м. Черкаси

Міністерство освіти і науки України
Черкаський державний фаховий бізнес-коледж

МАТЕРІАЛИ

XVII Студентської

науково-практичної конференції

студентів, аспірантів та молодих вчених

за тематикою

«Тенденції розвитку ІТ-технологій в Україні»

26-27 березня 2025 р.
м. Черкаси

Матеріали XVI Студентської науково-практичної конференції студентів, аспірантів та молодих вчених за тематикою «Тенденції розвитку ІТ-технологій в Україні»: збірка наукових праць. Черкаси, 2025, 176 с.

Доповіді наукової конференції містять результати досліджень за наступними напрямками: обробка та захист інформації; інженерні підходи до розробки програмного забезпечення; інформаційні технології в галузевих рішеннях; робототехніка та адміністрування комп'ютерних систем.

Роботи друкуються в авторській редакції. В збірці максимально зменшено втручання в обсяг та структуру відібраних до друку матеріалів. Редакційна колегія не несе відповідальності за достовірність досліджень, матеріалів та результатів досліджень, що надано в рукописах, та залишає за собою право не поділяти погляди деяких авторів на ті чи інші питання, висвітлені в роботах.

Збірник становить інтерес для студентів, аспірантів, викладачів та наукових працівників.

Оргкомітет конференції

Азьмук Н.А. – заступник директора з навчально-методичної роботи ЧДБК, д-р екон. наук - голова оргкомітету;

Заболотній С.В. - професор кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, д-р тех. наук;

Хотунов В.І. – завідувач відділення бакалаврської підготовки ЧДБК, канд. пед. наук; доцент;

Захарова М.В. – доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. тех. наук;

Бурмістров С.В. – доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. тех. наук;

Ночевнов Д.П. – доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. тех. наук;

Касьян Т.К. – завідувач кафедри дизайну та соціально-культурних дисциплін ЧДБК, канд. пед. наук;

Люта М.В. – завідувач відділення інженерії програмного забезпечення ЧДБК;

Бреус Р.В. – відповідальний секретар, доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. тех. наук.

ЗМІСТ

Секція 1.

ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

УДК 621.396.96:004

СИСТЕМА ІНТЕГРАЦІЇ КРИПТОГРАФІЧНИХ МЕТОДІВ У СЕРВІСИ ДЛЯ ЗАХИСТУ ДАНИХ КОРИСТУВАЧІВ

Гапченко В.С.
vovagapcenko3@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М.В.
м.Черкаси, Україна

Захист інформації у сучасних інформаційних системах набуває особливої актуальності через зростання обсягів даних та постійне підвищення вимог до безпеки мережевих сервісів. Інтеграція криптографічних методів дозволяє забезпечити конфіденційність, цілісність і автентичність інформації, що є критично важливим для захисту даних користувачів. Сучасні підходи до криптографічного захисту базуються на використанні як симетричних, так і асиметричних алгоритмів, кожен з яких має свої особливості та сфери застосування [5].

Криптографічні алгоритми поділяються на симетричні, які використовують один спільний секретний ключ, та асиметричні, що застосовують пару ключів – відкритий і закритий. Наприклад, алгоритм Advanced Encryption Standard (AES) демонструє високу ефективність завдяки використанню ключів довжиною 128, 192 або 256 біт, що дозволяє забезпечити високий рівень захисту за оптимальних обчислювальних витрат. Проте, для задач автентифікації та цифрового підпису частіше використовуються асиметричні алгоритми, такі як RSA або ECC, які незважаючи на більші обчислювальні вимоги, забезпечують додатковий рівень захисту завдяки використанню пари ключів [4].

Базові співвідношення відображають основні принципи симетричного шифрування, які використовуються, зокрема, в алгоритмі AES [2].

Для ілюстрації принципу роботи симетричного шифрування розглянемо спрощену математичну модель:

$$C = E(K, P) \quad (1)$$

де

C – зашифрований текст,

E –функція шифрування,

K – ключ шифрування,

P– відкритий текст.

Для відновлення вихідної інформації застосовується функція дешифрування, що задається наступним співвідношенням:

$$P = D(K,C) \quad (2)$$

де

P – plaintext (відкритий текст),

D – функція дешифрування,

K – ключ дешифрування,

C – ciphertext (шифротекст).

Застосування криптографічних методів у сервісах для захисту даних охоплює не лише шифрування, але й комплекс заходів, спрямованих на безпечну автентифікацію та забезпечення цілісності переданої інформації. Сучасні мережеві сервіси, зокрема, використовують протоколи TLS/SSL, що забезпечують захищене з'єднання між користувачем і сервером. За допомогою цих протоколів встановлюється сеанс, під час якого дані шифруються за допомогою як асиметричних алгоритмів (для обміну ключами), так і симетричних (для безпосереднього шифрування інформації). Крім того, впровадження багатофакторної автентифікації (наприклад, двофакторної аутентифікації) значно знижує ризик несанкціонованого доступу, оскільки вимагає підтвердження особистості користувача через додатковий канал, наприклад, мобільний телефон або біометричні дані [7].

Інтегровані системи захисту даних враховують як технологічні аспекти, так і правову базу. Закон України «Про захист персональних даних» (№2297-VI) встановлює нормативні вимоги до організацій, що обробляють персональні дані,

що підкреслює необхідність впровадження сучасних криптографічних методів як одного з ключових елементів інформаційної безпеки. Водночас, використання цифрових підписів і сертифікатів (наприклад, X.509) дозволяє гарантувати автентичність джерел інформації та запобігати модифікації даних під час їх передачі.

Таблиця 1. Основні характеристики деяких ключових криптографічних алгоритмів

№	Алгоритм	Тип	Довжина ключа (біт)	Рівень безпеки
1	AES	Симетричний	128, 192, 256	Високий
2	RSA	Асиметричний	1024, 2048, 4096	Високий
3	SHA-256	Хеш-функція	256	Високий
4	MD5	Хеш-функція	128	Низький (застарілий)

Джерело: створено автором на основі джерел [1, 5]

Процес інтеграції криптографічних засобів у сервіси представлено на рис. 1, де дані спочатку проходять етап автентифікації, після чого здійснюється шифрування за допомогою відповідних алгоритмів. Захищена передача здійснюється через протоколи TLS/SSL, що дозволяє мінімізувати ризики перехоплення або несанкціонованого доступу до даних [4].

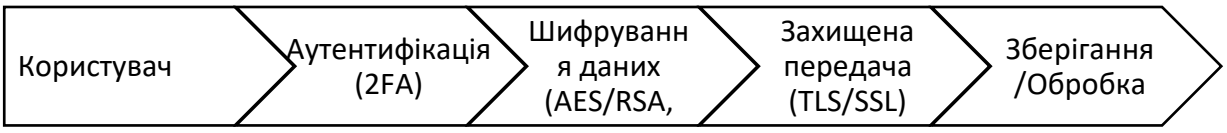

Рисунок 1. Інтеграція криптографічних засобів у сервіси

Таким чином, інтеграція криптографічних методів у сервіси для захисту даних користувачів є комплексним підходом, який враховує як технічні, так і правові аспекти захисту інформації. Основним завданням є створення системи, що поєднує ефективне шифрування, автентифікацію та контроль цілісності даних, що сприяє мінімізації ризиків кібератак та несанкціонованого доступу. Для реалізації такого підходу використовуються як сучасні технології, представлені в міжнародних стандартах і публікаціях, так і вимоги національного законодавства.

Список використаних джерел

1. Ваш повний посібник з SSL/TLS та HTTPS. DreamHost Blog . URL: https://www.dreamhost.com/blog/uk/ostatochnii-posibnik-z-ssl-tls/ (дата звернення: 15.03.2025)
2. Загальні відомості про AES-шифрування – TechVizor . URL: https://techvizor.info/zagalni-vidomosti-pro-aes-shyfruvannya/ (дата звернення: 19.03.2025).
3. Про захист персональних даних. Офіційний вебпортал парламенту України . URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 19.03.2025).
4. Цілісність інформації – Вікіпедія . URL::https://uk.wikipedia.org/wiki/Цілісність_інформації (дата звернення: 13.03.2025).
5. Шифрування: Типи й алгоритми. Що це і який тип кращий? – hostkoss blog . URL: https://hostkoss.com/b/uk/encryption-types-algorithms/ (дата звернення: 19.03.2025).
6. Що таке розширений стандарт шифрування (AES) і як він пов’язаний з NIST? – Lazarus Alliance . URL: https://lazarusalliance.com/uk/what-is-advanced-encryption-standard-aes-and-how-is-it-related-to-nist/ (дата звернення: 19.03.2025).
7. Як дати записуються у коді – 1С-СЕД . URL: https://1c- ed.com.ua/prohid/?Як%20забезпечити%20цілісність%20даних%20у%20БД (дата звернення: 15.03.2025).
8. TLS протокол – що це таке та як він захищає ваші дані в Інтернеті – Cityhost . URL: https://cityhost.ua/uk/blog/scho-take-protokol-tls-yak-vin-pracyu-ta-vid-chogo-zahischa (дата звернення: 19.03.2025).

УДК 004.891

МАЙБУТНЄ ЛЮДСТВА З AI – ЧИ ЗАМІНИТЬ ШТУЧНИЙ ІНТЕЛЕКТ ЛЮДИНУ?

Хлівенко Р.А.
r.hlivenko@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Ратайчук П.Є.
м. Черкаси, Україна

Штучний інтелект (AI) є однією з найбільш обговорюваних технологій сучасності, яка має потенціал змінити всі аспекти людського життя. Від автоматизації промислових процесів до розумних асистентів та діагностичних систем у медицині, AI відіграє все важливішу роль у нашому повсякденному житті. Однак, поряд з обіцянками науково-технічного прогресу виникають і питання, пов’язані з етикою, безпекою та впливом на людство в цілому. Чи замінить AI людину, чи стане лише потужним інструментом у її руках? Це питання потребує глибокого аналізу.

Штучний інтелект пропонує величезні можливості для покращення різних сфер людської діяльності. Насамперед, це стосується автоматизації рутинних процесів, що дозволяє значно підвищити ефективність та точність виконання завдань. Наприклад, використання AI в промисловості дозволяє оптимізувати виробничі лінії, покращити контроль якості та зменшити кількість помилок.

Важливим напрямком є застосування AI в медицині. Алгоритми глибокого навчання використовуються для діагностики захворювань, аналізу медичних зображень та розробки нових методів лікування. Персоналізована медицина, побудована на основі AI, здатна надавати індивідуальні рекомендації для пацієнтів, що підвищує ефективність лікування.

Крім того, AI знаходить застосування у кібербезпеці. Системи на базі AI здатні виявляти загрози та аномалії у мережах в реальному часі, що забезпечує більш надійний захист даних. В освітній сфері AI допомагає створювати адаптивні системи навчання, що враховують індивідуальні потреби учнів.

Попри значні переваги, AI створює і серйозні загрози. Однією з основних

проблем є упередженість алгоритмів, що може призвести до дискримінації та неправильного прийняття рішень. Неправильне навчання або навмисне маніпулювання даними можуть викликати небажані наслідки.

Використання AI може призвести до безробіття через автоматизацію багатьох професій. Особливо це стосується сфер, де рутинні завдання можуть бути виконані швидше і точніше за допомогою машин. Залежність від технологій також створює ризик зниження критичного мислення та навичок у людей.

Одна з найбільших загроз – можливість неконтрольованого розвитку AI. Якщо штучний інтелект вийде за межі контролю людини, це може призвести до катастрофічних наслідків. Саме тому необхідно створювати механізми регулювання та контролю над використанням AI.

Незважаючи на всі досягнення у сфері штучного інтелекту, повна заміна людини є малоймовірною. AI не здатний відтворити творчість, емоції та моральні цінності. Більше того, AI діє на основі завантажених даних і не має власної свідомості чи самосвідомості.

AI залишається інструментом, який може значно покращити можливості людини, але не здатний повністю замінити її. Його ефективність залежить від людського контролю та спрямування. Гармонійна взаємодія між людиною та AI є ключем до подальшого розвитку технологій.

Розвиток AI потребує встановлення чітких етичних стандартів та регулюючих норм. Важливо створити законодавчі рамки, що забезпечуватимуть безпеку та прозорість використання AI-технологій.

Також необхідно зосередитися на навчанні та перекваліфікації фахівців, оскільки автоматизація вимагає нових знань та вмінь. Підвищення обізнаності щодо AI та впровадження гуманітарних цінностей у технологічний прогрес дозволить зменшити ризики та максимізувати користь від використання AI.

AI є надзвичайно потужним інструментом, який може допомогти людству вирішувати глобальні проблеми та значно покращити якість життя. Однак, він не здатний повністю замінити людину, оскільки не має емоцій, креативності та морального компасу. Основне завдання – забезпечити відповідальне та безпечне

використання AI на благо суспільства.

Список використаних джерел:

1. GPT-1 to GPT-4: Each of OpenAI’s GPT Models Explained and Compared. URL: https://www.makeuseof.com/gpt-models-explained-and-compared/ (дата звернення: 17.03.2025).
2. How Does ChatGPT Work?. URL: https://www.baeldung.com/cs/chatgpt-model (дата звернення: 14.03.2025)
3. GPT-4 is OpenAI’s most advanced system, producing safer and more useful responses. URL: https://openai.com/gpt-4 (дата звернення: 19.03.2025).
4. New models and developer products announced at DevDay. URL: https://openai.com/blog/new-models-and-developer-products-announced-at-devday (дата звернення: 19.03.2025).

УДК 004.9:343

АВТОМАТИЗОВАНІ СИСТЕМИ НА ОСНОВІ ШІ У СФЕРІ БЕЗПЕКИ

Лисенкова К. С.
qwki256103@gmail.com
Ділягіна А. А.
aann61608@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Автоматизовані системи на основі штучного інтелекту відіграють все більшу роль у сфері безпеки, оскільки дозволяють ефективно аналізувати великі обсяги даних, прогнозувати потенційні загрози та оперативно реагувати на інциденти. Сучасні методи штучного інтелекту (ШІ), зокрема машинне навчання, глибоке навчання та обробка природної мови, дозволяють створювати адаптивні та автономні системи, які забезпечують вищий рівень захисту в порівнянні з традиційними підходами.

Одним із ключових напрямків застосування ШІ в безпеці є моніторинг

кіберпростору та виявлення аномалій. ШІ-алгоритми можуть аналізувати поведінкові моделі користувачів та пристроїв у мережі, виявляючи відхилення від норми, які можуть свідчити про можливу атаку. Наприклад, технології глибокого навчання використовуються для аналізу логів трафіку та пошуку ознак шкідливої активності, таких як спроби несанкціонованого доступу або розповсюдження шкідливого програмного забезпечення. Такі підходи значно скорочують час реагування на потенційні загрози та підвищують точність виявлення аномальної активності.

Ще одним важливим напрямом є автоматизація реагування на інциденти безпеки. Традиційні методи реагування потребують значних людських ресурсів, тоді як штучний інтелект може виконувати ці завдання швидше та ефективніше. Наприклад, система на основі ШІ здатна автоматично ідентифікувати спроби фішингових атак, блокувати підозрілі IP-адреси або шифрувати вразливі дані для запобігання їх витоку. Деякі рішення передбачають використання так званих «self-healing» систем, які здатні самостійно відновлювати нормальну роботу після атаки, аналізуючи її природу та адаптуючи захисні механізми для запобігання повторних інцидентів.

Інтеграція штучного інтелекту з іншими технологіями дозволяє створювати комплексні системи безпеки, здатні ефективно протидіяти складним загрозам. Наприклад, у поєднанні з блокчейном ШІ може підвищувати рівень захисту конфіденційних даних, забезпечуючи їхню автентичність та незмінність. Біометричні системи розпізнавання осіб, що використовують алгоритми глибокого навчання, вже сьогодні застосовуються для підвищення рівня фізичної безпеки на стратегічних об’єктах. Впровадження Інтернету речей (IoT) у сферу безпеки створює додаткові виклики, оскільки розширює поверхню атак, однак ШІ може аналізувати величезні потоки даних, що генеруються пристроями IoT, для виявлення загроз та підвищення захисту таких мереж.

Разом із перевагами використання штучного інтелекту в безпеці виникають і значні виклики. Одним із головних питань є конфіденційність та захист персональних даних. Автоматизовані системи безпеки обробляють величезні

обсяги інформації про користувачів, що потребує створення чітких механізмів регулювання та контролю доступу. Крім того, важливим аспектом є забезпечення прозорості алгоритмів ШІ, щоб уникнути потенційних упереджень та некоректних рішень, особливо в критичних сферах, таких як правозастосування чи фінансова безпека.

Ще одним викликом є використання штучного інтелекту кіберзлочинцями. ШІ здатен автоматизувати створення фішингових атак, обхід захисних механізмів та навіть розробку нових форм шкідливого програмного забезпечення. Це означає, що системи безпеки мають постійно вдосконалюватися та адаптуватися до нових загроз. Наприклад, розвиток генеративного ШІ дозволяє створювати фальсифіковані голосові повідомлення або відео (deepfake), що може бути використано для маніпуляцій, шантажу або компрометації осіб і організацій.

У майбутньому впровадження штучного інтелекту у сферу безпеки вимагатиме не лише технічного вдосконалення, а й розробки нових нормативних та етичних стандартів. Важливо знайти баланс між ефективністю систем безпеки та захистом прав людини. Використання ШІ для моніторингу та аналізу поведінки людей може викликати серйозні занепокоєння щодо надмірного контролю та потенційних зловживань. Саме тому розробка політик, які регулюватимуть використання штучного інтелекту в безпеці, є необхідною умовою його подальшого розвитку.

Штучний інтелект продовжує змінювати підходи до забезпечення безпеки, роблячи їх більш адаптивними, ефективними та автономними. Проте його подальший розвиток потребує обережного та відповідального впровадження, що враховуватиме як технічні аспекти, так і соціальні наслідки. Успішне використання ШІ у сфері безпеки залежатиме від тісної співпраці між науковцями, технологічними компаніями, державними органами та громадськістю для створення надійних, прозорих та етичних рішень.

Список використаних джерел

1. Microsoft. What is AI for cybersecurity? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity (дата звернення: 24.03.2025).
2. Інституційний репозитарій Вінницького національного технічного університету. Автоматизовані системи безпеки на основі штучного інтелекту URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/42057/20610.pdf (дата звернення: 24.03.2025).
3. Mindscope.biz.ua. Тенденції у використанні штучного інтелекту для покращення реагування охоронних систем на загрози URL: https://mindscope.biz.ua/tendencziyi-u-vykorystanni-shtuchnogo-intelektu-dlya-pokrashhennya-reaguvannya-ohoronnyh-system-na-zagrozy/ (дата звернення: 24.03.2025).
4. Європейська бізнес асоціація (EBA). Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам/ URL: https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam/ (дата звернення: 24.03.2025).

УДК 004.891:17

ШТУЧНИЙ ІНТЕЛЕКТ У КОНТЕКСТІ МОРАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ

Закорчменна А. О.
a.zakorchmenna@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Злочевська Д. С.
м. Черкаси, Україна

Штучний інтелект активно впроваджується у різні сфери життя, що породжує низку етичних викликів, пов’язаних із питанням моральної відповідальності. Важливо визначити, хто саме повинен відповідати за дії автономних систем, які можуть ухвалювати рішення без прямого контролю

людини. Традиційно моральна відповідальність передбачає усвідомлення наслідків власних вчинків і здатність діяти відповідно до етичних норм, проте застосування цього поняття до ШІ є проблематичним.

Питання морального агентства ШІ залишається відкритим. Моральним агентом можна вважати суб'єкта, здатного усвідомлювати свої вчинки, мати наміри та відповідати за результати своїх дій. Людина володіє такими характеристиками завдяки свідомості, емпатії та соціальному досвіду. Натомість сучасні системи ШІ, хоча й демонструють автономну поведінку, діють на основі алгоритмів і статистичних моделей, а їхня здатність до самостійного ухвалення моральних рішень є дискусійною. Навіть найскладніші моделі нейромереж не мають справжнього розуміння етичних принципів, оскільки їхні дії є результатом прогнозування, а не усвідомленого вибору. Деякі дослідники вважають, що майбутній розвиток ШІ може привести до створення систем, які зможуть самостійно оцінювати етичні наслідки своїх рішень. Проте поки що штучний інтелект не має властивостей, які дозволяють вважати його суб'єктом моральної відповідальності.

Оскільки ШІ не є самостійним моральним агентом, відповідальність за його дії має бути покладена на людину. Важливо розглянути різні рівні цієї відповідальності. Розробники та програмісти несуть важливу роль, оскільки саме вони створюють алгоритми та визначають принципи роботи ШІ. Від їхніх рішень залежить, чи буде система діяти неупереджено і чи зможе вона уникнути потенційних ризиків. Проте передбачити всі можливі наслідки використання ШІ неможливо, особливо якщо йдеться про системи, що самонавчаються.

Окрім розробників, відповідальність повинні нести компанії, які впроваджують ШІ у комерційних або державних проєктах. Вони визначають, у яких сферах використовуватиметься технологія, і встановлюють механізми контролю за її функціонуванням. Корпорації та державні органи повинні забезпечувати дотримання етичних стандартів та регламентів, щоб мінімізувати ризики, пов'язані з автономними системами.

Важливо враховувати відповідальність кінцевих користувачів, які

взаємодіють із ШІ у повсякденній діяльності. Наприклад, лікарі, що використовують системи на основі штучного інтелекту для діагностики захворювань, або судді, які звертаються до алгоритмів аналізу судових рішень, залишаються відповідальними за остаточні рішення. Чим більш автономним є ШІ, тим складніше визначити межі відповідальності між користувачем та технологією.

Використання ШІ породжує низку етичних викликів, одним із яких є проблема помилок. Якщо система ухвалює рішення, що призводить до негативних наслідків, потрібно визначити, хто відповідатиме за це. Наприклад, у випадку аварії за участю автономного автомобіля постає питання про відповідальність виробника, розробників програмного забезпечення або власника транспортного засобу.

Дискримінація, що виникає через алгоритмічні упередження, також є важливим викликом. ШІ навчається на основі великих обсягів даних, які можуть містити соціальні стереотипи. Це може призвести до несправедливого ставлення до певних груп людей у процесі ухвалення рішень у сферах кредитування, прийому на роботу або правозастосування. Використання штучного інтелекту у військовій сфері додає ще більше етичних дилем. Автономні бойові системи можуть приймати рішення про застосування сили без прямого втручання людини, що ускладнює контроль за їхніми діями.

Для регулювання моральної відповідальності за використання ШІ необхідно розробити юридичні механізми, що враховують специфіку автономних систем. На міжнародному рівні тривають дискусії щодо правового статусу ШІ та стандартів його використання. Важливими напрямами є запровадження ліцензування розробників, створення етичних кодексів для компаній, що працюють у сфері штучного інтелекту, а також розробка законодавчих актів для регулювання використання ШІ у критично важливих сферах.

Окрім правових інструментів, значну роль відіграють етичні принципи, які розробляються технологічними компаніями. Деякі корпорації, такі як Google і Microsoft, впроваджують внутрішні стандарти відповідального використання

ШІ, однак через відсутність єдиних міжнародних норм їхня ефективність залишається обмеженою. Технологічні підходи, такі як розвиток методів пояснюваного ШІ, можуть допомогти підвищити прозорість роботи алгоритмів, що сприятиме кращому розумінню рішень, які вони ухвалюють.

Залежно від подальших досягнень у сфері штучного інтелекту можна розглянути кілька можливих сценаріїв розвитку питання моральної відповідальності. Один із варіантів передбачає збереження чинної моделі, за якої відповідальність лежить виключно на людині. Інший сценарій допускає створення гібридних моделей відповідальності, за яких ШІ визнається частково автономним агентом, а його дії регулюються спеціальними юридичними нормами. У разі досягнення рівня загального штучного інтелекту питання моральної відповідальності може потребувати кардинального перегляду, адже ШІ потенційно зможе ухвалювати рішення на основі самостійних етичних міркувань.

Проблема моральної відповідальності у контексті використання штучного інтелекту є однією з ключових етичних дилем сучасного суспільства. Оскільки поточні технології не дозволяють вважати ШІ самостійним моральним агентом, відповідальність повинна бути покладена на розробників, компанії та користувачів. Для уникнення етичних ризиків необхідно розробляти ефективні правові механізми, впроваджувати етичні стандарти та покращувати технологічні рішення, що забезпечать прозорість і контрольованість рішень штучного інтелекту. Подальший розвиток технологій вимагатиме адаптації цих підходів, щоб уникнути ситуацій, коли автономні системи діятимуть без належного контролю та відповідальності.

Список використаних джерел

1. Які етичні загрози несе використання штучного інтелекту. Speka: медіа про підприємництво та технології. URL: https://speka.media/trendi-si-yaki-eticni-zagrozi-nese-vikoristannya-stucnogo-intelektu-v4q3wp (дата звернення: 13.03.2025).

2. Робоетика. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Робоетика.
3. Етика штучного інтелекту. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Етика_штучного_інтелекту (дата звернення: 13.03.2025).
4. Штучний інтелект та його застосування у різних сферах. Друкарня. URL: https://drukarnia.com.ua/articles/shtuchnii-intelekt-ta-iogo-zastosuvannya-u-riznikh-sferakh-WPHL2 (дата звернення: 13.03.2025).

УДК 004.94:004.8

СУЧАСНІ ТЕХНОЛОГІЇ РЕАЛІЗАЦІЇ ВИЯВЛЕННЯ ОБ'ЄКТІВ

Нечко Д. С.
dimanechkoq11@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Марченко С. В.
м. Черкаси, Україна

Виявлення об'єктів є одним із ключових напрямів розвитку комп'ютерного зору, що має значний вплив на автоматизацію та оптимізацію різних галузей. Застосування методів глибокого навчання та нейромережевих архітектур забезпечує високу точність і швидкодію при розпізнаванні об'єктів у реальному часі. У промисловості ця технологія використовується для контролю якості продукції, моніторингу виробничих процесів та автоматизації складських операцій. У сфері безпеки виявлення об'єктів підтримує роботу систем відеоспостереження, біометричної ідентифікації та виявлення аномальної поведінки, що підвищує рівень громадської безпеки. У транспортній галузі алгоритми комп'ютерного зору є основою для автономних транспортних засобів, допомагаючи їм ідентифікувати інші автомобілі, пішоходів та дорожні знаки, що критично важливо для безпечного пересування. Іншими галузями застосування є медицина, роздрібна торгівля тощо. Таким чином, виявлення об'єктів є критично важливою технологією, що забезпечує нові можливості для автоматизації, підвищення продуктивності та безпеки у різних сферах діяльності. З огляду на стрімкий розвиток алгоритмів глибокого навчання та зростання

обчислювальних потужностей, подальші дослідження у цій галузі відкривають перспективи для ще більш ефективних і точних систем розпізнавання об'єктів.

Методи виявлення об'єктів у цифрових зображеннях та відеопотоках значно розвинулись, переходячи від класичних алгоритмів до сучасних моделей глибокого навчання. Основними етапами еволюції цієї технології є використання традиційних методів на основі інформаційних ознак, впровадження згорткових нейронних мереж (CNN), адаптація архітектур трансформерів і подальші вдосконалення в напрямі підвищення продуктивності та ефективності.

Традиційні методи були обмежені через необхідність ручного вибору ознак і високу обчислювальну складність. Революційним проривом у виявленні об'єктів стало впровадження згорткових нейронних мереж, які автоматично навчаються витягувати релевантні ознаки. Однією з перших ефективних архітектур стала R-CNN (Regions with CNN), яка використовувала попереднє генерування регіонів-кандидатів для об'єктів та їх класифікацію. Удосконалені версії, такі як Fast R-CNN [1] та Faster R-CNN [2], значно зменшили час обчислень завдяки впровадженню мережі генерації регіонів (Region Proposal Network, RPN).

Останнім часом у комп'ютерному зорі набули популярності архітектури, засновані на механізмах самоуваги (self-attention), що використовуються в трансформерах. Одним із перших підходів став DETR (Detection Transformer) [3], який пропонує повністю диференційовану модель без необхідності в регіональних пропозиціях. Завдяки глобальному механізму уваги DETR забезпечує високу точність розпізнавання складних сцен, однак має обмеження у швидкості навчання. Подальші покращення, такі як Deformable DETR [4], дозволили прискорити збіжність моделі, зберігаючи переваги трансформерної архітектури.

Інші підходи, такі як Swin Transformer [5], застосовують ієрархічну структуру для зменшення обчислювальних витрат, що робить їх ефективними для детекції та сегментації об'єктів. Комбінація CNN і трансформерів у гібридних моделях, наприклад, в EfficientViT [6], демонструє перспективність

такого напрямку.

Для ще більшої оптимізації з'явилися одноетапні моделі, такі як YOLO (You Only Look Once) [7] та SSD (Single Shot MultiBox Detector) [8], які поєднували детекцію та класифікацію в єдиній моделі, що дозволило досягти високої швидкодії. Сучасні версії, такі як YOLOv11 та EfficientDet [9], оптимізовані для використання в реальному часі на мобільних пристроях і вбудованих системах.

Реалізація моделей виявлення об'єктів значною мірою базується на високорівневих бібліотеках для глибокого навчання, які забезпечують оптимізацію обчислень та підтримку апаратного прискорення. Найпопулярнішими фреймворками є TensorFlow та PyTorch, що надають широкий набір інструментів для розробки, навчання та оптимізації нейромережевих моделей.

Для реалізації детекторів часто використовуються спеціалізовані бібліотеки, такі як Detectron2 [10], яка підтримує сучасні архітектури (Faster R-CNN, Mask R-CNN, Cascade R-CNN). Іншою популярною платформою є MMDetection [11], яка пропонує модульну структуру для експериментування з моделями та їх адаптації до конкретних завдань. У задачах реального часу ефективним є використання YOLOv11, який підтримується фреймворком Ultralytics, оптимізований для високошвидкісної обробки відеопотоків та мобільних пристроїв.

Поточні дослідження спрямовані на підвищення ефективності виявлення об'єктів, зокрема шляхом оптимізації обчислювальних ресурсів і впровадження самоорганізованого навчання. Новітні методи, такі як Vision Transformers (ViTs) із масштабованими параметрами [12], демонструють конкурентні результати в задачах детекції та сегментації об'єктів.

Іншим перспективним напрямком є впровадження багатомодальних моделей, що поєднують зорову та текстову інформацію, наприклад, в OpenAI CLIP [13], що дає змогу здійснювати виявлення без потреби в специфічних анотаціях. Також розвиваються методи нейросетевого стиснення (neural network pruning) та квантизації (quantization), які сприяють впровадженню потужних

моделей у мобільних і вбудованих системах.

Таким чином, сучасні технології виявлення об'єктів продовжують розвиватися в напрямку підвищення точності, швидкодії та адаптації до різних обчислювальних середовищ. Подальші дослідження у сфері трансформерних архітектур, самоорганізованого навчання та енергоефективних нейромереж забезпечать ще більший прогрес у застосуванні цих технологій.

Список використаних джерел

1. Girshick R. Fast R-CNN. 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, 7–13 December 2015. 2015. URL: https://doi.org/10.1109/iccv.2015.169 (дата звернення: 19.03.2025).
2. Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks. 6 January 2016 / S. Ren et al. arXiv. Cornell University. URL: https://doi.org/10.48550/arXiv.1506.01497 (дата звернення: 19.03.2025).
3. End-to-End Object Detection with Transformers. 28 May 2020 / N. Carion et al. arXiv. Cornell University. URL: https://doi.org/10.48550/arXiv.2005.12872 (дата звернення: 19.03.2025).
4. Deformable DETR: Deformable Transformers for End-to-End Object Detection / Z. Xizhou et al. arXiv.org. URL: https://arxiv.org/abs/2010.04159 (дата звернення: 20.03.2025).
5. Swin Transformer: Hierarchical Vision Transformer using Shifted Windows / L. Ze et al. arXiv.org. URL: https://arxiv.org/abs/2103.14030 (дата звернення: 20.03.2025).
6. EfficientViT: Lightweight Multi-Scale Attention for High-Resolution Dense Prediction / H. Cai et al. 2023 IEEE/CVF International Conference on Computer Vision (ICCV), Paris, France, 1–6 October 2023. 2023. URL: https://doi.org/10.1109/iccv51070.2023.01587 (дата звернення: 27.03.2025).
7. You Only Look Once: Unified, Real-Time Object Detection / J. Redmon et al. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR),

Las Vegas, NV, USA, 27–30 June 2016. 2016. URL: https://doi.org/10.1109/cvpr.2016.91 (дата звернення: 27.03.2025).
8. SSD: Single Shot MultiBox Detector / L. Wei et al. arXiv.org. URL: https://arxiv.org/abs/1512.02325 (дата звернення: 20.03.2025).
9. Mingxing T., Ruoming P., Quoc L. EfficientDet: Scalable and Efficient Object Detection. arXiv.org. URL: https://arxiv.org/abs/1911.09070 (дата звернення: 20.03.2025).
10. Meta. Detectron2. AI at Meta. URL: https://ai.meta.com/tools/detectron2/ (дата звернення: 20.03.2025).
11. MMDetection. Welcome to MMDetection's documentation! – MMDetection 3.3.0 documentation. MMDetection. URL: https://mmdetection.readthedocs.io/en/latest/ (дата звернення: 21.03.2025).
12. Visual transformers: token-based image representation and processing for computer vision / W. Bichen et al. arXiv.org. URL: https://arxiv.org/abs/2006.03677 (дата звернення: 20.03.2025).
13. Learning transferable visual models from natural language supervision / A. Radford et al. arXiv.org. URL: https://arxiv.org/abs/2103.00020 (дата звернення: 20.03.2025).

УДК 004.42:929

ВІРТУАЛЬНИЙ МУЗЕЙ ІСТОРІЇ ТЕХНОЛОГІЙ З ДОПОВНЕНОЮ РЕАЛЬНІСТЮ

Ключка О.А
kluckaoleg273@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М.В.
м. Черкаси, Україна

У сучасному світі, де технології розвиваються з неймовірною швидкістю, виникає нагальна потреба у збереженні та популяризації історії їхнього розвитку. Віртуальний музей історії технологій з доповненою реальністю (AR) є

інноваційним підходом, що дозволяє не лише зберегти історичні артефакти, але й зробити їх доступними для широкого кола користувачів у інтерактивній формі. Цей підхід поєднує в собі можливості цифрового музейного простору та технології доповненої реальності, що дозволяє відвідувачам не лише дізнатися про минуле, але й безпосередньо взаємодіяти з експонатами, використовуючи можливості AR.

Концепція віртуального музею полягає у створенні цифрової платформи, яка надає доступ до історичних технологій у віртуальному просторі. Відвідувачі можуть досліджувати експонати, переглядати 3D-моделі, читати описи та дізнаватися про їхній вплив на розвиток суспільства. Доповнена реальність, у свою чергу, накладає цифрові елементи на реальний світ, дозволяючи відвідувачам бачити віртуальні експонати у своєму реальному оточенні та взаємодіяти з ними, отримуючи додаткову інформацію.

Основними компонентами такого віртуального музею є:

3D-моделі експонатів. Створення високоякісних 3D-моделей історичних технологій для віртуального відображення. Наприклад, детальні 3D-моделі перших комп'ютерів, таких як ENIAC або IBM PC, дозволяють відвідувачам розглянути їх з усіх боків.

- Мобільний додаток з AR. Розробка мобільного додатку, який дозволяє відвідувачам сканувати маркери у реальному світі та бачити віртуальні експонати. Наприклад, скануючи маркер, розташований біля фотографії телеграфа, користувач може побачити його віртуальну 3D-модель та анімацію його роботи;
- Інтерактивні елементи. Додавання інтерактивних елементів до експонатів, таких як анімації, відео та аудіо, для покращення досвіду відвідувачів. Наприклад, інтерактивна анімація, що показує процес роботи парової машини, або відео з розповіддю про історію створення першого автомобіля;
- Інформаційна база даних. Створення бази даних з інформацією про кожен експонат, включаючи історію, технічні характеристики та вплив на суспільство. Наприклад, детальна інформація про технічні характеристики

першого літака братів Райт або про вплив винаходу телефону на комунікацію;

- Віртуальні екскурсії. Розробка віртуальних екскурсій, які дозволяють відвідувачам досліджувати музей у віртуальному просторі. Наприклад, віртуальна екскурсія, що відтворює атмосферу лабораторії Томаса Едісона або історичної виставки технічних досягнень.

Переваги такого віртуального музею є очевидними: доступність для відвідувачів з усього світу, інтерактивність, що робить навчання більш захоплюючим, можливість надання більшого обсягу інформації про експонати, збереження цифрових копій рідкісних та цінних експонатів, а також високий освітній потенціал для студентів та дослідників.

Для реалізації такого проекту використовуються сучасні технології, такі як 3D-моделювання, розробка мобільних додатків з підтримкою AR, хмарні технології для зберігання та обробки даних, а також технології геолокації та картографії для прив'язки віртуальних об'єктів до реального простору.

Прикладами експонатів можуть бути перші комп'ютери, історичні засоби зв'язку, ранні моделі автомобілів та літаків, історичні фото- та відеокамери, а також історичні побутові прилади.

Отже, віртуальний музей історії технологій з доповненою реальністю є інноваційним та перспективним напрямком у музейній справі, що дозволяє зробити історію технологій доступною та захоплюючою для широкої аудиторії, сприяючи збереженню культурної спадщини та популяризації науки і техніки.

