МІНІСТЕРСТВО
ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ

КАФЕДРА РОБОТОТЕХНІКИ
ТА ТЕХНІЧНИХ СИСТЕМ

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «ПЕРСПЕКТИВИ ТА ПРОБЛЕМАТИКА ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ»

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

КАФЕДРА
РОБОТОТЕХНІКИ ТА ТЕХНІЧНИХ СИСТЕМ (ДУІКТ)

КАФЕДРА ПРИЛАДОБУДУВАННЯ (УжНУ)

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ ТА ПРОБЛЕМАТИКА ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ»

Дата проведення:
31 травня 2024 року.
Початок о 10:00.

Київ 2024

УДК 004.89:621.39(043.2)

Організатори:

Кравченко Владислав Ігорович, к.т.н., доцент, директор Навчально-наукового інституту телекомунікацій ДУІКТ;

Пепа Юрій Володимирович, к.т.н., доцент, завідувач кафедри Робототехніки та технічних систем ДУІКТ;

Нафєєв Ровіл Касимович, к.ф.-м.н., завідувач кафедри системного аналізу ДУІКТ;

Чичура Ігор Іванович, к.ф.-м.н., завідувач кафедри приладобудування УжНУ.

Комп'ютерна верстка та редагування:

Поночовний Петро Михайлович, старший викладач кафедри робототехніки та технічних систем ДУІКТ.

Рекомендовано до друку Вченою радою Навчально-наукового інституту телекомунікацій Державного університет інформаційно-комунікаційних технологій (протокол № 9 від 24.05.2024 р.).

Перспективи та проблематика інтелектуальних систем: збірник тез науково-практичної конференції (м. Київ, 31 травня 2024 року), Київ: РВЦ ДУІКТ. – 2024. – 57 с.

Збірник тез призначений для аспірантів, науковців, викладачів та інших зацікавлених осіб.

Ю.В. Пепа, П.М. Поночовний
Державний університет інформаційно-комунікаційних технологій, м. Київ

ІНТЕГРАЛЬНЕ ОЦІНЮВАННЯ СТІЙКОСТІ СИСТЕМ УПРАВЛІННЯ

Кожен із розглянутих вище прямих і непрямих показників якості характеризує лише одну ознаку (показник якості) перехідного процесу. При цьому всі показники пов'язані з параметрами регулятора чи системи складними залежностями, які мають, як правило, суперечливий характер: зміна будь-якого з параметрів призводить до покращання одних показників якості та погіршення інших [1]. Ця обставина істотно ускладнює вибір параметрів регулятора. Тому в інженерній практиці широко використовуються інтегральні показники (оцінки) якості, що відображають (або інтегрують у собі) одночасно багато з розглянутих вище показників.

Інтегральна оцінка якості – визначений інтеграл за часом (від 0 до ∞) від деякої функції керованої величини $x(t)$ або, частіше, сигналу помилки $\varepsilon(t)$

$$J = \int_0^\infty f\left[x(t), t\right]dt\,. \tag{1}$$

Підінтегральна функція $f\left[x(t), t\right]$ вибирається таким чином, щоб інтеграл (1) як найкраще характеризував якість і що найпростіше виражався через коефіцієнти передаточної функції замкнутої системи. Щоб інтеграл був таким, що сходиться, тобто мав обмежене значення, у функцію $f\left[x(t), t\right]$ вводять не абсолютні значення $x(t)$ або $\varepsilon(t)$, а їх відхилення від кінцевих, встановлених значень.

Інтегральна оцінка (1) враховує як величину динамічного відхилення, так і тривалість перехідних процесів. Чим менша за величиною оцінка, тим краща якість перехідного процесу.

Найпростішою інтегральною оцінкою є лінійна інтегральна оцінка $J_л$. Якщо перехідна характеристика є монотонною, то можна очікувати, що якість перехідного процесу тим краща, чим менша площа, яка обмежена кривою перехідного процесу і встановленим значенням керованої величини. У цьому сенсі лінійна інтегральна оцінка чисельно дорівнює площі, що обмежена кривою зміни вільної складової керованої величини і лінією рівня нового встановленого значення $x(\infty)$

$$J_Л = \int_0^\infty \left[x(\infty) - x(t)\right]dt\,. \tag{2}$$

Недоліком лінійної інтегральної оцінки $J_Л$ є те, що її можна застосовувати лише для аперіодичних перехідних процесів. Інтеграл (2), обчислений для аперіодичної кривої буде явно меншим за інтеграл, обчислений для знакозмінної кривої, хоча якість перехідного процесу в цьому випадку з перерегулюванням буде кращою).

Більш того, для незгасаючого гармонійного процесу, який відповідає вкрай незадовільному перехідному процесу, коли $J_Л = 0$, що дає мінімальну оцінку якості (як найкращу якість перехідного процесу).

У зв’язку з цим для коливальних перехідних процесів бажано застосовувати такі інтегральні оцінки, при яких знакозмінність підінтегральної функції тим чи іншим чином усунута.

Такою оцінкою є, наприклад, модульна інтегральна оцінка

$$J_{\text{М}} = \int_0^\infty |x(\infty) - x(t)| dt \,.$$

На практиці застосування модульної інтегральної оцінки обмежено труднощами аналітичного обчислення інтеграла від модуля. Тому більшого поширення через її вибірковість і відносну простоту визначення одержала квадратична інтегральна оцінка виду

$$J_{\text{К}} = \int_0^\infty \left[x(\infty) - x(t) \right]^2 dt \,.$$

Як можна побачити, різні за величиною ординати перехідного процесу входять у критерій з різною вагою (через піднесення до квадрату), в результаті чого вигляд початкової ділянки перехідної характеристики значно більше впливає на величину інтеграла, ніж її «хвіст». Меншому значенню квадратичного критерію тепер будуть відповідати перехідні процеси з меншим перерегулюванням, однак при цьому спостерігається повільне згасання. З метою усунення цього недоліку використовують різні покращені модифікації квадратичного критерію, які використовують інформацію не лише про змінну, а й про її похідні, наприклад, виду

$$J_{\text{КМ}} = \int_0^\infty \Delta x(t)^2 + \theta \Delta x(t)^2 dt \,,$$

де θ – ваговий коефіцієнт, який вибирається відповідно до бажаного часу наростання перехідного процесу.

Як лінійну, так і квадратичну оцінку якості можна обчислити і без побудови перехідного процесу за частотною характеристикою технічної системи та перетворенням Фур’є вхідного сигналу з використанням формули Релея [2]. Однак цей метод дуже трудомісткий і в даний час не знаходить застосування.

Необхідно зазначити, що абсолютні значення будь-якої інтегральної оцінки самі по собі не становлять інтересу. Вони, перш за все, слугують для зіставлення якості перехідних процесів при різних варіантах налаштувань однієї і тієї ж самої або подібних за структурою систем.

Усі розглянуті інтегральні показники використовують, крім того, для визначення оптимальних значень параметрів регулювальних пристроїв технічних систем з автоматичним управлінням. При цьому, оптимальними параметрами вважають такі, які відповідають мінімальному значенню інтегрального показника.

Література

1. Валюх О.А., Максимов В.М. Елементи теорії автоматичного керування. Лінійні системи неперервної дії: навч. посібник. – Львів: Афіша, 2009. – 124 с.

2. Åström K.J., Hägglund T. Advanced PID Control. – Research Triangle Park, NC: Instrumentation Systems and Automation Society, 2006. – 461 p.

І.М. Аверічев, І.Д. Данилов
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА СПЕЦИФІЧНИХ КРОС-ПЛАТФОРМНИХ МОДУЛІВ

Для створення крос-платформних програмних засобів є багато відомих підходів. Зупинимось на Kotlin native, який має кардинально інший підхід до створення та впровадження крос-платформної універсальної інтелектуальної системи. На відміну від Xamarin та React native, ця технологія не має можливостей до написання спільного користувацького інтерфейсу, що, в свою чергу, позбавляє від більшості системних залежностей, які вимагають специфічні платформні драйвери або створення додаткового шару виконання.

Основна ідея – створення спільної логіки, яка буде мати велику швидкодію за рахунок компіляції в бінарний код. Отже, розробники створюють лише спільну логіку, яка буде використовуватись інтерфейсом, написаним на офіційних технологіях, таких як Java або Kotlin для Android та Objective-C або Swift для iOS [1]. Робота на всіх платформах – це задача і явна мета Kotlin. Спільне використання коду між платформами є передумовою до цієї мети. Завдяки підтримці: JVM, Android, JavaScript, iOS, Linux, Windows, Mac і навіть вбудованих систем, таких як STM32, Kotlin може обробляти будь-які компоненти сучасної взаємодії з додатком і це приносить неоціненну користь від повторного використання коду та досвіду, заощаджуючи зусилля для виконання складніших завдань, ніж реалізувати все двічі або кілька разів.

Загалом, мультиплатформність не полягає у компіляції всього коду для всіх платформ. Ця модель має свої очевидні обмеження [2], а саме, що сучасним додаткам необхідний доступ до унікальних особливостей платформ, на яких вони працюють. Kotlin не обмежує загальною підмножиною всіх API у світі [3]. Кожен компонент може спільно використовувати інші коди, але може отримати доступ до API платформи в будь-який час за допомогою механізму expect/actual, передбаченого мовою програмування.

На рис. 1 зображено приклад спільного використання коду та взаємодії між загальною і платформною логікою отримання поточного часу системи.

Для сучасної розробки мобільних застосунків необхідна велика кількість сторонніх бібліотек. Незалежна логіка, що може використовуватись багаторазово виноситься в окремі модулі, для використання в інших проектах. Такий підхід економить багато часу на написання коду та його тестування. Це можуть бути специфічні бібліотеки для з певним модулем (камера, навігація), або бібліотеки сторонніх сервісів, таки як Google Maps або Firebase. Також сторонні бібліотеки можуть вирішувати типові проблеми програмування або реалізувати кардинально інші підходи для проектування програмного продукту, такі як RxJava (реалізація реактивних потоків) або Arrow (реалізація функціонально підходу програмування).

На жаль, більшість бібліотек, що використовуються в мобільній розробці під Android або iOS, не підтримують взаємодію з Kotlin Native, оскільки кожна з них в своїй реалізації має специфічні елементи. Однак ситуація стрімко покращується та розробники бібліотек додають підтримку Kotlin Native з окремими модулями-реалізаціями для кожної з платформ.