Список використаних джерел

1. Віртуальний музей – ефективний механізм збереження історичної пам’яті та культурної спадщини – Media League. Media League. URL: https://medialeague.com.ua/virtualnyj-muzej-efektyvnyj-mehanizm-zberezhennya-istorychnoyi-pamyati-ta-kulturnoyi-spadshhyny/ (дата звернення: 19.03.2025).

2. єМузей – Оцифрування культурної спадщини України. emuseum. URL: https://emuseum.com.ua/ (дата звернення: 19.03.2025).

УДК 004.9:007.5

УПРАВЛІННЯ РИЗИКАМИ В AI-СИСТЕМАХ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мишко І. С.
gloriolus225@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М. В.
м. Черкаси, Україна

Сучасні AI-системи відіграють ключову роль у забезпеченні інформаційної безпеки, проте самі вони піддаються численним загрозам. Управління ризиками таких систем є критично важливим завданням для мінімізації потенційних загроз і підвищення ефективності роботи AI у сфері безпеки. У статті розглядаються основні ризики, пов’язані з використанням AI, методи їх ідентифікації, аналізу та мінімізації.

Штучний інтелект (AI) є потужним інструментом для забезпечення інформаційної безпеки завдяки можливості автоматичного аналізу загроз, виявлення аномалій та прогнозування потенційних атак. Проте AI-системи самі можуть ставати об’єктами атак або чинниками нових ризиків. Розвиток гібридних атак, маніпуляцій із вхідними даними та експлуатація вразливостей алгоритмів машинного навчання потребують нових підходів до управління ризиками.

Атаки на моделі машинного навчання бувають двох типів. Adversarial attacks – маніпуляція вхідними даними для введення AI в оману. І Data poisoning – внесення шкідливих даних у процес навчання, що призводить до неправильної класифікації загроз.

Конфіденційність і витік даних. Використання великих масивів даних для навчання AI може призвести до загрози витоку конфіденційної інформації.

Інверсія моделі (Model inversion) – техніка, яка дозволяє зловмисникам відновлювати вихідні дані, використані для навчання AI.

Надмірна залежність від AI-рішень. Автоматизовані системи ухвалення рішень можуть мати хибнопозитивні або хибнонегативні результати, що впливає на ефективність безпеки. Відсутність людського контролю може сприяти помилковим діям AI у критичних ситуаціях.

Етичні та правові ризики. Алгоритмічна упередженість може призводити до несправедливого ухвалення рішень. Недостатнє регулювання AI у сфері безпеки може створювати юридичні прогалини [1].

Ризик-орієнтований підхід як один із методів управляннями ризиками. Використання методологій управління ризиками, таких як NIST Risk Management Framework або ISO/IEC 27005. Оцінка загроз та ймовірності їх виникнення для прогнозування потенційних атак.

Тестування та валідація моделей AI. Використання технік Adversarial Training для підвищення стійкості моделей до атак. Перевірка на наявність прихованих вразливостей у процесі навчання AI.

Захист даних та приватності. Впровадження методів диференційованої приватності (Differential Privacy) для захисту даних користувачів. Використання федеративного навчання (Federated Learning) для зменшення ризику централізованого витоку даних.

Аудит та моніторинг AI-систем. Постійний аналіз роботи AI для виявлення аномалій та можливих загроз. Впровадження політик пояснюваності (Explainable AI), що дозволяє розуміти логіку ухвалення рішень AI [2].

Розрахунок ризиків у AI-системах здійснюється за допомогою класичної формули:

$$R=P\times I \quad (1),$$

де

R – рівень ризику,

P – ймовірність виникнення загрози,

I – вплив (збитки), які можуть бути завдані у разі реалізації загрози.

Для AI-систем додатково враховують фактори похибок моделей, зокрема:

$$RAI=PI+EFP+EFNC \quad (2),$$

де:

EFP – ймовірність хибнопозитивного спрацювання,

EFN – ймовірність хибнонегативного спрацювання,

C – вартість помилки (фінансові або операційні втрати).

Таким чином, управління ризиками передбачає не лише оцінку класичних кіберзагроз, а й аналіз надійності AI-алгоритмів та їхню стійкість до атак і помилок ухвалення рішень [3, 4]. AI відіграє важливу роль у забезпеченні інформаційної безпеки, однак його використання супроводжується певними ризиками. Ризик-орієнтований підхід, тестування, захист даних та моніторинг є ключовими методами для зниження можливих загроз. Подальші дослідження у сфері безпечного застосування AI мають бути зосереджені на адаптивних стратегіях кіберзахисту, що враховують змінюваний характер атак та можливості штучного інтелекту.

Список використаних джерел

1. National Institute of Standards and Technology (NIST). AI Risk Management Framework. 2023. URL: https://www.nist.gov/itl/ai-risk-management-framework (дата звернення: 15.03.2025).
2. ISO/IEC 27005:2022 – Information security risk management. . URL: https://www.iso.org/standard/80585.html (дата звернення: 15.03.2025).
3. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. URL: https://arxiv.org/abs/1712.03141 (дата звернення: 19.03.2025).
4. Goodfellow, I., McDaniel, P., & Papernot, N. (2017). Adversarial examples: Attacks and defenses for deep learning.. URL: https://arxiv.org/abs/1708.06939 (дата звернення: 19.03.2025)

УДК 004.891:7

ШТУЧНИЙ ІНТЕЛЕКТ У МИСТЕЦТВІ: ТВОРЧІСТЬ БЕЗ ЛЮДИНИ?

Мелюхова М. Р.
12ritusya09@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.

Актуальність теми зумовлена стрімким розвитком технологій, які змінюють способи створення, сприйняття та оцінки художніх творів. ШІ відкриває нові горизонти для митців, сприяючи генерації задумів, автоматизації одноманітних операцій та дослідженням невідомих мистецьких форм. Разом з тим, він робить мистецтво ближчим до широкої аудиторії, надаючи можливість навіть тим, хто не володіє професійними вміннями, творити за допомогою таких програм, як Midjourney, DALL·E або Adobe Firefly.

В той же час вплив ШІ на художній ринок спричиняє чимало суперечок, включаючи питання авторських прав, переоцінку важливості ручної праці та комерціалізацію цифрового мистецтва. Застосування штучного інтелекту також підіймає питання авторства: чи можливо вважати оригінальними роботи, створені алгоритмами, та хто є їх справжнім творцем – сама програма, її розробник або користувач? Крім того, мистецтво, породжене ШІ, формує етичні та соціальні проблеми, що пов’язані з імовірним заміщенням людських митців, втратою автентичності та загрозою маніпуляцій за допомогою генеративних моделей.

Мистецтво штучного інтелекту – це, просто, мистецтво, створене за допомогою генеративного штучного інтелекту (рис. 1) – технології, яка знаходить шаблони у великих наборах даних і використовує цю інформацію для створення нового вмісту. Все, що для цього потрібно, — це генератор штучного інтелекту, наприклад Adobe Firefly, Midjourney, DALL·E і ідея. Художник вводить детальну характеристику, яку інструмент потім використовує для створення варіантів зображення на основі опису [3].

Рисунок 1. Автоматично згенероване мною зображення за допомогою ШІ Midjourney. Воно показує, як міг би виглядати Грегор Замза з повісті «Перевтілення» Франца Кафки

Художники використовують генеративний штучний інтелект, щоб створювати різні твори мистецтва, від віршів та оповідань до творінь, схожих на аналогові картини чи фотографії, тощо. Швидкість і гнучкість генеративного штучного інтелекту дозволяють творцям швидше починати та завершувати проєкти, а також відкриває різноманітні нові захоплюючі можливості для творчого самовираження.

Технологія, яка забезпечує цю здатність, називається нейронною мережею. Нейронна мережа – це математична система – алгоритм, який знаходить закономірності у великих наборах даних.

Ai-Da – перший у світі ультрареалістичний робот-художник, здатний малювати та створювати скульптури за допомогою вбудованих камер, алгоритмів штучного інтелекту та роботизованої руки. Вона є результатом поєднання електронних, AI та людських елементів, що робить її унікальною фігурою в сучасному мистецтві [4].

Ai-Da була задумана Айданом Меллером та створена компанією Engineered Arts у Великобританії, а її роботизована рука була розроблена та запрограмована

єгипетськими комп'ютерними вченими Салахом АльАбдом і Зіадом Абассом.

На відміну від програмного забезпечення, яке генерує цифрове мистецтво, Ai-Da поєднує штучний інтелект із робототехнікою. Вона оснащена камерами в очах, механічною рукою та алгоритмами, які дозволяють їй аналізувати зображення і концепції та створювати фізичні картини. Це робить її унікальною серед інструментів генеративного ШІ, оскільки вона працює не лише у цифровому просторі, а й у фізичному світі, створюючи аналогове мистецтво.

У листопаді 2024 року портрет Алана Тюрінга (рис. 2), створений Ai-Da, був проданий на аукціоні Sotheby's у Нью-Йорку за рекордні 1,08 мільйона доларів США, що значно перевищило попередні оцінки.

Рисунок 2. Портрет Алана Тюрлінга створений роботом-художником Ai-Da

Ai-Da не лише створює мистецтво, але й є живим прикладом інтеграції штучного інтелекту в творчий процес, спонукаючи нас переосмислити межі між людиною та машиною в мистецтві та суспільстві.

Протягом історії кожен радикальний мистецький рух був тісно пов’язаний із культурним духом часу, відображенням суспільних занепокоєнь і проблем, як Тернер і його індустріальні пейзажі та одержимість Да Вінчі наукою та математикою. ШІ нічим не відрізняється. Творці Ai-Da, галерист Ейдан Меллер

і дослідниця Люсі Сіл називають це основною причиною існування такого художника-гуманоїда, як Ai-Da. Вона є уособленням одного з нинішніх страхів сучасного суспільства: зростання алгоритмів штучного інтелекту, які викрадають робочі місця, і потенційного домінування роботів [1, 2].

«Творчість не може виникнути з нічого – усі митці, люди, роботи чи алгоритми, створюють роботи інших» – Остін Клеон.

У висновок можна сказати, що останні здобутки в царині штучного інтелекту радикально трансформують художній простір, відчиняючи двері до небачених раніше творчих перспектив, але водночас породжуючи серію спірних моментів. Художниця-робот Ai-Da – показовий приклад того, як ШІ може не лише копіювати людську творчість, але й активно долучатися до мистецького творення, поєднуючи цифрові коди з фізичним малюванням.

Основна трудність криється в переосмисленні питань авторства та унікальності в мистецтві. Чи можна визнавати штучні інтелекти та їхні роботи справжніми художниками та оригінальними твореннями? Кому належить авторське право на подібні роботи – самій програмі, її творцям чи користувачам? Окрім того, зростає загроза витіснення традиційних митців, що наражає на небезпеку людське самовираження в мистецтві.

Відтак, мистецтво штучного інтелекту не тільки розширює творчі обрії, а й змушує глибше замислитися над сутністю мистецтва, його етичними, юридичними та суспільними аспектами. У майбутньому ключовим завданням стане віднаходження гармонії між технологіями та людською творчістю, щоб вберегти самобутність та глибину мистецького вираження.

Список використаних джерел

1. AI art: The end of creativity or the start of a new movement? URL: https://www.bbc.com/future/article/20241018-ai-art-the-end-of-creativity-or-a-new-movement (дата звернення: 13.03.2025).
2. AI ARTIST Creepy ‘AI God’ art painted by humanoid robot fetches whopping $1million in ‘world first’ auction URL:

https://www.thesun.co.uk/tech/31585429/aida-humanoid-robot-art-auction-alan-turing-world-first/?utm_source=chatgpt.com (дата звернення: 13.03.2025)
3. What is AI art and how is it made? URL: https://www.adobe.com/products/firefly/discover/what-is-ai-art.html#:~:text=AI%20art%20is%2C%20simply%2C%20artwork,Adobe%20Firefly%2C%20and%20an%20idea. (дата звернення: 13.03.2025)
4. WHO IS AI-DA? URL: https://www.ai-darobot.com/about.

УДК 004.91:78

АЛГОРИТМІЧНЕ МИСЛЕННЯ У МУЗИЧНОМУ МИСТЕЦТВІ

Сагун О. С.
sahunoleksandr44@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р. В.
м. Черкаси, Україна

Штучний інтелект (ШІ) проникає у все більше сфер людської діяльності, включаючи музичну творчість. Сьогодні алгоритми демонструють вражаючі здібності у генеруванні музики – іноді настільки якісно, що її важко відрізнити від творів людини. Визначною подією стало офіційне визнання AI AIVA авторським товариством у 2017 році, що вперше в історії надало штучному інтелекту статус композитора та продемонструвало спроможність ШІ до творчої діяльності.

Поєднання ШІ та музики стрімко трансформує процес створення композицій, відкриваючи нову еру креативності, де композитори отримують додаткові інструменти для генерування мелодій та гармоній за допомогою алгоритмів. Ця технологія викликає як захоплення, так і занепокоєння щодо майбутнього музичної індустрії, авторського права та природи мистецтва.

Алгоритмічний підхід до композиції має давню історію. Задовго до сучасного ШІ композитори використовували математичні алгоритми та випадковість у творчості. Наприклад, Іанніс Ксенакіс генерував музичні структури за допомогою стохастичних моделей ще у 1950-х роках. Навіть

Моцарт експериментував із «музичними іграми з кубиками», де комбінації визначали послідовність нот. Ці ранні експерименти стали підґрунтям для сучасних AI-систем.

Ключова відмінність між традиційною алгоритмічною композицією та сучасними AI-підходами полягає в методі навчання. Старі системи базувалися на заданих людиною правилах, тоді як сучасні ШІ-моделі самостійно навчаються, аналізуючи величезні масиви музичних творів і виявляючи приховані закономірності. Прорив у глибокому навчанні дозволив нейромережам аналізувати тисячі пісень, «вивчати» музичну мову певного жанру і створювати нові мелодії на основі цього досвіду.

Сьогодні існує низка платформ для AI-композиції, кожна зі своїми особливостями. AIVA (Artificial Intelligence Virtual Artist) спеціалізується на класичній та оркестровій музиці, створюючи емоційні, виразні композиції. Ця система стала першим ШІ, офіційно зареєстрованим як композитор у авторських товариствах Люксембургу та Франції.

Amper Music пропонує швидке генерування музичних треків за заданими параметрами, такими як настрій, жанр і темп. Орієнтована на контент-мейкерів, ця платформа дозволяє створити оригінальний фоновий трек за лічені секунди, що знижує витрати на ліцензійні збори. Користувач обирає базові параметри, а далі AI самостійно складає музику, яку за потреби можна відредагувати.

Suno AI представляє передовий підхід до генерації музики, створюючи повноцінні пісні на основі текстового опису. Система використовує дві нейромережі: Bark для вокалу/тексту і Chirp для інструменталу, що дозволяє отримати готовий трек, який містить і музику, і спів.

Google MusicLM, представлена у 2023 році, також перетворює текстові описи на музику. Користувачу достатньо задати запит «спокійний джазовий трек для вечері», і система згенерує кілька варіантів композиції відповідно до запиту.

Технічна основа AI-композиторів – глибокі нейронні мережі, які навчаються на величезних колекціях музики. Мережа аналізує сотні чи тисячі людських творів для вивчення статистичних закономірностей: послідовностей нот, акордів,

ритмів, структури пісень – і потім відтворює ці закономірності, генеруючи нові композиції.

Ранні моделі використовували рекурентні нейронні мережі (RNN, зокрема LSTM), що аналізують музику нота за нотою в часі. Проте новіші Transformer-моделі з механізмом self-attention можуть оглядати всю послідовність нот одразу і враховувати довгострокові зв'язки, що дозволяє генерувати більш цілісні та структуровані музичні твори.

Для створення нової музики нейромережі застосовують різні підходи: авторегресивні моделі прогнозують наступну ноту по одній, варіаційні автоенкодери навчаються стискати та відновлювати музичні фрагменти, а генеративно-змагальні мережі (GAN) навчаються створювати музичні уривки через змагання двох мереж. Деякі системи генерують символічну музику (ноти, MIDI), яку можна виконати різними інструментами, тоді як інші моделі генерують безпосередньо аудіосигнал у форматі WAV/MP3.

Вплив AI-композиції на музичну індустрію значний і багатогранний. З одного боку, ці технології прискорюють та здешевлюють виробництво музики – генератори створюють треки буквально за секунди, що економить час і знижує витрати на ліцензування та замовлення саундтреків. З іншого боку, відбувається демократизація творчості: люди без спеціальної музичної освіти отримують доступ до інтуїтивних AI-сервісів, що розширює коло творців.

ШІ також відкриває можливості для експериментів та створення нових стилів, поєднуючи різні жанри та пропонуючи несподівані комбінації звуків. Багато музикантів вже використовують AI як інструмент для натхнення: алгоритм генерує варіанти мелодії, а людина відбирає та розвиває найкращі ідеї, створюючи продуктивний тандем людини і машини.

Однак автоматизація композиції несе й певні ризики. Бібліотеки стокової музики та композитори рекламних джинглів можуть втрачати замовлення, якщо компанії віддаватимуть перевагу згенерованим трекам. Існує також небезпека одноманітності: масове використання однакових моделей може призводити до схожого звучання багатьох треків.

Особливу увагу привертають етичні та авторські аспекти. Хто є автором музики, створеної ШІ? Це питання залишається відкритим. Законодавство більшості країн поки не дає однозначної відповіді. У США, наприклад, діє правило, що для авторського права потрібен внесок людини, тому твори, цілком згенеровані машиною без участі людини, не підлягають реєстрації авторського права. В Європі підходи різняться, і деякі юрисдикції розглядають можливість запровадження особливого статусу для комп'ютерно-генерованих творів.

Виникають також питання щодо справедливості використання стилів та напрацювань реальних авторів, на музиці яких навчаються AI-моделі. Якщо нейромережа генерує трек «у дусі» відомого композитора, чи слід згадати оригінального автора стилю? Існує також ризик неусвідомленого запозичення: алгоритм може випадково відтворити уривок мелодії з тренувальних даних, що спричинить спір про плагіат.

Багато фахівців вважають, що найбільш етичний та продуктивний підхід – розглядати ШІ як помічника композитора, а не конкурента. Ідеальна модель передбачає співпрацю людини і AI: алгоритм генерує варіанти, а людина спрямовує та редагує результат, зберігаючи контроль над творчим процесом.

У перспективі очікується, що AI-композиція стане звичною частиною музичної індустрії. ШІ-асистенти будуть вбудовані у програми для написання музики, допомагаючи композиторам генерувати ідеї та миттєво прослуховувати варіанти аранжувань. Технології продовжать удосконалюватися: майбутні моделі навчаться краще враховувати контекст та забезпечувати логічний розвиток композиції на великій тривалості.

Ймовірно, з'являться нові застосування AI в музиці: персоналізовані саундтреки, що генеруються в реальному часі під настрій користувача або події гри, динамічні плейлисти, що адаптуються до вподобань слухача, а також освітні інструменти, які допомагатимуть новачкам опановувати композицію.

У довгостроковій перспективі суспільство виробить норми щодо AI-музики, встановивши правила прозорості та нові моделі ліцензування для таких творів. Правові системи адаптуються, можливо створивши окремий режим прав для AI-

генерованого контенту. І так само, як колись синтезатори і семплери стали звичними інструментами, ШІ-моделі з часом увійдуть до стандартного креативного арсеналу музикантів.

Список використаних джерел

1. AIVA (офіційний сайт): AI-асистент для генерування музики у 250 стилях, від класики до попу . URL: https://www.aiva.ai/ (дата звернення: 15.03.2025).
2. Balcaitis R. Suno AI – огляд платформи (2024): Стаття, що пояснює підхід Suno AI до створення пісень з тексту (моделі Bark і Chirp). URL: https://empathizeit.com/from-inspiration-to-creation-how-suno-ai-lets-you-compose-music-your-way (дата звернення: 15.03.2025)
3. Clifford Chance (2023) – "AI-Generated Music and Copyright": Аналітична публікація юридичної фірми про авторське право до музики, створеної ШІ. URL: https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2023/04/ai-generated-music-and-copyright.html (дата звернення: 15.03.2025)
4. DigitalOcean (2023) – "10 AI Music Generators for Creators in 2025": Оглядова стаття, що порівнює 10 сучасних AI-платформ для генерування музики . URL: https://www.digitalocean.com/resources/articles/ai-music-generators (дата звернення: 16.03.2025).
5. Google AI Blog – MusicLM (2023): Офіційний анонс моделі MusicLM від Google, що генерує музику за текстовим описом. URL: https://blog.google/technology/ai/musiclm-google-ai-test-kitchen/ (дата звернення: 20.03.2025).
6. Magenta (Google Brain): Дослідницький проєкт з відкритим кодом, присвячений застосуванню машинного навчання в музиці і мистецтві . URL: https://magenta.tensorflow.org/ (дата звернення: 20.03.2025).

УДК 004.75:338.46

РОЛЬ НЕЙРОМЕРЕЖ У ПЕРСОНАЛІЗАЦІЇ ТА БЕЗПЕЦІ ЦИФРОВИХ ГАМАНЦІВ

Монько С. Ю.
stasmonko6@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

У сучасному світі цифровізація охоплює всі аспекти нашого життя, включаючи фінансові операції. Традиційні фізичні гаманці поступово поступаються місцем цифровим рішенням, які пропонують зручність, швидкість та безпеку. Розглянемо, яким може бути гаманець майбутнього, його ключові характеристики та технології, що лежать в його основі.

1. Цифрові гаманці: сучасний стан та перспективи.

Цифрові гаманці вже стали невід'ємною частиною фінансової екосистеми. Вони дозволяють зберігати платіжні картки, здійснювати безконтактні платежі та керувати фінансами через смартфони чи інші пристрої. Прикладом є сервіс Apple Pay, який використовує технологію NFC для безконтактних оплат, забезпечуючи безпеку даних через метод токенізації .

У майбутньому цифрові гаманці стануть ще більш інтегрованими в наше повсякденне життя, пропонуючи розширені можливості, такі як підтримка криптовалют, інтеграція з різними фінансовими сервісами та використання біометричної аутентифікації для підвищення безпеки.

2. Інтеграція криптовалют та блокчейн-технологій.

З розвитком блокчейн-технологій та криптовалют, гаманці майбутнього матимуть вбудовану підтримку різних цифрових активів. Наприклад, гаманець Aptos пропонує користувачам можливість зберігати та керувати токенами APT, забезпечуючи високу пропускну здатність та безпеку транзакцій.

Крім того, використання багатосторонніх обчислень (MPC) у гаманцях, таких як рішення від Binancex, забезпечує додатковий рівень безпеки для Web3-

транзакцій, дозволяючи кільком сторонам виконувати криптографічні обчислення без розкриття конфіденційних даних .

3. Європейські ініціативи та стандартизація.

Європейська платіжна ініціатива (EPI) працює над створенням єдиного цифрового гаманця під назвою «wero», який об'єднає різні платіжні сервіси та стандартизує процеси оплати в Європі. Це сприятиме спрощенню транзакцій, зниженню витрат та підвищенню безпеки фінансових операцій.

4. Біометрична аутентифікація та підвищення безпеки.

Гаманці майбутнього будуть оснащені біометричними методами аутентифікації, такими як відбитки пальців, розпізнавання обличчя чи голосу. Це забезпечить високий рівень безпеки та зручності для користувачів, знижуючи ризик несанкціонованого доступу до фінансових даних.

5. Інтеграція з іншими сервісами та IoT.

Майбутні гаманці будуть інтегровані з іншими сервісами, такими як програми лояльності, транспортні системи та інтернет речей . Наприклад, вони зможуть автоматично оплачувати проїзд у громадському транспорті або здійснювати покупки в автоматизованих магазинах без касирів.

6. Персоналізація та штучний інтелект.

Використання штучного інтелекту дозволить гаманцям аналізувати фінансові звички користувачів та надавати персоналізовані рекомендації щодо управління бюджетом, інвестування чи економії коштів. Це сприятиме більш усвідомленому підходу до фінансів та підвищенню фінансової грамотності.

7. Підтримка різних валют та глобалізація.

Гаманці майбутнього будуть підтримувати мультивалютність, дозволяючи легко конвертувати та зберігати різні валюти, включаючи національні та цифрові. Це спростить міжнародні транзакції та зробить фінансові послуги більш доступними для людей у всьому світі.

Отже, гаманець майбутнього – це багатофункціональний цифровий інструмент, який об'єднує в собі зручність, безпеку та інноваційні технології. Інтеграція криптовалют, біометричної аутентифікації, штучного інтелекту та IoT

зробить фінансові операції швидкими, безпечними та персоналізованими. Європейські ініціативи, такі як "wero", сприятимуть стандартизації та спрощенню платежів, а підтримка мультивалютності забезпечить глобальну доступність фінансових послуг. Майбутнє фінансів вже на горизонті, і цифрові гаманці відіграють ключову роль у цьому трансформаційному процесі.

Список використаних джерел

1. Apple Pay: цифровий гаманець майбутнього. Galka.if.ua. URL: https://galka.if.ua/apple-pay-tsyfrovyy-hamanets-maybutnoho/?utm_source=chatgpt.com (дата звернення: 21.03.2025).
2. Майбутнє Web3: інноваційний гаманець з MPC від Binance. URL: https://surl.li/pqgbix (дата звернення: 21.03.2025).

УДК 004.42:658.5

АНАЛІЗ ВРАЗЛИВОСТЕЙ ХМАРНИХ СЕРВІСІВ

Семизенко В.В.
Dorian5665@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М.В.
м. Черкаси, Україна

Хмарні сервіси відіграють важливу роль у сучасній інформаційній інфраструктурі, забезпечуючи ефективне управління даними та обчислювальними ресурсами. Однак, поряд із численними перевагами, вони мають ряд уразливих аспектів, що можуть створювати загрози для безпеки інформації. Аналіз цих аспектів є важливим для виявлення можливих загроз та розробки ефективних механізмів їх нейтралізації.

Метою дослідження є аналіз вразливостей хмарних сервісів та визначення основних загроз, що можуть впливати на їхню безпеку та стабільність.

Аналіз хмарних сервісів дозволяє виділити основні проблеми, які можуть впливати на безпеку даних. Однією з ключових вразливостей є загроза конфіденційності інформації. Дані, що зберігаються у хмарі, можуть бути

скомпрометовані через відсутність належного шифрування, помилки у налаштуванні доступу або атаки типу "людина посередині". Це створює значний ризик для користувачів та організацій, які працюють із чутливою інформацією.

Не менш важливою проблемою є збереження цілісності даних. У хмарних середовищах можливі атаки, що спрямовані на зміну або пошкодження інформації, що може призвести до серйозних наслідків для бізнесу. Особливо вразливими є механізми API, через які можуть здійснюватися несанкціоновані втручання. Відсутність належного контролю доступу до API підвищує ризик зловживань та маніпуляцій із даними.

Доступність хмарних сервісів також залишається критичним аспектом. Платформи можуть бути вразливими до атак типу DoS/DDoS, що призводять до тимчасового або повного відключення сервісів. Крім того, технічні збої у роботі хмарних провайдерів можуть спричиняти втрату доступу до інформації, що може впливати на стабільність функціонування компаній та організацій. Узагальнена інформація про основні уразливості наведена у Табл. 1.

Окрему увагу варто приділити типології хмарних сервісів, оскільки різні моделі їх надання можуть впливати на рівень інформаційної безпеки. Виділяють такі основні моделі хмарних сервісів:

- IaaS (Infrastructure as a Service) – забезпечує доступ до інфраструктурних ресурсів (віртуальні машини, сховища даних, мережеві ресурси). Ця модель дає гнучкість у налаштуванні серверних потужностей, але потребує високого рівня контролю безпеки з боку користувачів.
- PaaS (Platform as a Service) – надає готову платформу для розробки та тестування додатків. Користувачі можуть фокусуватися на розробці, але безпека залежить від налаштувань провайдера.
- SaaS (Software as a Service) – забезпечує доступ до готових програм через Інтернет, що зручно, але передбачає передачу контрольних функцій безпеки провайдеру.

– FaaS (Function as a Service) – орієнтована на виконання окремих функцій без управління серверною інфраструктурою, що дає змогу автоматизувати процеси, але створює додаткові ризики залежності від постачальника.

Таблиця 1. Основні уразливості хмарних сервісів

№	Вразливість	Опис	Потенційні наслідки
1	Конфіденційність даних	Відсутність шифрування або недостатній захист доступу.	Витік даних, крадіжка інформації
2	Цілісність даних	Можливість модифікації даних через атаки на API.	Підробка або втрата критичних даних
3	Доступність сервісів	DoS/DDoS-атаки, збої у роботі провайдерів.	Перебої у функціонуванні бізнес-процесів
4	Вразливості API	Відсутність автентифікації або контрольного механізму.	Несанкціонований доступ до хмарних ресурсів
5	Мультиорендність	Недостатня ізоляція користувачів у хмарному середовищі.	Використання даних конкурентами, витік інформації
6	Вразливість віртуалізації	Атаки на гіпервізор, що можуть надати доступ до віртуальних машин.	Компрометація всієї інфраструктури
7	Залежність від провайдера	Обмежений контроль користувача над безпекою сервісу.	Небезпека компрометації або втрата доступу до даних

Джерело: розробка автора

Недостатній рівень безпеки у цих моделях може призвести до серйозних ризиків для конфіденційності та доступності даних. Візуалізація класифікації ризиків інформаційної безпеки наведена на Рисунку 1, де демонструє відсоток популярності між типами хмарних сервісів та основними загрозами, що їм притаманні. Даний аналіз дозволяє оцінити потенційні вразливості та визначити напрями посилення безпеки у кожному з варіантів розгортання хмарної інфраструктури.

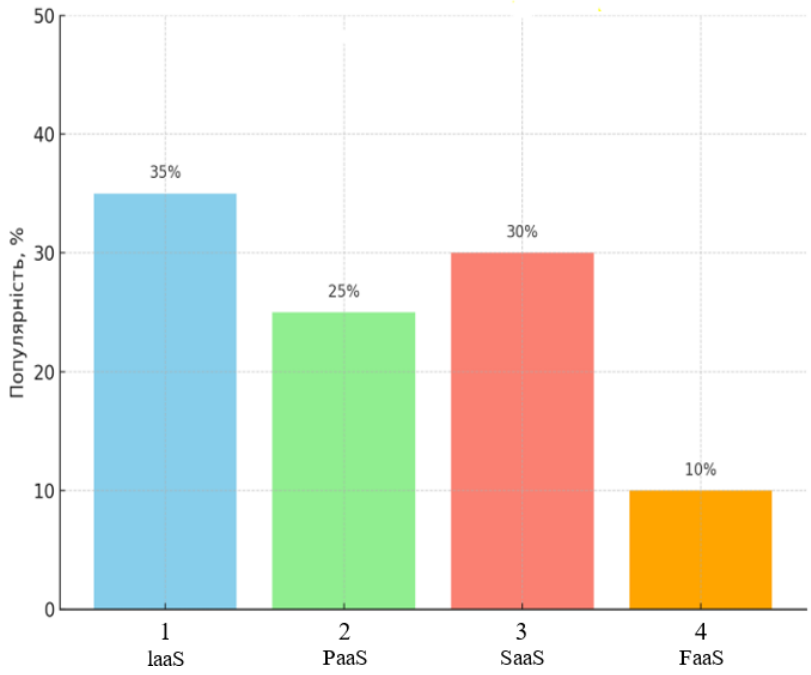

Рисунок 1. Візуалізація класифікації ризиків інформаційної безпеки

Таким чином, в роботі виконано аналіз основних вразливостей хмарних сервісів та визначено ключові загрози безпеки. З'ясовано, що найбільш критичними є проблеми конфіденційності, цілісності та доступності даних, а також вразливості API та мультиорендного середовища. Важливим аспектом є залежність користувачів від провайдера та потенційні загрози, пов'язані з віртуалізацією. Досягнута мета роботи сприяє формуванню розуміння сучасних загроз у сфері хмарних технологій та допомагає розробити ефективні стратегії захисту.

Список використаних джерел

1. AWS Security Documentation – Cloud Security Best Practices . URL: https://aws.amazon.com/documentation/ (дата звернення: 21.03.2025)
2. NIST Special Publication 800-190 – Application Container Security Guide . URL: https://csrc.nist.gov/publications/detail/sp/800-190/final (дата звернення: 21.03.2025)
3. Cloud Security Alliance – Cloud Controls Matrix . URL: https://cloudsecurityalliance.org/ (дата звернення: 21.03.2025).

4. Google Cloud Security Best Practices . URL: https://cloud.google.com/security/best-practices (дата звернення: 20.03.2025)
5. Microsoft Azure Security Documentation . URL: https://learn.microsoft.com/en-us/azure/security/ (дата звернення: 21.03.2025).

УДК 004.9:007.5

ГЕНЕРАТИВНИЙ AI (ChatGPT, MidJourney, DALL-E) – ТРЕНДИ ТА ВИКЛИКИ

Мотайленко О.О.
omotaylenko@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Ратайчук П.Є.
м. Черкаси, Україна

Актуальність теми обумовлена стрімким розвитком генеративних моделей штучного інтелекту, таких як ChatGPT, MidJourney та DALL-E, які перетворюються на потужний інструмент у різних сферах життя: від креативних індустрій до бізнесу, освіти та науки. Генеративний AI впливає на формування нових підходів до створення контенту, автоматизації процесів та інновацій у комунікаціях. Про актуальність та важливість теми свідчить зростаюча кількість досліджень, присвячених впливу генеративного AI на суспільство, економіку та культуру. Серед ключових дослідників у цій галузі можна відзначити таких науковців, як Й. Гудфеллоу, Д. Кінгсфорд, Е. Брайтман, А. Нг, а також праці компаній OpenAI, Google DeepMind та інших.

Генеративний AI виступає важливим фактором трансформації сучасних комунікацій, створення контенту та автоматизації креативних процесів. Він впливає на формування нових стандартів у сферах мистецтва, маркетингу, освіти та наукових досліджень, відкриваючи нові можливості для інновацій. У сучасному світі найбільш поширеними є такі генеративні моделі, як ChatGPT (для створення текстового контенту), MidJourney та DALL-E (для генерації зображень). Ці технології дозволяють автоматизувати процеси створення

контенту, забезпечуючи високу якість та швидкість виконання завдань. Вони знаходять застосування у маркетингу, дизайні, освіті, медіа та інших сферах.

Серед основних трендів генеративного AI можна виділити креативність та автоматизацію, персоналізацію контенту, інтеграцію у бізнес-процеси та розвиток мультимодальних моделей, які поєднують текст, зображення та аудіо. Креативність та автоматизація стають ключовими аспектами використання генеративного AI, оскільки він дозволяє зменшити витрати часу та ресурсів на створення унікального контенту. Персоналізація контенту за допомогою AI дозволяє задовольняти індивідуальні потреби користувачів, що особливо важливо в маркетингу та медіа. Інтеграція генеративних моделей у бізнес-процеси сприяє підвищенню ефективності та зниженню витрат, а розвиток мультимодальних моделей відкриває нові горизонти для створення комплексного контенту, що поєднує різні формати.

Однак разом із можливостями виникають і виклики, такі як етичні питання, пов’язані з авторським правом, плагіатом та маніпуляцією контентом. Важливим є також питання біасів у даних, які можуть посилювати соціальні стереотипи, а також проблеми безпеки та конфіденційності, пов’язані з використанням AI для створення дезінформації або шкідливого контенту. Технічні обмеження, такі як необхідність великих обсягів даних та енергоресурсів для навчання моделей, також залишаються актуальними.

Регулювання та стандартизація генеративного AI є необхідними для забезпечення безпечного та етичного використання технологій. Роль урядових та неурядових організацій у контролі за розвитком AI стає все більш значущою. У майбутньому генеративний AI може значно вдосконалитися, зокрема за рахунок покращення якості контенту та зменшення енерговитрат. Вплив на ринок праці також буде значним: зміна професійних навичок та поява нових спеціалізацій стануть неминучими. Потенціал генеративного AI для вирішення глобальних проблем, таких як освіта, охорона здоров’я та екологія, є величезним.

Таким чином, генеративний AI – це потужний інструмент, який змінює світ, але вимагає відповідального підходу до його використання. Важливим є баланс

між інноваціями та етикою, щоб забезпечити сталий розвиток технологій та їхню користь для суспільства. Розвиток генеративного AI потребує адекватних засобів регулювання, інтеграції у бізнес-процеси та підвищення обізнаності суспільства про його можливості та ризики. Це дозволить максимально ефективно використовувати потенціал технологій для розвитку сучасного світу.

Крім того, важливим аспектом є підвищення обізнаності суспільства про можливості та ризики генеративного AI. Освітні програми, тренінги та публічні дискусії можуть сприяти кращому розумінню того, як ці технології працюють і як їх можна використовувати етично та ефективно. Також важливо розвивати співпрацю між науковцями, бізнесом та урядовими органами для створення гармонійного регуляторного середовища, яке забезпечить сталий розвиток технологій.

У майбутньому генеративний AI може стати ключовим інструментом для вирішення складних глобальних проблем. Наприклад, у сфері освіти він може допомогти створювати персоналізовані навчальні програми, адаптовані до потреб кожного учня. У медицині генеративний AI може сприяти розробці нових ліків та методів лікування, а також автоматизації діагностики. У сфері екології він може бути використаний для моделювання кліматичних змін та розробки стратегій зменшення впливу на навколишнє середовище.