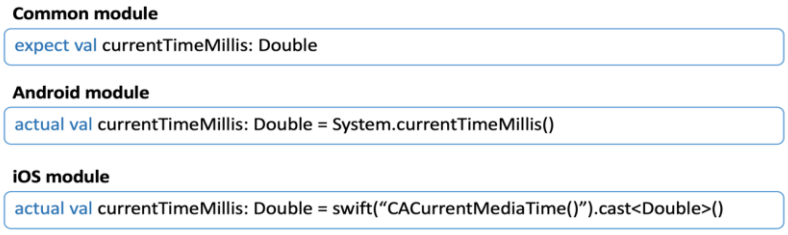

Рис. 1. Робота механізму expect/actual

На рис. 2 показано приклад використання бібліотеки SqlDelight, що використовується для зручної роботи з базою даних SQLite.

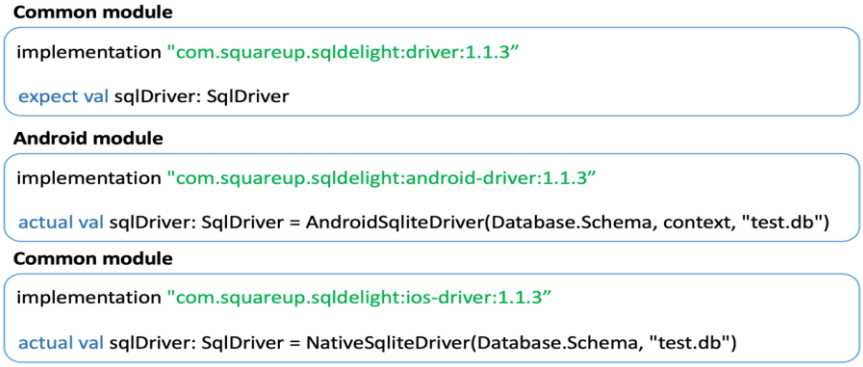

Рис. 2. Робота механізму expect/actual з використанням сторонньої бібліотеки

Такий підхід використовує абстрактний контракт для використання певної сутності, реалізація якої залежить від певних платформних засобів.

Недоліки технології Kotlin native.

Після детального аналізу проблем, що виникали під час розробки програмного продукту варто виділити дві основні проблеми, а саме – обмежена кількість сторонніх бібліотек, що мають підтримку цієї технології та нестабільність інструменту побудови проекту.

Обмежена кількість сторонніх бібліотек – надзвичайно вагома проблема, яка сильно впливає на швидкість розробки. Проте технологія дуже молода і ситуація стрімкими темпами покращується. А через популярність Kotlin та підтримку зі сторони Google та JetBrains можна з упевненістю сказати, що ця проблема буде вирішена.

Наступним недоліком стала нестабільність системи побудови проекту, а саме Gradle плагіна, що надає підтримку Kotlin native. Ситуація також покращується. За час роботи над проектом розробниками було представлено дві нові версії плагіна, що вирішили багато проблем та помилок, що виникали під час компіляції, моніторингу залежностей та побудови власних проектів.

Література

1. Проектування інформаційних систем: Посібник / За ред. В.С. Пономаренка. – К.: Академія, 2002. – 450 с.

2. Причини виникнення проблем сумісності програмного забезпечення [Електронний ресурс]. – Режим доступу до ресурсу: http://helpiks.org/7-46217.html.

3. Динамічний обмін даними (DDE) [Електронний ресурс]. – Режим доступу до ресурсу: https://vunivere.ru/work1279/page2.

В.В. Шевченко
Український державний університет імені Михайла Драгоманова, м. Київ

АКТУАЛЬНІСТЬ ПРОФЕСІЙНО-ПРАКТИЧНОЇ ПІДГОТОВКИ З БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ НАСЕЛЕННЯ У МИРНИЙ І ВОЄННИЙ ЧАС

Зміни, які відбуваються в останні роки в економічному, політичному та соціальному житті як у самій країни, так і в сфері міжнародних відносин, зумовили необхідність змін і системи освіти зокрема. Після повномасштабного вторгнення Росії в нашу державу 24 лютого 2022 року проблема питання охорони праці та безпеки життєдіяльності набула особливої уваги та значення а, тому формування світоглядної цінності життя і пов’язаною із нею компетентністю з безпеки життєдіяльності є пріоритетною задачею всіх соціальних інституцій та освіти в цілому. Модернізація системи освіти, її входження до загальноєвропейського освітнього простору висувають нові вимоги до всіх фахівців та порушують питання професійної компетентності педагога в цілому. Тим самим актуалізується необхідність безперервного процесу удосконалення підготовки педагогічних кадрів, у тому числі кваліфікованих фахівців у галузі безпеки життєдіяльності та охорони праці. Недостатня їхня компетентність у конкретних галузях безпеки життєдіяльності (інформаційної, екологічної, економічної, психологічної тощо) і, як наслідок, дефіцит професійної мобільності, у виконанні професійних обов'язків, порушують питання створення системи професіоналізації, удосконалення змісту, форм та процесів, що її формують.

Сучасному суспільству, що розвивається, потрібні компетентні фахівці, які можуть приймати відповідальні рішення в ситуаціях вибору, здатні до співпраці, відрізняються мобільністю, динамізмом, конструктивністю, мають почуття відповідальності за долю країни. Необхідність вирішення зазначених питань вимагає від системи освіти розробки програм підготовки фахівців, які здатні вирішувати їх кваліфіковано [1].

Руйнація розбудованої системи безпекової підготовки, сприятиме зниженню якості кадрового потенціалу. Майбутній фахівець, що не здатний ідентифікувати потенційну загрозу, наражає себе і оточуючих на небезпеку.

Не вчасно виконанні профілактичні заходи протидії загрозам – спричинюють важкі економічні та людські втрати. Загибель (або каліцтво) підготовленого фахівці – це прямі економічні збитки державі, і сім’ї.

Сучасний стан розвитку суспільних відносин, нові галузі діяльності та організації ринку праці вимагають оперативного реагування ЗВО на данні запити, зумовлює появу нових спеціальностей, відкриття у конкретному виші підготовки дипломованих кадрів, які традиційно готували лише вузькоспеціалізовані (фахові). Динамічність системи вищої школи, своєчасне задоволення виробничих потреб, збільшення спектру спеціальностей, отже створення умов для молоді мати широкий вибір подальшої діяльності є позитивною стороною питання. До негативної сторони належить те, що відкриття нових спеціальностей без достатньої та необхідної навчально-методичної, матеріально-технічної бази, висококваліфікованих викладачів, відповідного забезпечення освітнього процесу, як правило, призведе до спрощення системи та зниження якості підготовки фахівців. Крім того, в даний час кожен класичний ЗВО

прагне самодостатності у своєму бажанні охопити якнайбільше коло фахівців для підготовки.

Швидка зміна професійних знань, необхідність їхнього оновлення вимагають створення гнучких освітніх структур, в яких могли б реалізуватися програми безпекового спрямування (Охорони праці, безпеки життєдіяльності, цивільної безпеки, тощо). Складний системний зв'язок між змістом фахової освіти та діяльністю фахівця безпеки життєдіяльності усвідомлюється сучасними вченими, і саме він визначає логіку сучасних теоретичних підходів до пошуку шляхів забезпечення якості фахової підготовки [2].

Таким чином, зберігаються протиріччя між:

- потребою суспільства у підвищенні рівня професіоналізму вчителя безпеки життєдіяльності за допомогою педагогічних інновацій та традиційними підходами у закладі вищої освіти;

- жорстко стандартизованою оцінкою якості професійної компетентності майбутнього фахівця безпеки життєдіяльності та постійною зростаючою кількістю небезпек, що впливають на людину та потребують збільшення кількості та якості спеціалізованих знань, умінь та навичок;

- вимогами сучасної освіти до підготовки висококваліфікованих фахівців безпеки життєдіяльності та відсутністю навчально-методичного комплексу/бази забезпечення якості професійної компетентності;

- інформаційним потоком, що збільшується, і нездатністю майбутнього фахівця безпеки життєдіяльності ефективно її переробляти та якісно застосовувати у педагогічній практиці.

Також у уявленнях студентів про професійну компетентність фахівця безпеки життєдіяльності спостерігається неоднозначне розуміння значущості її окремих компонентів, зокрема недооцінка психолого - педагогічної підготовки.

Мета освіти в сфері безпеки життєдіяльності як міждисциплінарної галузі – розповсюдження інформації та комплексу системи знань про джерела, характер, наслідки ризиків повсякденного життя, надзвичайних ситуацій, виробничих аварій, технологій запобігання та протидії цим загрозам, що особливо актуально під час війни.

Література

1. Желібо Є.П. Проблеми викладання дисципліни «Безпека життєдіяльності» у ВНЗ України / Є.П. Желібо, І.С. Сагайдак // Безпека життєдіяльності, 2017. – № 12. – С.35-36.

2. Ігнатович М.В. Проблеми викладання курсу «Безпека життєдіяльності» студентам економічних спеціальностей / М.В. Ігнатович, В.Ю. Худолей // Безпека життєдіяльності, 2017. – № 10. – С.42-43.

Р.М. Кириченко, К.О. Домрачева
Державний університет інформаційно-комунікаційних технологій, м. Київ

ОБ'ЄДНАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА ІНТЕРНЕТУ РЕЧЕЙ ДЛЯ ТРАНСФОРМАЦІЇ УКРАЇНСЬКИХ МІСТ

Україна, як і багато країн світу, стикається зі складними викликами у сфері міського розвитку. Постійний ріст населення, зростаюча урбанізація та нестабільна економічна ситуація вимагають нових підходів до управління містами та забезпечення життєвих потреб їхніх мешканців [1]. Інтеграція Штучного Інтелекту (ШІ) та Інтернету Речей (ІР) може стати ключовим кроком у вирішенні цих проблем, проте цей процес потребує глибокого аналізу перспектив та визначення основних проблем.

Переваги інтеграції ШІ та ІР в управлінні містами:

Ефективне управління ресурсами:

Системи ІР дозволяють не лише моніторити використання енергії, води та інших ресурсів, але й автоматизувати їхнє керування. Наприклад, інтелектуальні лічильники енергії можуть оптимізувати використання електроенергії в будинках, враховуючи пікові та не пікові години споживання.

Інтеграція ШІ та ІР дозволяє реагувати на зміни в споживанні ресурсів в реальному часі, що дозволяє зменшити втрати та оптимізувати їхнє використання.

Покращення транспортної інфраструктури:

Інтелектуальні системи можуть не лише оптимізувати рух транспорту, але й покращувати комфорт пасажирів. Наприклад, системи моніторингу транспорту можуть надавати інформацію про заповненість автобусів та трамваїв, що дозволяє пасажирам планувати свої поїздки.

Розумне керування світлофорами за допомогою інтелектуальних систем допомагає зменшити час очікування на світлофорах та покращує рух транспорту по місту.

Розумне управління відходами:

Інтеграція ШІ та ІР дозволяє створити системи моніторингу та управління відходами, які оптимізують їхню збірку, сортування та переробку. Наприклад, сміттєзбірники з вбудованими сенсорами можуть автоматично надсилати повідомлення про заповненість, що дозволяє оптимізувати маршрути збирання сміття та уникнути його переповнення.

Підвищення безпеки:

Інтелектуальні системи можуть виявляти загрози безпеці та реагувати на них в реальному часі. Наприклад, системи відеоспостереження з аналізом зображення можуть виявляти небезпечні ситуації на вулицях та сповіщати відповідні служби.

Інтеграція інтелектуальних систем управління екстреними ситуаціями дозволяє швидко реагувати на кризові ситуації та координувати дії рятувальників.

Проблематика інтеграції ШІ та ІР:

Недостатня інфраструктура та фінансування:

Багато міст стикаються з обмеженими ресурсами для впровадження інтелектуальних систем через недостатню інфраструктуру та обмежені бюджетні кошти.

Необхідність інвестування у розробку та впровадження інтелектуальних технологій може стати великим викликом для міських влад.

Проблеми кібербезпеки:

Збільшення кількості підключених пристроїв створює нові кібербезпекові загрози. Інтегровані системи можуть стати об'єктом кібератак та порушень приватності, які можуть мати серйозні наслідки для міста та його мешканців.

Низька освіченість населення:

Впровадження інтелектуальних систем вимагає високого рівня технологічної освіченості серед населення. Низький рівень технологічної грамотності може стати перешкодою для успішної реалізації проектів та призвести до опору з боку мешканців.

У Києві вже проводяться деякі проекти з об'єднання ШІ та ІР для покращення якості життя мешканців. Наприклад, система "Smartcitykyiv" включає в себе ряд інтелектуальних рішень, ці проекти спрямовані на зменшення заторів, економію енергії та покращення якості повітря в місті. Розумні міські рішення створюють додаткові можливості для підвищення цінності міста. Інтеграція технологій підвищує ефективність використання ресурсів, створює нові можливості для бізнесу, а також підвищує рівень життя громадян.

Однією з головних сфер, де впроваджуються інновації, є транспортна система.

Системи моніторингу транспорту в Києві використовують дані, що надходять з різних джерел, включаючи GPS, камери відеоспостереження, датчики руху та інші сенсори. Ці дані аналізуються за допомогою алгоритмів ШІ для прогнозування трафіку та управління рухом. Наприклад, алгоритми можуть виявити затори та надати рекомендації водіям щодо альтернативних маршрутів або оптимальних часів руху. Також системи моніторингу транспорту дозволяють оптимізувати роботу світлофорів, щоб забезпечити плавний рух транспорту та зменшити час очікування на перехрестях.

Крім транспортної системи, в Києві впроваджуються інтелектуальні системи управління енергоефективністю будівель. Ці системи збирають дані про споживання енергії, температуру, вологість та інші параметри за допомогою мережі сенсорів. Дані аналізуються алгоритмами ШІ, що дозволяє автоматично регулювати опалення, кондиціонування повітря та освітлення в приміщеннях з метою максимально ефективного використання енергії та зменшення витрат на комунальні послуги.

Такі проекти сприяють покращенню якості життя мешканців Києва, зниженню транспортних заторів, енергоспоживанню та витратам на комунальні послуги. Ці інтегровані системи створюють більш інтелектуальне та ефективне середовище для проживання та розвитку міста.

Висновки та перспективи.

Інтеграція Штучного Інтелекту та Інтернету Речей в управління містами України має великий потенціал для покращення якості життя мешканців та ефективного використання ресурсів [2]. За допомогою цих технологій можна досягти значних позитивних змін у таких сферах, як транспорт, енергетика, управління відходами та безпека.

Проте впровадження інтегрованих систем ШІ та ІР стикається з рядом викликів, серед яких фінансові обмеження, проблеми кібербезпеки та недостатня технологічна освіченість населення. Ці проблеми потребують уважного вирішення для успішного впровадження інтелектуальних систем у містах.

Незважаючи на складнощі, інтеграція ШІ та ІР в міста України відкриває широкі перспективи для подальшого розвитку та модернізації. Передбачається, що з ростом

технологічних можливостей і зростанням досвіду впровадження таких систем, їхнє значення та вплив на міське середовище буде лише зростати.

Запровадження інтегрованих систем ШІ та ІР у містах сприятиме створенню більш інтелектуальних, сталих та комфортних для життя середовищ. Крім того, ці технології можуть стати основою для подальшого розвитку смарт-міст і розширення їхнього функціоналу на користь мешканців та громадськості в цілому.

Література

1. "Smartcitykyiv" – інформація про проекти та програми розвитку інтелектуальних систем управління містом. – Режим доступу до ресурсу: www.smartcitykyiv.com.

2. Маркевич К. Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України [Електронний ресурс] / Катерина Маркевич // Видавництво “Заповіт”. – 2021. – Режим доступу до ресурсу: https://razumkov.org.ua/uploads/other/2021-SMART-%D0%A1YTI-SITE.pdf.

Ю.О. Столбецький, С.В. Калугін
Харківський національний університет радіоелектроніки, м. Харків

СТВОРЕННЯ НАВЧАЛЬНИХ ЗАВДАНЬ НА ОСНОВІ МЕТОДИКИ ОПОРНИХ КОНСПЕКТІВ В.Ф. ШАТАЛОВА

Вступ Проблема ефективного запам'ятовування навчального матеріалу потребує нових підходів. Для вирішення цієї проблеми розроблено інтерактивну навчальну систему на основі методу опорних конспектів В.Ф. Шаталова, яка використовує графічне моделювання для систематизації інформації.

У сучасному світі освіта є ключовою для розвитку особистих здібностей та компетенцій, але традиційні методи навчання часто неефективні для засвоєння великої кількості інформації. Зростаюча конкуренція на ринку праці та швидкий розвиток технологій вимагають постійного навчання та оновлення знань. Для вирішення цієї проблеми ми розробляємо інтерактивну навчальну систему на основі методу опорних конспектів В.Ф. Шаталова [1], яка використовує графічне моделювання для узагальнення та систематизації навчального матеріалу. Ця система полегшить процес навчання, підвищить мотивацію та інтерес учнів, а також покращить їх розуміння та запам'ятовування інформації.

Аналіз аналогів. На сьогоднішній день не існує системи, що поєднує в собі можливості ефективного запам’ятовування нової інформації з використанням опорних конспектів В.Ф. Шаталова і можливості оцінки виконаних учнями завдань та перегляду статистики успішності навчання. Такі системи графічного дизайну, як Canva, пропонують зручний інтерфейс для створення візуальних дизайнів та конспектів, але в них відсутній функціонал перевірки знань. Водночас рішення на кшталт Google Classroom реалізують зручний функціонал перевірки знань та перегляду статистики успішності навчання кожного учня, але в них відсутня можливість створення інтерактивних конспектів.

Постановка задачі. Необхідно розробити функціонал для реалізації інтерактивних опорних конспектів В.Ф. Шаталова для застосування в сучасній системі онлайн-навчання. Для фронтенд-частини застосунку необхідно розробити графічний редактор для створення опорних конспектів та створення інтерактивних завдань на основі конспектів. Для бекенд-частини застосунку необхідно реалізувати функціонал валідації даних конспекту, збереження даних системи та алгоритм оцінки виконання завдань.

Опис рішення. Реалізацію графічного редактору системи зроблено за допомогою бібліотеки створення рішень, заснованих на інтерфейсах, зав'язаних на вузлах (node-based UI) React Flow [2]. Система надає зручний інтерфейс для створення конспекту: вчитель має перелік блоків різних типів (Заголовок, Визначення, Список-порівняння, Етапи процесу). Після того, як вчитель завершив створення конспекту, серверна частина валідує структуру конспекту та перевіряє правильність зв'язків між блоками конспекту. Для створення інтерактивних завдань вчитель має можливість скопіювати існуючий конспект, розташувати блоки в довільному порядку та виставити час на виконання завдання та рівень складності завдання, що вплине на вагу завдання в загальній оцінці за курс. Після того, як вчитель створив завдання, воно відправляється на сервер та валідується. Після цього учні зможуть переглянути конспект та спробувати виконати завдання по цьому конспекту розташувавши блоки в правильному порядку. Після того, як учень завершив свою спробу, результат відправляється на сервер. У разі вчасно виконаного завдання на боці сервера виставляється оцінка в залежності від кількості правильно розташованих блоків. Коли учень вперше отримує завдання, встановлюється стан виконання завдання як «in progress» та кожну секунду з клієнтської частини надсилається поточний результат, який фіксується на боці сервера. На боці серверної частини кожну годину перевіряє перелік незавершених вчасно завдань та автоматично виставляє оцінку базуючись на останньому збереженому стані виконання завдання та по закінченню відведеного часу змінюється стан завдання.

Висновки. Було реалізовано зручну систему для створення інтерактивних опорних конспектів В.Ф. Шаталова, використовуючи React Flow для графічного редактору з вузловим інтерфейсом. Система дозволяє вчителям створювати конспекти з різними типами блоків та завданнями, які учні можуть виконувати, розташовуючи блоки у правильному порядку. Серверна частина забезпечує валідацію конспектів та завдань, а також автоматичну перевірку та оцінювання завдань на основі останнього збереженого стану. Такий підхід забезпечує інтерактивне та ефективне навчання, дозволяючи учням краще засвоювати матеріал через активну участь.

Література

1. Методика Шаталова В.Ф.: сутність, здобутки, перспективи. – Режим доступу до ресурсу: https://metod.kpkitp.kiev.ua/wp-content/uploads/2019/12/7%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D0%BA%D0%B0.pdf (дата звернення 18.04.2024).