Таким чином, генеративний AI – це не лише інструмент для створення контенту, а й потужний механізм для трансформації суспільства. Його розвиток потребує комплексного підходу, який враховує як технічні, так і соціальні аспекти. Лише за умови відповідального використання та ефективного регулювання генеративний AI зможе реалізувати свій потенціал на благо людства.

Список використаних джерел

1. Kingford, D. (2020). AI Ethics and Bias: Challenges in Generative Models. AI Research Journal, 45(3), 123-140.
2. OpenAI. (2023). GPT-4 Technical Report. . URL: https://openai.com/research

3. Google DeepMind. (2023). Advancements in Multimodal AI: The Future of Generative Models. DeepMind Research Papers.
4. Brightman, E. (2022). Artificial Intelligence and Creativity: A New Era of Content Generation. Journal of AI Innovations, 7(1), 45-67.
5. Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? Proceedings of FAccT 2021, 610-623.
6. European Commission. (2023). AI Act: A European Approach to Artificial Intelligence Regulation. . URL: https://digital-strategy.ec.europa.eu (дата звернення: 21.03.2025).

УДК 004.056.5:343.12

АНАЛІЗ РИЗИКІВ ТА ВИКЛИКІВ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ В УМОВАХ ДИСТАНЦІЙНОГО ОФІСУ

Литовченко В.О.
lytovchenko15@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М.В.
м. Черкаси, Україна

У сучасних умовах дистанційної роботи питання захисту конфіденційної інформації набуває критичного значення. Віддалений доступ до корпоративних ресурсів створює нові виклики для організацій, що прагнуть зберегти безпеку даних. Основні ризики пов’язані з технічними вразливостями, недостатньою обізнаністю користувачів та обмеженими можливостями контролю з боку IT-відділів.

Метою роботи є аналіз ризиків та викликів захисту конфіденційних даних у віддаленому середовищі та визначення основних загроз кібербезпеки при дистанційній роботі.

Аналіз загроз та ризиків у сфері захисту конфіденційних даних в умовах дистанційного офісу показав, що найбільш поширеними є фішинг-атаки, використання незахищених Wi-Fi мереж, відсутність надійної автентифікації та

вразливості у системах віддаленого доступу. Фішингові атаки є небезпечними через використання зловмисниками підроблених електронних листів та веб-сайтів для отримання конфіденційних даних. Незахищені Wi-Fi мережі можуть бути використані для атак типу "людина посередині", що дає змогу перехоплювати передані дані. Відсутність двофакторної автентифікації та використання слабких паролів підвищують ризик несанкціонованого доступу до корпоративних ресурсів. Вразливості систем дистанційного доступу, такі як VPN та RDP, можуть використовуватися зловмисниками для проникнення в корпоративні мережі. Узагальнене представлення загроз подано в Табл 1.

Таблиця 1. Загрози кібербезпеки при віддаленій роботі

№	Загрози кібербезпеки при віддаленій роботі	Опис
1	Неавторизований доступ	Порушення політики безпеки через слабкі паролі, несанкціонований доступ.
2	Атаки типу Man-in-the-Middle	Використання незахищених Wi-Fi мереж для перехоплення даних.
3	Фішинг	Обман користувачів за допомогою фальшивих повідомлень або листів.
4	Шкідливе ПЗ	Віруси, трояни, програмне забезпечення-вимагачі.
5	Вразливості хмарних сервісів	Ненадійне зберігання даних у хмарах без належного захисту.
6	Втрата або крадіжка пристроїв	Втрата або крадіжка ноутбуків, смартфонів, на яких зберігаються важливі дані.
7	Вразливості систем дистанційного доступу	Проблеми з VPN або іншими системами віддаленого доступу.

Джерело: https://www.nist.gov

Для забезпечення належного рівня захисту конфіденційної інформації необхідно впроваджувати комплексні заходи. Це можна поділити на технічні та організаційні методи. До технічних методів належить використання шифрування даних, багатофакторної автентифікації та регулярного оновлення програмного забезпечення. Організаційні методи включають підвищення рівня обізнаності співробітників щодо основ кібербезпеки, контроль доступу до корпоративних ресурсів та запровадження політик інформаційної безпеки. Важливим елементом захисту є моніторинг мережевого трафіку та виявлення аномальної активності, що може свідчити про потенційні загрози. Алгоритм аналізу ризиків, що

дозволяє оцінювати рівень загроз та розробляти відповідні заходи протидії, подано на Рис.1.

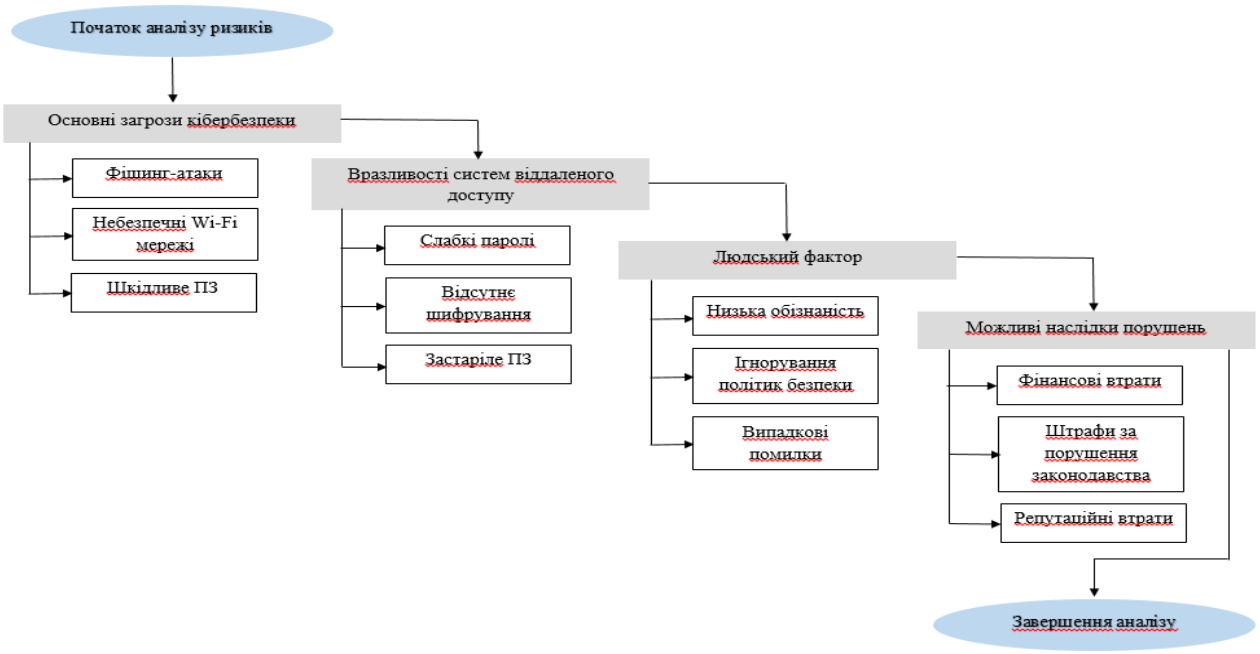

Рисунок 1. Алгоритм аналізу ризиків

Джерело: розробка автора

Таким чином, у ході роботи виконано аналіз основних ризиків та викликів, що виникають при захисті конфіденційних даних в умовах дистанційної роботи. Визначено основні загрози, такі як фішингові атаки, недостатня автентифікація, використання незахищених мереж та вразливості систем віддаленого доступу. Для мінімізації цих ризиків запропоновано комплекс заходів, що включає технічні та організаційні методи захисту. Досягнута мета роботи дозволяє сформувати загальне уявлення про кіберзагрози у віддаленому середовищі та сприяє підвищенню рівня інформаційної безпеки якоїсь певної організацій.

Список використаних джерел

1. ISO/IEC 27005:2022 – Інформаційні технології – Управління ризиками безпеки інформації . URL: https://www.iso.org/standard/27005.html (дата звернення: 20.03.2025).
2. NIST Special Publication 800-30 – Guide for Conducting Risk Assessments . URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 20.03.2025).

3. ENISA Threat Landscape 2024 – Огляд сучасних загроз кібербезпеки. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 20.03.2025).
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. URL: https://www.cl.cam.ac.uk/~rja14/book.html (дата звернення: 20.03.2025).

УДК 004.891

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ УМОВАХ

Літвинов Д. Д.
daniillitvynov1@gmail.com9
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Немає сумніву, що штучний інтелект за останні декілька років посів значне місце в нашому житті. Ми розглянемо які види штучного інтелекту існують і у яких сферах нашого життя він може бути застосований.

Спочатку розглянемо що таке штучний інтелект. Штучний інтелект (Artificial Intelligence (AI) – це метод змусити комп’ютер чи програмне забезпечення «мислити» як людський мозок. Це досягається шляхом вивчення закономірностей роботи людського мозку та аналізу когнітивних процесів. Результатом цих досліджень є розробка інтелектуального програмного забезпечення та систем [1].

По-друге, які бувають види штучного інтелекту? Найвідоміший у світі і найуживаніший – ChatGPT. Це такий чат-бот, який може відповісти на більшість питань стосовно проблем у різних галузях – у програмуванні, наприклад, допомагає згенерувати або знайти помилку в коді; в освіті його застосовують для рішення задач з точних наук; пошук необхідної інформації за допомогою нього стає набагато швидким і точним.

Один з найвідоміших голосових помічників – Siri. Що він може? Отримання відповідей на різні запитання. Наприклад, як зварити борщ; керувати додатками

та пристроями; налаштування нагадувань, будильників, таймерів; створення списків; прослуховування музики, аудіокниг, лекцій, підкастів; навігація на місцевості; комунікація: дзвінки, повідомлення [2].

Midjourney – це нейромережа для генерації зображень, що базується на штучному інтелекті. Вона може створювати нові зображення, використовуючи вже наявні зображення як початкову точку. Наприклад, якщо ви надаєте зображення квітки, Midjourney може згенерувати нове зображення квітки, яке не існує в реальному світі, але виглядає дуже реалістично [3].

У яких сферах використовується штучний інтелект? У транспорті, наприклад, машини з автопілотом набувають популярності. У медицині діагностика стає найточнішою і швидкою, і як наслідок лікування стає більш ефективним. У сфері безпеки, штучний інтелект застосовують для ідентифікації осіб через розпізнавання облич, що попереджає кримінальні дії. У фінансовій сфері штучний інтелект допомагає спрогнозувати результати ринкових угод, аналізувати дані для подальших інвестиційних рішень. В освіті процес навчання стає більш ефективним і різноманітним, завдяки цій технології кожен учень може отримати персональну увагу до свого рівня знань і згодом отримати швидкий прогрес і кращий результат.

Штучний інтелект як одна з провідних технологій стрімко розвивається. На сьогодні він може домогти майже в усьому: навчанні, пошуку інформації, захисту, медицині, тощо. Завдяки ньому вчені можуть більш швидко робити розрахунки. Отже, зараз це тільки початок розвитку цієї технології, з кожним роком штучний інтелект буде тільки вдосконалюватись як і людство в цілому. Важко уявити як він може розвинутись впродовж найближчих років і вплинути на наше життя.

Список використаних джерел

1. Midjourney - Все про штучний інтелект в Україні. Все про штучний інтелект в Україні. URL: https://gptchat.in.ua/midjourney (дата звернення: 24.03.2025).
2. Привіт, Siri: ТОП корисних голосових команд. URL: https://ti.ua/ua/news/privet_siri_top_poleznykh_komand/?srsltid=AfmBOoqh9bj

w2n2ehqOG4IiHz4s3F1-CJf03nblpMHDZzyVfeLIdkXMA (дата звернення: 21.03.2025).
3. Що таке штучний інтелект: історія, види та складові - GigaCloud. GigaCloud. URL: https://gigacloud.ua/articles/shho-take-shtuchnyj-intelekt-istoriya-vydy-ta-skladovi/ (дата звернення: 24.03.2025).

УДК 004.9:003.8

МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ У РАМКАХ КОНФЛІКТНИХ ВЗАЄМОДІЙ

Тамуров М.Г.
tamurovmaksym@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М.В.
м. Черкаси, Україна

У сучасному цифровому середовищі конфліктні взаємодії стають невід'ємною частиною роботи інформаційних систем. Вони можуть виникати між користувачами, між співробітниками різних підрозділів або між самими елементами системи через неузгодженість даних чи процедур. Ефективне моделювання таких взаємодій дозволяє вчасно виявляти проблеми, аналізувати їхні причини та знаходити оптимальні рішення для забезпечення злагодженої роботи системи.

Одним із ключових підходів до моделювання конфліктів є використання методів аналізу поведінки користувачів та автоматизованих алгоритмів. Зокрема, теорія ігор допомагає визначати стратегії учасників конфлікту та прогнозувати їхні дії [1]. Агентне моделювання дозволяє створювати віртуальні симуляції взаємодій, що дає змогу тестувати різні сценарії та виявляти потенційні проблеми ще до їхнього фактичного виникнення. Системний аналіз, у свою чергу, допомагає оцінити структуру системи, виявити критичні точки та визначити оптимальні шляхи усунення конфліктів.

Важливу роль у запобіганні та вирішенні конфліктних взаємодій відіграють UI/UX-рішення. Зручний та продуманий інтерфейс може значно зменшити

кількість конфліктів, спричинених неправильним розумінням функціоналу системи або складною навігацією. Використання зрозумілого дизайну, інтеграція автоматизованих підказок та рекомендацій, а також впровадження механізмів швидкого вирішення суперечностей сприяють зменшенню ризику виникнення конфліктів і підвищенню загальної ефективності роботи системи [2].

Для покращення управління конфліктами в організаціях доцільно розробити веб-платформу на базі Webflow, яка дозволяє структурувати та автоматизувати процес фіксації та аналізу конфліктних ситуацій (Рисунок 1). Співробітники різних підрозділів можуть подавати інформацію про конфлікти, що виникають у процесі роботи, через зручну онлайн-форму. Отримані дані автоматично спрямовуються у відповідні таблиці, закріплені за конкретними підрозділами, що дозволяє керівникам швидко отримувати доступ до актуальної інформації [3]. Це дає можливість не лише виявляти найпоширеніші проблеми, але й оцінювати їхній вплив на ефективність роботи команди.

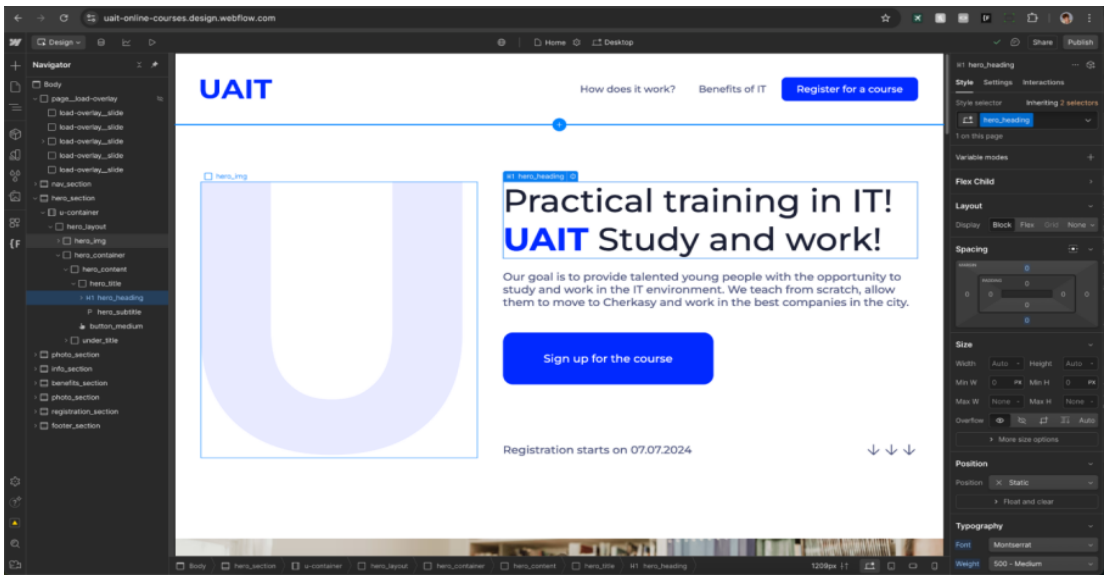

Рисунок 1. Інтерфейс платформи Webflow на якій відбуватиметься розробка системи управління конфліктами.

Розроблена система на базі Webflow також спрощує аналіз отриманих даних. Керівники можуть переглядати статистику конфліктних ситуацій, визначати найбільш критичні проблеми та ухвалювати обґрунтовані рішення щодо їхнього усунення [4]. Використання автоматизованого збору та обробки

даних значно скорочує час реагування на конфліктні ситуації та дозволяє швидко впроваджувати необхідні зміни. Крім того, реалізація такої системи у Webflow не вимагає складного програмування, що робить її доступною для широкого кола організацій та зменшує витрати на її розробку і впровадження.

Моделювання конфліктних взаємодій в інформаційних системах дає змогу не лише виявляти потенційні проблеми, а й активно впливати на їхнє вирішення. Розробка спеціалізованих платформ для збору, аналізу та управління конфліктами значно підвищує ефективність командної роботи та забезпечує комфортні умови для взаємодії всередині організацій. Запропонована система управління конфліктами дозволяє оперативно реагувати на проблеми, покращувати комунікацію між підрозділами та створювати більш ефективне робоче середовище.

Список використаних джерел

1. Комп'ютерне моделювання інформаційних систем в умовах конфліктних взаємодій .URL: https://essuir.sumdu.edu.ua/handle/123456789/73557 (дата звернення: 19.03.2025).
2. Командні конфлікти в IT компанії та методи їх вирішення .URL: https://careers.computools.ua/it-workplace-conflicts-and-solutions/ (дата звернення: 19.03.2025)
3. Як вирішити конфлікти у розробці систем через переговори .URL: https://monolith.law/uk/it/disputes-related-to-system-development (дата звернення: 19.03.2025).
4. Webflow .URL: https://webflow.com/ (дата звернення: 19.03.2025).

УДК 004.42:004.7

ДЕЦЕНТРАЛІЗОВАНІ МЕТОДИ ВІДНОВЛЕННЯ КРИПТОГАМАНЦЯ: ЯК ЗАХИСТИТИ ЗАСОБИ БЕЗ ЗБЕРІГАННЯ ПРИВАТНОГО КЛЮЧА

Панчішин К. Ю.
kirilpanchishin06@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р. В.
м. Черкаси, Україна

Криптовалюти стають все більш популярними, що вимагає нових підходів до збереження та захисту доступу до цифрових активів. Традиційні методи відновлення, засновані на приватних ключах та сид-фразах, мають серйозні недоліки, такі як ризик втрати або викрадення. Децентралізовані методи відновлення пропонують альтернативні рішення, що дозволяють забезпечити безпеку активів без необхідності централізованого зберігання чутливих даних.

Стандартні підходи до відновлення доступу, зокрема використання сид-фрази або зберігання резервної копії ключа, мають такі недоліки:

- Ризик втрати – у разі втрати приватного ключа або сид-фрази користувач втрачає доступ до своїх активів.
- Централізоване зберігання – зберігання копій ключів на сторонніх серверах або у хмарних сервісах створює додаткові вразливості.
- Фішингові атаки – зловмисники можуть змусити користувача розкрити приватний ключ або сид-фразу через шкідливі сайти чи електронні листи.
- Зломи та компрометація пристроїв – якщо ключ зберігається на незахищеному пристрої, він може бути викрадений через віруси або шкідливе ПЗ.

Децентралізовані методи відновлення базуються на кількох ключових принципах, що дозволяють уникнути централізованого зберігання приватного ключа:

- Розподіл секретів (Shamir’s Secret Sharing) – розбиття приватного ключа на частини, що зберігаються у різних учасників і потребують мінімальної кількості для відновлення.

- Мультипідпис (Multisignature) – доступ до гаманця здійснюється лише за підтвердженням кількох довірених осіб або пристроїв.
- Соціальне відновлення (Trusted Guardians) – користувач визначає довірених осіб, які можуть допомогти відновити доступ у разі його втрати.
- Блокчейн-орієнтовані механізми – використання смарт-контрактів для автоматизації відновлення та управління доступом.

Для реалізації децентралізованих методів відновлення застосовуються наступні технології:

- Shamir’s Secret Sharing (SSS) – розподіл секретного ключа на частини, що дозволяє відновити доступ лише при наявності достатньої кількості фрагментів.
- Мультипідписні гаманці – вимога підпису від кількох довірених сторін перед здійсненням транзакцій або відновленням доступу.
- Смарт-контракти – автоматизовані механізми відновлення доступу на основі визначених умов та алгоритмів.
- Децентралізовані ідентифікаційні системи (DID) – дозволяють прив’язати відновлення доступу до унікальних ідентифікаторів користувача, таких як біометричні дані.

Серед переваг децентралізованих методів відновлення можна назвати наступні:

- Відсутність централізованої точки відмови – оскільки дані розподілені між кількома учасниками або механізмами, зловмисники не можуть отримати повний доступ до приватного ключа одним методом атаки.
- Гнучкість у налаштуванні – користувач може вибирати методи відновлення, які найкраще відповідають його потребам і рівню довіри до інших учасників.
- Підвищена безпека – навіть якщо одна з частин ключа буде скомпрометована, зловмисники не зможуть отримати доступ без інших частин.

- Стійкість до атак – децентралізовані підходи ускладнюють атаки типу "єдиної точки відмови", які є характерними для централізованих систем.

Дана технологія має і свої недоліки, зокрема:

- Складність у налаштуванні – багато користувачів не знайомі з такими механізмами і можуть зробити помилки під час налаштування, що призведе до втрати доступу.
- Необхідність довіри до учасників – у випадку соціального відновлення користувач повинен довіряти визначеним особам, що не завжди є ідеальним рішенням.
- Відсутність єдиних стандартів – різні блокчейни та платформи використовують різні механізми відновлення, що ускладнює інтеграцію та масштабування.

Децентралізовані методи відновлення криптогаманця є важливим кроком у розвитку безпечних і надійних механізмів управління криптоактивами. Вони надають користувачам більше контролю над своїми даними і активами, знижуючи ризики, пов'язані з централізованими сервісами. Для покращення роботи даної технології можна розвивати стандарти безпеки, що в свою чергу гарно вплине на децентралізоване відновлення. Інтеграція штучного інтелекту призведе до покращеного виявлення підозрілих спроб відновлення. Створення простих інструментів покращить роботу кінцевих користувачів.

Список використаних джерел

1. Shamir, A. How to Share a Secret. // Communications of the ACM, 1979. URL: https://web.mit.edu/6.857/OldStuff/Fall03/ref/Shamir-HowToShareASecret.pdf (дата звернення: 21.03.2025).
2. Bitcoin Wiki. Multisignature. URL: https://en.bitcoin.it/wiki/Multisignature (дата звернення: 21.03.2025).
3. Ethereum Improvement Proposals. ERC-7093: Social Recovery Interface. URL: https://eips.ethereum.org/EIPS/eip-7093 (дата звернення: 21.03.2025).

4. Bogdanov, A. Foundations and Properties of Shamir’s Secret Sharing Scheme. // University of Tartu, 2007. URL: https://kodu.ut.ee/~peeter_l/teaching/seminar07k/bogdanov.pdf (дата звернення: 21.03.2025).
5. Maji, H. K., Nguyen, H. H., Paskin-Cherniavsky, A., Ye, X. Constructing Leakage-resilient Shamir’s Secret Sharing: Over Composite Order Fields. // Purdue University, 2023. URL: https://www.cs.purdue.edu/homes/hmaji/papers/MNPY23b.pdf (дата звернення: 21.03.2025).

УДК 004.41:519.2

ГЕНЕРАТОРИ ВИПАДКОВИХ ЧИСЕЛ ТА ЇХ ЗАСТОСУВАННЯ

Шемшур С. О.
qfordrefy@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Фальченко Н. Г.
м. Черкаси, Україна

Генератор випадкових чисел – це апаратний або програмний пристрій, що створює послідовності чисел, які не мають жодної закономірності. Його головне завдання – забезпечити непередбачуваність результатів[1]. У сучасних інформаційних технологіях роль ГВЧ особливо важлива, оскільки вони є критично необхідними для криптографії, штучному інтелекті, моделюванні, фінансових операціях і навіть у розвагах

Істинні генератори випадкових чисел (TRNG) - це пристрої або алгоритми, які генерують числа на основі фізичного процесу, а не детермінованого алгоритму. Ці фізичні процеси за своєю суттю непередбачувані та можуть включати такі явища, як електронний шум, радіоактивний розпад або інші квантово-механічні ефекти. Ключовою характеристикою TRNG є те, що вони покладаються на ентропію з фізичного світу, що робить їхні результати справді випадковими та невідтворюваними [2].

Псевдовипадкові генератори (PRNG) - це алгоритми, які використовують математичні формули або попередньо обчислені таблиці для створення послідовностей чисел, які виглядають випадковими. Ключова відмінність між PRNG і TRNG полягає в тому, що PRNG є детермінованими; вони починаються з початкового значення та використовують його для створення послідовності чисел. Якщо початкове значення відоме, можна відтворити всю послідовність [2].

Криптографічно стійкі генератори (CSPRNG) - це спеціальний клас PRNG, призначений для задоволення вимог безпеки криптографічних програм. Вони виробляють псевдовипадкові послідовності, які обчислювально неможливо відрізнити від справжніх випадкових послідовностей, що означає, що зловмисник не може передбачити майбутні результати, навіть якщо він частково знає послідовність [2].

Генератори випадкових чисел широко застосовуються в різних галузях. У криптографії та захисті даних використання CSPRNG дозволяє забезпечити безпечне шифрування, надійність ключів і ефективне застосування одноразових систем шифрування, таких як one-time pad. У наукових дослідженнях та симуляціях активно використовують PRNG, де абсолютна випадковість не завжди є критичною, а високошвидкісний алгоритм дозволяє отримувати необхідні результати в реальному часі. Крім того, ГВЧ відіграють ключову роль у кібербезпеці, забезпечуючи створення надійних токенів та автентифікаційних механізмів, а також у системах онлайн-розіграшів і лотерей, де застосування криптографічно стійких алгоритмів гарантує чесність і прозорість процесу.

Оскільки тема моєї дипломної роботи стосується систем онлайн-розіграшів, де використовуються ГВЧ, розглянемо цей приклад більш детально. Інтеграція ГВЧ у подібну систему вимагає чіткого розмежування функцій різних типів генераторів. Для забезпечення абсолютної непередбачуваності та захисту від маніпуляцій критично важливо використовувати криптографічно стійкі генератори (CSPRNG). Вони відповідають за генерацію основних результатів розіграшу, гарантуючи рівні шанси для всіх учасників та унеможливлюючи

прогнозування наступних чисел, навіть при частковому розкритті внутрішнього стану алгоритму.

З іншого боку, псевдовипадкові генератори (PRNG) можуть використовуватися для допоміжних завдань, де абсолютна криптографічна стійкість не є критичною. Наприклад, вони можуть застосовуватися для обробки супутніх даних або візуалізації процесу, завдяки високій швидкодії та ефективності обчислень. Проте основний вибір переможців повинен здійснюватися виключно за допомогою CSPRNG, щоб гарантувати максимальну безпеку та чесність процесу. В моїй системі застосовано ГВЧ на основі генерації унікальних ідентифікаторів UUIDv4 та криптографічного алгоритму RSA. Це поєднання дозволяє забезпечити як унікальність кожного учасника, так і захист інформації на етапах її передачі та збереження. Зокрема, UUIDv4 використовується для створення унікальних ідентифікаторів учасників розіграшу, що унеможливлює дублювання та підробку. RSA, у свою чергу, застосовується для шифрування даних, автентифікації учасників та підпису результатів, що гарантує неможливість зміни результатів після завершення розіграшу.

Таким чином, у системах онлайн-розіграшів ключовим є використання криптографічно стійких алгоритмів для основного функціоналу, щоб забезпечити непередбачуваність, захист від підробки даних та несанкціонованого доступу, можливість перевірки результатів. Це дозволяє досягти оптимального балансу між безпекою, продуктивністю і масштабованістю системи.

Отже, вибір конкретного типу генератора випадкових чисел залежить від поставлених задач. TRNG забезпечують абсолютну випадковість, але мають технічні обмеження щодо швидкодії. PRNG характеризуються високою швидкістю, проте можуть бути вразливими, якщо відомий початковий стан. CSPRNG, у свою чергу, пропонують оптимальний баланс між швидкістю та безпекою, що робить їх незамінними в сучасних системах вибору переможців.

Список використаних джерел

1. «Генератори випадкових чисел та сфери їх використання» URL: https://mykyivregion.com.ua/news/generatori-vipadkovix-cisel-ta-sferi-yix-vikoristannya (дата звернення: 19.03.2025).
2. «Які ключові відмінності між генераторами справжніх випадкових чисел (TRNG), генераторами псевдовипадкових чисел (PRNG) і генераторами криптографічно безпечних псевдовипадкових чисел (CSPRNG)?» URL: https://uk.eitca.org/cybersecurity/eitc-is-ccf-classical-cryptography-fundamentals/stream-ciphers/stream-ciphers-random-numbers-and-the-one-time-pad/examination-review-stream-ciphers-random-numbers-and-the-one-time-pad/what-are-the-key-differences-between-true-random-number-generators-trngs-pseudorandom-number-generators-prngs-and-cryptographically-secure-pseudorandom-number-generators-csprngs/ (дата звернення: 19.03.2025).

УДК 004.42:004.75

ДОСЛІДЖЕННЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ МОБІЛЬНИХ ПЛАТФОРМ

Соболевський Д.А
den4uk0990@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М.В.
м. Черкаси, Україна

У сучасному цифровому суспільстві мобільні пристрої стали невід’ємною частиною повсякденного життя, що супроводжується інтенсивним зростанням обсягів персональних та корпоративних даних, що циркулюють через них. Внаслідок цього мобільні платформи стають дедалі привабливішою ціллю для кібератак. Основними причинами цього явища є їхня масовість, мобільність, гнучкість підключення до різних мереж, у тому числі. публічних Wi-Fi, обмежена ресурсна база для реалізації повноцінного захисту, а також фрагментованість екосистем мобільних операційних систем [4].

Згідно з дослідженнями провідних компаній у сфері інформаційної безпеки (Symantec, Kaspersky, McAfee), кількість зловмисних атак на Android- та iOS-пристрої зростає щорічно на 25–40%. Основними загрозами є шкідливе ПЗ, фішинг, підміна сертифікатів, атаки типу "man-in-the-middle" та несанкціонований доступ до системних ресурсів. У таких умовах виникає об’єктивна потреба у впровадженні ефективних систем виявлення вторгнень (IDS), які здатні аналізувати поведінку користувача, трафік, внутрішню активність системи та своєчасно виявляти підозрілу діяльність [2].

Системи виявлення вторгнень є ключовим елементом кіберзахисту, що виконує функції моніторингу, аналізу та реагування на аномальні або ворожі дії у цифровому середовищі. На відміну від традиційних антивірусних засобів, IDS не лише ідентифікують відомі загрози, а й мають потенціал до виявлення нових атак, що ще не мають сигнатур. Особливої актуальності набуває реалізація таких систем саме у мобільному середовищі, де обмежені ресурси пристрою диктують специфічні вимоги до енергоефективності, обчислювальної складності алгоритмів та мінімізації впливу на користувацький досвід.

Основні підходи до IDS у процесі розробки систем виявлення вторгнень застосовуються кілька базових підходів, кожен з яких має свої переваги, недоліки та сферу ефективного застосування. Характеристика типів систем виявлення вторгнень представлена в табл.1.

Зазначене порівняння дозволяє дійти висновку, що жодна з систем IDS не є універсальною. Вибір конкретної архітектури залежить від завдань, які стоять перед системою захисту, технічних характеристик пристрою, середовища експлуатації, а також характеру даних, які потребують захисту. Відповідно, актуальним напрямком досліджень є побудова адаптивних IDS з можливістю динамічного налаштування на змінні параметри загрозового середовища [7].

Таблиця 1. Порівняльна характеристика типів систем виявлення вторгнень

№	Тип системи IDS	Принцип дії	Переваги	Недоліки
1	Signature-based IDS	Аналіз даних на основі попередньо відомих сигнатур атак	Висока точність виявлення відомих атак; низький рівень хибнопозитивних спрацювань	Неможливість виявлення нових (0-day) атак; необхідність регулярного оновлення бази сигнатур
2	Anomaly-based IDS	Виявлення відхилень від нормальної поведінки системи чи користувача	Можливість виявлення нових, невідомих атак; адаптація до середовища	Високий рівень хибнопозитивних спрацювань; потреба у ретельному налаштуванні моделей
3	Hybrid IDS	Поєднання сигнатурного та поведінкового підходів	Баланс між точністю та гнучкістю; покращення якості виявлення атак	Ускладнена архітектура системи; вищі вимоги до обчислювальних ресурсів

Джерело: створено автором на основі даних [2, 7]

Зазначене порівняння дозволяє дійти висновку, що жодна з систем IDS не є універсальною. Вибір конкретної архітектури залежить від завдань, які стоять перед системою захисту, технічних характеристик пристрою, середовища експлуатації, а також характеру даних, які потребують захисту. Відповідно, актуальним напрямком досліджень є побудова адаптивних IDS з можливістю динамічного налаштування на змінні параметри загрозового середовища [7].

Формалізація задачі IDS Завдання побудови системи виявлення вторгнень можна представити у вигляді задачі машинного навчання або класифікації. Нехай існує множина об'єктів $X = \{x, x_2, \dots, x_n, \}$, де кожен об'єкт $x_i \in R^m$ описується вектором ознак, що характеризують поведінку користувача або стан системи. Метою є побудова функції класифікації:

$$f(x) = \{0, \text{нормативна активність} \quad 1, \text{аномальна активність}$$

Кожен вектор ознак може включати такі параметри, як: обсяг вхідного/вихідного трафіку, частота системних викликів, доступ до критичних ресурсів, використання CPU/RAM, спроби підключення до зовнішніх IP-адрес тощо.

Система IDS може навчатися у двох режимах [1]:

- З навчанням з учителем (supervised learning) для тренування використовується мітковий датасет (містить як нормальні, так і аномальні зразки), що дозволяє точно класифікувати майбутню поведінку.
- З навчанням без учителя (unsupervised learning) застосовується для виявлення невідомих шаблонів або кластеризації поведінки без попереднього маркування.

Математично задача оптимізації IDS зводиться до мінімізації функції втрат: де — функція втрат (наприклад, логістична або крос-ентропія), — реальні мітки об’єктів. У реальних мобільних системах для розв’язання цього завдання застосовуються алгоритми Support Vector Machines, Random Forest, нейронні мережі (CNN, RNN), а також гібридні моделі [3].

Формалізація задачі IDS створює теоретичне підґрунтя для побудови адаптивних, самонавчальних систем, здатних ефективно працювати в умовах постійної зміни характеру загроз та обмеженості мобільних ресурсів.

Для реалізації ефективної системи виявлення вторгнень у середовищі Android необхідно забезпечити послідовну обробку даних, що надходять від користувача до системи. Архітектура IDS для Android представлена на рисунку 1. Типова архітектура IDS включає декілька ключових компонентів, кожен з яких виконує свою специфічну функцію в процесі аналізу та реагування на загрози.

Рисунок 1. Архітектура IDS для Android

Порівняння IDS-систем для Android представлена на Рис. 2. На сьогодні розроблено ряд практичних реалізацій систем виявлення вторгнень, орієнтованих на мобільну платформу Android. Кожна з них має власну архітектуру, алгоритмічну основу та функціональні особливості.

Таблиця 2. Порівняльна характеристика IDS-систем для Android

№	Назва системи	Технологія	Тип IDS	Особливості
1	Andromaly	Machine Learning	Anomaly-based	Працює на рівні ядра Android; аналізує поведінкові характеристики
2	DroidDetector	Hybrid Model	Hybrid	Поєднує сигнатурний та поведінковий аналіз для підвищення точності
3	MADAM	Multilevel	Hybrid	Рівнева модель: Permissions, Events, Network; мультиаспектний підхід

Джерело: створено автором на основі даних [4, 9]

Дані системи демонструють різні рівні ефективності, гнучкості та інтеграції з мобільною операційною системою. Вибір конкретного рішення залежить від цілей захисту, ресурсоємності пристрою, а також вимог до швидкості реакції та точності класифікації загроз. У майбутньому очікується розширення функціональності таких IDS-систем за рахунок впровадження методів глибокого навчання та адаптивного аналізу контексту користувацької активності [6].

Отже, мобільні системи виявлення вторгнень є важливою складовою забезпечення кібербезпеки в умовах зростаючих цифрових загроз. Найефективнішими вважаються гібридні моделі, що поєднують сигнатурний та поведінковий аналіз. Подальший розвиток IDS повинен базуватись на інтеграції інтелектуальних технологій, врахуванні обмежень мобільного середовища та збереженні приватності користувача. Ефективна IDS дозволяє не лише своєчасно виявляти атаки, а й адаптуватись до нових загроз у реальному часі.

Список використаних джерел

1. G.V. Dias, K.N. Levitt, and B. Mukherjee, ‘‘Modeling Attacks on Computer Systems: Evaluating Vulnerabilities and Forming a Basis for Attack Detection,’’ Technical Report CSE-90-41, University of California, Davis, Jul. 1990 (дата звернення: 16.03.2025).

2. T.F. Lunt, A. Tamaru, F. Gilham, R. Jagannathan, C. Jalali, H.S. Javitz, A. Valdes, and P.G. Neumann, ‘‘A Real-Time Intrusion-Detection Expert System (IDES),’’ Interim Progress Report, Project 6784, SRI International, May 1990.
3. J.R. Winkler, ‘‘A Unix Prototype for Intrusion and Anomaly Detection in Secure Networks,’’ Proc. 13th National Computer Security Conference, pp. 115-124, Washington, D.C., Oct. 1990.
4. Партика О., Фіголь Б., Наконечний Т. Інтегрований підхід до виявлення загроз у bluetooth-протоколі за допомогою wireshark та splunk siem | електронне фахове наукове видання «кібербезпека: освіта, наука, техніка». 2024. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/684 (дата звернення: 16.03.2025).
5. DIDS (Distributed Intrusion Detection System) − Motivation, Architecture, and An Early Prototype. UC Davis Computer Security Lab. URL: https://seclab.cs.ucdavis.edu/papers/DIDS.ncsc91.pdf
6. Kupershtein L., Malinovskyi V. Cyber security of mobile devices and internet of things. 2024. URL: https://www.researchgate.net/publication/379257182_CYBER_SECURITY_OF_MOBILE_DEVICES_AND_INTERNET_OF_THINGS_KIBERBEZPEKA_MOBILNIH_PRISTROIV_TA_INTERNETU_RECEJ (дата звернення: 16.03.2025).
7. MITRE ATT&CK. URL: https://attack.mitre.org/
8. Spectrogram: A Mixture-of-Markov-Chains Model for Anomaly Detection in Web Traffic. Academic Commons. URL: https://academiccommons.columbia.edu/doi/10.7916/D8891G6G (дата звернення: 16.03.2025).

УДК 004.75:004.42

БРАУЗЕР TOR: НАЙАНОНІМНІШИЙ ВЕБ-БРАУЗЕР У СВІТІ

Пошитнюк Д.Ю.
dp80025080@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Фальченко Н.Г.
м. Черкаси, Україна

Браузер Tor використовується для доступу до прихованої мережі DarkNet, яка в свою чергу асоціюється з не дуже законними речами (чорні ринки, заборонені товари, відео-, фото- та аудіоматеріали, тощо.).

Tor (скор. від англ. The Onion Router) — це браузер, створений для забезпечення анонімності в мережі Інтернет. Клієнтське програмне забезпечення Tor маршрутизує Інтернет-трафік через всесвітню мережу добровільно встановлених серверів з метою приховування розташування користувача[1]. Змоделюємо ситуацію: вам потрібно зайти на сайт з якимось мемом, який вам скинув друг. Звичайний браузер встановить пряме підключення з сервером, надаючи йому та інколи не дуже добросовісним людям ваш IP та дані про вашу мережу, відповідно відслідкувати чи дізнатися інформацію про вас буде дуже просто. Натомість Tor, зроблений з мережі тисяч серверів (вузлів), зашифрує вашу інформацію в кілька етапів та перенаправить трафік через кілька з цих серверів, на кожному з яких багатошарово зашифрована інформація буде розшифровуватися по одному шару за кожен вузол (що нагадує шари цибулі). Це забезпечує більшу анонімність та безпеку вашого з’єднання.

Tor не створений суто для доступу в DarkNet, а є тільки одним з варіантів як туди потрапити. Для цього потрібно провести деякі махінації, які можна без проблем знайти в Інтернеті. За замовчуванням Tor використовує браузер DuckDuckGo, який сам по собі є конфіденційним (не збирає даних користувачів) доповнюючи його своїми системами шифрування, описаними раніше. В свою чергу DuckDuckGo не дуже відрізняється від того ж Google в плані пошуку інформації.

Tor використовує як основні протоколи TLS (Transport Layer Security) та TCP (Transmission Control Protocol) (TLS поверх TCP). TCP (частіше TCP/IP) – набір мережевих протоколів, за аналогією до поштової системи з нашого життя (написати листа, помістити в конверт з адресою, штампування його на пошті, тощо.). TLS в свою чергу займається шифруванням всіх даних методом публічних та приватних ключів.

Переваги браузера:

- Безкоштовний. Переглядач Tor безплатний для Android, Linux, macOS і Windows.
- Відкритий вихідний код. Оскільки Tor є проєктом з відкритим вихідним кодом, його можна завантажити й змінювати за бажанням.
- Незалежний. Tor працює завдяки волонтерам, тож він не потребує інвестицій у побудову власної інфраструктури. Оскільки він не розроблений для отримання прибутку, державні та правоохоронні органи не можуть впливати на його послуги.
- Шифрування. Tor забезпечує підвищену конфіденційність в Інтернеті та шифрує трафік, тому відстежити особу користувача по його інтернет-слідам неможливо.
- Приховує IP-адресу. У базових налаштуваннях Tor встановлено приховувати IP-адресу користувача, тому ніхто не зможе побачити ваше справжнє місцеперебування.
- Доступ до сайтів .onion. Tor дозволяє отримати доступ до невидимої частини Інтернету та переглядати Даркнет.
- Недоліки браузера:
- Репутація. Tor використовується не тільки людьми, що піклуються про свою конфіденційність в Інтернеті, але й злочинцями. Отже, деякі служби блокують Tor через його погану репутацію, і можна зіткнутися з обмеженнями під час спроби отримати доступ до законних сайтів.

- Швидкість. Оскільки трафік користувача переміщується між різними вузлами і шифрується кілька разів, швидкість інтернету буде повільнішою, ніж зазвичай.

Стереотипи з приводу використання мережі DarkNet виявляються в тому, що більшість користувачів DarkNet – це читачі новинних видань країн з жорсткою цензурою, піратських форумів (зачасту поширення книг з авторським правом) чи звичайні форуми, де можна поспілкуватися з іншими людьми анонімно. Відповідно, більшість сайтів зроблені саме під ці запити користувачів. Звісно, є і ресурси з набагато більш незаконним контентом. Оскільки браузер Tor має високу степінь шифрування користувачі мережі DarkNet надають перевагу цьому браузеру для збереження власної анонімності.

Браузер Tor вважається найанонімнішим браузером у світі. Цей статус дотримується шляхом ефективних методів шифрування. Також проект має відкритий програмний код та працює завдяки волонтерам, через що є безкоштовним. Звісно ж він має і мінуси, як от низька швидкість з'єднання. Також браузер надає доступ до DarkNet, який вважають осередком злочинності, але чи так є насправді кожен вирішує сам для себе.

Список використаних джерел:

1. Wikipedia. Tor. URL: https://uk.wikipedia.org/wiki/Tor (дата звернення: 19.03.2025).
2. YouTube. What is Tor and Should You Use It? | Mashable Explains. URL: https://www.youtube.com/watch?v=6czcc1gZ7Ak (дата звернення: 19.03.2025).
3. Wikipedia. Transport Layer Security. URL: https://uk.wikipedia.org/wiki/Transport_Layer_Security (дата звернення: 19.03.2025).
4. Wikipedia. TCP. URL: https://uk.wikipedia.org/wiki/TCP (дата звернення: 19.03.2025).

5. NordVPN. Чи Tor безпечний браузер?. URL: https://nordvpn.com/uk/blog/chy-tor-bezpechnyy-brauzer/ (дата звернення: 19.03.2025).
6. Wikipedia. Darknet. URL: https://en.wikipedia.org/wiki/Darknet (дата звернення: 19.03.2025).

УДК 004.42:004.9

ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ ТА ЇХ РОЛЬ У КІБЕРБЕЗПЕЦІ

Хохлов К. Д.
hohlovkosta777@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Віртуальні приватні мережі (VPN) – це технологія, яка створює безпечне з'єднання поверх менш захищеної мережі, такої як Інтернет. Вона дозволяє користувачам безпечно передавати дані, приховуючи свою IP-адресу та шифруючи інтернет-трафік, що забезпечує секретність і захищеність особистої інформації. VPN також надає можливість обходити географічні обмеження, надаючи доступ до контенту, який може бути недоступним у певному регіоні. Це досягається шляхом підключення до серверів, розташованих в інших країнах, що дозволяє змінити віртуальне місцезнаходження користувача. Використання VPN є важливим для забезпечення безпеки в Інтернеті, особливо при підключенні через загальнодоступні Wi-Fi мережі, оскільки воно захищає дані від потенційних загроз і несанкціонованого доступу.

VPN-тунель – це віртуальне зашифроване стійким алгоритмом з’єднання. Наочно, його можна представити у вигляді непрозорої труби, а ще краще тунелю, один кінець якого входить в комп'ютер рядового користувача, а другий в спеціалізований сервер, що знаходиться, як правило, в іншій країні.

Сучасні види VPN підключення:

1. PPTP
2. OpenVPN
3. L2TP

PPTP (Point-to-point tunneling protocol) – це такий тунельний протокол типу «point-point», який дозволяє комп'ютеру користувача встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеною мережі. Цей протокол (PPTP) став відомий, тому що, це перший VPN протокол, який підтримала корпорація Microsoft. Це найвідоміший і простий в налаштуванні варіант підключення до VPN-сервісу.

OpenVPN – це вільна реалізація технології Віртуальної Приватної Мережі (VPN) з відкритим вихідним кодом для створення зашифрованих каналів виду «point-point» або «server-clients» між комп'ютерами. Вона може встановлювати з'єднання між комп'ютерами, які знаходяться за NAT-firewall без необхідності зміни його налаштувань.

L2TP (Layer 2 Tunneling Protocol) – це мережевий протокол тунелювання канального рівня, що поєднує в собі протокол L2F (layer 2 Forwarding), розроблений компанією Cisco, і протокол від корпорації Microsoft. Дозволяє створювати VPN із заданими пріоритетами доступу, однак не містить в собі засобів шифрування і механізмів аутентифікації (для створення захищеної VPN його використовують спільно з IPSec). За відгуками експертів, є найбільш захищеним варіантом VPN підключення, незважаючи на труднощі його налаштування.

VPN-сервіс – це сервіс, за допомогою якого користувач налаштовує захищене, зашифроване з’єднання між пристроєм та віддаленим сервером. Це з’єднання відображається як тунель, оскільки воно приховує фактичнку IP-адресу та шифрує інтернет-з’єднання для додаткового рівня конфіденційності та безпеки, зокрема при використанні публічних Wi-Fi або обходженні географічних обмежень.

Ось кілька прикладів VPN-сервісів:

1. NordVPN – один з головних сервісів з клієнтами який володіє величезним сервенним парком по всьаму світу, високою швидкістю та сильним шифруванням.
2. ExpressVPN; принципово відомий великим типом пристроїв, які підтримують Б Більш активне зношення після розкриття рекламного ролика з розламом хостових мегоніторів.
3. ProtonVPN – швейцарський VPN, орієнтований на забезпечення максимальної конфіденційності, із відкритим вихідним кодом та незалежними аудитами політики «no-logs».
4. Surfshark VPN – пропонує необмежену кількість одночасних з'єднань, має сучасні функції, такі як блокування реклами та трекерів, і відзначається конкурентною ціною.
5. IPVanish – забезпечує високу швидкість і ефективну безпеку, дозволяючи використовувати VPN на великій кількості пристроїв одночасно.
6. Atlas VPN – freemium-сервіс, який пропонує безкоштовний базовий функціонал, а також платні плани з додатковими можливостями захисту.
7. Amnezia VPN – відкритий VPN-інструмент для створення власного VPN-сервера, який не вимагає реєстрації та не веде логів, що особливо цінується користувачами, які хочуть мати повний контроль над своїми даними.

Служби VPN відіграють важливу роль у забезпеченні мережевої безпеки і допомагають захистити дані та конфіденційність під час обміну інформацією через Інтернет. Ось деякі з основних елементів їхньої ролі:

Шифрування трафіку. VPN створюють безпечний тунель, який шифрує дані, що передаються між користувацьким пристроєм і віддаленим сервером. Це не дозволяє зловмисникам, інтернет-провайдерам та державним органам перехоплювати інформацію та відстежувати діяльність в Інтернеті.

Маскування та секретність IP-адреси. VPN змінює IP-адресу на адресу VPN-сервера, ризик відстеження користувацьких дій в Інтернеті або визначення фізичного місцезнаходження зводиться до мінімуму. Це важливо для

користувачів, які бажають зберегти анонімність, а також для журналістів та активістів, які працюють в авторитарних режимах.

Захищене підключення до публічних мереж. Підключення до громадських мереж Wi-Fi, таких як кафе та аеропорти, часто скомпрометовані через відсутність належного шифрування; VPN забезпечують безпечне з'єднання з цими мережами, мінімізуючи ризик викрадення конфіденційної інформації.

Безпечний віддалений доступ. Являючись важливим інструментом для організацій, VPN дозволяють співробітникам безпечно і віддалено підключатися до мереж компанії. Це захищає конфіденційну інформацію та забезпечує безпечну віддалену роботу.

Уникнення цензури та географічних обмежень. VPN дозволяють отримати доступ до контенту, який заблокований або обмежений у країні, змінюючи віртуальне місцезнаходження.

Список використаних джерел

1. Fearn N. What is a VPN and how does it work?. New York Post. URL: https://nypost.com/shopping/what-is-a-vpn-and-how-does-it-work/ (date of access: 24.03.2025).
2. Віртуальні приватні мережі (VPN). КомпБест – інтернет-магазин брендових ПК з Європи. URL: https://compbest.com.ua/ua/virtualnye-chastnye-seti-vpn/?srsltid=AfmBOooFizBOi140bDnW3SGXy3znLceI-JnseW1nZqaVpF-JEPcXQX-j (дата звернення: 24.03.2025).
3. Що таке мережа VPN і як вона працює. Experience - Discover How Dropbox Empowers Teams - Dropbox. URL: https://experience.dropbox.com/uk-ua/resources/what-is-vpn (дата звернення: 24.03.2025).

УДК 004.9:070.3

АВТОМАТИЗОВАНИЙ АНАЛІЗ ФЕЙКОВИХ НОВИН ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Воробйова В.Ю.
vorobyova.valentina2005@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р.В.
м. Черкаси, Україна

Фейкові новини стали серйозною загрозою для сучасного інформаційного середовища, оскільки можуть маніпулювати громадською думкою, поширювати дезінформацію та створювати соціальну напругу. Ручні методи перевірки фактів вимагають значних ресурсів і часу, тому автоматизовані підходи, що базуються на штучному інтелекті, є перспективним рішенням для виявлення неправдивої інформації. Завдяки сучасним алгоритмам штучного інтелекту можна аналізувати великі обсяги даних, визначати ненадійні джерела та виявляти маніпуляції у текстах, зображеннях і відео.

Штучний інтелект використовує різні підходи для аналізу та виявлення фейкових новин. Один із ключових методів – обробка природної мови (Natural Language Processing, NLP), що дозволяє аналізувати структуру та зміст тексту. Алгоритми штучного інтелекту виявляють характерні ознаки неправдивих новин, такі як емоційно забарвлена лексика, упередженість чи сенсаційність. Завдяки глибокому навчанню нейромережі здатні розпізнавати мовні патерни та логічні невідповідності, що часто присутні у фейкових матеріалах.

Інший важливий аспект – перевірка достовірності джерел. Алгоритми аналізують репутацію джерела, наявність надійних посилань та кореляцію з іншими авторитетними медіа. Для цього використовуються великі бази даних, які містять інформацію про довіреність різних новинних порталів. Окрім текстового аналізу, ШІ здатен розпізнавати змінені зображення та відео за допомогою алгоритмів комп’ютерного зору. Це особливо актуально у боротьбі з так званими "deepfake"-технологіями, які дозволяють створювати відео, що візуально ідентичні реальним, але містять неправдивий зміст.

Сучасні методи боротьби з дезінформацією ґрунтуються на кількох технологічних підходах. По-перше, застосовуються алгоритми машинного навчання (Machine Learning, ML) та глибокого навчання (Deep Learning, DL). Такі моделі навчаються на великих наборах даних, де аналізують мільйони статей, соціальних постів і коментарів для виявлення спільних рис фейкових новин. Нейромережі можуть розпізнавати структуру речень, тональність тексту та логічну послідовність викладених фактів.

По-друге, активно розвивається метод Explainable AI (XAI), який робить результати аналізу штучного інтелекту більш зрозумілими для користувачів. Це дає змогу не лише виявити фейк, а й пояснити, чому певна новина класифікується як неправдива. Також використовуються технології блокчейну для перевірки автентичності новин. Блокчейн дозволяє відстежувати походження інформації, запобігаючи маніпуляціям та зміні вмісту публікацій після їх розповсюдження.

Попри значні досягнення у сфері автоматизованого аналізу фейкових новин, існують певні виклики. Одним із головних є постійна адаптація методів створення фейкових новин, що змушує ШІ-моделі постійно оновлюватися та вдосконалюватися. Додатковою складністю є неоднозначність деяких новин, що містять змішані факти, що ускладнює їх класифікацію. Крім того, надмірне використання автоматизованих алгоритмів може призводити до блокування правдивої, але суперечливої інформації, що може викликати питання щодо цензури та свободи слова.

Майбутні дослідження у сфері автоматизованого аналізу фейкових новин можуть зосередитися на кількох напрямках. По-перше, важливо створювати більш точні та адаптивні моделі ШІ, які здатні швидко реагувати на нові методи дезінформації. По-друге, інтеграція технологій блокчейну для перевірки джерел може забезпечити більшу прозорість і незмінність інформації. По-третє, необхідно розробляти інструменти пояснюваного ШІ (Explainable AI), які дозволять зробити аналіз прозорішим для користувачів.

У перспективі можливе створення глобальних платформ перевірки фактів,

що поєднуватимуть штучний інтелект із експертною оцінкою журналістів та аналітиків. Це дозволить підвищити ефективність боротьби з дезінформацією та зробити цифровий інформаційний простір безпечнішим для користувачів.

Штучний інтелект відіграє ключову роль у боротьбі з фейковими новинами, забезпечуючи ефективний аналіз інформації, перевірку джерел і виявлення маніпуляцій. Однак для досягнення максимальної ефективності необхідно поєднувати автоматизовані методи з людським контролем та вдосконалювати алгоритми аналізу. Використання сучасних технологій, таких як машинне навчання, глибокі нейромережі, Explainable AI та блокчейн, може значно підвищити ефективність боротьби з фейками та забезпечити достовірність інформації в медіа-просторі.

Список використаних джерел

1. BBC Україна. Посилання на статтю. URL: https://www.bbc.com/ukrainian/topics/c6vzyzw21qnt (дата звернення: 19.03.2025).
2. Mind.ua. Найновіші розробки алгоритмів для автоматичного розпізнавання фейкових новин. URL: https://mindua.org/dif/naynovishi-rozrobky-alhorytmiv-dlia-avtomatychnoho-rozpiznavannia-feykovykh-novyn.html (дата звернення: 19.03.2025).
3. Wikipedia. Обробка природної мови. URL: https://uk.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%BE%D0%B1%D0%BA%D0%B0_%D0%BF%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%BD%D0%BE%D1%97_%D0%BC%D0%BE%D0%B2%D0%B8 (дата звернення: 19.03.2025).
4. Unite.ai. Що таке обробка природної мови?. URL: https://unite.ai/uk/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BE%D0%B1%D1%80%D0%BE%D0%B1%D0%BA%D0%B0-%D0%BF%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%BD%D0%B

E%D1%97-%D0%BC%D0%BE%D0%B2%D0%B8/ (дата звернення: 19.03.2025).

5. Oksim.ua. Наскільки ми близькі до точного детектора фейкових новин зі штучним інтелектом. URL: https://www.oksim.ua/2024/12/09/naskilky-mi-blizki-do-tochnogo-detektora-fejkovih-novin-zi-shtuchnim-intelektom-2/ (дата звернення: 19.03.2025).
6. IEEE Spectrum. What is Deepfake?. URL: https://spectrum.ieee.org/what-is-deepfake (дата звернення: 19.03.2025).
7. IBM. Machine Learning. URL: https://www.ibm.com/think/topics/machine-learning (дата звернення: 19.03.2025).
8. GeeksforGeeks. Introduction to Deep Learning. URL: https://www.geeksforgeeks.org/introduction-deep-learning/ (дата звернення: 19.03.2025).
9. GeeksforGeeks. Explainable Artificial Intelligence (XAI). URL: https://www.geeksforgeeks.org/explainable-artificial-intelligencexai/ (дата звернення: 19.03.2025).
10. IBM. Explainable AI. URL: https://www.ibm.com/think/topics/explainable-ai (дата звернення: 19.03.2025).
11. Binance Academy. *What is Blockchain and How Does it Work?*. URL: https://academy.binance.com/uk-UA/articles/what-is-blockchain-and-how-does-it-work (дата звернення: 19.03.2025).

УДК 004.9:616

AI УМЕДИЦИНІ – ДІАГНОСТИКА, ПРОГНОЗУВАННЯ ХВОРОБ, ПЕРСОНАЛІЗОВАНА МЕДИЦИНА

Ковальчук В.М
vladislav72k@gmail.con
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Ратайчук П.Є.
м. Черкаси, Україна

Актуальність теми обумовлена стрімким розвитком штучного інтелекту в медицині, особливо в діагностиці, прогнозуванні хвороб та персоналізованій медицині. Сучасні AI-технології відіграють важливу роль у трансформації системи охорони здоров'я, підвищуючи точність діагностичних процедур, оптимізуючи лікувальні процеси та забезпечуючи індивідуальний підхід до кожного пацієнта. Вплив AI на медицину підтверджується численними дослідженнями та впровадженням технологій у клінічну практику. Такі компанії, як IBM Watson Health, Google DeepMind та OpenAI, активно розробляють алгоритми, що допомагають лікарям приймати обґрунтовані рішення, аналізувати великі обсяги медичних даних та прогнозувати розвиток захворювань.

Одним із найбільш значущих застосувань AI є рання діагностика раку. Алгоритми глибокого навчання здатні аналізувати рентгенівські знімки, МРТ та КТ, виявляючи патологічні зміни з високою точністю. Наприклад, штучний інтелект, розроблений компанією Google Health, продемонстрував здатність діагностувати рак молочної залози точніше, ніж досвідчені радіологи. Дослідження показало, що алгоритм зменшив кількість хибно позитивних і хибно негативних діагнозів, що значно підвищило ефективність скринінгових програм. Також AI використовується для прогнозування ефективності лікування онкологічних захворювань, аналізуючи генетичні дані пацієнта та підбираючи найбільш ефективні методи терапії.

Персоналізована медицина – ще один важливий напрямок, де AI відіграє ключову роль. Аналізуючи генетичні, біохімічні та клінічні дані, штучний

інтелект допомагає створювати індивідуальні плани лікування, що значно підвищує ефективність терапії. Наприклад, в онкології AI сприяє розробці таргетної терапії, яка враховує особливості геному пацієнта та дозволяє максимально точно впливати на ракові клітини, мінімізуючи побічні ефекти.

AI також використовується у прогнозуванні захворювань, аналізуючи великі обсяги медичних записів та виявляючи закономірності, що можуть свідчити про ризик розвитку певних патологій. Це особливо важливо для раннього виявлення серцево-судинних захворювань, діабету та нейродегенеративних хвороб.

Наприклад, дослідження показали, що AI-моделі можуть прогнозувати ризик серцевого нападу за допомогою аналізу очного дна, що відкриває нові можливості для неінвазивної діагностики.

Попри численні переваги, застосування AI у медицині супроводжується викликами, такими як етичні питання, безпека даних та необхідність розробки регуляторних стандартів. Важливим аспектом є забезпечення прозорості алгоритмів, адже лікарі повинні розуміти, на основі яких критеріїв AI ухвалює рішення. Також необхідно врегулювати питання конфіденційності медичних даних та захисту персональної інформації пацієнтів.

Регулювання та стандартизація AI в медицині є необхідними для його ефективного та безпечного використання. Співпраця між медичними установами, дослідниками, урядовими органами та технологічними компаніями сприятиме гармонійному розвитку цієї сфери. У майбутньому AI може значно вдосконалити діагностичні та лікувальні методи, сприяючи появі нових підходів до лікування складних захворювань та персоналізованої медицини. Штучний інтелект вже сьогодні допомагає лікарям рятувати життя, і його роль у медицині буде лише зростати, забезпечуючи ефективніші, доступніші та безпечніші медичні послуги для пацієнтів у всьому світі.

Список використаної літератури

1. Topol, E. (2019). Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again. Basic Books.
2. Obermeyer, Z., & Emanuel, E. J. (2016). Predicting the Future — Big Data, Machine Learning, and Clinical Medicine. New England Journal of Medicine, 375(13), 1216–1219.
3. Rajpurkar, P., Irvin, J., Zhu, K., Yang, B., Mehta, H., Duan, T., ... & Ng, A. Y. (2017). CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning. arXiv preprint arXiv:1711.05225.
4. Esteva, A., Kuprel, B., Novoa, R. A., Ko, J., Swetter, S. M., Blau, H. M., & Thrun, S. (2017). Dermatologist-level classification of skin cancer with deep neural networks. Nature, 542(7639), 115-118.
5. McKinney, S. M., Sieniek, M., Godbole, V., Godwin, J., Antropova, N., Ashrafian, H.,& Suleiman, A. (2020). International evaluation of an AI system for breast cancer screening

УДК 004.42:004.9

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ВИЯВСЕННІ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Ганжуга А. Ю.
hanguga2005@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р.В.
м. Черкаси, Україна

Штучний інтелект (ШІ) є однією з найперспективніших технологій сучасності, яка активно впроваджується у сферу кібербезпеки. Зокрема, його використання для виявлення шкідливого програмного забезпечення (ПЗ) відкриває нові можливості для захисту інформаційних систем від загроз, які стають дедалі складнішими та витонченішими. У контексті України, де цифровізація набирає обертів, розвиток таких технологій має стратегічне значення для захисту державної інфраструктури, бізнесу та персональних даних

громадян.

Традиційні методи виявлення шкідливого ПЗ, такі як сигнатурний аналіз, поступово втрачають ефективність через зростання кількості нових видів загроз, зокрема поліморфного ПЗ та атак нульового дня (zero-day attacks). Це обумовлено тим, що сучасні віруси здатні змінювати свій код або приховувати свою активність, щоб уникнути виявлення. У цьому контексті ШІ пропонує принципово новий підхід до боротьби зі шкідливим ПЗ. Завдяки алгоритмам машинного навчання та глибинного аналізу даних, ШІ може розпізнавати складні патерни поведінки програм, які залишаються непоміченими для традиційних систем.

Одним із ключових аспектів використання ШІ є поведінковий аналіз. Замість того щоб орієнтуватися на відомі сигнатури шкідливого ПЗ, системи на основі ШІ аналізують дії програм у реальному часі. Наприклад, якщо програма намагається отримати несанкціонований доступ до конфіденційних даних або змінити системні налаштування без дозволу користувача, ШІ може миттєво заблокувати її активність. Такий підхід дозволяє ефективно боротися навіть із новими загрозами, про які раніше не було інформації.

ШІ також здатний працювати з великими обсягами даних і швидко адаптуватися до змін. Наприклад, моделі машинного навчання можуть навчатися на історичних даних про атаки та прогнозувати появу нових варіантів шкідливого ПЗ. Це дає можливість створювати проактивні системи захисту, які не лише реагують на загрози, але й передбачають їхню появу. Крім того, ШІ дозволяє автоматизувати процес класифікації шкідливого ПЗ, що значно прискорює розробку контрзаходів.

Практичне застосування ШІ у сфері кібербезпеки охоплює широкий спектр завдань. Наприклад, він використовується для моніторингу кінцевих точок (комп’ютерів, смартфонів тощо), аналізу мережевого трафіку та фільтрації електронної пошти й веб-контенту. Системи на основі ШІ можуть блокувати фішингові атаки шляхом аналізу поведінки відправника та змісту повідомлень або виявляти командні сервери ботнетів у реальному часі. Також вони здатні

розпізнавати аномалії у роботі пристроїв і мережі, що є важливим для запобігання складним атакам.

Однак впровадження ШІ у кібербезпеку супроводжується певними викликами. Одним із них є ризик хибних спрацьовувань: система може помилково визначити безпечний файл як загрозу, що призводить до затримок у роботі або втрати даних. Крім того, хакери можуть використовувати адверсаріальні атаки — маніпуляції з даними для обходу алгоритмів ШІ. Ще одним викликом є необхідність постійного вдосконалення моделей машинного навчання через швидкий розвиток технологій і появу нових видів загроз.

Важливо також враховувати етичні аспекти використання ШІ у кібербезпеці. Автоматизація процесів виявлення загроз може призводити до порушення конфіденційності даних користувачів або до надмірного контролю за їхньою діяльністю. Тому необхідно розробляти регуляторні механізми, які забезпечуватимуть баланс між ефективністю технологій та правами людини.

Таким чином, роль штучного інтелекту у виявленні шкідливого програмного забезпечення є визначальною для сучасної кібербезпеки. Його інтеграція дозволяє значно підвищити ефективність боротьби зі складними загрозами та забезпечити захист інформаційних систем від атак нового покоління. У контексті України розвиток таких рішень має стратегічне значення для захисту критичної інфраструктури й інформаційної безпеки держави. Інвестиції у дослідження та впровадження технологій ШІ стануть важливим кроком до побудови стійкої цифрової екосистеми країни.

Список використаних джерел:

AI in Malware Detection and Analysis. Insights2Techinfo. URL: https://insights2techinfo.com/ai-in-malware-detection-and-analysis/ (date of access: 15.03.2025).

AI in Malware Detection. Redress Compliance - Just another WordPress site. URL: https://redresscompliance.com/ai-malware-detection/ (date of access: 15.03.2025).

Kosinski M. How to Fight AI Malware | IBM. IBM - United States. URL: https://www.ibm.com/think/insights/defend-against-ai-malware (date of access: 15.03.2025).

N-iX. Tech Landscape in Ukraine: Market Trends and Highlights for 2025. LinkedIn: Log In or Sign Up. URL: https://www.linkedin.com/pulse/ukrainian-tech-landscape-2025-market-overview-n-ix-tks1f/ (date of access: 15.03.2025).

Sibanda I. Why we need advanced malware detection with AI-powered tools | Computer Weekly. ComputerWeekly.com. URL: https://www.computerweekly.com/feature/Why-we-need-advanced-malware-detection-with-AI-powered-tools (date of access: 15.03.2025).

The Role of Artificial Intelligence in Malware Detection. Siberoloji. URL: https://www.siberoloji.com/the-role-of-artificial-intelligence-in-malware-detection/ (date of access: 15.03.2025).

Top Malware Detection Techniques – Key Methods Explained. AMATAS. URL: https://amatas.com/blog/top-malware-detection-techniques-key-methods-explained/ (date of access: 15.03.2025).

Ukraine’s Tech Landscape: Market Trends for 2025. Software Development Company - N-iX. URL: https://www.n-ix.com/news/n-ix-releases-2025-report-ukraine-tech-landscape/ (date of access: 15.03.2025).

What Is the Role of AI in Threat Detection?. Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection (date of access: 15.03.2025).

УДК 004.42:004.7

СИСТЕМА ОЦІНКИ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

Шпак М.О.
Maksimshpak20047a@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: М.В.
м. Черкаси, Україна

Хмарні технології стали основою цифрової трансформації багатьох галузей. Проте зростаюча кількість кіберзагроз актуалізує питання надійної системи оцінки безпеки хмарних сервісів. Різні моделі розгортання (IaaS, PaaS, SaaS) мають свої унікальні ризики, тому для забезпечення інформаційної безпеки важливо впровадити комплексну систему оцінки [2].

У сучасних умовах активного впровадження хмарних технологій постає необхідність розробки ефективних методів оцінки ризиків, пов'язаних із їх використанням. Пропонується багаторівнева модель оцінки безпеки хмарних сервісів, яка базується на таких компонентах:

1. Ідентифікація ризиків (R) - визначення потенційних загроз, які можуть вплинути на безпеку хмарних сервісів.
2. Аналіз вразливостей (V) - виявлення слабких місць у системі, які можуть бути використані для реалізації загроз.
3. Критичність активів (C) - оцінка важливості інформаційних активів для організації та наслідків їх компрометації.
4. Можливий вплив (I) - оцінка потенційних наслідків реалізації ризику для організації.

Для кількісної оцінки ризику Q використовується наступна формула:

$$Q = R \times V \times C \times I \quad (1),$$

де

R - ймовірність реалізації загрози,

V - вразливість активу (ступінь сприйнятливості до загрози),

C - цінність активу або вартість можливих збитків,

I - можливий вплив або наслідки реалізації ризику для організації.

Дана модель дозволяє систематично підходити до оцінки ризиків у хмарних сервісах, враховуючи специфіку їх використання та потенційні загрози. Зокрема, важливо враховувати такі аспекти:

- Надійність роботи та інформаційна безпека - оцінка показників надійності збереження даних, захисту даних при передачі, автентифікації користувачів, інтеграції криптографічних методів, наявності політик безпеки та контролю доступу.
- Фінансові та юридичні аспекти – аналіз можливих фінансових або юридичних проблем постачальника хмарних послуг, які можуть вплинути на безперебійність та безпеку сервісів.
- Операційні ризики: оцінка можливих експлуатаційних проблем або простоїв постачальника, які можуть вплинути на доступність та якість хмарних сервісів.

Використання даної моделі сприяє більш обґрунтованому прийняттю рішень щодо впровадження та використання хмарних технологій, забезпечуючи баланс між інноваціями та безпекою [4].

Оцінка безпеки хмарних сервісів є критичним аспектом для забезпечення надійності та захисту даних в інформаційних системах. Оцінка кожного з цих критеріїв за шкалою від 1 до 5 дозволяє визначити рівень безпеки хмарного сервісу та виявити області, які потребують покращення (табл.1).

Таблиця 1. Критерії оцінки безпеки

№	Критерій	Пояснення	Оцінка (1–5)
1	Захист даних при зберіганні	Використання шифрування, резервного копіювання	4
2	Контроль доступу	Механізми автентифікації/авторизації	4
3	Безпека при передачі даних	TLS, VPN, захист каналів	3
4	Аудит та моніторинг	Журнали подій, аналітика, SIEM-системи	4
5	Відповідність стандартам (ISO/IEC)	Стандарти безпеки (ISO 27001, GDPR тощо)	5

Оцінка безпеки хмарних сервісів передбачає використання структурованого підходу, який дозволяє системно аналізувати наявні ризики, визначати слабкі місця та формувати обґрунтовані заходи щодо підвищення рівня захисту. Одним

із ключових елементів цього процесу є побудова архітектури системи оцінки безпеки (рис. 1), що охоплює всі основні етапи інформаційного аналізу[7].

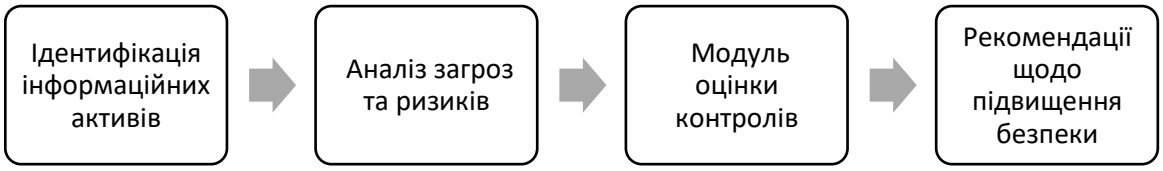

Рисунок 1. Архітектура системи оцінки

На першому етапі відбувається ідентифікація ключових інформаційних активів, які є об’єктами захисту. Далі здійснюється аналіз потенційних загроз та оцінка відповідних ризиків з урахуванням специфіки хмарної інфраструктури. Після цього проводиться аналіз ефективності наявних заходів захисту – контрольних механізмів, політик доступу, шифрування тощо. Завершальним етапом є формування комплексу рекомендацій, спрямованих на усунення виявлених недоліків та підвищення загального рівня безпеки системи [3].

Запровадження такої архітектури дозволяє організаціям забезпечити системний моніторинг стану безпеки хмарних сервісів, своєчасно реагувати на зміни в ризиковому середовищі та дотримуватись вимог міжнародних стандартів у сфері інформаційної безпеки.

Для забезпечення практичної реалізації ефективної системи оцінки безпеки хмарних сервісів доцільним є використання сучасних технологічних рішень та перевірених методик, які дозволяють комплексно контролювати рівень інформаційного захисту [2].

Підхід до реалізації на практиці включає такі ключові елементи:

1) Впровадження автоматизованих інструментів безпеки:

- Cloud Security Posture Management (CSPM) – інструменти, що забезпечують автоматичне виявлення конфігураційних помилок, відстеження політик безпеки та виявлення відхилень від нормативних стандартів у хмарному середовищі.

- Cloud Access Security Broker (CASB) – проміжне ПЗ між користувачем та хмарним сервісом, яке забезпечує контроль доступу, моніторинг трафіку, виявлення аномалій та захист від витоку даних.

2) Регулярне проведення пентестів та аудиту безпеки – імітація атак з метою виявлення вразливих місць у хмарній інфраструктурі, а також аудит конфігурацій, доступів та відповідності політик безпеки.
3) Оцінка ризиків за методикою CVSS (Common Vulnerability Scoring System) – стандартизований підхід до оцінки рівня небезпеки вразливостей. Він дозволяє кількісно оцінити потенційну загрозу та визначити пріоритети щодо її усунення.