2. React Flow. – Режим доступу до ресурсу: https://reactflow.dev (дата звернення 18.04.2024).

В.А. Мотрич
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЗНАЧЕННЯ БЛОКЧЕЙН ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

Застосування блокчейн технологій для забезпечення кібербезпеки є перспективним напрямом, що здатен значно підвищити надійність та захищеність інформаційних систем. Зростання кількості кіберзагроз, таких як хакерські атаки, крадіжка даних та інші форми кіберзлочинності, вимагає розробки нових підходів та інструментів для захисту інформаційних систем. Одним із таких інноваційних рішень є застосування блокчейн технологій.

Блокчейн, як децентралізована і розподілена система зберігання даних, пропонує унікальні можливості для забезпечення кібербезпеки. Його архітектура, заснована на незмінності записів та криптографічному захисті, дозволяє створити високонадійні системи, що унеможливлюють несанкціонований доступ та маніпуляції з даними. Важливо підкреслити, що блокчейн може бути застосований у різних галузях, починаючи від фінансових послуг і закінчуючи охороною здоров'я, де захист конфіденційної інформації є надзвичайно важливим [1].

Аналіз механізмів безпеки, які пропонує блокчейн, показує, що його використання може суттєво знизити ризики, пов'язані з кіберзагрозами. Зокрема, децентралізація даних робить неможливим здійснення централізованих атак, а криптографічні алгоритми гарантують автентичність та цілісність інформації. Крім того, смарт-контракти, що реалізуються на базі блокчейну, дозволяють автоматизувати процеси та мінімізувати людський фактор, що також сприяє підвищенню рівня безпеки.

Однією з ключових переваг блокчейну є його здатність забезпечувати високий рівень конфіденційності даних. У традиційних системах безпеки, де дані часто зберігаються в централізованих базах даних, існує високий ризик витоку інформації через зовнішні атаки або внутрішні загрози. Блокчейн технології, завдяки своїй розподіленій природі, забезпечують децентралізоване зберігання даних, що ускладнює їхнє викрадення або маніпулювання [2]. Також, використання криптографічних методів дозволяє забезпечити високу ступінь захисту даних, гарантуючи, що доступ до них матимуть лише авторизовані користувачі.

Незважаючи на переваги, впровадження блокчейн технологій супроводжується певними викликами та обмеженнями. Серед основних проблем можна виділити питання масштабованості, високе енергоспоживання, а також необхідність розробки та впровадження відповідного нормативно-правового регулювання. Блокчейн-системи, особливо ті, що працюють на основі консенсусу Proof of Work (PoW), потребують значних обчислювальних ресурсів, що призводить до високого споживання енергії. Це може бути серйозною перешкодою для їх масового впровадження, особливо в умовах зростаючого занепокоєння щодо екологічної стійкості. Водночас, питання масштабованості стосуються здатності блокчейн-систем обробляти велику кількість транзакцій за одиницю часу, що є критичним для багатьох застосувань, таких як фінансові послуги та логістика.

Крім технічних викликів, важливу роль відіграють також соціальні та економічні аспекти. Зокрема, впровадження блокчейн технологій може вимагати значних

фінансових інвестицій, зміни організаційних процесів та навчання персоналу. Також важливо враховувати можливі правові та регуляторні перепони, оскільки блокчейн технології можуть стикатися з існуючими нормативними обмеженнями або вимагати розробки нових правових рамок для забезпечення їх ефективного використання [3].

Отже, блокчейн технології мають значний потенціал для зміцнення кібербезпеки та створення більш надійних і прозорих інформаційних систем. Однак для досягнення цього потенціалу необхідно подолати існуючі технічні та організаційні бар'єри, а також продовжувати науково-дослідні роботи у цій сфері. Важливою є також співпраця між різними секторами – державним, приватним та науковим – для розробки ефективних стратегій впровадження блокчейн технологій та їх інтеграції у вже існуючі системи кібербезпеки.

Література

1. Костюк П.П. Використання технології блокчейн для забезпечення інформаційної безпеки // Сучасний захист інформації, 2020. – № 3(43). – С.22-28.

2. Яровенко Г.М., Ковач В.О. Перспективи застосування технології блокчейн у системах забезпечення кібербезпеки банків // Підприємництво та інновації, 2020. – № 12. – С.206-214. – Режим доступу до ресурсу: https://doi.org/10.37320/2415-3583/12.36.

3. Liu Y., Zhang Q. Blockchain and Trustworthy Systems // Communications of the ACM, 2020. – № 63(8). – P.45-53.

В.Л. Пархоменко, А.С. Щепак, В.В. Пархоменко
Державний університет інформаційно-комунікаційних технологій, м. Київ

ГАРМОНІКИ СИГНАЛУ І ЇХ ВПЛИВ НА ПЕРЕДАЧУ ІНФОРМАЦІЇ

Засоби бездротової передачі інформації стали невід'ємною частиною повсякденного життя, забезпечуючи швидкий і надійний доступ до даних у будь-який час і в будь-якому місці. Від смартфонів і планшетів до складних систем Інтернету речей (IoT) та 5G-мереж, бездротові технології суттєво підвищують ефективність комунікацій і створюють нові можливості для розвитку різних галузей, таких як медицина, промисловість, транспорт і розваги [1]. Водночас, зростаюча складність і щільність цих систем потребує глибокого розуміння різних аспектів передачі сигналу, включаючи аналіз гармонік, які можуть значно впливати на якість і стабільність бездротового зв'язку. Дослідження гармонік сигналу та їх впливу на передачу інформації стає критично важливим для подальшого вдосконалення і оптимізації сучасних бездротових технологій.

Гармоніки сигналу відіграють ключову роль у системах передачі інформації, визначаючи якість, надійність та ефективність комунікаційних процесів. У сучасних інформаційних технологіях бездротової передачі інформації важливо розуміти природу гармонічних компонентів сигналу, їхні властивості та вплив на різні аспекти розповсюдження радіосигналу. Синусоїдальні складові, що складають гармонічний спектр сигналу, можуть як покращувати, так і погіршувати якість переданої інформації в залежності від умов та характеристик системи бездротової передачі інформації. У

бездротових телекомунікаційних системах надійність доставки інформації є критичним параметром, що визначає ефективність і стабільність зв'язку [2]. Одним з ключових факторів, що впливають на надійність передачі даних, є гармоніки сигналу. Вищі гармоніки, що виникають у процесі генерації та передачі сигналів, можуть спричиняти спотворення та інтерференцію, що негативно позначається на якості прийнятої інформації або швидкості передачі сигналу на одиницю часу.

Це особливо важливо у високошвидкісних мережах, де навіть незначні відхилення можуть призвести до втрати даних або зниження пропускної здатності. Тому дослідження методів забезпечення надійності доставки інформації, зокрема, шляхом управління та мінімізації впливу гармонік, є актуальним і необхідним для покращення роботи сучасних бездротових телекомунікаційних систем передачі. Тому важливим етапом у вирішені такої проблематики є розв'язання задачі аналізу впливу гармонік на сигнал та розробці ефективних методів для забезпечення високої надійності засобів бездротової передачі інформації в телекомунікаційних системах.

Розуміння та ефективне управління гармоніками сигналу є необхідним для оптимізації роботи сучасних телекомунікаційних мереж, радіозв'язку, а також інших технологій, що базуються на принципі бездротової передачі інформації. Гармоніки – це синусоїдальні складові сигналу, частоти яких є цілими кратними основної (фундаментальної) частоти. Вони виникають у будь-якому періодичному сигналі і можуть значно впливати на його характеристики та якість передачі. Гармоніки поділяються на основну частоту (перша гармоніка) і вищі гармоніки (друга, третя і т.д.).

Основна частота (перша гармоніка) є найнижчою частотою періодичного сигналу і визначає його основний тон або основну частотну складову. Вона є базовим компонентом, навколо якого формуються всі інші гармоніки. Вищі гармоніки – це частоти, що кратні основній частоті. Наприклад, якщо основна частота сигналу становить 50 Гц, то друга гармоніка буде мати частоту 100 Гц, третя – 150 Гц, і так далі. Вищі гармоніки можуть впливати на загальну форму радіосигналу, додаючи до нього додаткові коливання або змінюючи певні характеристики сигналу.

Математично гармоніки можна описати як складові ряду Фур'є, де будь-який періодичний сигнал можна представити у вигляді суми синусоїдальних функцій з різними частотами, амплітудами та фазами:

$$x(t) = A_0 + \sum_{n=1}^{\infty} \left\{ A_n \cos(2\pi n \varphi_0 t) + B_0 \sin(2\pi n \varphi_0 t) \right\},$$

де:

$x(t)$ – це періодичний сигнал;

A_0 – середнє значення сигналу (постійна складова);

A_n та B_0 – амплітуди косинусоїдальних і синусоїдальних компонент відповідно;

φ_0 – основна частота;

n – номер гармоніки.

Гармоніки мають значний вплив на якість передачі інформації у комунікаційних системах. Наявність вищих гармонік може призводити до спотворення переданого сигналу, особливо якщо ці гармоніки попадають у смугу пропускання каналу передачі. Це може знижувати якість прийнятого сигналу. Вищі гармоніки можуть викликати інтерференцію з іншими сигналами, що передаються в сусідніх каналах, а також створювати додаткові завади. Це особливо актуально у системах бездротового зв'язку,

де частотний спектр є обмеженим ресурсом. Частина енергії сигналу може бути витрачена на генерацію вищих гармонік, що знижує ефективність передачі основної інформації.

Для аналізу гармонік використовуються різні методи, зокрема, перетворення Фур'є, яке дозволяє представити сигнал у частотній області і визначити амплітудно-частотні характеристики гармонік. Сучасні інструменти і програмне забезпечення дозволяють детально аналізувати гармонічний склад сигналів і оцінювати їх вплив на системи передачі інформації. Загалом, розуміння природи гармонік і їх впливу на сигнали є важливим для оптимізації роботи комунікаційних систем, підвищення якості передачі даних та зменшення впливу завад і спотворень.