Таблиця 2. Приклад оцінки за CVSS

№	Показник	Значення
1	Базова метрика (Base)	7,8
2	Темпова метрика (Temporal)	6,9
3	Експлуатаційна метрика (Environmental)	5,5

Зазначені значення свідчать про високий рівень ризику, що потребує оперативного реагування та впровадження додаткових захисних заходів. Системна інтеграція таких підходів забезпечує не лише оцінку поточного стану безпеки, але й створює умови для його постійного вдосконалення.

Отже, безпека хмарних сервісів є одним із найважливіших аспектів сучасної цифрової інфраструктури. З огляду на зростаючі обсяги обробки, передачі та зберігання даних у хмарному середовищі, організаціям необхідно впроваджувати системний підхід до оцінки рівня інформаційного захисту. Запропонована багаторівнева модель оцінки безпеки, яка включає ідентифікацію ризиків, аналіз вразливостей, критичність активів і потенційний вплив, дозволяє здійснювати комплексну оцінку ризиків та приймати обґрунтовані управлінські рішення [1].

Використання чітких критеріїв безпеки, таких як захист даних, контроль доступу, аудит, відповідність міжнародним стандартам, а також застосування сучасних інструментів – CSPM, CASB, методик CVSS – сприяє підвищенню загального рівня кіберзахисту хмарної інфраструктури. Крім того, регулярний

аудит, моніторинг подій та пентестування дозволяють своєчасно виявляти та усувати потенційні загрози.

Список використаних джерел

1. Камінський О. Є. Моделювання оцінки ризиків при використанні «хмарних» сервісів. URL: https://ir.kneu.edu.ua/server/api/core/bitstreams/e04afaf6-e1da-4b41-91db-48e6803eaa87/content (дата звернення: 15.03.2025).
2. Малярчук І., Смолинець М. Підвищення ефективності бізнес-процесів через застосування хмарних технологій: безпековий аспект | економіка та суспільство. 2024. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3546 (дата звернення: 15.03.2025).
3. Моделі хмарних сервісів. Фундаментальні та прикладні проблеми сучасних технологій: матеріали Міжнародної науково-технічної конференції. Тернопіль : ТНТУ ім. І. Пулюя, 2018. С. 226–227.
4. Charnes A., Cooper W. W., Rhodes E. Measuring the efficiency of decision-making units. European Journal of Operational Research. 1978. Vol. 2. P. 429–444.
5. Hwang C.L., Yoon K. Methods for Multiple Attribute Decision Making. Multiple Attribute Decision Making. (Lecture Notes in Economics and Mathematical Systems). Berlin: Springer, 1981. P. 58-191.
6. Opricovic S. Multicriteria Optimization in Civil Engineering (in Serbian), Faculty of Civil Engineering, Belgrade, 1998. 302 p.
7. Saaty T. L. How to make a decision: The analytic hierarchy process. Interfaces. 1994. Vol. 24. № 6. P. 19–43.

УДК 004.4:004.9

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В ТЕСТУВАННІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Володін Г. Ф.
glebvolliodin@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р. В.
м. Черкаси, Україна

У сучасному світі інформаційних технологій якість програмного забезпечення (ПЗ) є особливо важливою. Одним із ключових етапів його розробки є тестування, яке допомагає виявити помилки та гарантувати стабільність роботи системи. Сьогодні технології штучного інтелекту (ШІ) активно використовуються для автоматизації багатьох рутинних процесів, що значно підвищує ефективність QA (Quality Assurance).

QA-тестування – це процес перевірки ПЗ на відповідність встановленим вимогам, пошук дефектів і забезпечення високої якості кінцевого продукту. Існує кілька основних видів тестування:

- Функціональне тестування – перевіряє правильність виконання функцій.
- Нефункціональне тестування – оцінює продуктивність, безпеку, юзабіліті тощо.
- Автоматизоване тестування – використовує скрипти та спеціальні інструменти для автоматизації перевірок.
- Ручне тестування – тестувальники вручну перевіряють роботу ПЗ.

Тестування відіграє важливу роль у всьому життєвому циклі ПЗ, оскільки забезпечує:

- Раннє виявлення дефектів, що знижує витрати на їх виправлення.
- Покращення користувацького досвіду завдяки стабільній роботі системи.
- Підвищення безпеки програмного продукту.
- Відповідність стандартам та вимогам.

Якщо програмне забезпечення не проходить належне тестування, воно може містити критичні помилки, що призводять до фінансових втрат і втрати довіри користувачів.

Використання ШІ змінює підхід до тестування та контролю якості:

- Автоматизація рутинних завдань – ШІ може самостійно створювати тестові сценарії, виконувати їх і аналізувати результати.
- Швидке виявлення аномалій – алгоритми машинного навчання допомагають знаходити приховані дефекти в коді.
- Оптимізація тестування – ШІ здатен прогнозувати потенційні помилки ще до їх виникнення.
- Менша потреба у ручному тестуванні – це скорочує час тестування, але змінює роль тестувальника: тепер він більше займається аналізом даних і контролем роботи ШІ.

Серед переваг використання ШІ можна виділити:

- Автоматизація тестування скорочує витрати часу.
- Підвищення точності та мінімізація людських помилок.
- Можливість аналізувати великі обсяги даних за короткий час.
- Безперервне тестування без необхідності втручання людини.

До недоліків слід віднести:

- Високі початкові витрати на впровадження ШІ-рішень.
- Потрібні спеціалісти, які вміють працювати з ШІ.
- ШІ не може повністю замінити людський аналіз у складних сценаріях.
- Можливі помилки, якщо навчальні дані є неповними або неякісними.

Штучний інтелект змінює підхід до тестування програмного забезпечення, роблячи його швидшим, точнішим і ефективнішим. Однак, незважаючи на значні переваги, ШІ не може повністю замінити людський досвід та експертизу. Найкращих результатів можна досягти, поєднуючи традиційне тестування та можливості штучного інтелекту. Майбутнє тестування – це гармонійне

співіснування ШІ та людини, де тестувальники виконують стратегічні завдання, а машини беруть на себе рутинну роботу.

Список використаних джерел

1. Hnatushenko V.V., Pavlenko I.V. (2024). "Використання генеративного штучного інтелекту в тестуванні програмного забезпечення." Системні технології, вип. 2(151), с. 10-20.
2. Колощук М.С., Дячук О.Ю., Окунькова О.О., Пірог О.В. (2024). "Інструменти штучного інтелекту для автоматизації тестування на проникнення." Технічна інженерія, № 2(94), с. 121-128.
3. Fan A., Gokkaya B., Harman M., Lyubarskiy M., Sengupta S., Yoo S., Zhang J.M. (2023). "Large Language Models for Software Engineering: Survey and Open Problems." arXiv preprint arXiv:2310.03533.
4. Wang J., Huang Y., Chen C., Liu Z., Wang S., Wang Q. (2023). "Software Testing with Large Language Model: Survey, Landscape, and Vision." arXiv preprint arXiv:2307.07221.
5. Nguyen-Duc A., Cabrero-Daniel B., et al. (2023). "Generative Artificial Intelligence for Software Engineering – A Research Agenda." arXiv preprint arXiv:2310.18648.

УДК 004.9:781

РОЗВИТОК МУЗИЧНОЇ ІНДУСТРІЇ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Ситник П. В.
polina.sytnyk08@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Штучний інтелект активно впроваджується в музичну індустрію, кардинально змінюючи способи створення, виконання та просування музики. Сьогодні існує безліч програм, які використовують його алгоритми для генерації музики, що не тільки полегшує творчий процес, але й дозволяє музикантам зосередитися на ідеях, а не на технічних деталях.

Сучасні музичні ШІ працюють на основі глибоко навчання та нейронних мереж. Вони аналізують великі масиви музичних даних і на їх основі створюють нові композиції.

Технологія OpenAI MuseNet здатна генерувати музику в стилі різних композиторів і жанрів.

Потужним інструментом також є AIVA(Artificial Intelligence Virtual Artist), який використовується для створення саундтреків до фільмів та ігор.

Експериментальна платформа Google Magenta, яка працює на основі штучного інтелекту та машинного навчання створена для генерації музики та її інтеграції з людською творчістю.

Хоча він і може генерувати мелодії, його основна слабкість – відсутність емоцій і творчого задуму. Людські композитори вкладають у музику власні почуття, філософію та культурний контекст, тим часом як ШІ працює шляхом аналізу та змішування існуючих музичних зразків, але не може створювати щось нове.

Крім того, ШІ також використовується для покращення виконання музичних творів. Наприклад, алгоритми, що підтримують комп’ютерне акомпанементу, здатні слухати живого виконавця та адаптувати свою гру в

реальному часі. Це дозволяє музикантам мати більш гнучкий підхід до виконання, створюючи нові можливості для співпраці між людьми та машинами.

З розвитком цифрових платформ, таких як Spotify, Apple Music та YouTube, популярність нової музики досягла небувалих висот. Ці платформи не лише сприяють розповсюдженню музики, але й формують нові тренди. Слухачі мають можливість відкривати нові жанри та виконавців з усього світу, що значно розширює межі традиційної музичної індустрії.

Штучний інтелект уже сьогодні здатний генерувати музику, аналізуючи стилі та особливості різних композиторів. Однак він поки що не може повністю замінити людську творчість, адже йому бракує емоцій, індивідуального бачення та справжнього натхнення. Адже ШІ – це інструмент, а не творець. Найімовірніше, майбутнє музики – це співпраця людини та Штучного Інтелекту, а не повна заміна композиторів.

Список використаних джерел:

1. DSpace: ELAKPI: Репозитарій КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/server/api/core/bitstreams/c27bcdba-04ef-43c1-9a41-678efeea3c11/content (дата звернення: 24.03.2025).
2. Перегляд Застосування нейронних мереж для вирішення завдання генерації музики. Мікросистеми, Електроніка та Акустика. URL: https://elc.kpi.ua/article/view/105200/145659 (дата звернення: 24.03.2025).
3. Як штучний інтелект змінює музичну індустрію сьогодні. KURAZH. URL: https://kurazh.org/yak-shtuchnyj-intelekt-zminyuye-muzychnu/ (дата звернення: 24.03.2025).

УДК 004.056.5:004.056.6

ШТУЧНИЙ ІНТЕЛЕКТ У СВІТІ КІБЕРБЕЗПЕКИ

Павлишин А.І.
arturpavlishin6@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р.В.
м. Черкаси, Україна

Штучний інтелект – це технологія, що імітує людське мислення та здатність до навчання. Його розвиток значно впливає на всі сфери життя, від медицини до фінансів, забезпечуючи автоматизацію процесів та підвищення ефективності роботи.

У сучасному цифровому світі обробка даних відіграє ключову роль у прийнятті рішень, аналізі тенденцій і прогнозуванні майбутнього. Проте разом із цим виникає необхідність у захисті інформації від несанкціонованого доступу та кібератак.

ШІ може використовуватися як для покращення кібербезпеки, так і для створення нових загроз. З одного боку, він допомагає виявляти аномалії та попереджати атаки, з іншого – використовується хакерами для створення більш витончених методів злому.

Методи обробки даних за допомогою ШІ (глибинне навчання, нейронні мережі, машинне навчання). Завдяки цим технологіям ШІ може швидко аналізувати великі обсяги даних, знаходити закономірності та прогнозувати події, що неможливо зробити традиційними методами.

ШІ дозволяє ефективно працювати з Big Data, виявляючи корисну інформацію з хаотичних потоків даних, що є критично важливим у бізнесі, медицині та інших галузях. Він застосовується для оптимізації процесів, наприклад, у фінансовому секторі для визначення кредитоспроможності клієнтів або в логістиці для оптимізації маршрутів доставки.

Штучний інтелект здатний створювати реалістичні фальшиві відео (deepfake), підробляти голосові повідомлення або зламувати системи захисту, що створює нові виклики у сфері кібербезпеки.

Для захисту даних застосовуються криптографічні алгоритми, такі як шифрування, цифрові підписи та блокчейн, що ускладнюють несанкціонований доступ до інформації.

Алгоритми машинного навчання аналізують мережевий трафік, виявляють підозрілу активність та реагують на загрози в реальному часі, що значно підвищує рівень безпеки.

Оскільки ШІ приймає важливі рішення, постає дилема серед відповідальності, хто саме має відповідати за помилки – розробники, користувачі чи ж сам алгоритм. Введення законодавчих норм щодо використання ШІ допомагає запобігти зловживанням, забезпечуючи контроль та прозорість технологій. Важливо забезпечити, щоб алгоритми ШІ були справедливими, прозорими та не дискримінаційними, а також дотримувалися прав людини.

Подальший розвиток технологій ШІ відкриває нові можливості для автоматизації, аналізу даних та забезпечення кібербезпеки. Необхідність балансу між технологічним прогресом та безпекою даних. Використання ШІ має супроводжуватися чіткими правилами та засобами захисту для уникнення можливих загроз. Розвиток технологій має йти поруч із удосконаленням методів безпеки, щоб уникнути ризиків, пов’язаних із цифровізацією суспільства.

Список використаних джерел

1. Russell S., Norvig P. Artificial Intelligence: A Modern Approach – Pearson, 2021. URL: https://www.pearson.com/store/p/artificial-intelligence/P100000401736 (дата звернення: 20.03.2025).
2. Goodfellow I., Bengio Y., Courville A. Deep Learning – MIT Press, 2016. URL: https://www.deeplearningbook.org/ (дата звернення: 20.03.2025).
3. Bishop C. Pattern Recognition and Machine Learning – Springer, 2006. URL: https://www.springer.com/gp/book/9780387310732 (дата звернення: 20.03.2025).

4. Stallings W. Cryptography and Network Security – Pearson, 2020. URL: https://www.pearson.com/store/p/cryptography-and-network-security/P100000784107 (дата звернення: 20.03.2025).
5. Bostrom N. Superintelligence: Paths, Dangers, Strategies – Oxford University Press, 2014. URL: https://global.oup.com/academic/product/superintelligence-9780198739838 (дата звернення: 20.03.2025).
6. ISO/IEC, NIST, GDPR, OECD. Офіційні документи та звіти щодо етики ШІ та кібербезпеки. URL: ISO, NIST, GDPR, OECD (дата звернення: 20.03.2025).
7. Дослідницькі статті з IEEE Xplore, ACM Digital Library, arXiv про штучний інтелект і кібербезпеку. URL: IEEE Xplore, ACM Digital Library, arXiv (дата звернення: 20.03.2025).

УДК 004.62

МЕХАНІЗМ ІНТЕГРАЦІЇ ЦИФРОВИХ ПІДПИСІВ У БАГАТОКОРИСТУВАЦЬКІ СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ

Коваленко О.Л.
kovalenkoaleksey14@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Захарова М.В.
м. Черкаси, Україна

У сучасних цифрових системах, що передбачають одночасний доступ багатьох користувачів, питання безпеки даних набуває критичного значення. Багатокористувацькі інформаційні системи широко застосовуються у сферах фінансів, охорони здоров’я, державного управління, електронного документообігу, а також у корпоративному середовищі. Одним з основних викликів є забезпечення автентичності користувачів та цілісності переданих даних.

Метою роботи є аналіз механізмів інтеграції цифрових підписів у

багатокористувацькі системи, існуючих технологічних рішень та дослідження їх впливу на забезпечення цілісності та автентичності інформації.

Цифровий підпис є криптографічним механізмом, що забезпечує перевірку автентичності та цілісності електронних даних. Він базується на алгоритмах асиметричного шифрування, які використовують пару ключів: приватний (секретний) та публічний (відкритий) [1,2]. Найпоширеніші алгоритми цифрових підписів:

- RSA (Rivest-Shamir-Adleman) – один з найпоширеніших методів, що забезпечує високий рівень криптографічної стійкості.
- DSA (Digital Signature Algorithm) – алгоритм, затверджений NIST, який використовується у багатьох урядових і корпоративних системах [3].
- ECDSA (Elliptic Curve Digital Signature Algorithm) – оптимізований метод, що базується на еліптичних кривих, забезпечуючи високу безпеку при меншій довжині ключів.

Цифровий підпис виконує три основні функції:

1. Перевірка автентичності – гарантує, що підпис належить певному користувачеві.
2. Гарантія цілісності – запевняє, що дані не були змінені після підписання.
3. Незаперечність – підпис не може бути відкликаний або підроблений без виявлення.

Реалізація цифрових підписів у багатокористувацьких системах вимагає врахування кількох ключових технічних аспектів, що забезпечують їхню ефективність, безпеку та продуктивність. Серед основних напрямків варто виділити використання криптографічних алгоритмів, оптимізацію швидкодії перевірки підписів, масштабування системи та інтеграцію з хмарними та мобільними рішеннями (Рис. 1).

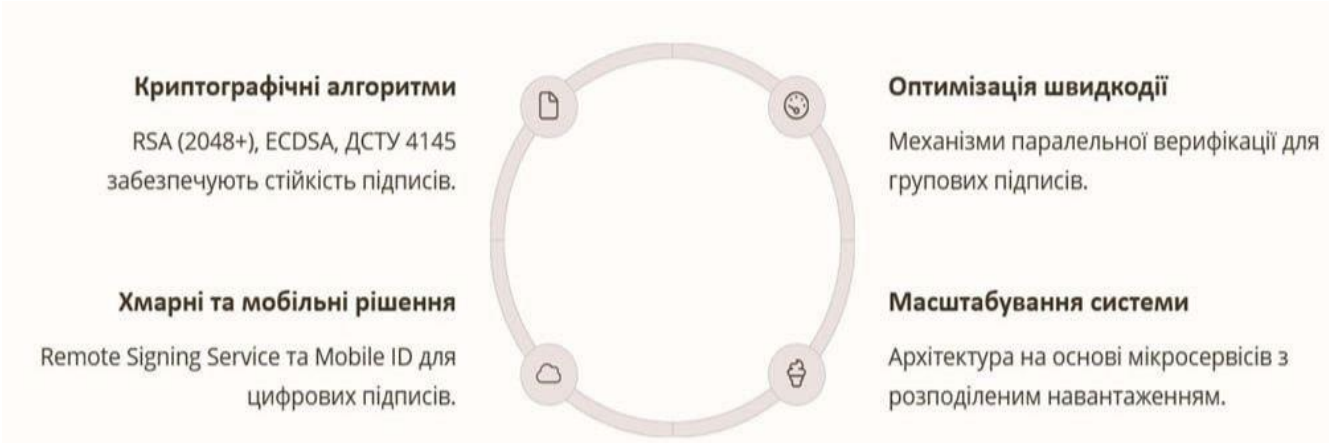

Рисунок 1. Технічні аспекти реалізації

Інтеграція цифрових підписів у багатокористувацькі системи здійснюється через два основні підходи: централізований (з використанням інфраструктури відкритих ключів – PKI) та децентралізований (на основі блокчейну та смарт-контрактів). Централізована модель передбачає використання сервера сертифікації, який видає цифрові сертифікати користувачам та зберігає інформацію про ключі (Рисунок 2). Основою цього підходу є інфраструктура відкритих ключів (PKI), яка включає:

- Сертифікаційний центр (CA) – організація, що видає та відкликає сертифікати.
- Реєстраційний центр (RA) – підтверджує особу користувачів перед видачею сертифікатів.
- Сховище сертифікатів – централізована база даних, де зберігаються відкриті ключі та інформація про користувачів.

Рисунок 2. Відображення інфраструктури відкритих ключів

Блокчейн забезпечує безпечне зберігання цифрових підписів та гарантує їх незмінність. Використання смарт-контрактів дозволяє автоматизувати перевірку автентичності та підписання документів без необхідності залучення сторонніх сертифікаційних органів. Основним перевагами децентралізованого підходу є відсутність центральної точки відмови, висока стійкість до атак на сервери сертифікації, автоматизація процесів підписання та перевірки підпису.

Таким чином, інтеграція цифрових підписів у багатокористувацькі системи сприяє вирішенню таких завдань:

- Захист від фальсифікації – підпис гарантує, що інформація не була змінена сторонніми особами.
- Контроль доступу – автентифікація користувачів перед підписанням документів.
- Верифікація підписаних даних – можливість перевірки авторства та цілісності інформації в будь-який момент часу. У корпоративних системах цифровий підпис часто використовується разом із двофакторною автентифікацією (2FA), що забезпечує додатковий рівень безпеки.

Список використаних джерел

1. ISO/IEC 14888-3:2018 – Міжнародний стандарт, що визначає механізми цифрового підпису, включаючи специфікації для генерації та перевірки підписів, а також вимоги до ключів та алгоритмів. URL: https://www.iso.org/standard/76382.html
2. NIST Digital Signature Standard (DSS) – Стандарт цифрового підпису, розроблений Національним інститутом стандартів і технологій США, який визначає алгоритми та вимоги для створення та перевірки цифрових підписів. URL: https://nvlpubs.nist.gov/nistpubs/fips/
3. nis.fips.186-4.pdf
4. Постанова Кабінету Міністрів України від 12 грудня 2023 року – Уряд ухвалив постанову, яка регулює технічні вимоги до створення та перевірки удосконалених електронних підписів або печаток, спрощуючи їх

використання для отримання електронних послуг. URL: https://zakon.rada.gov.ua/laws/show/1309-2023-%D0%BF#Text
5. Забезпечення безпеки корпоративних інформаційних систем шляхом застосування електронно-цифрового підпису (ЕЦП). URL: https://pnn.com.ua/ua/blog/detail/digital-signature-for-business-processes-automation

УДК 004.771:004.056:614.8

ХМАРНІ ТЕХНОЛОГІЇ У ДИСТАНЦІЙНОМУ КЕРУВАННІ БЕЗПЕКОЮ

Мазур П. Ю.
pasha.mazur.05@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Розломій І. О.
м. Черкаси, Україна

Хмарні технології дедалі ширше використовуються у різних сферах, серед яких дистанційне керування системами безпеки є однією з перспективних областей. Їх використання забезпечує високу доступність, масштабованість та зручність керування системами безпеки. Це особливо важливо для організації дистанційного контролю, що надає змогу швидко реагувати на потенційні загрози.

Переваги використання хмарних технологій у сфері безпеки:

- Централізоване управління – хмарні технології дозволяють інтегрувати різні системи безпеки (відеоспостереження, сигналізації, датчики) в єдиний інтерфейс, що доступний з будь-якого пристрою, підключеного до інтернету.
- Масштабованість – рішення на основі хмари легко адаптуються до потреб користувача, дозволяючи додавати нові пристрої чи функції без значних фінансових витрат.
- Захист даних – хмарні провайдери забезпечують сучасні методи шифрування та багаторівневу автентифікацію, що гарантує надійний захист даних.

– Цілодобовий моніторинг – завдяки хмарним сервісам можливо здійснювати постійний моніторинг об’єктів і оперативно отримувати сповіщення про потенційні загрози.

На сьогодні хмарні технології вже активно використовуються у системах відеоспостереження. Камери, підключені до хмарних платформ, дозволяють зберігати відео архіви та отримувати доступ до записів у режимі реального часу. Прикладом такого сервісу є Google Nest Cam – це хмарна система відеоспостереження. Камери дозволяють користувачам переглядати відеопотоки в реальному часі, отримувати сповіщення про рух чи звук, а також зберігати записи в хмарі для подальшого перегляду. Основні можливості: розумне розпізнавання облич, інтеграція з Google Assistant, доступ до даних із будь-якого пристрою.

Використання хмарних технологій пришвидшує обробку зображень з камер та дозволяє швидше реагувати на загрози. Уявімо систему відеоспостереження, яка використовує хмарну обробку відеопотоку.

– Без хмарної обробки відеопотік з камер надходить на локальний сервер, який аналізує його за допомогою AI. Це займає 5 секунд на кожен кадр (через обмеження обчислювальних ресурсів локального сервера).
– З використанням хмарних технологій, таких як Google Cloud AI або AWS Rekognition, той самий кадр аналізується за 0,5 секунди завдяки потужним GPU в хмарі.

В результаті отримуємо скорочення часу реагування у 10 разів. Наприклад, при виявленні вторгнення охоронна служба отримує сигнал за 1 секунду, а не за 10 секунд, що дозволяє швидше реагувати на загрози.

Також варто згадати про Інтернет Речей та системи доступу. Датчики руху, диму чи температури інтегруються з хмарними сервісами для миттєвого сповіщення про небезпечні ситуації. Для прикладу Amazon Ring пропонує рішення для домашньої безпеки, включаючи відеодзвінки, камери спостереження та розумні сигналізації. Усі пристрої інтегруються з хмарним сервісом Ring Cloud, що дозволяє отримувати повідомлення на смартфон у разі

виявлення загрози.

Використання хмар для керування доступом до приміщень забезпечує зручне налаштування прав доступу та моніторинг активності. До прикладу надання доступу за допомогою біометричних даних. Багато сучасних хмарних рішень для розпізнавання облич мають точність понад 95% завдяки тренованим моделям AI.

- Локальна система розпізнавання облич має точність 85% через обмежені ресурси для навчання моделі.
- Хмарна система (наприклад, Microsoft Azure Face API) має доступ до значно більшого обсягу даних і обчислювальних потужностей, тому забезпечує точність 98%.

В результаті завдяки хмарі зменшується кількість хибних тривог та помилкових спрацьовувань. Наприклад, у системі з 1000 спроб входу за день, хибні тривоги зменшуються з 150 (15%) до 20 (2%)

Окрім зручності, швидкості, та надійності використання хмарних технологій є доволі вигідною інвестицією. За даними аналітиків з McKinsey & Company, компанії, які впровадили хмарні рішення, повідомляють про:

- Скорочення витрат на IT-інфраструктуру до 40% завдяки відмові від локальних серверів.
- Зростання продуктивності персоналу до 20-30%, оскільки працівники мають доступ до ресурсів у будь-який час і з будь-якої точки.
- Швидкість впровадження нових сервісів у середньому скорочується на 50-70%, що дозволяє швидше запускати нові продукти та сервіси.

Для прикладу можна розглянути компанію з витратами на IT у 100 000 доларів на рік. Вона може скоротити ці витрати до 60 000 доларів, використовуючи хмарну інфраструктуру.

Хмарні технології на перший погляд є зручним та безпечним інструментом для керування системами безпеки, але вони також мають свої недоліки. Найбільші проблеми це залежність від стабільного інтернет-з’єднання та ризики кібератак. Для роботи хмарних систем потрібне стабільне підключення до

мережі. У разі його відсутності функціональність системи може бути обмеженою. Загрози кібератак залишаються значним викликом. Необхідно впроваджувати багаторівневий захист даних, шифрування інформації та двофакторну аутентифікацію для мінімізації ризиків.

З розвитком технологій недоліки перелічені вище вирішуються. Використання супутникового інтернету вирішує проблему у стабільному інтернет підключенні. Розвиток квантових обчислень дозволить значно посилити захист даних і підвищити швидкість обробки інформації, а використання штучного інтелекту дозволяє пришвидшити реагування на загрози та оптимізувати реагування на них

Хмарні технології у дистанційному керуванні безпекою продовжують розвиватися, відкриваючи нові можливості для підвищення ефективності та надійності систем захисту. Це перспективна область, яка стає дедалі важливішою у сучасному світі.

Список використаних джерел

1. Хмарні сервіси та їхня безпека для бізнесу. URL:https://business.diia.gov.ua/entrepreneur handbook/item/hmarni_servisi_ta_yihnya_bezpeka_dlya_biznesu?utm_source=chatgpt.com (дата звернення: 18.03.2025).
2. Хмарні технології 2025 – що це таке та які хмари найкращі? URL: https://ucloud.ua/hmarni-tehnologiyi-shho-cze-take/ (дата звернення: 18.03.2025).
3. Ризики хмарної безпеки: на що звернути увагу та як захиститися. URL: https://gigacloud.ua/articles/ryzyky-hmarnoyi-bezpeky-na-shho-zvernuty-uvagu-ta-yak-zahystytysya/ (дата звернення: 18.03.2025).
4. Переваги хмарних сервісів безпеки. URL: https://surli.cc/rehodc (дата звернення: 18.03.2025).

Секція 2.

ІНЖЕНЕРНІ ПІДХОДИ ДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

UDC 658.5:004.6

PROJECT DEVELOPMENT BY AGILE, SCRUM APPROACH

Kordonska A.O.
kordonskanastya@gmail.com
Cherkasy State Business College
Research Supervisor: Khotunov V.I.
Cherkasy, Ukraine

The dynamic nature of software development has necessitated the adoption of flexible methodologies to enhance efficiency, adaptability, and collaboration. Agile, particularly the Scrum framework, has emerged as one of the most effective project management approaches. Agile enables teams to deliver high-quality software incrementally, ensuring that customer requirements are met through continuous iterations. Scrum, as a subset of Agile, structures these iterations into time-boxed sprints, fostering transparency, collaboration, and continuous improvement [1][7].

Agile development is an iterative approach that prioritizes customer feedback, flexibility, and teamwork. Unlike traditional waterfall models, Agile emphasizes short development cycles that incorporate ongoing testing and modifications. The Agile Manifesto, published in 2001, introduced four core values and twelve principles that focus on delivering value efficiently. Agile's success is driven by its ability to accommodate changing requirements without disrupting the project’s workflow. By fostering regular communication between developers, stakeholders, and end-users, Agile ensures that the final product aligns with business objectives and user expectations [2].

Scrum is a highly structured Agile framework designed to manage complex software development projects efficiently. It is based on defined roles, events, and artifacts that facilitate smooth collaboration within teams. The key roles in Scrum include the Product Owner, Scrum Master, and Development Team. The Product Owner represents the business interests, the Scrum Master ensures adherence to Scrum principles, and the Development Team focuses on implementation. The structured approach of Scrum helps teams break down large projects into manageable units, enabling continuous delivery of valuable software components [3].

The Scrum process follows a series of well-defined stages, starting with product backlog creation and refinement. The backlog consists of prioritized tasks that the development team works on during sprints, which typically last two to four weeks. Each sprint begins with planning, followed by daily stand-up meetings where team members discuss progress and address challenges. At the end of each sprint, a review and retrospective meeting is conducted to assess the outcomes and identify areas for improvement. This iterative process ensures that software development is adaptive and responsive to changes in requirements [4].

The Agile-Scrum methodology offers several advantages over traditional project management models. First, it enhances adaptability by allowing teams to respond to changes rapidly. Second, it promotes collaboration among cross-functional teams, fostering a culture of transparency and accountability. Third, Agile ensures continuous delivery, reducing the risk of project failure by providing incremental updates. Additionally, Scrum's emphasis on sprint retrospectives helps teams identify inefficiencies and implement improvements continuously. These benefits make Agile and Scrum an ideal choice for modern software development [5].

Despite its advantages, implementing Agile and Scrum comes with challenges. Organizations transitioning from traditional methodologies may face resistance to change. Additionally, the success of Scrum depends on disciplined execution and commitment from all team members. Without proper training, teams may struggle with role clarity, sprint planning, and backlog management. Furthermore, Agile projects require close collaboration with stakeholders, which can be challenging in large, distributed teams. Addressing these challenges requires strong leadership, proper training, and a culture of continuous learning [6].

The Agile-Scrum approach to project development has revolutionized the software industry by providing a flexible, customer-centric framework that enhances productivity and quality. By breaking projects into iterative cycles, Agile enables teams to adapt to evolving requirements and deliver incremental improvements. Scrum's structured process ensures efficiency through defined roles, ceremonies, and feedback mechanisms. While challenges exist, proper implementation and adherence to best

practices can maximize the benefits of Agile and Scrum in project management. As businesses continue to embrace digital transformation, Agile methodologies will remain a cornerstone of effective software development.

List of references

8. Schwaber, K. (2004). Agile Project Management with Scrum. URL: https://www.microsoftpressstore.com/store/agile-project-management-with-scrum-9780735619937 (дата звернення: 19.03.2025).
9. Beck, K., et al. (2001). Manifesto for Agile Software Development. URL: https://agilemanifesto.org/ (дата звернення: 19.03.2025).
10. Schwaber, K., & Sutherland, J. (2020). The Scrum Guide. URL: https://scrumguides.org/scrum-guide.html (дата звернення: 19.03.2025).
11. Rubin, K. S. (2012). Essential Scrum: A Practical Guide to the Most Popular Agile Process. URL: https://www.informit.com/store/essential-scrum-a-practical-guide-to-the-most-popular-9780137043293 (дата звернення: 19.03.2025).
12. Sutherland, J. (2014). Scrum: The Art of Doing Twice the Work in Half the Time. URL: https://www.randomhouse.com/books/227326/ (дата звернення: 19.03.2025).
13. Cohn, M. (2009). Succeeding with Agile: Software Development Using Scrum. URL: https://www.informit.com/store/succeeding-with-agile-software-development-using-scrum-9780321579362 (дата звернення: 19.03.2025).
14. VersionOne. (2019). 13th Annual State of Agile Report. URL: https://stateofagile.com/ (дата звернення: 19.03.2025)

УДК 004.42:004.7

СУЧАСНІ ТЕХНОЛОГІЇ РОЗРОБКИ ЦИФРОВИХ ГАМАНЦІВ

Комиш В. М.
komisvadim6@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Марченко С. В.
Черкаси, Україна

Актуальність роботи. Стрімке поширення та зручність онлайн-платежів сприяють активному розвитку технологій цифрових гаманців. Застосування сучасних технологій безпеки, наприклад, шифрування даних та біометричної аутентифікації, забезпечує високий рівень захисту фінансової інформації користувачів. Фундаментальним безпековим компонентом зі здійсненням децентралізованого контролю над транзакціями виступають блокчейн-технології. Разом із стабільним ростом ринку цифрових послуг [1] та повсюдного прийняття криптоопераций [2] потреба в якісній розробці захищених, зручних та функціональних цифрових гаманців тільки зростає. Вироблення уніфікованих інженерних підходів до створення відповідних програмних продуктів значно спрощуватиме розроблення та впровадження як готових, стандартизованих рішень, так і програмних інструментів для їх побудови.

Мета дослідження. Дослідити та проаналізувати сучасний стан технологій розробки цифрових криптогаманців, визначити ключові аспекти та рішення, що впливають на хід розроблення, а також корисні інструменти програмної інженерії, що формують цикл розробки.

Формування архітектури цифрових гаманців залежить від їхнього типу, рівня безпеки та механізмів доступу до приватних ключів. Некатодіальні рішення, що забезпечують повний контроль користувачів над активами, використовують криптографічні алгоритми ECDSA та EdDSA для підпису транзакцій, а також стандарти BIP-39 і BIP-44 для генерації ключів. У кастодіальних гаманцях реалізується система керування ключами із застосуванням Multi-Party Computation (MPC), що підвищує рівень безпеки [3].

Збереження та передача облікових даних у криптогаманцях забезпечуються стандартами CCSS та ISO/IEC 27001 [4].

Розробка фронтенд-інтерфейсів цифрових гаманців здійснюється на основі JavaScript та TypeScript із використанням бібліотек React та Vue. Взаємодія з блокчейнами реалізується через web3.js, ethers.js та bitcoinjs-lib, що надають API для створення та підпису транзакцій. Компоненти для створення високопродуктивних сервісів для обробки запитів на стороні бекенду розробляються на Node.js, Go або Rust. Бази даних, зокрема PostgreSQL та MongoDB, використовуються для зберігання метаданих, тоді як приватні ключі зберігаються у захищених модулях, таких як Hardware Security Modules (HSM) [5].

Смартконтракти відіграють важливу роль у функціонуванні цифрових гаманців, особливо тих, що працюють у децентралізованих фінансових сервісах. Основна розробка здійснюється мовою Solidity для Ethereum та Rust для Solana. Для забезпечення безпечності коду використовуються аудиторські інструменти, зокрема Slither та Mythril, що дозволяють виявляти потенційні вразливості до їхнього розгортання. Механізми Zero-Knowledge Proofs (ZKP) впроваджуються для підвищення конфіденційності транзакцій.

Розробка цифрових гаманців базується на принципах Agile та DevSecOps, що забезпечують інтеграцію процесів безпеки на всіх етапах життєвого циклу продукту. Контейнеризація бекенд-сервісів виконується за допомогою Docker та Kubernetes, що гарантує гнучкість розгортання та масштабованість. CI/CD-процеси автоматизують тестування та аудит безпеки за допомогою GitHub Actions та GitLab CI/CD. Впровадження інструментів моніторингу, таких як Prometheus та Grafana, сприяє своєчасному виявленню аномалій у роботі цифрових гаманців [6].

Масштабованість цифрових гаманців є критичним аспектом їхньої ефективності, особливо з огляду на високу завантаженість блокчейн-мереж. Інтеграція з рішеннями другого рівня, такими як Optimistic Rollups та ZK-Rollups, дозволяє значно знизити комісії за транзакції та підвищити швидкість обробки

операцій. Важливим напрямом розвитку є також підтримка протоколів кросчейн-взаємодії, зокрема Cosmos IBC та Polkadot XCM, що забезпечують обмін активами між різними блокчейн-мережами [7].

Висновки. Сучасні технології розробки цифрових гаманців включають широкий спектр програмних засобів, криптографічних механізмів та архітектурних рішень, що забезпечують їхню безпеку, продуктивність та інтеграцію з блокчейн-екосистемами. Використання сучасних мов програмування, бібліотек для взаємодії з блокчейнами, а також смартконтрактних рішень сприяє підвищенню ефективності таких гаманців. Застосування методологій гнучкої розробки та автоматизованих процесів тестування забезпечує стабільність роботи систем, тоді як інтеграція масштабованих рішень другого рівня дозволяє адаптувати цифрові гаманці до високих навантажень. Подальший розвиток технологій, зокрема впровадження Multi-Party Computation та постквантових криптографічних алгоритмів, сприятиме підвищенню рівня безпеки та користувацького досвіду.

Список використаних джерел

1. Fiat and Crypto Wallet Services Market [2024-2032] | Size Report. Business Research Insights | Global Market Research Report & Consulting. URL: https://www.businessresearchinsights.com/market-reports/fiat-and-crypto-wallet-services-market-113585 (дата звернення: 18.03.2025).
2. 2024 Western Europe Crypto Adoption: Stablecoins dominate. Chainalysis. URL: https://www.chainalysis.com/blog/2024-western-europe-crypto-adoption/ (дата звернення: 18.03.2025).
3. Shared-Custodial Wallet for Multi-Party Crypto-Asset Management / Y. Erinle et al. Future Internet. 2024. Vol. 17, no. 1. P. 7. URL: https://doi.org/10.3390/fi17010007 (дата звернення: 18.03.2025).
4. CCSS v9.1 Table - CryptoCurrency Certification Consortium (C4). CryptoCurrency Certification Consortium (C4). URL: https://cryptoconsortium.org/ccss-table-v9/ (дата звернення: 18.03.2025).

5. Riza G. The study of the HSM as a solution to file encryption and security. Proceedings of the 5th International Conference on Recent Trends and Applications in Computer Science and Information Technology, Tirana, 26–27 April 2023. University of Tirana, 2023. P. 80–88. URL: https://ceur-ws.org/Vol-3402/paper10.pdf (дата звернення: 18.03.2025).
6. Bipin Gajbhiye, Shalu Jain, Akshun Chhapola. Secure SDLC: Incorporating Blockchain for Enhanced Security. Scientific Journal of Metaverse and Blockchain Technologies. 2024. Vol. 2, no. 2. P. 97–110. URL: https://doi.org/10.36676/sjmbt.v2.i2.40 (дата звернення: 18.03.2025).
7. Li L., Wu J., Cui W. A review of blockchain cross-chain technology. IET Blockchain. 2023. URL: https://doi.org/10.1049/blc2.12032 (дата звернення: 18.03.2025).

УДК 004.9:658.8

ОСОБЛИВОСТІ РОЗРОБКИ, РЕЄСТРАЦІЇ, ПІДТРИМКИ І МОНЕТИЗАЦІЇ ІГОР В ІГРОВОМУ СЕРВІСІ STEAM

Івченко В.В.
valera2071w@gmail.com
Левченко С.С.
lev4enkostanislav@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Ночевнов Д.П.
м. Черкаси, Україна

Представлена робота присвячена питанню розробки, реєстрації, підтримки та монетизації ігор в ігровому сервісі Steam, який, в свою чергу, є найбільшою цифровою платформою дистрибуції відеоігор, і пропонує розробникам широкий спектр інструментів для створення, публікації та просування своїх продуктів.

Серед основних факторів розробки гри можна виділити наступні:

1. Інтуїтивно зрозуміла концепція і дизайн гри.
2. Вікова категорія гравців.
3. Локалізація гри на різних мовах.
4. Вибір ігрового рушія, який має інтегрувати Steam, працювати на різних

пристроях, підтримувати багатокористувацький інтерфейс і збереження досягнень гравців у хмарі.

5. Можливість подальшої монетизації гри, її підтримки та просування.
6. Врахування юридичних аспектів, правил та вимоги сервісу Steam.

Маючи визначену ідею гри, з урахуванням цих факторів, після огляду існуючих рішень було обрано:

- для розробки гри: ігровий рушій Unity та мову програмування C#;
- для генерації картинок, персонажів, фонів гри: ШІ stabble-defusion;
- для генерації анімацій персонажів: ComfyUI в яку інтегровано Hunyan Video;
- для спільної розробки: GitHub;
- локалізація тексту і озвучення українською, японською та англійською мовами за допомогою ШІ.

Вибір рушія Unity був обумовлений тим, що він дозволяє розробляти ігри з використанням Steamworks SDK як для персональних комп'ютерів та ноутбуків з операційними системами Windows, macOS, Linux, так і для смартфонів, планшетів та ігрових консолей. Окрім цього в Unity є багато докладних гайдів і готових плагінів, які допомагають інтегрувати можливості Steamworks SDK у Unity, зокрема роботу з досягненнями гравців, збереження у хмарі, багатокористувацький режим тощо.

Після завершення розробки необхідно зареєструвати гру у Steamworks, сплативши разовий Steam Direct Fee у розмірі 100 доларів США за проєкт, після чого розробник вносить дані про юридичну особу, такі як: юридична назва, податкова інформація (W-8BEN для нерезидентів США), банківські реквізити (SWIFT, IBAN тощо для міжнародних виплат). Перевіривши цю інформацію Steam надає розробнику доступ до панелі Steamworks, де заповнюються дані про гру та створюється AppID — унікальний ідентифікатор гри. Далі розробник повинен пройти перевірку контенту та підготувати сторінку гри, додавши графічні матеріали, трейлери та опис, що відповідає вимогам маркетингової ефективності.

Монетизація на платформі Steam може здійснюватися через різні моделі: разову покупку, мікротранзакції, DLC, підписки або free-to-play підхід із внутрішніми покупками. Компанія-власник Valve утримує 30% доходу, проте для проєктів, що генерують значні прибутки, комісія може знижуватися. Для збільшення продажів і залучення нової аудиторії також використовуються розпродажі, локалізована цінова політика та різноманітні акції. Деякі розробники використовують стратегію раннього доступу (Early Access), що дозволяє залучити фінансування ще до повноцінного релізу гри, отримати зворотний зв'язок і поступово вдосконалювати проєкт.

Серед важливих кроків після реєстрації гри є її подальше просування і підтримка, що включає випуск оновлень та виправлення помилок, а також активну взаємодію з гравцями через форуми Steam та соціальні мережі. Розробники можуть використовувати Steam Curators і співпрацювати з інфлюенсерами для підвищення популярності гри.

Для успішного просування гри Steam надає аналітичні інструменти моніторингу продажів, поведінки гравців та ефективності рекламних кампаній, а також детальну статистику динаміки продажів, впливу знижок та реакції спільноти на зміни у грі.

Перспективними є розвиток гри на нових платформах - в VR-проєктах, і на мобільних платформах через Steam Link, а також інтеграція гри з іншими сервісами, такими як Twitch або YouTube Gaming, що допоможе залучити додаткову аудиторію через трансляції та огляди.

З точки зору юридичних аспектів, розробники повинні враховувати питання ліцензування, дотримання авторських прав та політики використання контенту в Steam. Особливо це стосується використання сторонніх саундтреків, графіки чи механік, що можуть бути захищені правами інтелектуальної власності. Крім того, важливим є дотримання вимог щодо вікового рейтингу гри, оскільки обмеження за віком впливає на доступність проєкту у певних країнах.

Таким чином можна зробити висновок, що успішний запуск гри у Steam – це складний, але захопливий процес, що вимагає комплексного підходу,

стратегічного мислення та розуміння ринку. Платформа надає широкі можливості для розробників будь-якого рівня, проте ключовими чинниками успіху залишаються якість продукту, ефективний маркетинг, постійна підтримка та глибока інтеграція з ігровою спільнотою. Уміння адаптуватися до змін, експериментувати з бізнес-моделями та бути відкритим до фідбеку дозволяє не лише створювати конкурентоспроможні проєкти, але й будувати стабільний бізнес у сфері ігрової індустрії.

Список використаних джерел

1. Steamworks Documentation – Офіційна документація Steam для розробників, що містить інформацію про реєстрацію, інтеграцію, підтримку та монетизацію ігор. URL: https://partner.steamgames.com/doc/home (дата звернення: 18.03.2025).
2. Valve Corporation – Політика та умови публікації ігор на платформі Steam, включаючи вимоги до контенту, комісійні збори та особливості розподілу доходів. . URL: https://store.steampowered.com Steam Community Market Trends – Аналітика щодо динаміки продажів, впливу розпродажів та поведінки гравців у Steam. . URL: https://steamcommunity.com/market/ (дата звернення: 18.03.2025).
3. Indie Game Business Podcast – Практичні поради з просування ігор у Steam від незалежних розробників та маркетологів. . URL: https://indiegamebusiness.com (дата звернення: 18.03.2025).
4. Gamasutra – Monetization Strategies for Indie Games – Огляд успішних бізнес-моделей, які використовують розробники для заробітку на Steam. . URL: https://www.gamedeveloper.com (дата звернення: 18.03.2025).
5. YouTube Gaming & Twitch Integration – Інструменти для стримерів і розробників для залучення аудиторії через платформи прямих трансляцій. . URL: https://www.twitch.tv/creatorcamp (дата звернення: 18.03.2025).
6. Unity & Unreal Engine Steam Integration – Інструкції щодо інтеграції Steamworks API у популярні рушії для ігор. . URL: https://docs.unrealengine.com , https://docs.unity3d.com (дата звернення: 18.03.2025).

УДК 004.42:004.7

ПРОГРАМНА ІНЖЕНЕРІЯ РОЗРОБКИ МАГАЗИНІВ ДОДАТКІВ

Цьома В. С.
tsyomav@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Марченко С. В.
м. Черкаси, Україна

Актуальність роботи. Нині розроблено сотні тисяч програмних застосунків для різних платформ, що значно ускладнює користувачеві пошук потрібного рішення. Проте, навіть для знайденого програмного продукту, користувач, у більшості випадків, не матиме можливості чи бажання перевіряти його безпечність, сумісність з апаратним забезпеченням чи актуальність. Наслідки цього різні: неробочий або некоректно працюючий продукт, проникнення шкідливого програмного забезпечення на машину користувача, пошкодження апаратного забезпечення тощо.

Мета дослідження. Проаналізувати інженерні підходи, що забезпечують здійснення розробки магазину додатків від початкової концепції до розгорнутого програмного рішення, та імплементувати вироблений процес за допомогою актуальних інструментів.

У роботі [1] автори визначають магазин додатків як механізм онлайн-дистрибуції, який:

1. надає доступ до комплексної колекції програмного забезпечення або сервісів, заснованих на програмному забезпеченні (“додатків”), які розширюють функції наявного середовища виконання;
2. активно підтримується, тобто надає деякий рівень гарантії щодо додатків, таких як забезпечення базової функціональності та відсутність вірусів;
3. надає наскрізний досвід “магазину”, тобто користувачі мають змогу придбати додаток через магазин, а процес інсталяції додатків координований автоматично.

З наведеного визначення випливає, що основні функції магазину додатків можна сформулювати таким чином:

- запуск процесів встановлення та оновлення додатків;
- вивчення каталогу – магазини додатків надають механізми для знаходження потрібного рішення. Подальша інформація про якість вибраного рішення може надаватись через огляди користувачів або форуми;
- гарантоване середовище виконання — зазвичай магазини додатків є доповненням до середовища виконання (ОС чи ПЗ на базі модульної архітектури), яке виконує роль менеджера додатків. У деяких випадках, магазини додатків тісніше інтегруються з середовищем виконання, розширюючи його своїми функціями.

Додаткова функціональність магазинів застосунків постійно змінюється, зокрема вбудована опція монетизації Chrome Web Store була згодом видалена [2].

Незважаючи на те, що монолітний стиль дозволить зекономити ресурси у короткостроковій перспективі, такі системи працюють нестабільно при збільшенні навантаження. Як приклад можна навести реєстр JS-пакетів npm [3]. У 2013 році їх монолітна система зіткнулась з десятикратним підвищенням попиту, що призвело до частих збоїв. Звідси, пріоритетами при проєктуванні архітектури магазину додатків повинні виступати гнучкість, модульність та слабка зв’язаність. Використання мікросервісного стилю архітектури задовольняє ці вимоги, також даючи змогу масштабувати окремі елементи архітектури. Варто відзначити, що впровадження мікросервісної архітектури несе за собою додаткові вимоги, зокрема налаштування CI/CD конвеєру, сервісів оркестрації, логування та моніторингу.

Для реалізації можна виділити такі групи функцій [4]: інтерфейс користувача; API-шлюз; сервіси авторизації та автентифікації; сервіси для роботи з додатками; сервіси безпеки.

Сервіс інтерфейсу користувача надає інтуїтивний спосіб взаємодії з програмною системою для кінцевих користувачів та видавців додатків. API шлюз забезпечує комунікацію зовнішніх клієнтів, зокрема сервісів інтеграції та додатків магазину з внутрішніми сервісами. Логіка авторизації та автентифікації розподілена між API шлюзом та сервісами, призначеними для цього, при тому шлюз виконує тільки валідацію токенів для запобігання проблем з продуктивністю при подальшому розширенні системи [5].

Група сервісів для роботи з додатками містить щонайменше:

- сервіс каталогу – надає дані про додатки, використовує БД метаданих;
- сервіс заявок – керує заявками про подання додатків, розміщує заявки в окремій БД, при прийнятті заявки переміщує дані про додаток у БД метаданих;
- сервіс пакетів – сервіс-надбудова над БД пакетів. Дозволяє адміністраторам керувати пакетами, а користувачам – їх завантажувати.

Безпекові сервіси перевіряють пакети при надходженні разом з заявкою. Пакети розміщуються у відокремленому сховищі, а для перевірки використовується зовнішній API, наприклад, VirusTotal. За умови відсутності шкідливого ПЗ, пакетний файл переноситься у сховище пакетів. У майбутньому для покращення безпеки планується розширення таких сервісів, поглиблення рівня контейнеризації та побудова власних рішень для виявлення інших типів загроз та запобігання надмірної залежності від зовнішніх систем.

Висновки. Отже, магазин додатків – це система онлайн дистрибуції додатків, що забезпечує механізми запуску встановлення та оновлення застосунків. Архітектура такої програмної системи може бути монолітною, але, як правило, такі системи починають функціонувати нестабільно зі збільшенням потоку користувачів. Розбиття системи на окремі мікросервіси підвищує складність її підтримки, впроваджуючи додаткові сервіси для журналювання, оркестрації та моніторингу, але запобігає масштабним збоям. Початковий рівень безпеки забезпечується стороннім рішенням, яке у майбутньому може бути замінене на власне задля запобігання збоям. Реалізація магазину також

потребуватиме чіткого визначення правил модерації контенту. Організація монетизації залежатиме від потреб замовника та не є обов'язковим елементом архітектури. Тим не менш, мікросервісна архітектура відкрита для розширення новими сервісами.

Список використаних джерел

1. What is an app store? The software engineering perspective / W. Zhu et al. Empirical software engineering. 2024. Vol. 29, no. 1. URL: https://doi.org/10.1007/s10664-023-10362-3 (дата звернення: 20.03.2025).
2. Google. Chrome Web Store payments deprecation. Chrome for Developers. URL: https://developer.chrome.com/docs/webstore/cws-payments-deprecation (дата звернення: 20.03.2025).
3. Robbins C. Node.js – keeping the npm registry awesome. Node.js – Run JavaScript Everywhere. URL: https://nodejs.org/en/blog/npm/2013-outage-postmortem/ (дата звернення: 20.03.2025).
4. A modular app store reference architecture (MASRA) / D. Antoniou et al. EDA research, technology, and innovation papers award 2023. 2023. P. 110–119.
5. Brankovic M. Dissolving the monolith: patterns. Medium. URL: https://milanbrankovic.medium.com/dissolving-the-monolith-patterns-bf4b06c96fd6 (дата звернення: 20.03.2025).

УДК 004.42:004.7

РОЗРОБКА TELEGRAM ЧАТ-БОТА ПРО РОБОТУ ВІДДІЛЕНЬ НОВОЇ ПОШТИ

Лісун І.
vanlisun@ukr.net
Черкаський державний фаховий бізнес-коледж
м. Черкаси, Україна
Науковий керівник: Немченко В.Ю.

У сучасному цифровому світі автоматизація та інтеграція технологій у сфері логістики стають дедалі важливішими. Одним із найзручніших та доступних інструментів для покращення комунікації між клієнтами та компаніями є чат-боти. Telegram-боти дозволяють оперативно надавати користувачам необхідну інформацію, спрощуючи взаємодію з сервісами. У рамках цієї роботи розглянуто процес розробки Telegram чат-бота, який надаватиме актуальну інформацію про роботу відділень Нової пошти.

1. Обґрунтування вибору платформи
   - Telegram має відкритий API, що дозволяє легко створювати та інтегрувати ботів.
   - Велика аудиторія користувачів Telegram в Україні.
   - Підтримка роботи з хмарними сервісами для швидкого доступу до інформації.
2. Функціональні можливості бота
   - Перегляд графіка роботи відділень Нової пошти.
   - Отримання інформації про найближчі відділення за геолокацією.
   - Надання даних про завантаженість відділень.
   - Автоматичні сповіщення про зміни в розкладі роботи.
3. Вибір технологічного стеку
   - Мова програмування: Python – зручний синтаксис, наявність потужних бібліотек (telebot, requests).

- Середовище розробки: PyCharm – надає всі необхідні інструменти для роботи з Telegram API.
- Хостинг: Heroku – надає можливість розгортання бота в хмарі та його стабільну роботу.

4. Реєстрація та налаштування бота
   - Створення бота через @BotFather та отримання API-токену.
   - Налаштування інтеграції з сервером та базою даних.
   - Використання вебхуків для обробки запитів користувачів у реальному часі.
5. Значення автоматизації процесів у логістиці
   - Покращення користувацького досвіду завдяки швидкому доступу до інформації.
   - Оптимізація роботи відділень шляхом зменшення навантаження на операторів.
   - Скорочення часу очікування клієнтів та підвищення рівня сервісу.

Отже, розробка Telegram чат-бота для Нової пошти є актуальним рішенням, яке дозволяє оптимізувати взаємодію між компанією та її клієнтами. Вибір технологій, зокрема Python та Heroku, сприяє створенню ефективного, гнучкого та зручного інструменту для оперативного отримання інформації. Подальший розвиток бота може включати додаткові функції, такі як інтеграція з CRM-системами або голосові команди, що ще більше покращить якість обслуговування клієнтів.

Список використаних джерел:

1. Dexway. "English for IT, why is it important in language teaching?" URL: https://www.dexway.com/english-for-it-why-is-it-important-in-language-teaching/ (дата звернення: 20.03.2025)
2. ETS Global. "The Importance of Learning English" URL: https://www.etsglobal.org/pl/en/blog/news/importance-of-learning-english (дата звернення: 20.03.2025)

УДК 004.42:796

РОЗРОБКА ВЕБ-ПЛАТФОРМИ ДЛЯ ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ СПОРТИВНИМИ ЗМАГАННЯМИ

Голець А. В.
anton142rrri@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Немченко В. Ю.
м. Черкаси , Україна

Організація спортивних змагань потребує значних адміністративних ресурсів. Існуючі рішення не завжди відповідають потребам організаторів аматорських та локальних заходів. Розробка веб-платформи дозволить автоматизувати ключові процеси управління змаганнями.

Проведено огляд сучасних платформ для управління спортивними подіями. Виявлено недоліки таких рішень: відсутність гнучкості для різних видів спорту та складність використання для тих, хто тільки почав користуватись платформою.

Формулювання функціональних та нефункціональних вимог до системи:

- Реєстрація та управління змаганнями
- Додавання учасників
- Створення змагань
- Автоматичне оновлення результатів
- Зручний інтерфейс для учасників та організаторів
- Вибір технологій для створення веб сайту

Платформа складається з таких технологій як:

- React – створення інтерфейсу сайту
- Node.js – оброблення запитів
- MongoDB – збереження інформації користувачів платформи.

Основне завдання сайту: створення та реєстрація змагань, управління учасниками та ведення результатів. Перспективи розвитку передбачають

розширення функціональності для різних видів спорту, позитивний досвід від користування сайтом учасниками та організаторами зустрічей.

Список використаних джерел:

1. React. URL: https://react.dev/ (дата звернення: 12.03.2025).
2. Express.js. URL: https://expressjs.com/ (дата звернення: 12.03.2025).
3. MongoDB. URL: https://www.mongodb.com/ (дата звернення: 12.03.2025).

УДК 004.4:004.42

КЛЮЧОВІ АСПЕКТИ ІНЖЕНЕРІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В СУЧАСНОМУ ПРОЦЕСІ РОЗРОБКИ

Ващенко М.М.
maks.vaschenko23042005@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р.В.
м. Черкаси, Україна

Розробка програмного забезпечення відбувається за певною структурою, яка називається життєвим циклом. Вибір моделі залежить від проєкту та вимог замовника:

- Каскадна модель – послідовний підхід, коли кожен етап (аналіз, проєктування, розробка, тестування, впровадження) виконується окремо.
- V-модель – вдосконалений варіант каскадної моделі з акцентом на тестування після кожного етапу.
- Спіральна модель – поєднує етапи каскадної моделі та гнучкого підходу, передбачає поступове вдосконалення продукту.
- Agile, Scrum, Kanban – сучасні гнучкі методології, що дозволяють швидко адаптувати програмне забезпечення до змін.

Програмна інженерія базується на ключових принципах, які допомагають створювати ефективний і масштабований код:

- Модульність – розбиття системи на незалежні компоненти.

- Інкапсуляція та абстракція – приховування внутрішньої логіки та створення зрозумілих інтерфейсів.
- Автоматизоване тестування – зменшення ризику помилок через автоматичну перевірку коду.
- Контроль версій – використання Git та інструментів CI/CD для зручного керування кодом.

На етапі проєктування вибирається структура майбутнього програмного продукту:

- Монолітна архітектура – коли вся система працює як єдине ціле, що підходить для невеликих проєктів.
- Мікросервісна архітектура – розбиття на незалежні модулі, що дає можливість легко масштабувати систему.
- Патерни проєктування (MVC, MVVM, Singleton) – шаблони, що допомагають створювати ефективні й гнучкі рішення.
- Безпека та продуктивність – важливі аспекти, що враховуються під час розробки для запобігання вразливостям.

Якість програмного забезпечення залежить від ефективного тестування:

- Юніт-тестування – перевірка окремих компонентів програми.
- Інтеграційне тестування – перевірка взаємодії модулів між собою.
- Автоматизоване тестування – використання інструментів Selenium, JUnit для скорочення часу тестування.
- Контроль коду – аналіз якості за допомогою Code Review та спеціальних інструментів (SonarQube).

Список використаних джерел

1. «Popular Software Development Life Cycles» / QATestLab. – https://training.qatestlab.com/blog/technical-articles/popular-software-development-life-cycles/ (дата звернення: 23.03.2025).

2. «Підходи до розробки програмного забезпечення» / Foxminded. – https://foxminded.ua/pidkhody-do-rozrobky-prohramnoho-zabezpechennia/ (дата звернення: 23.03.2025).
3. «Flexible Software Development Methodology: Agile» / QATestLab. – https://training.qatestlab.com/blog/technical-articles/flexible-software-development-methodology-agile/ (дата звернення: 23.03.2025).
4. «Інженерія програмного забезпечення» / BDU-T. – https://bdut.co.ua/pro-nas/inzheneriya-programnogo-zabezpechennya/ (дата звернення: 23.03.2025).

Секція 3.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ГАЛУЗЕВИХ РІШЕННЯХ

УДК 004.738.5:004.75

ПЛАТФОРМА ДЛЯ ПЛАНУВАННЯ ТА ВІДСТЕЖЕННЯ ЗАВДАНЬ У КОМАНДАХ

Лук'яненко Дар'я Владиславівна
lukianenko1305@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Розломій І.О.
м. Черкаси , Україна

У сучасному бізнес-середовищі ефективне управління завданнями та проєктами є критично важливим для досягнення успішних результатів. Платформи для планування та відстеження завдань у командах допомагають організаціям підвищити продуктивність, покращити комунікацію та забезпечити прозорість робочих процесів.

Таблиця 1. Порівняння сучасних платформ

Платформа	**Основні можливості**	**Переваги**	**Недоліки**
Asana	Управління завданнями, командна співпраця, таймлайн	Гнучкість, зручний інтерфейс	Висока вартість преміум-функцій
Trello	Канбан-дошка, інтеграції, простота у використанні	Інтуїтивний інтерфейс, безкоштовний тариф	Обмежений функціонал у безкоштовній версії
Jira	Agile-управління, звіти, гнучка настройка	Потужний інструмент для розробників	Складний для початківців
ClickUp	Управління завданнями, документи, автоматизація	Великий набір функцій, кастомізація	Може бути перевантаженим
Monday.com	Візуальне управління, аналітика, автоматизація	Зручність у використанні, інтеграції	Висока ціна для малих команд

Одним із основних принципів таких платформ є централізоване управління завданнями, що дозволяє учасникам команди бачити загальний прогрес, визначати пріоритети та своєчасно виконувати роботу. Відомі системи, такі як Asana, Trello, Jira, ClickUp та Monday.com, демонструють широкий спектр

можливостей, включаючи інтеграцію з іншими інструментами, автоматизацію процесів та аналітику виконання завдань.

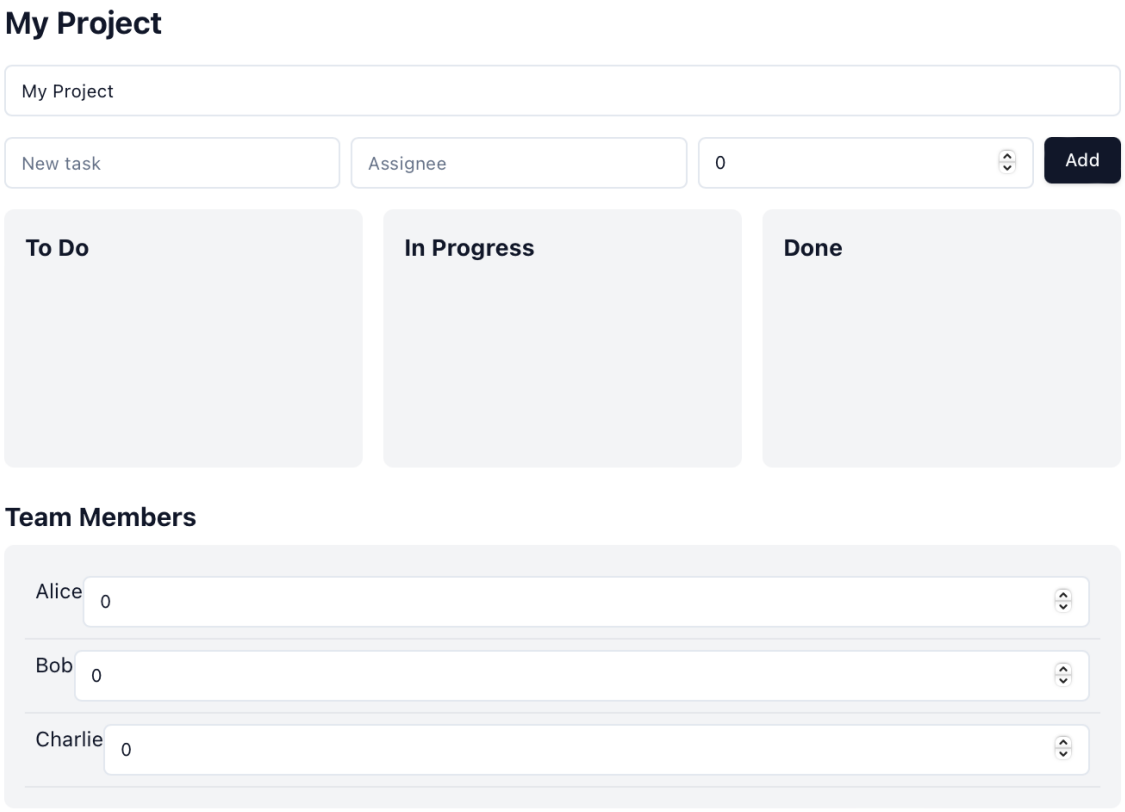

Рисунок 1. Скріншот першої ітерації у створенні власної платформи для відстеження задач команди

Основні функціональні можливості платформ для управління завданнями включають створення та призначення завдань, що дозволяє розподіляти роботу між членами команди з чіткими дедлайнами. Календар та тайм-менеджмент забезпечують відображення термінів виконання завдань та контроль навантаження команди. Спільна робота та комунікація включають коментарі, обговорення, згадки та інтеграцію з месенджерами. Автоматизація робочих процесів реалізується через використання тригерів та шаблонів для спрощення повторюваних завдань. Звіти та аналітика дозволяють відстежувати продуктивність команди та ефективність процесів.

Впровадження таких платформ має значні переваги. По-перше, вони сприяють підвищенню ефективності роботи завдяки автоматизації та централізації процесів. По-друге, покращують комунікацію між членами

команди, що знижує ризик непорозумінь та дублювання завдань. Нарешті, забезпечують можливість аналізу продуктивності, що допомагає керівникам приймати обґрунтовані управлінські рішення.

Однак, існують і певні виклики. Наприклад, для деяких команд може бути складним процес адаптації до нових інструментів. Крім того, занадто велика кількість функцій ускладнює використання платформи, що може знижувати її ефективність.

Перспективи розвитку таких систем включають застосування штучного інтелекту для автоматизації рутинних процесів, інтеграцію з більшою кількістю сервісів та покращену персоналізацію інтерфейсу відповідно до потреб користувачів. Враховуючи сучасні тенденції, можна очікувати, що подібні платформи стануть невід'ємною частиною бізнес-процесів у більшості компаній.

Список використаних джерел

1. Trello vs Asana vs Monday: The Ultimate Project Management Tool Comparison. URL: https://www.techradar.com (дата звернення: 21.03.2025).
2. The Future of Task Management Software. URL: https://www.forbes.com (дата звернення: 21.03.2025).
3. How AI is Transforming Task Management Platforms. URL: https://www.wired.com (дата звернення: 21.03.2025).

УДК 004.77:004.4

АВТОМАТИЗАЦІЯ ВЗАЄМОДІЇ З TELEGRAM-ГРУПАМИ

Янчишен Я. В.
yyanchishen@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Медолиз М. М.
м. Черкаси, Україна

Автоматизація процесів у цифрових комунікаціях є важливим напрямом у сфері інформаційних технологій. Telegram, як один із найпопулярніших месенджерів активно використовується для створення спільнот, ведення бізнесу,

розповсюдження інформації та комунікації між користувачами. Однак адміністрування великих Telegram-груп потребує значних зусиль, зокрема для модерування, приєднання нових учасників, масової розсилки повідомлень та ведення аналітики. Вирішенням цієї проблеми може бути автоматизація ключових процесів, що дозволяє мінімізувати людське втручання та підвищити ефективність управління Telegram-спільнотами [1].

Дослідження сучасних підходів до автоматизації взаємодії з Telegram-групами за допомогою мови програмування Python та бібліотеки Telethon, яка забезпечує прямий доступ до Telegram API [2] є актуальним питанням. Необхідно розглядати можливості Telegram API, принципи роботи з його функціоналом та обмеження, що існують при взаємодії з месенджером [3], як найперспективніший напрямок автоматизації.

Одним із головних аспектів автоматизації керування меседжером є приєднання до Telegram-груп та каналів. Ключовими питаннями при цьому є методи автентифікації користувача, алгоритми надсилання запитів на приєднання, а також можливі обмеження та ризики, пов’язані з автоматичним приєднанням до великої кількості груп. Стратегії уникнення блокувань та використання проміжних рішень для безпечного адміністрування Telegram-акаунтів [4] визначають основні алгоритми автоматизації.

Важливим питанням є реалізація механізму масової розсилки повідомлень у Telegram-групах та каналах. Базовими алгоритмами роботи при розгляді цього питання є алгоритми з текстовими та мультимедійними повідомленнями, а також підходи до зменшення ризиків блокування акаунтів через надсилання великої кількості повідомлень. Варто застосовувати динамічне регулювання інтервалів між повідомленнями, використання різних Telegram-акаунтів для розсилки та обхід лімітів API [5].

Окрему увагу варто приділити механізму логування та ведення бази даних успішних і невдалих операцій. Для збереження даних про надсилання повідомлень, приєднання до груп та інші автоматизовані дії, варото використовувати SQLite як легковагову базу даних. Це дозволить створити

централізовану систему контролю за всіма процесами, а також забезпечить можливість подальшого аналізу ефективності роботи автоматизованого програмного забезпечення [6].

Важливим питанням при автоматизації адміністрування меседжерів є обробки помилок і винятків при взаємодії з Telegram API. Оскільки Telegram встановлює певні ліміти на використання API, важливо розробити механізми, які дозволять уникати перевищення допустимих запитів та забезпечать безперебійну роботу програмного засобу. Впровадження системи автоматичного перезапуску процесів у разі збоїв та використання методів виявлення потенційних проблем у роботі API [7] значно спростить процес автоматизації.

Оптимально, якщо архітектура програмного засобу автоматизації адмінфістрування меседжеру буде включати модульну систему, яка може складатися з таких компонентів: Модуль взаємодії з Telegram API – для забезпечення основного функціоналу підключення до Telegram-акаунтів, взаємодія з чатами, надсилання повідомлень та адміністрування груп. Модуль управління розсилками – дозволить користувачам створювати повідомлення, планувати їх надсилання та аналізувати результати. Модуль логування – відповідатиме за ведення записів про всі операції та збереження їх у базі даних. Модуль обробки помилок – виявлятиме та аналізуватиме помилки під час взаємодії з API, забезпечуючи стабільну роботу всієї системи [8].

Для проведення тестування програмного засобу застосовуються різні сценарії використання, зокрема приєднання до груп, масової розсилки повідомлень та обробки відповідей користувачів. Буде оцінено швидкість виконання операцій, рівень стабільності та можливі ризики, пов’язані з обмеженнями Telegram API [9].

У майбутньому система може бути розширена шляхом додавання функцій автоматичного аналізу контенту та інтеграції з іншими сервісами. Наприклад, можливе впровадження алгоритмів машинного навчання для модерації повідомлень у групах, визначення рівня активності користувачів та оптимізації комунікаційних процесів.

Автоматизація взаємодії з Telegram-групами дозволить значно зменшити навантаження на адміністраторів, прискорити комунікацію та оптимізувати процеси керування спільнотами. Це особливо важливо для бізнесу, маркетингу, новинних ресурсів та будь-яких організацій, що використовують Telegram як основний канал комунікації [10].

Список використаних джерел

1. Telegram API Documentation . URL: https://core.telegram.org/api (дата звернення: 20.03.2025)
2. Telethon: Python API for Telegram . URL: https://docs.telethon.dev/ (дата звернення: 20.03.2025)
3. Python and Telegram API Integration Guide. URL: https://realpython.com/python-telegram-bot/ (дата звернення: 20.03.2025)
4. Best Practices for Avoiding Bans on Telegram. URL: https://telegram.org/blog/safe-bot-usage (дата звернення: 20.03.2025)
5. Automating Telegram Message Sending with Telethon . URL: https://medium.com/automation-telegram-messages (дата звернення: 20.03.2025)
6. SQLite Database Management for Telegram Bots. URL: https://www.sqlitetutorial.net/ (дата звернення: 20.03.2025)
7. Handling Telegram API Errors and Limits . URL: https://github.com/LonamiWebs/Telethon/issues (дата звернення: 20.03.2025)
8. Structuring a Modular Telegram Bot . URL: https://dev.to/python/telegram-bot-best-practices (дата звернення: 20.03.2025)
9. Performance Testing of Telegram Automation Tools . URL: https://towardsdatascience.com/testing-telegram-bots (дата звернення: 20.03.2025)
10. Future Trends in Telegram Automation . URL: https://arxiv.org/abs/2303.14567 (дата звернення: 20.03.2025)

УДК 004.415:658.5

АНАЛІЗ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПОТРЕБ ОРГАНІЗАЦІЇ

Мазурок В. В.
mazurokviktoria22@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Медолиз М. М.
м. Черкаси, Україна

Ми живемо в епоху цифрової трансформації, де хмарні технології стали не просто інструментом, а фундаментом для ефективної роботи організацій. Вони кардинально змінюють підхід до управління IT-інфраструктурою, дозволяючи знижувати витрати, підвищувати продуктивність і забезпечувати гнучкість бізнес-процесів. Чому ця тема така актуальна? Стрімкий попит на хмарні рішення пояснюється потребою компаній оптимізувати операції, але успішне впровадження вимагає глибокого аналізу: від вибору платформи до забезпечення безпеки. Розглянемо, як хмари відкривають нові горизонти для бізнесу та що потрібно знати для їх ефективного використання.

Хмарні технології - це модель надання обчислювальних ресурсів через інтернет за принципом "плати за використання"[2]. Замість інвестування у власні сервери компанії отримують доступ до віртуальної інфраструктури, яка масштабується відповідно до їхніх потреб. За стандартом NIST, хмари мають п’ять ключових характеристик: самообслуговування на вимогу, доступність через мережу, об’єднання ресурсів, еластичність та вимірюваність послуг.

Існують три основні моделі хмарних сервісів [3]. IaaS (інфраструктура як послуга) - це оренда серверів або сховищ даних, як-от Amazon EC2. PaaS (платформа як послуга) надає середовище для розробки додатків, наприклад, Google App Engine. SaaS (ПЗ як послуга) - це готові рішення на кшталт Microsoft 365, де користувачі просто працюють з додатками, не турбуючись про технічну частину.