Для аналізу гармонік сигналів використовуються різні програмні засоби, які надають потужні інструменти для спектрального аналізу, обробки сигналів та візуалізації результатів. MATLAB є одним з найпопулярніших програмних середовищ для чисельних розрахунків і аналізу сигналів. Він містить потужний інструментарій для аналізу гармонік, зокрема, функції для перетворення Фур'є, спектрального аналізу та обробки сигналів. Python є популярною мовою програмування з великою кількістю бібліотек для аналізу даних та обробки сигналів. Відкритий код і велика спільнота розробників роблять його зручним інструментом для наукових досліджень в цій сфері.

Дослідження гармонік сигналу та їх впливу на передачу інформації у телекомунікаційних системах показало, що гармонічні спотворення можуть суттєво знижувати якість і надійність зв'язку. Виявлено, що вищі гармоніки, викликаючи інтерференцію та завади, негативно впливають на стабільність передачі даних. Ефективне управління гармоніками, зокрема через фільтрацію та оптимізацію спектральних характеристик сигналу, є ключовим для покращення надійності телекомунікаційних систем. Сучасні методи та підходи до мінімізації впливу гармонік можуть бути використані для вдосконалення технологій бездротового зв'язку, забезпечуючи стабільну і якісну передачу інформації навіть у високошвидкісних мережах бездротової передачі інформації.

Література

1. Shchepak A., Parkhomenko V., Parkhomenko V. (2021). Developing solution for using artificial intelligence to obtain more accurate results of the basic parameters of radio signal propagation // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 2021. – №11(1), P.36-39. – Режим доступу до ресурсу: https://doi.org/10.35784/iapgos.2577.

2. Пархоменко В.В. Метод забезпечення надійності доставляння інформації у телекомунікаційній системі / Ю.В. Мельник, В.Л. Пархоменко, В.В. Пархоменко, А.С. Щепак, С.А. Мрожик // Зв'язок, 2020. – №2(144). – С.21-27.

М.С. Тішков
Державний університет інформаційно-комунікаційних технологій, м. Київ

МЕТОДИ КІБЕРЗАХИСТУ ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В сучасному світі вбудовані системи займають все більше місця у повсякденному житті, забезпечуючи функціонування автомобілів, медичних пристроїв, промислових систем управління, розумних домашніх пристроїв та гаджетів, які ми носимо. Зростаюча інтеграція цих систем в Інтернет робить їх вразливими до кіберзагроз. Кіберзахист вбудованого програмного забезпечення є надзвичайно важливою задачею для забезпечення безпеки даних та безперебійної роботи цих систем.

Атаки на вбудовані системи можуть відбуватись різними способами [1]:

- Експлуатація вразливостей у програмному забезпеченні або мікропрограмі;
- Фізичне втручання в пристрій.

Атакуючи вбудовану систему, зловмисники можуть:

- Викрадати конфіденційні дані;
- Пошкоджувати або видаляти дані;
- Вимикати пристрої;
- Використовувати пристрої для атак на інші системи;
- Методи кіберзахисту.

Кіберзахист вбудованих систем включає в себе комплексний підхід, який охоплює кілька рівнів захисту: апаратний, мікропрограмний та програмний. Розглянемо основні методи кіберзахисту вбудованих систем [2]:

- Шифрування: Захист даних, що зберігаються на пристрої або передаються по мережі, шляхом їх шифрування.
- Аутентифікація: Забезпечення доступу до пристрою тільки авторизованим користувачам.
- Контроль доступу: Обмеження доступу до певних функцій або можливостей пристрою.
- Безпечне завантаження: Гарантія виконання тільки довіреного програмного забезпечення на пристрої.
- Оновлення безпеки: Регулярне оновлення програмного забезпечення та мікропрограм для виправлення відомих вразливостей.

Окрім технічних заходів, важливо впроваджувати найкращі практики безпеки на організаційному рівні:

- Проектування систем з урахуванням безпеки: Врахування вимог безпеки на стадії проектування системи та впровадження заходів безпеки на всіх рівнях системи.
- Використання безпечних практик розробки програмного забезпечення: Використання безпечних методів програмування, проведення тестування безпеки та використання безпечних інструментів і бібліотек.
- Моніторинг системи: Спостереження за системою на предмет підозрілої активності, такої як незвичайний мережевий трафік або несанкціоновані спроби доступу.
- Використання надійного ланцюжка постачання: Закупівля компонентів та програмного забезпечення у надійних постачальників для зниження ризику впровадження шкідливих компонентів або програмного забезпечення.

Як висновок, захист вбудованого програмного забезпечення від кіберзагроз є складним і багаторівневим завданням. Використання сучасних методів захисту, таких як шифрування, аутентифікація, контроль доступу та безпечне завантаження, у поєднанні з найкращими практиками безпеки на організаційному рівні, дозволяє значно підвищити рівень захисту вбудованих систем від кіберзагроз. Впровадження комплексного підходу до кіберзахисту допоможе забезпечити безпеку даних і стабільну роботу критично важливих систем, як і підприємств так і всієї країни.

Література

1. Hongmei He, Carl Shaw, Muhammad Ali Khan. Analytical Review of Cybersecurity for Embedded Systems By Abdulmohsan Aloseel. – Режим доступу до ресурсу: https://www.researchgate.net/publication/347802412_Analytical_Review_of_Cybersecurity_for_Embedded_Systems.

2. Establishing Cyber Resilience in Embedded Systems for Securing Next-Generation Critical Infrastructure By Fahad Siddiqui, Matthew Hagan, Sakir Sezer. – Режим доступу до ресурсу: https://www.researchgate.net/publication/340474508_Establishing_Cyber_Resilience_in_Embedded_Systems_for_Securing_Next-Generation_Critical_Infrastructure.

В.С. Тищенко
Державний університет інформаційно-комунікаційних технологій, м. Київ

ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ ЧЕРЕЗ АНАЛІЗ ЕМОЦІЙНОГО КОНТЕНТУ НЕЙРОННИМИ МЕРЕЖАМИ

Фейкові новини та дезінформація стали значною проблемою в сучасному суспільстві, а їхнє виявлення – важливим завданням. Одним із підходів до виявлення фейкових новин є використання нейронних мереж, зокрема, фокусуючись на емоційному впливі інформації. Аналіз емоцій відіграє ключову роль у визначенні поведінки користувача щодо певної теми, а фейкові новини мають навмисну мету збудити емоції читачів, щоб їм повірили.

Виявлення фейкових новин стає дедалі важливішим, оскільки вони негативно впливають на суспільство. Проте ефективність виявлення фейків за їхнім змістом часто недостатня. Для покращення цього процесу потрібні методи та інструменти, які враховують взаємозв'язок між характеристиками фейкової інформації та поведінкою користувачів у соціальних мережах [1].

Дослідження ефективності реальних методів класифікації у завданнях машинного навчання акцентується на використанні різноманітних класифікаторів, таких як логістична регресія, модель LDA, модель QDA, KNN-модель, дерево рішень та випадковий ліс, з метою виявлення фейкових новин. В ході дослідження використовується комбінація даних з набору "Liar liar pants on fire" та участь у змаганні з фейкових новин Kaggle Fake News. Розроблена методологія класифікації представлена у вигляді послідовності етапів, яку зображено на рис. 1.

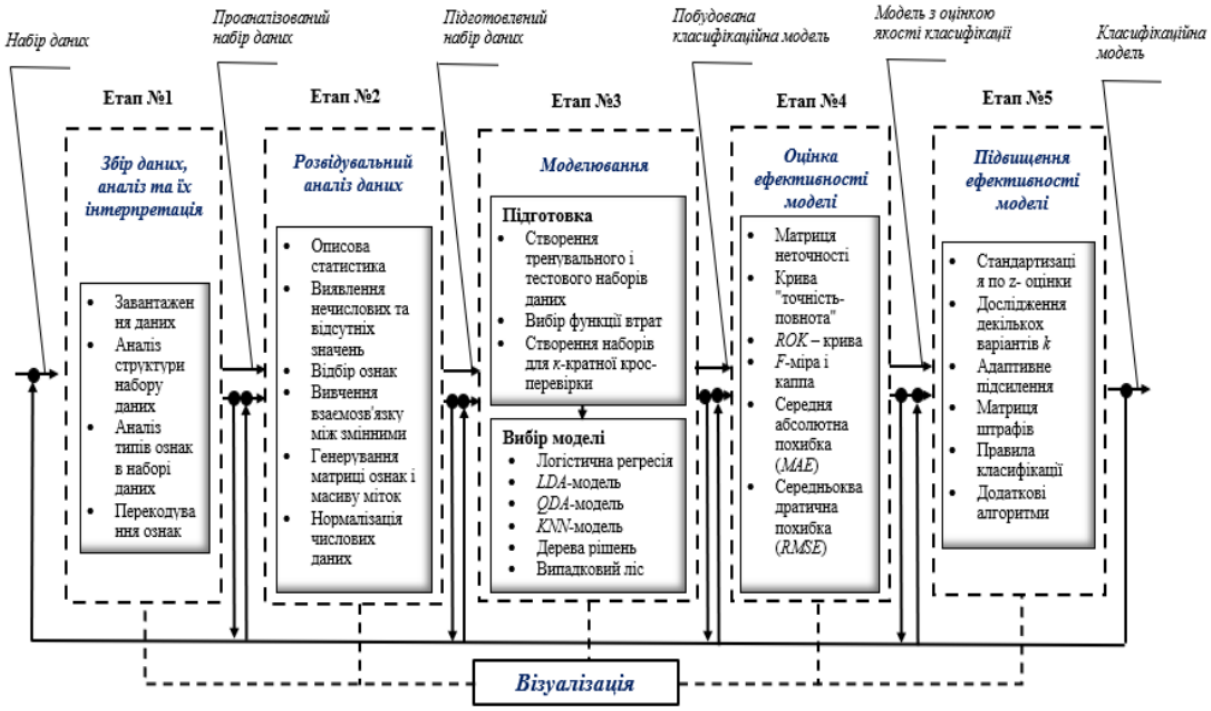

Рис. 1. Послідовність етапів вирішення завдань класифікації

Основною передумовою для поширення недостовірних новин є існування Інтернету та соціальних мереж як основних платформ, на яких більшість людей отримує свіжі новини та інформацію. За даними DataReportal на 2024 рік, кількість користувачів Інтернету становить 5,32 мільярда, а соцмереж – 4,65 мільярда. Для успішного поширення фейків необхідні інструменти та послуги для маніпулювання та поширення неправдивих повідомлень, які доступні в різних онлайн-спільнотах по всьому світу [2].