Щодня ми стикаємося з хмарами, навіть не замислюючись: синхронізація файлів у Google Drive, перегляд фільмів на Netflix або спілкування через Zoom -

усе це можливе завдяки хмарним технологіям. Їхні переваги очевидні: зменшення витрат, масштабованість, захист даних та підтримка віддаленої роботи. Наприклад, технологія віртуалізації дозволяє ефективно розподіляти ресурси, ізолюючи процеси для підвищення безпеки.

Чому компанії обирають хмари? Вони забезпечують безперебійність роботи, глобальну доступність і спрощують управління. У світі, де швидкість та адаптивність визначають успіх, хмарні технології стали необхідністю, а не вибором [1].

Сьогодні на ринку домінують такі гіганти, як AWS, Microsoft Azure та Google Cloud Platform. Вибір платформи залежить від конкретних потреб: AWS славиться масштабованістю, Azure — інтеграцією з продуктами Microsoft, а GCP - потужними інструментами аналітики та ШІ. Наприклад, Uber використовує Google Cloud для обробки даних у реальному часі, а Coca-Cola - AWS для аналітики ланцюгів поставок. Однак впровадження хмарних технологій має й виклики [4]. Безпека даних, залежність від постачальника та нестача кваліфікованих фахівців - це фактори, які потребують уваги. Тенденції свідчать, що майбутнє за гібридними хмарами, які поєднують приватні та публічні рішення, та безсерверними обчисленнями, де ресурси керуються автоматично.

IaaS залишається основою хмарної інфраструктури [7]. Наприклад, Netflix, який обслуговує мільйони користувачів, використовує AWS для потокової передачі контенту. Контейнеризація за допомогою Docker та Kubernetes робить розгортання додатків швидшим, а віртуалізація підвищує ефективність використання апаратних ресурсів.

Безпека в хмарі - пріоритет. Шифрування, контроль доступу та відповідність стандартам (наприклад, GDPR) - це основа захисту. Microsoft Azure, інтегрований з корпоративними рішеннями Windows, ідеально підходить для компаній, які прагнуть поєднувати локальні та хмарні системи.

Впровадження хмарних технологій - це стратегічний крок для будь-якої організації, що прагне лідерства [1]. Вони відкривають доступ до інновацій, але вимагають розумного підходу: від вибору платформи до управління ризиками.

Майбутнє належить тим, хто вміє поєднувати гнучкість хмар з надійністю традиційних систем. Тому сьогодні важливо не лише розуміти технології, але й вміти їх застосовувати - заради конкурентоспроможності та сталого розвитку.

Список використаних джерел

1. Хмарні сервіси та огляд їх постачальників/ Т. Панченко та ін. InterConf. 2024. № 43(193). С. 550–559. URL: https://doi.org/10.51582/interconf.19-20.03.2024.053 (дата звернення: 15.03.2025).
2. Андрієвський Б. М. Упровадження хмарних технологій в освіту: проблеми та перспективи. Інформаційні технології в освіті. 2013. Вип. 14. С. 7–10 (дата звернення: 15.03.2025).
3. Бунке О.С. Ефективні сценарії використання хмарних технологій на підприємстві. Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. 2020. Т. 31. № 6. Р. 44–49. URL: https://doi.org/10.32838/tnu-2663-5941/2020.6-1/08 (дата звернення: 15.03.2025).
4. Що таке гібридна хмара: Ваш гід по IT-інфраструктурі . URL: https://ucloud.ua/shho-take-gibrydna-hmara/ (дата звернення: 15.03.2025)
5. АНАЛІЗ ПОНЯТТЯ ХМАРНІ ТЕХНОЛОГІЇ: ВИДИ, КАТЕГОРІЇ, ПЕРЕВАГИ ТА НЕДОЛІКИ / О. Андрощук та ін. Молодий вчений. 2021. № 6 (94). С. 83–87. URL: https://doi.org/10.32839/2304-5809/2021-6-94-19 (дата звернення: 15.03.2025).
6. Ястремська, . О. М., Стадниченко, . А. В., & Колобов, . І. Ю. (2024). Аналіз впливу технологій хмарних обчислень на стратегічне управління конкурентоспроможністю підприємств. Академічні візії, (27). (дата звернення: 15.03.2025)

УДК 004.94:004.9

ГОЛОГРАФІЧНІ ІНТЕРФЕЙСИ: МАЙБУТНЄ КОРИСТУВАЦЬКОГО ДОСВІДУ

Чабаненко Д. О.
chabanenkodenis77@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Тривимірне зображення в останній час набуває широкого розвитку за рахунок відкриття нових матеріалів з нелінійними властивостями. Різні методи формування тривимірного зображення дали сильний поштовх для створення різних технологій, які використовуються в багатьох сферах, таких як – медицина, сфера розваг, експериментальна фізика, побут та інше. В різних наукових лабораторіях зібрані результати досліджень великої кількості матеріалів з нелінійними властивостями. Основні проблеми пов’язані із: складністю створення таких систем, формуванням композитних матеріалів, та зручних методів формування тривимірного зображення.

Голографічні інтерфейси – це інтерфейси користувача, які використовують технології голографії для створення тривимірних зображень або об'єктів, що можуть взаємодіяти з користувачем у реальному часі. Такі інтерфейси дозволяють користувачам взаємодіяти з віртуальними об'єктами, які виглядають і ведуть себе так, як якщо б вони існували у фізичному просторі, але вони створюються і маніпулюються за допомогою цифрових технологій [1].

Голограма може бути зареєстрована на деякій поверхні (двовимірна голограма) або в деякому об’ємі світлочутливого матеріалу (тривимірна голограма). Двовимірний запис здійснюється за умови, коли товщина (h) світлочутливого матеріалу набагато менша від просторового періоду (d) інтерференц. картини, що реєструється. У тривимірних голограмах h набагато більша, ніж d. Така голограма із суцільного спектра відтворює випромінювання лише з тією довжиною хвилі, яка була використана для її запису, що спричинено інтерференцією хвиль, які відбиті послідовністю пучностей розподілу

диференціалів картини, присутніх у голограмі.

Голографія виникла в 1948 р, коли англійський фізик Габор вперше ввів поняття голограми, тобто системи повного запису просторової структури світлової хвилі (за амплітудою і по фазі) шляхом спостереження інтерференції між дифрагуючою хвилею, що йде від предмета, і однорідним когерентним фоном. Габор довів, що така система реєстрації має властивість оборотності, що дозволяє на другому ступені відновити зображення предмета [2].

На сьогодні розроблені різні типи AR-інтерфейсів: традиційні екрани або монітори, вікна, шоломи та маски, окуляри тощо. Найбільша частка ринку належить портативним дисплеям AR смартфонів зважаючи на їх мобільність, вдосконалені камери, високоякісні дисплеї, висока обчислювальна потужність. Окуляри з технологією AR (Google Glass, Vizix, Optinvent, Meta-Space, Reckon Jet) також заслуговують уваги, але зараз їх поширення обмежене через проблеми конфіденційності. Кожна з названих технологій AR створює 2D-образ, що дає дуже подібне, але не дійсне представлення реального світу. Візуальне сприйняття може дезінформувати користувача, який сприймає 2D зображення, про реальне середовище, як це відбувається з анаморфними оптичними ілюзіями.

Серед можливих інтерфейсів розширеної реальності ті, які використовують 3D голограми для змішування реальних і віртуальних об'єктів, досі не були достатньо детально досліджені. Як реалізація такого голографічного інтерфейсу AR, напівпрозорі дзеркала можуть бути використані як дисплеї, в яких користувачі можуть бачити свої відображення та навколишні об'єкти, змішані із заздалегідь спроектованим віртуальним вмістом.

У складних умовах комбінованого освітлення можуть бути розроблені деякі вдосконалення початкового підходу, а саме: регулювання відсоткового відношення пропущеного світла шляхом введення додаткових частково прозорих поверхонь. Найбільш поширені методи використовують систему Microsoft Kinect для визначення позиції користувача та вирівнювання віртуальних об'єктів до зображень реальних. Захоплення позиції, руху та колективної поведінки користувачів вимагає інтенсивного обміну даними між

датчиками та серверами, з попередньою обробкою даних, сортуванням та анонімізацією [3].

У таких інтерфейсах зазвичай використовується технологія для розпізнавання жестів або рухів рук. Наприклад, користувач може торкатися або рухати руками в просторі, і система визначає ці рухи, щоб виконати певні дії з голограмами. Також можуть використовуватися технології, які розпізнають погляд користувача, щоб вибирати або взаємодіяти з певними елементами голографічного інтерфейсу.

Головною перевагою голографічних інтерфейсів є можливість взаємодії з тривимірними об'єктами в реальному часі. Це може включати перетягування об'єктів, їх змінювання, масштабування або взаємодію з ними за допомогою віртуальних або реальних інструментів (наприклад, за допомогою спеціальних рукавичок, які передають тактильні відчуття).

Отже з усього вище сказаного можна зробити висновок, що голографія – наука, що активно розвивається на даний час, та в майбутньому буде незамінимою частиною життя людей, зокрема для зручних інтерфейсів програм, розваг, медицини, проектування і т.д.

Список використаних джерел

1. WORLD of SCIENCE and TECHNOLOGIES : Що таке голографія - історія виникнення. Wayback Machine. URL: https://web.archive.org/web/20150402184654/http://scitechspace.blogspot.com/2015/03/blog-post_22.html (дата звернення: 24.03.2025).
2. Білоус В. М. Голографія. Енциклопедія Сучасної України. URL: https://esu.com.ua/article-25436 (дата звернення: 24.03.2025).
3. О. Крамар, Ю. Скоренький, Т. Крамар, І. Воробець. Застосування проективних голограм для фізичної реалізації засобів доповненої реальності. URL: https://elartu.tntu.edu.ua/bitstream/lib/27178/2/IMST_2018_Kramar_O_I-Zastosuvannia_proektyvnykh_105.pdf (дата звернення: 23.03.2025).

УДК 004.94:51

МАТЕМАТИЧНІ АЛГОРИТМИ В КОМП'ЮТЕРНІЙ ГРАФІЦІ

Кроть В.С.
vktr244@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Фальченко Н.Г.
м. Черкаси, Україна

Абсолютна більшість цифрових зображень є растровими. Основний елемент тут піксель – найменший логічний елемент двовимірного цифрового зображення у растровій графіці. Кожна точка цифрового зображення характеризується координатами x і y, яскравістю V (x, y) і кольором, якщо це кольорова картинка. Растр – зображення, побудоване з окремих растрових елементів, зазвичай, розташованих регулярно. Растрові елементи в основному є квадрати або прямокутники, але найефективнішим елементом вважається шестикутник, хоча створення гексагонального растру є складнішим.

Растеризація – це переклад зображення, описаного у векторному форматі, у піксел. Розглянемо растеризацію прямої. Перший спосіб перетворення у піксельне зображення реалізовується знаходженням модуля різниці наступної координати та попередньої, що записується у змінну помилки (помилка - неідеальна відповідність піксельної картинки до векторної), а потім за допомогою перевірки на максимум чи мінімум помилки визначається чи змінювати положення пікселя відносно осі Y. У другому способі обчислюється кутовий коефіцієнт та додається до помилки, і якщо її значення не відповідає умові незмінності по Y, то ордината пікселя змінюється.

Векторна графіка - вид комп'ютерної графіки, у якому зображення представляється у виді об’єктів, описаних математично. Елементарним об’єктом ВГ є лінія (не важливо, пряма чи крива).

Головними перевагами ВГ є велика точність зображення, особливо при масштабуванні, легкість перетворення у растрову картинку, та менший розмір файлу. Недоліками ж є складність експорту із растра та менша бібліотека ефектів.

До кривих другого порядку відносяться параболи, гіперболи, окружності, еліпси та інші лінії, рівняння яких не мають степені вище 2. В цілому, вони не сильно розповсюдженні через відсутність точок перегину. Загальна формула (1) кривої 2 порядку:

$$ax2+by2+cxy+dx+ey+f=0 \quad (1)$$

Крім присутності у своїх рівняннях 3 степені, криві третього порядку мають точки перегину, що дозволяє відтворити ті лінії, які ми бачимо у житті, наприклад, вигини людського тіла. Загальна формула (2) кривої 3 порядку:

$$ax3+by3+cx2y+dxy2+ex2+fy2+gxy+hx+iy+j=0 \quad (2)$$

Побудова кубічної кривої за коефіцієнтами її рівняння не є простою процедурою. Щоб спростити це завдання, використовуються криві Без'є, які описуються 8 параметрами, замість 10 у звичайних кривої третього порядку.

Для побудови кривої використовуються спеціальні точки, яких не може бути менше 2. Крива фактично проходить через дві, тому вони є опорними. Інші точки є керуючими та для зручності поєднуються прямою, по якій будується сама крива.

Фрактал - структура, що складається з частин, які в якомусь сенсі подібні до цілого.

Фрактал як термін ввів в обіг французький і американський математик Б. Мандельброт у 1975 році. Найвідомішими та наочними фрактальними об'єктами є дерева. Від кожної гілки відокремлюються менші, схожі на неї, від тих ще менші і так далі. За окремою гілкою можна простежити властивості всього дерева.

На сьогодні фрактали можна розподілити за способом побудови (алгебраїчні, які будуються по формулам, та геометричні, що створюються на основі геометричного об’єкта (відрізок, трикутник, квадрат)) та за закономірністю повторів (симетричні та стохастичні, або несиметричні). У цій роботі будуть розглядатися математичні алгоритми у методах побудови фракталів та їх причетність до комп'ютерної графіки.

Даний вид запису інформації спочатку був створений як інструмент для

дослідження розвитку живих організмів біологом Ліденмаєром, згодом їхня функція розширилася – моделювання складних структур, що гілкуються. Принцип створення цієї системи складається із 3 компонентів: змінних, що беруть участь в алгоритмі (у більшості випадків букви латинського алфавіту), аксіоми (початковий рядок) та правила, за яким рядки будуть перетворюватися. Приклад алгоритму:

Аксіома: A

Змінні: A B C

Правило: A→AB, B→BC, C→A

У висновку, за допомогою L-систем можна створювати різноманітні об’єкти, що не будуть сильно навантажувати процесор пристрою.

Система ітераційних функцій (IFS) — основний метод побудови геометричних фракталів. Називається системою функцій, тому що сам фрактал складається з об’єднання декількох власних копій, кожна з яких перетворюється функцією. Основне використання СІФ – стиснення зображень та шифрування інформації, але є дочірній алгоритм цього методу, який сильно пов'язаний із КГ.

Фрактальне полум’я – алгоритм, що використовує для створення зображень системи ітераційних функцій. Головною відмінністю від інших алгоритмів є додавання кольору в залежності від структури об’єкта. Хоч і зображення може не містити візуально самого фракталу, результат є досить цікавим та естетичним, тому алгоритм фрактального полум'я застосовується у комп'ютерній графіці для створення реалістичних ефектів. Також можна генерувати фрактальний шум, який може бути використаний для створення рельєфу поверхні, хмар, води та інших текстур.

У 3D графіці основним засобом трансляції об’єктів є матриця перетворень – математичний інструмент, який використовується для перетворення координат точок у просторі. Вона дає змогу виконувати такі операції, як переміщення, масштабування та обертання об'єкта, що необхідно для створення анімацій і динамічних сцен. Матриці переміщення та масштабування:

$$\begin{matrix} 1 & 0 & 0 & Tx \\ 0 & 1 & 0 & Ty \\ 0 & 0 & 1 & Tz \\ 0 & 0 & 0 & 1 \end{matrix} \quad \begin{matrix} Sx & 0 & 0 & 0 \\ 0 & Sy & 0 & 0 \\ 0 & 0 & Sz & 0 \\ 0 & 0 & 0 & 1 \end{matrix}$$

У повороту є одна особливість, наприклад, якщо повернути куб спочатку навколо осі Y, а потім навколо осі X, то результати будуть відрізнятися [5].

Є й інші особливості, наприклад, якщо куб повернути на 90 градусів за віссю X, потім на 90 градусів за віссю Y, і нарешті, на 90 градусів навколо осі Z, то останній поворот навколо Z, скасує поворот навколо X, і вийде такий самий результат, як якщо б ви просто повернули фігуру на 90 градусів навколо осі Y [5]. Саме через ці проблеми поворот за допомогою матриць не завжди ефективний.

Комплексні числа дуже гарно задають поворот на площині: якщо z1 і z2 задано в геометричній формі ($z1=|z1|(\cos\phi1+i\sin\phi1)$, $z2=|z2|(\cos\phi2+i\sin\phi2)$), то добутком цих чисел є $z1z2=|z1|\cdot|z2|[\cos(\phi1+\phi2)+i\sin(\phi1+\phi2)]$. Тобто модуль добутку двох комплексних чисел у тригонометричній формі дорівнює добутку модулів співмножників, а аргумент (кут) дорівнює сумі аргументів (кутів) співмножників. Така властивість КЧ розповсюдилась і на кватерніони, хоч в них використовуються 4 виміри для поворота, замість очікуваних 3.

Математика – рушій сучасного прогресу. За її допомогою тільки у комп'ютерній графіці створюються картинки та форми, яких ніколи не буде існувати в реальності. Абсолютно різні математичні алгоритми, на перший погляд не причетні до ІТ, доповнюють та покращують існуючі технології формування цифрових зображень та анімацій: векторні зображення, що задаються математичними функціями, складні перетворення об'єктів за допомогою матриць та недійсних чисел, нескінченні та загадкові фрактали. Саме тому математика, особливо в роботі новітнього ШІ, є фундаментальною складовою ІТ.

Список використаних джерел

1. Кейс-урок «Фрактали та їх застосування». URL: https://naurok.com.ua/keys-urok-fraktali-ta-h-zastosuvannya-290839 (дата звернення: 21.03.2025).
2. АЛГОРИТМІЧНІ ОСНОВИ КОМП'ЮТЕРНОЇ ГРАФІКИ. URL: https://stud.com.ua/156197/informatika/algoritmichni_osnovi_kompyuternoyi_g

rafiki_rastrovi_algoritmi_viznachennya_vidimosti_zafarbovuvannya (дата звернення: 21.03.2025).
3. Що таке векторна графіка? URL: https://www.run-it.com.ua/shcho-take-vektorna-hrafika/ (дата звернення: 21.03.2025).
4. Криві Безьє. Основні поняття та властивості кривих Безьє. URL: Криві Безьє. Основні поняття та властивості кривих Безьє - www.mathros.net.ua
5. 3D своими руками. Часть 2: оно трехмерное. URL: https://habr.com/ru/articles/497808/ (дата звернення: 21.03.2025).

УДК 004.9:615.851

НЕЙРОІНТЕРФЕЙСИ: МАЙБУТНЄ ВЗАЄМОДІЇ ЛЮДИНИ З КОМП’ЮТЕРОМ

Заїка М. В.
zaikamihaylo@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

З розвитком новітніх технологій нейроінтерфейс це одна з важливих складових систем обміну інформацією між мозком та іншими пристроями. У деяких випадках нейроінтерфейс просто передає дані на зовнішній пристрій, але іноді система дає змогу керувати іншими пристроями, наприклад комп'ютерною програмою або спеціальними приладами чи об'єктами, зокрема персонажами комп'ютерних ігор.

Основні види нейроінтерфейсів:

1. Інвазивні нейроінтерфейси – імплантовані пристрої, що взаємодіють безпосередньо з нейронами. Вони забезпечують високу точність, але потребують хірургічного втручання. Прикладами є Neuralink Ілона Маска, технології контролю протезів для людей з обмеженими можливостями.
2. Неінвазивні нейроінтерфейси – пристрої, що зчитують сигнали мозку без хірургічного втручання (наприклад, EEG). Вони простіші у використанні, але мають нижчу точність через перешкоди у зчитуванні сигналів.

3. Гібридні нейроінтерфейси – комбінують елементи інвазивних і неінвазивних технологій, намагаючись досягти балансу між ефективністю та безпекою.

На основі існуючих видів нейроінтерфейсів можна зробити висновок, що на сьогоднішній день ще не існує універсального нейроінтерфейсу без будь-яких мінусів,проте не дивлячись на це вони вже встигли знайти своє застосування в найрізноманітніших сферах.

На сьогодні сферами застосування нейроінтерфейсів є:

У медицині лікування нейродегенеративних хвороб (Альцгеймера, Паркінсона), реабілітація після інсультів, керування протезами через мозкові сигнали.

У кібернетиці управління роботизованими протезами та екзоскелетами, покращення можливостей людини за допомогою імплантів.

У сфері геймінгу та розваг управління комп'ютерними іграми за допомогою думок, створення повністю інтерактивних VR-досвідів.

У сфері комунікацій допомога людям із порушеннями мовлення та руху, можливість передавати думки у цифровій формі без використання фізичних пристроїв.

У військовій сфері управління дронами, поліпшення координації військових операцій.

Нейроінтерфейси мають широке застосування у різних галузях, починаючи від медицини і закінчуючи військовими технологіями. Вони можуть значно покращити якість життя людей з обмеженими можливостями, розширити можливості взаємодії з цифровим світом та автоматизованими системами, а також сприяти появі нових форм комунікації та розваг. Разом з тим, їх впровадження потребує ретельного дослідження та контролю з боку наукової спільноти та законодавчих органів, щоб забезпечити безпеку та етичність використання цих технологій.

У майбутньому нейроінтерфейси можуть стати ключовою технологією для створення повноцінного симбіозу людини та машини. Очікується, що вони

сприятимуть розширенню можливостей людського мозку, зміні способів комунікації та управління технологіями. Розробки, такі як мозкові імпланти для покращення пам’яті, можуть стати реальністю у найближчі десятиліття.

Нейроінтерфейси мають значний потенціал для трансформації багатьох сфер людської діяльності, забезпечуючи прямий зв’язок між мозком та цифровими системами.

У Медицині очікується поява більш ефективних методів реабілітації після травм, нових способів лікування нейродегенеративних хвороб, а також розширення можливостей для людей з інвалідністю через високоточні нейропротези та екзоскелети.

У сферах кібернетики та робототехніки майбутнє передбачає розробку удосконалених мозкових імплантів, що розширять когнітивні та фізичні можливості людини, а також розвиток біонічних протезів, які будуть інтегровані в нервову систему.

У сферах комунікаційних та інформаційних технологій створення мозково-комп’ютерних інтерфейсів нового покоління дозволить людям взаємодіяти з пристроями без фізичного контакту, що змінить підходи до використання мобільних гаджетів, Інтернету та навіть соціальних мереж.

У освіті та науці застосування нейроінтерфейсів у навчальному процесі може сприяти швидшому засвоєнню інформації, персоналізованому навчанню та навіть передачі знань безпосередньо у свідомість.

У сферах геймінгу та розваг буде можливим створення повноцінних імерсивних віртуальних середовищ, де користувачі зможуть взаємодіяти зі світом гри силою думки, що докорінно змінить індустрію розваг.

У військовій та космічній галузі розвиток технологій дасть змогу керувати дронами та бойовими машинами силою думки, а також сприятиме дослідженню космосу через безпосереднє управління складними технічними системами.

Попри величезний потенціал, розвиток нейроінтерфейсів потребує вирішення важливих етичних, безпекових і правових питань. Важливим викликом залишається забезпечення захисту особистих даних та усунення

ризиків втручання в людську свідомість.

Загалом, нейроінтерфейси мають всі передумови для того, щоб стати ключовою технологією майбутнього, яка зможе розширити межі людських можливостей та забезпечити принципово новий рівень взаємодії з навколишнім цифровим світом.

Список використаних джерел:

1. Elon Musk’s Neuralink: Progress and Challenges in Brain-Computer Interface Technology. Nature Neuroscience, 2023 (дата звернення 20.03.2025).
2. Ethical and Legal Challenges of Brain-Computer Interfaces. Frontiers in Neuroscience, 2022 (дата звернення 20.03.2025).
3. IEEE Brain Initiative: Current Research and Future Directions of Neurotechnology. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 2022 (дата звернення 20.03.2025).
4. Lebedev, M. A., & Nicolelis, M. A. L. Brain-machine interfaces: past, present and future. Trends in Neurosciences, 2006. 29(9), P. 536-546.
5. Neuronal Signal Processing and the Future of BCIs. Journal of Neural Engineering, 2021 (дата звернення 20.03.2025).
6. Nuffield Council on Bioethics. Neural interfaces: ethical considerations 2021.
7. Vidal, J. J. Toward direct brain-computer communication. Annual Review of Biophysics and Bioengineering, 1973. 2(1), P. 157-180.
8. Wolpaw, J. R., & Wolpaw, E. W. Brain-Computer Interfaces: Principles and Practice. Oxford University Press. 2012. (дата звернення 20.03.2025).

УДК 004.45:004.4

РЕАЛІЗАЦІЯ ВІРТУАЛЬНОГО СЕРЕДОВИЩА ЗА ДОПОМОГОЮ VIRTUALBOX ДЛЯ ІНТЕГРАЦІЇ WINDOWS 7 ТА WINDOWS 10

Матюшенко Д.В.
matrd0960@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Медолиз М.М.
м. Черкаси, Україна

У сучасному світі інформаційних технологій постійно зростає кількість операційних систем, які використовуються в різних сферах життя — від корпоративних мереж до домашніх пристроїв. Організація взаємодії між Windows 7 та Windows 10 на сьогоднішній день є актуальним питанням, особливо можливість безпечної та ефективної взаємодії між різними версіями операційних систем у спільному мережевому середовищі та встановити оптимальні засоби організації мережевого доступу для їх сумісної роботи.

За допомогою VirtualBox, що виступає лише як інструмент для моделювання, можна перевірити можливість об’єднання ОС у єдине мережеве середовище, де навіть системи одного типу спільно виконують завдання, забезпечуючи стабільний обмін даними з низькою затримкою.

Процес розгортання VirtualBox дозволяє налаштувати мережевий адаптер кожної віртуальної машини у режим Internal Network, завдяки чому всі системи підключаються до єдиного логічного сегменту [6]. Це означає, що Windows 7 та Windows 10 можуть ефективно обмінюватися інформацією з середнім часом відповіді ping у межах 2–5 мс, що свідчить про високу продуктивність навіть у випадках, коли різниця у версіях ОС може викликати певні нюанси в налаштуваннях.

Під час тестування інтеграції може виникнути потреба в коригуванні мережевих параметрів, таких як встановлення статичних IP-адрес, налаштування масок підмереж і конфігурація правил брандмауера. Оскільки Windows 7 і Windows 10 можуть мати відмінності в налаштуваннях безпеки, важливо, щоб адміністратор приділив увагу налаштуванню ICMP-запитів та інших мережевих

протоколів, що забезпечує безпечну та стабільну передачу даних між системами [1].

Використання VirtualBox як інструменту для моделювання дозволяє проводити тестування інтегрованих мереж без впливу на основну інфраструктуру, оскільки всі експерименти відбуваються у віртуальному, ізольованому середовищі [2]. Завдяки функції знімків стану системи, у разі виникнення помилок можна швидко повернутися до попередньої стабільної конфігурації, що значно прискорює процес оптимізації налаштувань мережі.

Інтеграція Windows 7 та Windows 10 у спільну мережу демонструє, що навіть операційні системи різних поколінь можуть працювати разом, забезпечуючи економію ресурсів та зниження витрат на модернізацію апаратного забезпечення [6]. Такий підхід дозволяє організаціям використовувати наявні серверні ресурси для обслуговування критично важливих додатків, оптимізувати роботу мережі та підвищити безпеку даних без необхідності придбання нового обладнання.

Реалізація віртуального середовища за допомогою VirtualBox довела, що інтеграція різних версій операційних систем, зокрема Windows 7 та Windows 10, може створити суцільну мережу, яка є ефективною та безпечною. VirtualBox виступає як зручний інструмент для перевірки можливостей інтеграції, дозволяючи організаціям експериментувати з різними конфігураціями, оптимізувати використання ресурсів та впроваджувати інноваційні IT-рішення, що сприяє підвищенню конкурентоспроможності та стабільності мережевої інфраструктури.

Список використаних джерел

1. Налаштування мережі у VirtualBox. . URL: https://daad.org.ua/10192-nalashtuvannya-merezhi-v-virtualbox.html (дата звернення: 22.03.2025)
2. Особливості налаштування локальної мережі у Windows XP/7/10. . URL: https://analityk.com.ua/localna-merega/ (дата звернення: 22.03.2025)

3. Увімкнення спільного доступу до принтера Windows 7 . URL: https://daad.org.ua/2307-yak-vklyuchiti-zagalniy-dostup-do-printera-windows-7.html (дата звернення: 22.03.2025)
4. Як підключити принтер через мережу у Windows – від XP до Windows 10 . URL: https://www.moyo.ua/ua/news/kak_podklyuchit_printer_po_seti_v_windows_ot_xp_do_windows_10.html (дата звернення: 22.03.2025)
5. How to add a printer in Windows 10 . URL: https://www.laptopmag.com/articles/add-printer-windows-10 (дата звернення: 22.03.2025)
6. Створення та налаштування віртуальної машини VirtualBox на Windows завдяки ISO-образу Ubuntu URL: https://hackyourmom.com/pryvatnist/vstanovlennya-virtualbox-na-ubuntu/ (дата звернення: 22.03.2025)

УДК 004.9:006.8

МЕТА-ВСЕСВІТ: ІНТЕГРАЦІЯ ВІРТУАЛЬНОЇ РЕАЛЬНОСТІ ТА ШТУЧНОГО ІНТЕЛЕКТУ У ПОВСЯКДЕННЕ ЖИТТЯ

Пидорич Н. С.
pydorychn@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Мета-Всесвіт є новою епохою в розвитку технологій, яка включає інтеграцію віртуальної реальності (VR) та штучного інтелекту (AI) у різні аспекти повсякденного життя. Ця концепція охоплює створення цифрових просторів, які стають природним продовженням фізичного світу. Вона не лише відкриває нові горизонти для взаємодії між людьми та технологіями, але й ставить питання про наше розуміння реальності, соціальних норм і майбутнього суспільного розвитку. Теза розглядає можливості, переваги та виклики цієї інтеграції, досліджує її позитивний вплив, одночасно аналізуючи потенційні

ризики, такі як етичні дилеми чи нерівний доступ до технологій.

Мета-Всесвіт передбачає інтеграцію віртуальної реальності (VR) та штучного інтелекту (AI) у різні аспекти повсякденного життя. У професійній сфері ця інтеграція відкриває величезні перспективи, такі як створення реалістичних VR-симуляцій для навчання працівників у безпечному середовищі. Використання AI сприяє автоматизації рутинних задач, аналізу великих обсягів даних і підтримці прийняття стратегічних рішень. Наприклад, віртуальні робочі простори можуть замінити традиційні офіси, дозволяючи співробітникам спільно працювати над проектами з будь-якої точки світу. Це підвищує гнучкість робочих процесів та загальну ефективність компаній.

В освітньому середовищі VR та AI допомагають переосмислити сам підхід до навчання. Створення інтерактивних віртуальних класів і лабораторій надає можливість студентам вивчати складні поняття через досвід. AI адаптує освітній контент під індивідуальні потреби кожного учня, допомагаючи їм досягти максимальних результатів. Крім того, віртуальні екскурсії та симуляції дозволяють побачити історичні події, досліджувати космос чи аналізувати молекулярні структури, що робить навчання більш захопливим та доступним.

У медичній сфері VR використовується для розробки інноваційних методів реабілітації та терапії, наприклад, допомагаючи пацієнтам із неврологічними розладами відновлювати втрачені функції. AI допомагає лікарям точніше діагностувати захворювання, аналізуючи медичні дані, і рекомендує найбільш ефективні методи лікування. Завдяки віртуальним клінікам пацієнти можуть отримувати консультації від фахівців, не виходячи з дому, що значно розширює доступ до якісної медичної допомоги.

У сфері розваг і соціальних взаємодій інтеграція VR та AI відкриває простір для створення унікальних форм дозвілля. Наприклад, віртуальні світи дозволяють гравцям переживати незабутні пригоди, тоді як AI-аватари забезпечують гнучкий і персоналізований соціальний досвід. Також ці технології сприяють розвитку нових способів спілкування, допомагаючи людям залишатися на зв’язку навіть на відстані.

Нарешті, економічні та етичні аспекти цієї інтеграції вимагають особливої уваги. Наприклад, швидкий розвиток VR та AI створює нові професії та змінює структуру ринку праці, але також викликає занепокоєння щодо заміни людської праці автоматизованими системами. Етичні питання включають забезпечення конфіденційності даних користувачів і розробку принципів відповідального використання технологій. У той же час VR і AI відкривають нові можливості для економічного зростання, створюючи інноваційні бізнес-моделі.

Інтеграція віртуальної реальності та штучного інтелекту в повсякденне життя є не лише технологічним проривом, але й філософським викликом для людства. Вона здатна значно покращити якість життя і створити нові можливості, водночас вимагаючи від нас усвідомленого підходу до її впровадження, враховуючи як потенціал, так і ризики.

Список використаних джерел:

1. Everyday Metaverse: The Metaverse as an Integral Part of Everyday Life / Wang G. and others. Journal of Management Information Systems. 2025. VOL. 42, №. 1, P. 310–342.
2. How AI Is Impacting Society And Shaping The Future. Forbes. URL: https://www.forbes.com/sites/kalinabryant/2023/12/13/how-ai-is-impacting-society-and-shaping-the-future/ (date of access: 24.03.2025).
3. Partida D. How will the metaverse impact our everyday lives?. https://technologymagazine.com/ai-and-machine-learning/how-will-the-metaverse-impact-our-everyday-lives?form=MG0AV3. URL: https://technologymagazine.com/ai-and-machine-learning/how-will-the-metaverse-impact-our-everyday-lives?form=MG0AV3 (date of access: 24.03.2025).
4. Вплив метавсесвіту на сучасне суспільство та технології. ProIT. URL: https://proit.com.ua/news/mozhlyvosti-ta-vplyv-metavsesvitu-na-suchasnist/?form=MG0AV3 (дата звернення: 24.03.2025).

УДК 004.42:336.76

АВТОМАТИЗОВАНИЙ МОНІТОРИНГ ЦІН НА ПАЛЬНЕ ТА ВПРОВАДЖЕННЯ ІТ-РІШЕНЬ У ЦИФРОВУ ЕКОНОМІКУ

Чернишов Р.С.
romarioriw2005@gmail.com
Черкаський державний фаховий бізнес-коледж,
Науковий керівник : Немченко В.Ю.
м.Черкаси, Україна

Сучасний ринок пального є динамічним та непередбачуваним, оскільки ціни на пальне можуть змінюватися залежно від регіону, постачальника та інших економічних факторів.В умовах високої конкуренції та нестабільності споживачам важливо мати доступ до актуальної інформації про вартість пального, щоб приймати обґрунтовані фінансові рішення [5].

Розширення для Google Chrome, яке автоматизує процес збору та відображення цін на пальне, є важливим інструментом для користувачів, які прагнуть економити час і кошти. Це рішення дозволяє водіям оперативно отримувати актуальні дані та знаходити найбільш вигідні пропозиції на ринку [6].

Значення такого розширення можна розглянути через кілька ключових аспектів:

- Ефективний збір та обробка даних. Подібно до того, як банківські установи аналізують фінансові ринки для прийняття стратегічних рішень, ІТ-інструменти для збору інформації про пальне повинні швидко та точно обробляти великі обсяги даних. Автоматизовані системи дозволяють оперативно отримувати та оновлювати інформацію, що сприяє її точності та актуальності [1].
- Управління інформаційними потоками.Як і в банківській сфері, управління великими масивами даних відіграє ключову роль у функціонуванні сервісів, пов’язаних із цінами на пальне. Впровадження Google Chrome Extension дозволяє оптимізувати процеси обробки запитів та інтегрувати інформацію з різних джерел [2].

- Прозорість та доступність інформації.Важливим аспектом у розробці подібних розширень є забезпечення користувачів якісною, прозорою та достовірною інформацією. Це дозволяє мінімізувати ризики та робити більш обґрунтовані фінансові рішення щодо витрат на пальне [5].

В умовах глобалізації та технологічного прогресу розширення для Google Chrome виконує кілька важливих функцій:

- Глобальна доступність та інтеграція.Оскільки сучасний світ переходить до діджиталізації, важливою перевагою такого рішення є можливість інтеграції з міжнародними сервісами моніторингу цін на пальне. Використання API дозволяє забезпечити доступ до оновлених даних незалежно від географічного положення користувача [1].
- Доступ до ресурсів та інформації.Більшість платформ, що надають інформацію про ціни на пальне, використовують англомовну технічну документацію. Володіння англійською мовою дозволяє розробникам ефективно працювати з API, інтегрувати нові функції та використовувати світові практики у створенні IT-рішень [3].
- Перспективи для розробників та бізнесу.Наявність такого інструменту підвищує конкурентоспроможність не тільки окремих водіїв, а й компаній, що працюють у сфері логістики, транспорту та енергетики. Автоматизація збору даних про пальне може стати важливим компонентом у стратегічному плануванні витрат [6].
- Інновації та технологічний прогрес.Використання JavaScript, API сервісів та платформи Vercel дозволяє створити ефективний та масштабований продукт. Такий підхід сприяє швидкій адаптації до змін на ринку та покращенню функціональності розширення [3].

Отже,розробка розширення для Google Chrome для моніторингу цін на пальне є важливим кроком у цифровізації галузі та підвищенні доступності інформації для користувачів. Це рішення дозволяє водіям та компаніям оптимізувати витрати, приймати обґрунтовані рішення та ефективніше планувати витрати на пальне [4].

Впровадження таких інструментів сприяє створенню єдиного інформаційного середовища для аналізу та прогнозування цінових тенденцій. Подальший розвиток проекту може включати розширення підтримки нових функцій, інтеграцію з картографічними сервісами та вдосконалення алгоритмів обробки даних для ще більш точної та персоналізованої інформації [2].

Список використаних джерел

1. «API Fuel Prices”. "Access to Real-Time Fuel Price Data for Developers». .URL:https://www.fuelapi.com/(дата звернення: 25.03.2025).
2. “Google Developers “."Developing Chrome Extensions: Best Practices and Guidelines.". URL:https://developer.chrome.com/docs/extensions/ (дата звернення: 25.03.2025).
3. “Vercel”."Deploying and Scaling Serverless Applications." . URL: https://vercel.com/docs (дата звернення: 25.03.2025).
4. “Highload.tech“."10 корисних розширень Google Chrome для фронтенд-розробників". .URL:https://highload.tech/uk/10-korisnih-rozshiren-google-chrome-dlya-frontend-rozrobnikiv/ (дата звернення: 25.03.2025).
5. “AUTO.RIA. “ "Ціни на бензин, дизель (дп), газ на АЗС сьогодні." . URL: https://auto.ria.com/uk/toplivo/ (дата звернення: 25.03.2025).
6. “Minfin.com.ua «Ціни на бензин, дизпаливо, газ на АЗС України» URL:https://index.minfin.com.ua/ua/markets/fuel/ (дата звернення: 25.03.2025).

УДК 37.036:004.9

СУЧАСНІ ІНФОРМАЦІНІ ТЕХНОЛОГІЇ НАВЧАННЯ ІЗ ВИКОРИСТАННЯМ ІНТЕРАКТИВНИХ ЗАСОБІВ

Монько С.Ю.
stasmonko6@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Швиденко А.В
м. Черкаси, Україна

Сучасні інформаційні технології значно змінили підходи до освіти, дозволяючи створювати інтерактивні навчальні середовища. Використання інтерактивних засобів сприяє підвищенню мотивації студентів, покращенню засвоєння матеріалу та розвитку критичного мислення [1]. Онлайн-платформи, мультимедійні технології та віртуальна реальність відкривають нові можливості для освіти, особливо в умовах дистанційного навчання [4].

Окрім цього, цифровізація освітнього процесу дозволяє адаптувати навчальні матеріали під індивідуальні потреби студентів, сприяє персоналізації навчання та підтримує активну взаємодію між учнями та викладачами [2]. Використання інтерактивних засобів дозволяє підвищити рівень залученості студентів у навчальний процес, сприяє розвитку комунікативних навичок та формуванню компетентностей, необхідних у сучасному інформаційному суспільстві.

Основні інтерактивні засоби та їх застосування:

1. Мультимедійні презентації. Програми, такі як Microsoft PowerPoint, Prezi, Canva, дозволяють створювати інтерактивні презентації з відео, анімаціями та графікою. Вони допомагають зробити подання навчального матеріалу більш динамічним і наочним, що сприяє кращому розумінню та запам’ятовуванню інформації [1].
2. Онлайн-платформи для дистанційного навчання. Moodle, Google Classroom, Microsoft Teams забезпечують ефективну організацію навчального процесу. Вони надають можливість розміщення навчальних матеріалів, проведення

тестування, організації зворотного зв’язку та інтерактивного спілкування між викладачем і студентами [4] .

3. Технології віртуальної та доповненої реальності. VR- та AR-додатки, такі як Google Expeditions, CoSpaces Edu, дозволяють створювати віртуальні навчальні тури та симуляції. Ці технології особливо корисні для навчання природничих дисциплін, медицини, інженерії, оскільки дозволяють студентам взаємодіяти з навчальним матеріалом у тривимірному просторі [3].
4. Інтерактивні дошки та платформи для спільної роботи. Miro, Jamboard, Padlet сприяють груповій роботі та взаємодії студентів у реальному часі. Вони дозволяють створювати спільні проєкти, обговорювати ідеї, організовувати мозкові штурми, що сприяє розвитку командної роботи [2].
5. Системи автоматизованого тестування та гейміфікація навчання. Kahoot!, Quizizz, Mentimeter допомагають оцінювати знання студентів в інтерактивній формі. Гейміфікація навчального процесу сприяє залученню студентів, підвищенню їх мотивації та створенню сприятливої атмосфери для навчання [5].
6. Адаптивні навчальні системи. Використання технологій штучного інтелекту, таких як Coursera, Duolingo, дозволяє автоматично підлаштовувати навчальний матеріал під рівень підготовки студента. Це сприяє персоналізованому підходу до навчання та покращенню засвоєння знань [3].

Впровадження інтерактивних технологій в освітній процес потребує ретельного планування та адаптації до існуючих навчальних програм. Однією з ключових особливостей є необхідність підготовки викладачів до ефективного використання цифрових інструментів. Це вимагає спеціальних тренінгів та курсів підвищення кваліфікації, що дозволяють педагогам ознайомитися з можливостями інтерактивних платформ, методами створення цифрового контенту та принципами організації онлайн-взаємодії зі студентами. Крім того, важливим аспектом є забезпечення технічної підтримки та наявність необхідного

обладнання в навчальних закладах, що дозволяє ефективно інтегрувати сучасні технології в освітній процес [1-2].

Ще однією важливою особливістю є необхідність розробки нових методичних підходів до оцінювання знань студентів. Традиційні методи тестування можуть бути не завжди ефективними при використанні інтерактивних технологій, тому необхідно впроваджувати адаптивні системи оцінювання, які враховують рівень підготовки студента та його індивідуальний темп навчання. Використання гейміфікації, адаптивного навчання та інтерактивних симуляцій дозволяє зробити процес оцінювання більш об’єктивним і мотивуючим для студентів.

Подальші дослідження можуть бути зосереджені на розробці нових методик адаптивного навчання, інтеграції штучного інтелекту у навчальний процес та розширенні можливостей використання VR і AR у різних галузях освіти. Особливо актуальним є дослідження ефективності використання інтерактивних платформ у різних вікових групах та їх впливу на когнітивний розвиток учнів. Також перспективним напрямком є розробка інструментів для автоматизованого аналізу прогресу студентів та розширення можливостей віртуальних лабораторій.

Список використаних джерел

1. Биков В. Ю. Сучасні інформаційні технології та засоби навчання / В. Ю. Биков, М. П. Лещенко. – Київ: НАПН України, 2021. – 320 с.
2. Семеніхіна О. В. Теоретичні та практичні аспекти використання інтерактивних технологій у навчальному процесі / О. В. Семеніхіна, Л. М. Чайка. – Суми: СумДУ, 2020. – 250 с.
3. Siemens G. Connectivism: A Learning Theory for the Digital Age / G. Siemens // International Journal of Instructional Technology and Distance Learning. – 2005. – Vol. 2, No. 1. – P. 3-10.
4. Дистанційне навчання в сучасній освіті: теорія і практика / За ред. В. Г. Кремень. – Київ: Педагогічна думка, 2019. – 280 с.

5. Online Learning Platforms: Current Trends and Future Directions / Ed. by J. Baker. – New York: Springer, 2022. – 400 p.

УДК 004.42:006.7

АЛГОРИТМИ МАШИННОГО НАВЧАННЯ В РЕКОМЕНДАЦІЙНИХ СИСТЕМАХ ДЛЯ ВІДЕО ТА АУДІОПЛАТФОРМ

Путря А.С.
putrianastia9@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Люта М. В.
м. Черкаси, Україна

Рекомендаційні системи стали невід'ємною частиною сучасного цифрового світу. Вони визначають, які фільми нам запропонує Netflix, які відео ми побачимо у стрічці YouTube, яку музику рекомендуватиме Spotify або Apple Music. Цей проєкт дослідить механізми, які стоять за персоналізацією контенту, принципи роботи сучасних алгоритмів рекомендацій і можливі проблеми, які вони створюють.

Рекомендаційні системи використовують різні підходи до персоналізації контенту. Колаборативна фільтрація, яка аналізує вподобання багатьох користувачів, щоб знайти людей, подібних один до одного. Якщо фільм, який сподобався певній особі, також сподобався іншій групі, система запропонує людні контент, який їм подобається. Використовується в YouTube, Netflix та Amazon.

Фільтрація на основі контенту аналізує цільові характеристики (наприклад,жанр,тривалість, акторський склад) і пропонує схожі варіанти. Якщо людині подобається детективний серіал, система порекомендує інші детективні серіали. Використовується також в Spotify та Apple Music.

Гібридні рекомендаційні системи-поєднують обидва підходи для підвищення точності. Зокрема, Netflix використовує гібридну систему, яка враховує як поведінку користувача, так і характеристики контенту.

YouTube використовує гібридну систему. Аналізація поведінки людини(що дивиться,що лайкає і коментує) та реакції інших користувачів на цей же контент. Враховується час, витрачений на перегляд кожного відео. Якщо особа додивилися відео до кінця – це сигнал, що відео її зацікавило. Впроваджує моделі глибокого навчання, щоб передбачити, які відео можуть сподобаються далі.

Netflix створює персоналізований каталог – аналізує, які фільми та серіали людина дивилися, як довго вона їх дивилися і чи дивилися схожі програми. Класифікує глядачів за схожими смаками.

Якщо людині до вподоби комедії, Netflix може показати кумедні кавер-версії тих самих фільмів.

Spotify використовує технологію аудіоаналізу, яка розбиває пісні за ритмом, темпом і стилем виконання та аналізує їхню схожість з іншими піснями. Застосунок додає дані про вподобання інших слухачів (спільна фільтрація).

Сервіс Discover Weekly створює персоналізовані плейлисти на основі того, що слухають люди зі схожими музичними смаками.

Amazon аналізує історію покупок і поведінку на сайті для показу товарів, які можуть зацікавити користувача.

Попри користь, алгоритми мають і певні недоліки. "Ефект інформаційної бульбашки" – користувачам показується лише той контент, що підтверджує їхні поточні погляди, обмежуючи можливість знайомства з новими ідеями. У соціальних мережах люди отримують новини лише з одного боку політичного спектру, що впливає на їхній світогляд. Поведінкові маніпуляції – платформи можуть навмисно показувати контент, який змушує користувачів залишатися на сайті довше, навіть якщо це не приносить користі.

Якщо розглянути TikTok у якому заохочення користувачів відбувається на снові взаємодії з платформою, шляхом популяризації відео контенту, які викликають сильні емоції.

Персональні дані та конфіденційність – сервіси збирають велику кількість інформації про користувачів, що викликає питання про безпеку даних. Щоб

краще зрозуміти, як працюють рекомендаційні алгоритми, можна провести кілька експериментів та аналізів.

Аналіз рекомендацій у маркетплейсах (Amazon, Rozetka, Aliexpress) починається з відкриття сторінки будь-якого товару, наприклад, смартфона. Наступним кроком буде перегляд супутніх товарів, запропонованих сайтом: чохли, зарядні пристрої, навушники. Якщо кілька разів переглянути певну категорію товарів, алгоритм почне пропонувати схожі продукти, навіть якщо їх не шукали.

Дослідження ефекту "інформаційної бульбашки" у Google або Facebook можна шукати інформацію на певну політичну або наукову тему. Через деякий час алгоритм почне підсовувати матеріали лише тієї точки зору, яку ви спочатку шукали, обмежуючи альтернативні думки. Цей ефект можна подолати, шукаючи інформацію у різних джерелах та активно переключаючись між різними тематиками.

Вивчення персоналізованої реклами може відбуватися через сайт великих магазинів та пошуку товарів. Після цього варто звернути увагу на рекламу в Facebook, Instagram, Google – почнуть з’являтись оголошення з пропозиціями купити саме цей або аналогічний товар. Це результат роботи алгоритмів ретаргетингу, які відстежують активність користувача і на основі неї налаштовують рекламу.

Рекомендаційні алгоритми зробили цифровий світ зручнішим, допомагаючи швидше знаходити потрібну інформацію, музику, фільми та товари. Вони економлять час і персоналізують контент відповідно до наших уподобань. Однак такі алгоритми мають і недоліки. "Інформаційна бульбашка" обмежує наше світосприйняття, показуючи лише знайомі теми. Також є ризик втрати конфіденційності, оскільки сервіси збирають багато даних про користувачів.

Щоб ефективно користуватися рекомендаційними системами, важливо розуміти їхню роботу, контролювати цифрові сліди та критично ставитися до пропонованого контенту. Баланс між персоналізацією та відкритістю до нового допоможе уникнути ризиків і отримати максимум користі від сучасних технологій.

Список використаних джерел

1. Алгоритми рекомендаційних систем для персоналізації контенту та послуг веб платформ. DSpace: ELAKPI: Репозитарій КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/items/25e8d7d3-de96-4eee-865e-159b8e239bef?utm_source=chatgpt.com (дата звернення: 25.03.2025).
2. Реалізація алгоритмів рекомендаційних. DSpace: ELAKPI: Репозитарій КПІ ім. Ігоря Сікорського. URL: https://ela.kpi.ua/items/25e8d7d3-de96-4eee-865e-159b8e239bef?utm_source=chatgpt.com (дата звернення: 25.03.2025).
3. Гайд з персональних товарних рекомендацій: технологія в деталях та кейси. eSputnik. URL: https://esputnik.com/uk/blog/gajd-z-personalnih-tovarnih-rekomendacij-tehnologiya-ta-kejsi?utm_source=chatgpt.com (дата звернення: 25.03.2025).
4. Обробка даних реальних користувачів для створення рекомендацій на відеостримінгових платформах. URL: https://dou.ua/forums/topic/39070/?utm_source=chatgpt.com (дата звернення: 25.03.2025).
5. "5 речей, які варто знати про персоналізацію контенту в онлайн-медіа. Домени – перевірка та реєстрація доменів в Україні | Imena.ua. URL: https://www.imena.ua/blog/personalization/?utm_source=chatgpt.com (дата звернення: 25.03.2025).

УДК 004.75:351.86

ШЛЯХИ РОЗВИТКУ ЦИФРОВІЗАЦІЇ У ГАЛУЗІ ЦИВІЛЬНОГО ЗАХИСТУ В СУЧАСНИХ УМОВАХ

Сапожніков Л. В.
lugmaster.zero@gmail.com;
Іщенко А. С.
yalerada4@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Швиденко А. В.
Черкаси, Україна

Цифровізація є ключовим чинником підвищення ефективності системи цивільного захисту. В умовах зростання технологічних можливостей та посилення ризиків надзвичайних ситуацій (НС) використання цифрових технологій дозволяє оперативно реагувати на загрози, прогнозувати їх розвиток та мінімізувати наслідки [1]. Впровадження програмних комплексів та онлайн-платформ сприяє покращенню координації дій екстрених служб, підвищенню рівня інформування населення та забезпеченню безперервного моніторингу надзвичайних ситуацій [2].

Основні напрямки цифровізації у цивільному захисті представлені нижче:

1. Розвиток геоінформаційних систем (ГІС). Важливу роль у прогнозуванні та управлінні НС відіграють ГІС, які дозволяють візуалізувати потенційні зони ризику та координувати дії служб. Приклад: ArcGIS, QGIS [3].

2. Впровадження систем моніторингу та раннього оповіщення. Автоматизовані системи аналізу загроз та оперативного інформування громадян сприяють швидкому реагуванню на небезпеки (WebEOC). Приклад: Система раннього попередження EWS.

3. Використання хмарних технологій та онлайн-платформ. Вони забезпечують централізоване зберігання даних, доступ до інформації в режимі реального часу та взаємодію між зацікавленими сторонами [4]. Приклад: Google Crisis Map, WebEOC.

4. Застосування штучного інтелекту (ШІ) та машинного навчання. Алгоритми аналізу великих даних сприяють прогнозуванню надзвичайних ситуацій та оптимізації ресурсів для їх ліквідації [4, 5]/

5. Мобільні додатки для населення та рятувальних служб. Вони дозволяють оперативно отримувати критично важливу інформацію та координувати дії в екстрених ситуаціях (Disaster Alert App). Приклад: Додаток "Повідомлення про надзвичайні ситуації" [5].

Впровадження новітніх інформаційних технологій у сфері цивільного захисту потребує комплексного підходу, що включає адаптацію існуючих систем, інтеграцію різних цифрових платформ та забезпечення їх сумісності. Наприклад, використання штучного інтелекту та машинного навчання дозволяє автоматизувати аналіз великих обсягів даних, що значно покращує прогнозування можливих надзвичайних ситуацій та планування дій рятувальних служб. Водночас, важливим аспектом є кібербезпека, оскільки цифрові системи управління та моніторингу можуть стати об’єктами кібератак [6].

Ще одним критичним фактором є навчання персоналу та населення використанню нових технологій. Впровадження мобільних застосунків для оперативного інформування громадян та систем раннього попередження потребує широкої інформаційної кампанії та роз’яснювальної роботи. Крім того, для ефективного функціонування цифрових платформ необхідно забезпечити їхню стійкість до збоїв та доступність у надзвичайних умовах, що включає створення резервних каналів зв’язку та використання децентралізованих баз даних.

В умовах воєнного стану цифровізація цивільного захисту набуває ще більшого значення, оскільки забезпечення швидкого обміну інформацією, ефективного прогнозування загроз та оперативного реагування стає критично важливим. Використання геоінформаційних систем дозволяє точно визначати місця атак, зони евакуації та гуманітарні коридори, що значно підвищує ефективність роботи рятувальних служб. Крім того, цифрові платформи для координації дій між державними органами, волонтерськими організаціями та

міжнародними партнерами допомагають оперативно мобілізувати ресурси та реагувати на виклики в режимі реального часу.

Ще одним важливим аспектом є інформаційна безпека та протидія кібератакам, які можуть бути спрямовані на дестабілізацію системи цивільного захисту. Використання блокчейн-технологій для захисту критично важливих даних, впровадження розподілених обчислювальних потужностей та резервних каналів зв'язку дозволяє забезпечити безперебійне функціонування цифрових платформ навіть у випадку пошкодження основної інфраструктури [6]. Крім того, мобільні додатки та системи сповіщення допомагають населенню оперативно отримувати інформацію про небезпеки та безпечні маршрути евакуації.

Цифровізація відіграє вирішальну роль у підвищенні ефективності системи цивільного захисту. Використання сучасних інформаційних технологій дозволяє оперативно реагувати на загрози, ефективно координувати дії рятувальних служб та підвищувати рівень готовності населення. Подальший розвиток цифрових рішень у галузі цивільного захисту сприятиме створенню більш стійкої та захищеної інфраструктури.

Подальші дослідження у сфері цифровізації цивільного захисту повинні бути спрямовані на розробку адаптивних алгоритмів штучного інтелекту для прогнозування надзвичайних ситуацій, вдосконалення кібербезпеки цифрових платформ, інтеграцію блокчейн-технологій для забезпечення прозорості та достовірності даних, а також дослідження ефективності мобільних застосунків у сфері громадської безпеки.

Список використаних джерел

1. ISO 22320:2018. Security and resilience – Emergency management – Guidelines for incident management.
2. National Institute of Standards and Technology (NIST). Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86, 2021.

3. ArcGIS Online. Official website. URL: https://www.arcgis.com (дата звернення: 21.03.2025).
4. IBM Watson for Disaster Response. URL: https://www.ibm.com/watson (дата звернення: 21.03.2025).
5. Disaster Alert App. Pacific Disaster Center. URL: https://disasteralert.pdc.org (дата звернення: 21.03.2025).
6. Білецький В.С. Інформаційна безпека та кіберзахист: підручник / В.С. Білецький, М.В. Ткаченко. – Київ: Наукова думка, 2020. – 312 с.

УДК 004.056.5:621.396

ОСОБЛИВОСТІ ВИКОРИСТАННЯ SDN ТА NFV В СУЧАСНИХ МЕРЕЖАХ

Федоренко Д. В.
fedorenkobmx@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р.В.
м. Черкаси, Україна

Програмно-визначена мережа (Software-Defined Networking, SDN) — це концепція управління комп’ютерними мережами, яка передбачає відокремлення (абстрагування) функцій управління мережею (control plane) від рівня пересилки пакетів (data plane) [3].

Такий підхід дозволяє здійснювати централізоване адміністрування мережевих ресурсів і керування трафіком за допомогою програмних засобів. Завдяки використанню інтерфейсів прикладного програмування (API) програмам верхнього рівня надається можливість гнучкого налаштування та оптимізації мережевих процесів. Це, своєю чергою, сприяє прискоренню впровадження нових мережевих сервісів і спрощенню їх розгортання.

Віртуалізація мережевих функцій (NFV, Network Functions Virtualization) — це сучасна технологія, що передбачає перенесення мережевих функцій із традиційних апаратних платформ до програмних модулів, які працюють на стандартних серверних архітектурах (переважно x86) у середовищі віртуальних машин (VM) [1].

Завдяки цьому мережеві функції, які раніше реалізовувалися виключно апаратними засобами, можуть динамічно розгортатися, масштабуватися та взаємодіяти між собою, забезпечуючи гнучке та ефективне надання телекомунікаційних послуг.

SDN і NFV загалом не залежать один від одного, хоча NFV може значною мірою доповнювати SDN. Архітектура SDN/NFV представлена на рисунку 1.

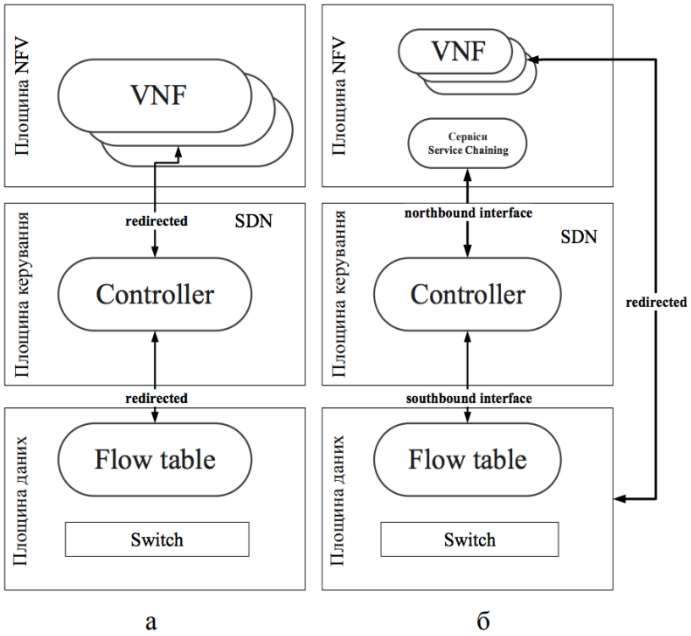

Рисунок 1. Архітектура SDN: а – традиційна, де NFV знаходиться під управлінням контролера; б – NFV знаходиться в стороні від контролера

Джерело: [2, с. 137].

SDN усувають обмеження, зумовлені апаратними характеристиками мережевого обладнання, що дозволяє створювати більш гнучкі та адаптивні мережеві інфраструктури. Хоча потенційні переваги SDN для локальних систем є добре дослідженими, їх інтеграція у хмарне середовище відкриває додаткові можливості для підвищення ефективності мережевого управління. Застосування гібридного підходу, що поєднує принципи SDN та хмарних технологій, надає досвідченим IT-менеджерам інструменти для оптимізації інфраструктури підприємства, забезпечуючи гнучкість, економічну ефективність і підвищений рівень безпеки.

Впровадження технології SDN усуває значні капітальні витрати, ліквідуючи залежність мережевих функцій від фізичного обладнання. Це дозволяє гнучко переміщувати мережеві сервіси в хмарне середовище, що сприяє додатковій економії ресурсів та підвищенню загальної ефективності мережевої інфраструктури.

Керування мережею значно спрощується завдяки можливості динамічного розміщення політик безпосередньо у мережевих функціях. Більш того, управління мережею може бути інтегроване з іншими рівнями адміністрування, такими як API, сервіси та управління даними. Це забезпечує контрольований доступ до ресурсів відповідно до ролей і привілеїв користувачів, що підвищує рівень безпеки та адміністрування мережі.

Технологія SDN також забезпечує гнучку масштабованість мережевої інфраструктури. Хоча використання власного фізичного мережевого обладнання залишається прийнятним рішенням, максимальна ефективність досягається при розгортанні SDN у загальнодоступних хмарних середовищах. Завдяки можливостям автоматичного масштабування хмарних платформ SDN може динамічно виділяти додаткові логічні сервери для обробки зростаючого навантаження. Таким чином, користувачі звільняються від необхідності самостійно керувати масштабуванням мережі, покладаючись на автоматизовані механізми хмарних платформ [1].

NFV пропонує принципово новий підхід до проєктування, розгортання та управління мережевими сервісами. NFV дозволяє відокремити мережеві функції, такі як NAT, брандмауер, система виявлення вторгнень, DNS, фільтрація трафіку тощо, від апаратного забезпечення, що сприяє гнучкості та масштабованості мережевих рішень.

Технологія SDN є важливою складовою сучасних інформаційних технологій і здебільшого застосовується в центрах обробки даних (ЦОД) для віртуалізації мережевих ресурсів. Натомість NFV виникла в телекомунікаційному секторі та використовується телефонними компаніями,

операторами зв’язку й інтернет-провайдерами, зокрема такими як Telefonica, Deutsche Telekom, AT&T.

В Україні впровадження технологій SDN та NFV відбувається повільними темпами, незважаючи на їхні очевидні переваги. Однією з ключових причин цього явища є недостатня кількість практичних кейсів використання SDN/NFV на ринку. Для системних інтеграторів першочергове значення мають фінансові аспекти та ретельний аналіз ризиків, пов’язаних із впровадженням нових технологій. Додатковим викликом є необхідність гарантій безперебійного функціонування компонентів нової інфраструктури з боку вендорів.

Водночас, віртуалізація мережевих функцій відкриває значні можливості порівняно з традиційними IP-мережами. Очікується, що впровадження SDN/NFV трансформує класичну модель операторського бізнесу, сприяючи його поступовій переорієнтації в бік програмно-орієнтованих рішень. У результаті телекомунікаційні оператори отримають змогу проєктувати сервіси відповідно до індивідуальних запитів клієнтів, що підвищить їхню ефективність і адаптивність до сучасних вимог ринку.

Таким чином, SDN і NFV - це різні, але пов'язані технології, покликані зробити мережі більш гнучкими. SDN відокремлює площину керування від площини даних, забезпечуючи централізоване керування мережею та більш ефективну маршрутизацію трафіку. NFV віртуалізує мережеві функції, дозволяючи їм працювати на стандартних серверах, що підвищує гнучкість та економію коштів.

Список використаних джерел

1. Зац О. Д., Стрілець В. Є., Шматков С. І., Ющенко В. С. Віртуалізація мереж – підхід до оптимізації комп’ютерних мереж. Вісник Харківського національного університету імені В.Н. Каразіна, сер. «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». 2024. Вип. 61. С. 33-43.

2. Зінченко О. В. Аналітичне моделювання SDN/NFV / О. В. Зінченко, В. В. Вишнівський, В. М. Гладких, С. В. Прокопов, О. С. Звенігородський // Системи управління, навігації та зв'язку. 2021. Вип. 2. С. 136-139.
3. Лунтовський А. О. Застосування технологій SDN для програмної реалізації провайдерського ядра систем мобільного зв’язку 5G майбутнього покоління / А. О. Лунтовський, А. І. Семенко // Зв'язок. 2014. № 3. С. 13-19.

Секція 4.

РОБОТОТЕХНІКА ТА АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ

УДК 621.8:338.46

УКРАЇНСЬКІ СТАРТАП-ПРОЄКТИ У СФЕРІ РОБОТОТЕХНІКИ ТА ЇХ ОСОБЛИВОСТІ

Рак Б. О.
bohdanrak36@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Злочевська Д. С.
м. Черкаси, Україна

Робототехніка – одна з найбільш перспективних галузей сучасних інформаційних технологій, що активно розвивається в усьому світі. Вона охоплює широкий спектр застосувань: від промислової автоматизації та агротехнічних рішень до медичних роботів і військових безпілотних систем. Україна, попри економічні виклики, активно долучається до глобального технологічного процесу, розвиваючи власні стартапи у сфері робототехніки.

Українські робототехнічні стартапи зосереджені на створенні інноваційних рішень, орієнтованих як на внутрішній, так і на зовнішній ринок. Багато з них впроваджують передові технології, такі як штучний інтелект, машинне навчання, Інтернет речей (IoT) та автономні системи. Однак розвиток цієї сфери в Україні має свої особливості, пов’язані з фінансуванням, кадровим потенціалом та виробничими можливостями.

TEMERLAND – унікальний проєкт української компанії з розробки безпілотних роботизованих комплексів та платформ, модернізації транспортних засобів в безпілотні наземні комплекси. Інноваційні безпілотні роботизовані комплекси TEMERLAND покликані рятувати і захищати людські життя, а також бути ефективним інструментом військових дій – розвідки, патрулювання, наступу та оборони. [1]

Український стартап Deus Robotics – виробник складських роботів, що автоматизує потужності «Нової пошти» та знайшов вихід на британський ринок. Вони спеціалізуються на автоматизації складських процесів, пропонуючи: унікальну ШІ-платформу, що інтегрує різні типи логістичних роботів від будь-

яких виробників в єдину систему, та розумні ШІ-роботи, здатні автоматизувати більшість складських операцій. [2]

Esper Bionics — стартап, який розробляє роботизовані кінцівки, заснований у 2019 році серійним підприємцем Дмитром Газдою, економісткою Анною Белеванцевою, колишнім юристом Ігорем Ільченко й інженером Борисом Лобановим. Зараз у стартапі працює понад 55 фахівців, більшість з яких технічні спеціалісти. За останніх півтора року команда збільшилась у понад два рази. В Україні в рамках соціальної програми Esper for Ukraine, яка фінансується ща благодіні кошти, біонічні протези отримали вже 80 українських захисників. [3]

Dynamic Division — стартап, який конструює автоматизованих роботів-прибиральників для великих комерційних площ. Dynamic Division пропонують «Robots as a Service». Їх підхід в тому, щоб прибрати ручну працю в прибиранні складів, ангарів, заводів. При цьому не потрібно купувати собі робота, досить платити за передплатою за прибрані квадратні метри. На момент звернення до нас клієнт встиг привернути перший раунд інвестицій і зробити прототип. Для остаточної розробки продукту і виходу на іноземні ринки йому потрібні були додаткові інвестиції. [4]

Вектор розвитку українського ринку стартапів визначається перш за все рівнем розвитку держави загалом. Невисокий рівень користування населенням Інтернетом (лише 44%), особливо серед старшого покоління, відносно невисока платоспроможність українців, відсутність розвиненої клієнтської бази та інші фактори здійснюють прямий вплив на формування ринку. З огляду на це стартап-проекти України націлені на внутрішнього споживача й значно поступаються за масштабністю проектам з Азії та США, що робить неможливим їх застосування на міжнародному рівні. Проте існують випадки, коли українські компанії, що працюють у цій сфері, розробляють проекти для зарубіжних споживачів, використовуючи Україну лише як так званий «будмайданчик». Також в Україні дуже слабо розвинене ризикове фінансування. Сьогодні більшість підприємців вважає за краще купити готовий бізнес з обігом, ніж інвестувати в будь-які інновації. [5]

Українські стартапи у сфері робототехніки демонструють високий рівень інноваційності та адаптивності до сучасних технологічних викликів. Вони активно розробляють рішення для промисловості, медицини, сільського господарства та військової сфери. Успішні проєкти, такі як автономні бойові платформи, безпілотні літальні апарати та автоматизовані системи для аграрного сектору, підтверджують конкурентоспроможність ринку українських розробників на світовому ринку.

З урахуванням стрімкого розвитку технологій та зростання попиту на робототехнічні рішення Україна має всі шанси стати кількістю гравців на цьому ринку. Головне завдання – створити сприятливі умови для розвитку стартапів, що дозволяють їм масштабувати свої проекти та впливати на глобальні технологічні тренди.

Список використаних джерел

1. Temerland. URL: https://temerland.com/ (дата звернення: 21.03.2025).
2. Український стартап робототехніки Deus Robotics. Fintech Insider. URL: https://fintechinsider.com.ua/ukrayinskyj-startap-robototehniky-deus-robotics-zaluchyv-3-mln-investyczij/ (дата звернення: 21.03.2025).
3. Український стартап Esper Bionics. dev.ua. URL: https://dev.ua/news/esper-bionics-zaluchyv-5-mln.
4. Пітч-дек для стартапу Dynamic Division. Reprezent. URL: https://reprezent.ua/ua/portfolio-item/dynamic-division-pitch-deck (дата звернення: 21.03.2025).
5. ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ СТАРТАПІВ В УКРАЇНІ. URL: http://market-infr.od.ua/journals/2019/32_2019_ukr/18.pdf (дата звернення: 21.03.2025).

УДК 004.056.5:004.42:621.391

ІННОВАЦІЙНІ РІШЕННЯ В АДМІНІСТРУВАННІ КОРПОРАТИВНИХ МЕРЕЖ ТА ЇХ ВПЛИВ НА КІБЕРБЕЗПЕКУ

Шакалов О.С.
alex070shakalov@gmail.com
Черкаський державний фаховий бізнес-коледж
Науковий керівник: Бреус Р.В
м. Черкаси, Україна

В сучасних корпоративних мережах кількість комп'ютерів нерідко досягає декількох сотень, тому для забезпечення ефективного функціонування та належного рівня кібербезпеки необхідні інноваційні рішення в галузі адміністрування. Традиційні методи ручного управління стають неефективними та ризикованими з погляду безпеки, адже збільшення масштабу мережі створює зростання потенційних вразливостей та точок входу для зловмисників.

Складність сучасних корпоративних мереж, які включають не лише стаціонарні ком'пютери, але й мобільні пристрої, IoT-обладнання, хмарні сервіси та різноманітні програмні рішення, вимагає комплексного підходу до їх адміністрування.

Інноваційні технології, такі як програмно-визначені мережі (SDN) та Zero Trust архітектура, докорінно змінюють підходи до управління великими IT-інфраструктурами.

Програмно-визначені мережі (SDN) — це інноваційний підхід до мережевих технологій, що відокремлює управління мережею від фізичного обладнання. SDN централізує контроль мережі через програмне забезпечення, замість традиційного налаштування окремих пристроїв.

Ключова особливість SDN полягає у використанні контролера, який керує всією мережею з єдиної точки. Це забезпечує глобальне бачення мережі та дозволяє швидко впроваджувати зміни. Контролер взаємодіє з мережевими пристроями через API, найчастіше використовуючи протокол OpenFlow.

У сфері кібербезпеки SDN відкриває нові можливості. Централізація управління дозволяє швидко реагувати на загрози, а покращена видимість

мережі допомагає виявляти аномалії. Технологія мікросегментації обмежує поширення атак, а гнучкі політики безпеки можуть миттєво застосовуватися до всієї мережі.

SDN сприяє еволюції мережевих інфраструктур від статичних до динамічних, що відповідають сучасним вимогам бізнесу та кібербезпеки. Zero Trust — це сучасна архітектура безпеки, яка кардинально змінює традиційний підхід до захисту корпоративних мереж. Вона базується на принципі «ніколи не довіряй, завжди перевіряй», відмовляючись від застарілої моделі захисту периметра, де системи всередині мережі вважалися безпечними.

Ключова концепція Zero Trust полягає в тому, що довіра ніколи не надається автоматично, незалежно від того, де знаходиться користувач або пристрій – всередині корпоративної мережі чи поза нею. Кожен запит на доступ до ресурсів строго перевіряється та авторизується, навіть якщо він надходить з традиційно безпечних внутрішніх мереж.

Архітектура Zero Trust впроваджує постійну верифікацію ідентичності користувачів та стану пристроїв перед наданням доступу до ресурсів. Авторизація базується не лише на облікових даних, але й на контексті запиту – місцезнаходженні, часі, поведінці користувача та стані пристрою. Це дозволяє значно зменшити ризик несанкціонованого доступу.

У сфері кібербезпеки Zero Trust забезпечує суттєві переваги. Цей підхід мінімізує можливість бічного руху зловмисників у мережі, оскільки всі сегменти мережі ізольовані одне від одного. Використання принципу найменших привілеїв обмежує доступ користувачів лише необхідними для роботи ресурсами. Постійний моніторинг і аналіз поведінки користувачів дозволяє виявляти підозрілу активність і своєчасно реагувати на загрози.

Сучасні корпоративні мережі, що включають сотні пристроїв, IoT, хмарні сервіси та гібридні інфраструктури, потребують радикальної трансформації підходів до управління та безпеки. Програмно-визначені мережі (SDN) та архітектура Zero Trust стають ключовими інструментами для подолання цих викликів. Разом вони формують захист, здатний протистояти сучасним

кіберзагрозам, мінімізувати вплив людського фактора та забезпечити стабільність IT-систем незалежно від їх складності чи масштабу. Впровадження цих рішень – не просто тренд, а критична необхідність для будь-якої організації, що прагне залишатися конкурентною в епоху цифрових трансформацій.

Список використаних джерел:

1. Zero Trust: новий стандарт безпеки у цифрову епоху. URL: https://itez.com.ua/blog/zero-trust-new-security-standard-digital-era.html (дата звернення: 12.03.2025).
2. Software-defined networking (SDN): визначення й особливості програмно-визначених мереж. URL: https://netwave.ua/blog/software-defined-networking-sdn-viznachennya-j-osoblivosti-programno-viznachenih-merezh/ (дата звернення: 12.03.2025).