Ключовим елементом поширення фейкових новин є мотивація поширювачів, яка може включати фінансову вигоду, політичні та кримінальні цілі. Успішність дезінформації визначається її впливом на реальний світ. З огляду на глобальний розмах і зростання дезінформації в інтернеті, необхідно запобігати та протидіяти цьому явищу як інструменту маніпулювання громадською думкою.

Запропоновані підходи поєднують критичне мислення і сучасні технології, зокрема нейронні мережі:

1. Перевірка джерела новин:

- Використання нейронних мереж для автоматичної перевірки легітимності та надійності джерел.
- Аналіз стандартів точності, збалансованості та об'єктивності.

2. Аналіз змісту та заголовків:

- Виявлення упередженості, сенсаційних заголовків і перекручення даних.
- Критична оцінка контенту для ідентифікації непідтверджених джерел і статистики.

3. Перевірка інформації про автора:

- Оцінка надійності автора на основі досвіду, репутації та попередньої діяльності.
- Визначення авторитетності статей за допомогою нейронних мереж.

4. Перевірка посилань на новини:

- Аналіз інформації про згаданих осіб з оцінкою їхньої кваліфікації та об'єктивності.
- Виявлення відсутності належних посилань або сумнівності анонімних джерел.

5. Перевірка актуальності новин:

- Підтвердження своєчасності новин шляхом аналізу дати та часу публікації та порівняння з іншими джерелами.

Застосування нейромережевих технологій підвищує ефективність виявлення фейкових новин і сприяє зростанню довіри користувачів до інформації. Однак основні навички критичного мислення залишаються ключовими у протидії дезінформації навіть за використання передових технологій.

Література

1. Заброда В.Є., Льовкін В.М. Програмне забезпечення розпізнавання неправдивих новин / Харківська ювілейна міжнародна науково-практична конференція, Харків, 20-22 листопада 2018. – Харків, 2018. – С.66. – Режим доступу до ресурсу: https://foss.kn-it.info/uploads/foss-2018-theses.pdf.

2. DataReportal. – Режим доступу до ресурсу: https://datareportal.com/reports/digital-2024-deep-dive-5-billion-social-media-users?rq=users.

Ю.В. Щавінський, О.В. Будзинський
Державний університет інформаційно-комунікаційних технологій, м. Київ

ТЕХНІЧНІ АСПЕКТИ УДОСКОНАЛЕННЯ ЗАХИСТУ КОРПОРАТИВНИХ БАЗ ДАНИХ

Корпоративні бази даних (КБД) є сховищами найбільш значущих і цінних даних. Із зростанням використання баз даних зросла і частота атак на ці бази даних. Загальною метою атак на БД є доступ до критично важливої інформації. Порушення безпеки, включаючи втрату критично важливих даних, стали звичайним явищем в останні роки.

Багато підприємств стикаються з такими проблемами, як піратство даних, реплікація даних і атаки типу «відмова в обслуговуванні». Найбільш поширеним мотивом злому бази даних є незаконне отримання конфіденційних даних, таких як дані кредитних карток, банківські дані та особисті ідентифікатори.

Аналіз досліджень показує, що для того щоб проникнути в КБД компанії, кіберзлочинці шукають вразливості системи та використовують їх за допомогою спеціалізованих інструментів [1, 2]. За визначенням науковців атаки на КБД характеризуються як події, які ставлять під загрозу ресурс шляхом зміни або знищення життєво важливих даних [3].

Тому захист корпоративних баз даних є однією з найважливіших задач у сфері інформаційної безпеки підприємств та організацій і для захисту КБД необхідний ряд заходів і методологій [4, 5].

З ростом обсягів даних та ускладненням кіберзагроз особливо актуальним є необхідність удосконалення технічних засобів захисту баз даних. Аспект безпеки

повинен бути пріоритетним при розробці КБД. З точки зору розробки програмного забезпечення, питання безпеки повинні вирішуватися на кожному етапі циклу розробки.

Основними напрямками удосконалення захисту КБД є:

- використання алгоритмів шифрування, таких як AES (Advanced Encryption Standard), які дозволяють захистити дані навіть у випадку фізичного доступу до носіїв інформації;

- захист даних під час їх передачі між клієнтом і сервером за допомогою протоколів SSL/TLS (Secure Sockets Layer/Transport Layer Security), що дозволяє запобігти перехопленню і модифікації даних під час передачі через мережу;

- рольове управління доступом (Role-Based Access Control, RBAC), яке забезпечує доступ до бази даних на основі ролей користувачів та дозволяє легко управляти доступом в великих організаціях;

- мультифакторна автентифікація (MFA), яка вимагає від користувачів підтвердження своєї особи за допомогою декількох факторів, таких як пароль, токен і біометричні дані, що значно підвищує рівень безпеки, оскільки злом одного фактора не дозволить отримати доступ до даних;

- постійний моніторинг усіх дій у базі даних в режимі реального часу за допомогою розроблених систем DAM (Database Activity Monitoring);

- ведення журналів подій та аудит для відслідковування всіх операції в базі даних, що допомагає виявляти аномальні дії, розслідувати інциденти та забезпечувати відповідність політикам безпеки та нормативним вимогам.

Але найбільш ефективним сучасним засобом удосконалення безпеки КБД є використання інтелектуальних систем, які створюються на основі використання передових технологій: машинне навчання та штучний інтелект (Machine Learning and Artificial Intelligence); блокчейн (blockchain); хмарні сервіси (AWS RDS, Google Cloud SQL, та Azure SQL Database).

Інтеграція технологій машинного навчання та штучного інтелекту в системи захисту баз даних дозволяє автоматично виявляти аномалії та нові типи загроз. Ці системи можуть аналізувати великі обсяги даних і виявляти шаблони, які можуть свідчити про злом або інші види атак. Удосконалення захисту корпоративних баз даних за допомогою машинного навчання та штучного інтелекту можливе завдяки здатності цих технологій до аналізу поведінкових патернів, прогнозування загроз, автоматизації реагування на інциденти, моніторингу внутрішніх дій користувачів та інтеграції з існуючими системами безпеки. Це дозволяє значно підвищити рівень безпеки, забезпечити своєчасне виявлення та запобігання загрозам, а також мінімізувати вплив людського фактора на процеси захисту.

Використання технології blockchain забезпечує високий рівень захисту цілісності даних, дозволяє створювати незмінні записи всіх транзакцій, що робить будь-які несанкціоновані зміни легко виявленими.

Таким чином, захист корпоративних баз даних вимагає комплексного підходу, який включає використання передових технологій та методів. Шифрування даних, контроль доступу, моніторинг активності та застосування машинного навчання і blockchain є ключовими технічними аспектами, які допомагають забезпечити високий рівень безпеки. Впровадження цих заходів допоможе організаціям ефективніше використовувати свої дані, забезпечуючи надійність та захист інформації від сучасних

кіберзагроз. Постійний розвиток технологій та адаптація до нових загроз є необхідністю для збереження конфіденційності, цілісності та доступності даних.

Література

1. Toapanta S.M. Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks // IEEE, 2020. – Vol. 8. – P.169367-169384.
2. Humayun M. Security threat and vulnerability assessment and measurement in secure software development // Comput. Mater. Contin., 2022. – Vol. 71. – P.5039-5059.
3. Almufareh M.F., Humayun M. Improving the safety and security of software systems by mediating SAP verification // Applied Sciences, 2023. – Vol. 13. – № 1. – P.647.
4. Chakraborty S. Database Security Threats and How to Mitigate Them / In Proceedings of the MOL2NET'22, Conference on Molecular, Biomed., Comput. & Network Science and Engineering, 8th ed., 1-15 January 2023, MDPI: Basel, Switzerland. DOI:10.3390/mol2net-08-12642.
5. Alisawi W.C., Hussain A.A.A., Alawsi W.A. Estimate new model of system management for database security // Indones. J. Electr. Eng. Comput. Sci., 2019. – Vol. 14. – №. 3. – P.1391-1394.

О.С. Горохов, В.П. Яковець, А.О. Макаренко
Державний університет інформаційно-комунікаційних технологій, м. Київ

МЕТОДИ ПОКРАЩЕННЯ ЄМНОСТІ ТРАНСПОРТНИХ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ

Транспортна мережа (Backhaul) це сегмент системи мобільного зв'язку, що пов'язує базові станції з функціональними елементами стільникової мережі. Транспортні мережі також відомі як опорні системи передачі даних. У випадку LTE транспортна мережа також забезпечує зв'язок базових станцій між собою та повинна забезпечувати синхронізацію, якість обслуговування та інші необхідні послуги.

Ємність мережі це максимальна кількість інформації, що може передати система за деякий період часу. Основними метриками ємності мережі є пропускна здатність, затримка, джитер (спотворення сигналу) та втрата пакетів. Для забезпечення необхідної якості обслуговування, пропускна здатність повинна бути якомога більшою, в той час як затримка, джитер та втрата пакетів повинні бути мінімальними. Планування ємності дозволяє обчислювати поточне використання мережі, документувати обмеження ресурсів та передбачувати можливі зміни в вимозі користувачів. З моніторингом основних вимірювань мережі стає можливим виявляти недоліки або проблеми, здатні вплинути на доступність або пропускну здатність мережі у довгостроковій перспективі.

Для швидкого реагування на можливі зміни ємності мережі можливе налаштування сигналізації при перевищенні граничних значень ключових показників [1]. Загальні критичні мережні умови, що викликають оповіщення, включають затримки часу відповіді, вичерпання ємності, високі рівні затримки, перевантажені сервери, збої в роботі, перевищення критичних порогових значень та високе завантаження ЦП або пам'яті. Оповіщення надсилаються мережевим адміністраторам електронною поштою,

текстовими повідомленнями або іншими засобами зв'язку для швидкого усунення несправностей.

Прогнозування пропускної спроможності мережі допомагає відстежувати використання пропускної спроможності та прогнозувати ресурси, необхідні для реагування на зміни у мережній інфраструктурі. Це дозволяє мережевим інженерам уникнути перевантажень мережі та збоїв, викликаних вичерпанням пропускної спроможності. Виділяються два методи прогнозування вичерпання ємності на рівні вузла, інтерфейсу та тому:

- Піковий розрахунок: цей метод прогнозує тенденції використання потужності з урахуванням щоденних максимальних значень. Він використовується для критично важливих пристроїв та з'єднань, щоб уникнути надмірного використання ємності.
- Розрахунок середнього значення. Цей метод ґрунтується на середньодобових значеннях для прогнозування використання ємності. Він використовується для мережних пристроїв або з'єднань, де допустиме використання високої ємності протягом короткого часу [2].

Завдяки швидкому розвитку штучного інтелекту (ШІ) автоматизація мережі в поєднанні зі штучним інтелектом може при відносно невеликих витратах знизити операційні витрати (орех) мікрохвильової мережі. Ресурсномісткі сфери, такі як споживання енергії, усунення несправностей, відвідування об'єктів і навіть витрати на використання спектру, можуть бути зменшені. Енергоспоживання можна зменшити за допомогою автоматичного планування глибокого сну радіостанції. Проблеми мережі, такі як розгойдування вежі, несумісність антен і погіршення поширення сигналу, можна виявити і швидко вирішити завдяки точному аналізу першопричини. Крім того, профілактичне обслуговування, таке як сповіщення про деградацію обладнання, раннє попередження про високу температуру і прогнозування зростання мережевого трафіку, може зменшити витрати на пожежі, що вимагають значних коштів. Ще однією перевагою є покращена доступність мережі в результаті меншої кількості відключень, що призводить до збільшення та збереження доходів.

Енергозбереження та автоматизація сприяють розвитку мікрохвильової індустрії. Оскільки масштаби розгортання мікрохвильового транзитного зв'язку збільшуються, автоматизація є ідеальним інструментом для ефективної експлуатації та обслуговування мікрохвильових мереж. Мікрохвильові мережі використовують існуючі вежі мобільного зв'язку для побудови транзитних мереж, а передача на великі відстані дозволяє зменшити кількість пристроїв у мережах, тим самим розширюючи сфери застосування мікрохвильових мереж.

В [3] та [4] наведені приклади систем, які пропонують автоматизацію традиційним транспортним мережам.

Обмін квантованими сигналами, що приймаються, пред'являє високі вимоги до пропускної здатності. З цієї причини було проведено багато досліджень методів реалізації розподілених антенних систем з максимальною ефективністю транзитного зв'язку, таких як планування з урахуванням транзитного зв'язку, схеми кластеризації та стиснення. В [1] описується метод кооперації базових станцій, що використовує новий підхід. Пропонується регулювати точність квантування таким чином, щоб можна було досягти оптимального компромісу між продуктивністю декодування та вимогами до транспортного зв'язку.

В [4] та [5] описані методи повторного використання каналу та призначення базових станцій з урахуванням витрат з забезпечення якості обслуговування для транспортних мереж стільникового зв’язку.

Література

1. Grieger M., Marsch P., Fettweis G. Ad Hoc Cooperation for the Cellular Uplink with Capacity Constrained Backhaul / «ICC 2010» IEEE International Conference on Communications, Cape Town, South Africa, 23-–27 May 2010, 2010. – Режим доступу до ресурсу: https://doi.org/10.1109/icc.2010.5502503.

2. Galeana H., Novillo F., Ferrus R. A Cost-Based Approach for Base Station Assignment in Mobile Networks with Limited Backhaul Capacity / IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, New Orleans, LA, USA, 30 November - 4 December 2008, 2008. – URL: https://doi.org/10.1109/glocom.2008.ecp.965.

3. Ericsson Transport Automation Controller. – URL: https://www.ericsson.com/en// mobile-transport/transport-automation-controller (дата звернення: 28.05.2024).

4. iMaster NCE-IP. – Режим доступу до ресурсу: https://e.huawei.com/en/products /network-analysis/imaster-nce-ip (дата звернення: 28.05.2024).

5. Channel Reuse for Backhaul in UAV Mobile Networks with User QoS Guarantee / M. Nikooroo et al. / ICC 2023 - IEEE International Conference on Communications, Rome, Italy, 28 May - 1 June 2023, 2023. – URL: https://doi.org/10.1109/icc45041.2023.10278940.

Ю.М. Якименко
Державний університет інформаційно-комунікаційних технологій, м. Київ

ВИЗНАЧЕННЯ ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В західних розвинених країнах інформаційні системи з використанням штучного інтелекту прийнято відносити до класу «інтелектуальних» систем. Дані системи представляють собою особливу категорію інформаційних сучасних технологій, що об'єднують різні методи, такі як: нейтронні мережі; генетичні алгоритми, нечіткі системи; експертні системи; системи динамічного структурного моделювання. Загальною спільною властивістю інтелектуальних систем є те, що вони імітують процеси, схожі до тих, що відбуваються в природі [1]. Комплекс технологічних рішень завдяки цим системам, дозволяє імітувати когнітивні функції людини та отримувати при виконанні конкретних завдань результати, що дорівнюють результатам інтелектуальної діяльності людини.

Інтелектуальна інформаційна система (ІІС) – це один з видів автоматизованих інформаційних систем, інколи ІІС називають системою, засновану на знаннях. ІІС є комплексом програмних, лінгвістичних і логіко-математичних засобів для реалізації основного завдання: здійснення підтримки діяльності людини і пошуку інформації в режимі розширеного діалогу між ними.

У загальному випадку всі ІІС, відповідно до запропонованої класифікації [2], засновані на знаннях, можна поділити на системи, що вирішують задачі аналізу, і на

системи, які вирішують задачі синтезу. Основна відмінність задач аналізу від задач синтезу полягає в тому, що якщо в задачах аналізу множина рішень може бути перерахована і включена в систему, то в задачах синтезу множина рішень потенційно необмежена. Задачею аналізу є: інтерпретація даних, діагностика, підтримка прийняття рішення; до завдань синтезу відносять проектування, планування, управління. Комбіновані задачі: навчання, моніторинг, прогнозування.

Як показує практика, використання ІІС в інформаційній безпеці обумовлено, насамперед, необхідністю оперативного реагування під час настання інцидентів безпеки та нестачею кваліфікованих спеціалістів з захисту інформації. В деяких компаніях є системи, які збирають масиви даних, аналізують їх за допомогою технологій класу штучного інтелекту, виявляють закономірності, проводять кластеризацію даних та прогнозують загрози. Без таких технологій обробляти подібний обсяг інформації практично неможливо.

Кращою стратегією інформаційної безпеки є випереджальний комплексний підхід, який охоплює такі напрями: виявлення та аналітика загроз, безпека даних та додатків, управління ідентифікацією, безпека мережі та систем.

Технології використання ІІС відкривають нові перспективи для розвитку сучасних засобів захисту інформації. Внаслідок останніх тенденцій в галузі діджиталізації аналітики інформаційної безпеки в Україні відзначають неухильне зростання як обсягу, так і складності даних, які генеруються в інформаційному просторі.

Основними важливими типами технологій використання ІІС в системі інформаційної безпеки будь-якої організації і її забезпеченні є:

- SIEM (Security Information and Event Management) – рішення, які здійснюють моніторинг інформаційних систем в режимі реального часу аналізують події безпеки, що поступають від мережевих пристроїв, засобів захисту інформації, IT-сервісів, інфраструктури систем та додатків, та допомагають виявити інциденти інформаційної безпеки;
- SOAR (Security Orchestration and Automated Response) – системи, що дозволяють виявляти загрози інформаційній безпеці та автоматизувати реагування на інциденти. В рішеннях даного типу, на відміну від SIEM-систем, штучний інтелект допомагає не тільки проводити аналіз. Але й автоматично реагувати відповідним чином на виявлені загрози.

Основне призначення SIEM включає ще автоматичне слідкування за всім потоком інформації в об’єктах комп’ютерної системи організації (стаціонарних і мобільних АРМ, серверів і віртуальних машин, комутаторів, мостів і точок доступу) і в засобах захисту інформації. Таким призначенням виключається перевантаження в роботі працівника, як це було при традиційному управлінні автоматизованою системою без SIEM. SIEM використовується практично і як система управління інформацією і подіями в області інформаційної безпеки. Створення повноцінного центру управління інформаційною безпекою SOC (Security Operation Center) в організації – це завжди наступний етап після розгортання SIEM. SOC у першу чергу – це люди, а SIEM – це всього лише засіб автоматизації праці, що дозволяє скоротити працезатрати персоналу SOC [3].

Прийняття рішень за допомогою технологій ІІС допомагають знаходити загрози, попереджувати ризики та виконувати відповідні організаційні і технічні дії з захистом інформації - відіграють вирішальну роль у покращенні забезпечення інформаційної

безпеки на високому рівні - проектувати створення ефективної системи управління (менеджменту) інформаційної безпеки організації (компанії, підприємства, фірми), її впровадження і експлуатації.

Література

1. Ковтуненко Ю.В. Застосування штучного інтелекту у системі управління підприємством: проблеми та переваги // Economic journal Odessa polytechnic university, 2019. – 7 с. – Режим доступу до ресурсу: https://economics. net.ua/ejopu/2019/No2/93.pdf.

2. Коцовський В.М. Інтелектуальні інформаційні системи Конспект лекцій. Ужгород: ДВНЗ «Ужгородський національний університет», 2019. – 73 с. – Режим доступу до ресурсу: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/25833/1/%D0%9A%D0%BE%D0%BD%D1%81%D0%BF%D0%B5%D0%BA%D1%82%20%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D0%B9.pdf.

3. Якименко Ю.М., Легомінова С.В., Щавінський Ю.В., Рабчун Д.І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби: навчальний посібник. – К.: ДУТ, 2023. – 241 с.

О.В. Костікова, С.О. Кульчицький, М.С. Широкопетлєва
Харківський національний університет радіоелектроніки, м. Харків

ПРОЕКТУВАННЯ СИСТЕМИ РЕКОМЕНДАЦІЇ СУКУПНИХ ТОВАРІВ ДЛЯ ПРОГРАМНОЇ СИСТЕМИ З ВЕДЕННЯ ОБЛІКУ ПРОДАЖУ ТА РЕМОНТУ ОФІСНОЇ ТЕХНІКИ

У сучасному світі бізнесу автоматизація процесів стає ключовим чинником успіху. Системи управління продажами та ремонтом офісної техніки відіграють важливу роль у забезпеченні безперервної роботи офісів та підвищенні ефективності обслуговування клієнтів. Одним із важливих елементів таких систем є механізм рекомендацій сукупних товарів, який дозволяє підвищити рівень задоволеності клієнтів та збільшити доходи компанії.

Основною метою проектування такої системи є не лише полегшення процесу замовлення для користувачів, але й оптимізація продажів компанії. Використовуючи інформацію з бази даних, система може аналізувати попередні замовлення, визначати найчастіше замовлювані товари та послуги в комплексі та пропонувати їх користувачам у якості рекомендацій.

Завдяки впровадженню такої системи, компанія отримує змогу не лише збільшити обсяги продажів супутніх товарів, але й зменшити час обробки замовлень, що є важливим фактором у умовах сучасного динамічного бізнес- середовища. Розробка та впровадження системи рекомендації сукупних товарів є важливим кроком на шляху до створення ефективного та клієнтоорієнтованого сервісу у сфері продажу та ремонту офісної техніки.

Для реалізації підсистеми формування рекомендацій спроектована ER- діаграма, фрагмент якої наведено на рис. 1. Сутності "Товари", "Послуги", "Пакет послуг", "Товар у замовленні", "Послуга у замовленні", "Пакет у замовленні", "Замовлення" є основними

для формування рекомендацій щодо товарів та послуг.

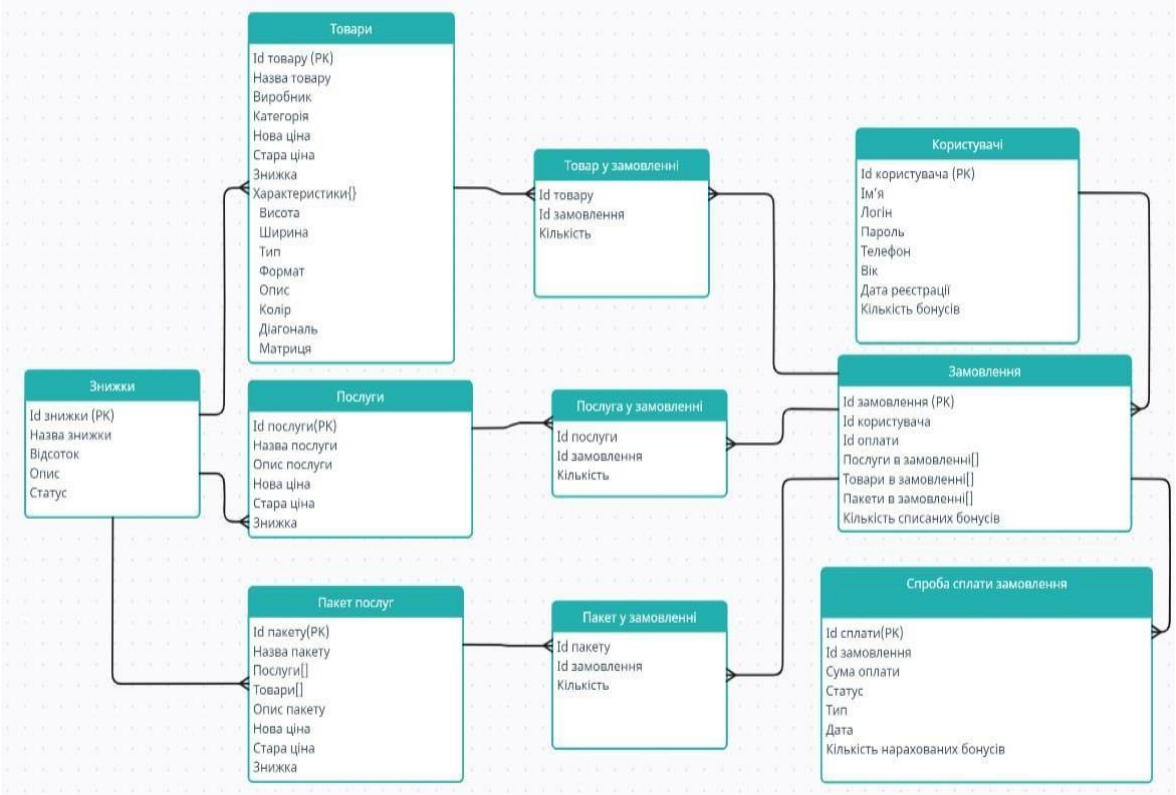

Рис. 1. Фрагмент ER-діаграми

Під час створення замовлення, необхідно проаналізувати, чи є замовлений товар чи послуга елементом будь-якого пакету і чи були продажі цих пакетів. Якщо є, тоді обираються товари чи послуги, які були продані із замовленим товаром найчастіше. Користувачеві пропонується по 5 найпопулярніших товарів/ послуг з використанням механізму пагінації.

Під час створення пакету послуг здійснюється наступна послідовність дій. Спочатку отримується масив ідентифікаторів продуктів та послуг із запиту. Після цього перевіряється, чи існують продукти та послуги з вказаними ідентифікаторами у базі даних. Якщо всі ідентифікатори є коректними, створюється новий об'єкт "Пакет послуг" з зазначеними ідентифікаторами продуктів та послуг, ціною (яка розраховується як сума цін продуктів та послуг) та іншими необхідними полями. Далі новий пакет послуг зберігається у базі даних.

При отриманні пакету послуг виконується наступний процес. Спочатку отримується ідентифікатор пакету послуг із запиту. Потім здійснюється запит до бази даних для отримання об'єкта "Пакет послуг" з вказаним ідентифікатором. Інформація про продукти та послуги, включені до пакету, заповнюється на основі їх ідентифікаторів, що містяться в об'єкті "Пакет послуг". Нарешті, повертається повний об'єкт пакету послуг з детальною інформацією про продукти та послуги, які в нього входять.

Процедура оновлення пакету послуг включає кілька етапів. Спочатку отримується ідентифікатор пакету послуг та дані для оновлення із запиту. Потім здійснюється запит до бази даних для отримання об'єкта "Пакет послуг" з вказаним ідентифікатором. Після цього поля пакету послуг оновлюються відповідно до отриманих даних. Оновлений пакет послуг зберігається у базі даних, забезпечуючи актуальність інформації.

Для реалізації даної системи використані технології, що забезпечують ефективне зберігання та обробку даних, а також створення надійного API для взаємодії з користувачами. в якості СУБД обрана MongoDB [1], яка забезпечує високу гнучкість та масштабованість, необхідну для зберігання різноманітних даних. MongoDB використовує формат документів BSON, що дозволяє зберігати складні структури даних у вигляді вбудованих документів та масивів. Для роботи з колекціями у MongoDB було використано Mongoose [2] – ODM для Node.js [3]. Mongoose надає можливість створення схем даних, які визначають структуру документів у колекціях. Основні методи Mongoose, що були використані для роботи з даними: find() – для пошуку документів у колекції, що відповідають певним критеріям; findById() – для пошуку документа за унікальним ідентифікатором; create() – для створення нових документів у колекції; updateOne() – для оновлення існуючих документів відповідно до заданих критеріїв; deleteOne() – для видалення документів з колекції за заданими умовами. Для обробки HTTP-запитів до API використана бібліотека Express.js [4]. Це мінімалістичний веб-фреймворк для Node.js, який забезпечує гнучкість та простоту створення серверної частини додатків.

Отже, запропонована система рекомендації сукупних товарів для програмної системи з ведення обліку продажу та ремонту офісної техніки демонструє ефективність у забезпеченні автоматизованої підтримки користувачів при виборі та замовленні послуг і товарів. Використання технологій MongoDB, Mongoose та Express.js дозволяє створити надійну та масштабовану інфраструктуру для управління даними та обробки запитів.

Література

1. Alexander S. Gillis. What is MongoDB? Technical Writer and Editor, 2023. – Режим доступу до ресурсу: https://www.techtarget.com/searchdatamanagement/definition/Mongo DB (дата звернення: 18.05.2023).

2. Jesse Hall. Getting Started with MongoDB & Mongoose. – Режим доступу до ресурсу: https://www.mongodb.com/developer/languages/javascript/ getting-started-with- mongodb-and-mongoose/ (дата звернення: 18.05.2023).

3. What is Express.js? – Режим доступу до ресурсу: https://www.codecademy.com/article/what-is- express-js (дата звернення: 18.05.2023).

4. About Node.js. – Режим доступу до ресурсу: https://nodejs.org/en/about (дата звернення: 21.04.2023).

С.В. Легомінова, Т.М. Мужанова, Д.О. Пильнов
Державний університет інформаційно-комунікаційних технологій, м. Київ

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ Й МАШИННОГО НАВЧАННЯ У РЕАЛІЗАЦІЇ «РОЗУМНИХ» КІБЕРЗАГРОЗ

У динамічному технологічному ландшафті, де штучний інтелект (AI) і машинне навчання (ML) змінюють усі сфери життєдіяльності суспільства, ці інноваційні технології несуть не тільки прогрес, але й широко використовуються зі зловмисною метою. Загрози кібербезпеці також розвиваються із загрозливою швидкістю. Оскільки

суспільство стає все більш взаємопов'язаним і залежить від «розумних» пристроїв, експоненціально зростає потенціал інтелектуальних і складних кібератак. Поява «розумних» кіберзагроз спричиняє еру нових викликів, коли зловмисники використовують передові технології для експлуатації вразливостей і руйнування цифрових екосистем.

«Розумні» кіберзагрози мають здатність адаптуватися, навчатися і навіть обманювати системи безпеки [1]. Вони використовують передові методи, такі як алгоритми ML, автоматизовані бот-мережі й тактики соціальної інженерії для ураження окремих осіб, організацій та об'єктів критичної інфраструктури.

Однією із першопричин зростання розумних кіберзагроз є експоненціальне зростання обсягу даних. З поширенням підключених пристроїв, включаючи розумні будинки й мобільні технології, генерується величезна кількість даних, які не часто використовують зловмисники, щоб отримати інформацію про поведінку, уподобання та вразливі місця об'єкта атак, що дозволяє реалізувати цілеспрямовані атаки з більшою точністю й ефективністю.

Одними із найбільших «розумних» загроз є штучний інтелект і машинне навчання [2].

Штучний інтелект став потужним інструментом у різних сферах, революціонізувавши галузі та змінивши спосіб життя й діяльності людини. Однак у міру розвитку AI зростають і потенційні кіберризики, пов'язані з його неправильним використанням або експлуатацією. Злиття AI та кібербезпеки пропонує як можливості для покращеного захисту, так і виклики з боку інтелектуальних і складних кіберзагроз.

Зловмисники можуть використовувати алгоритми AI для автоматизації різних етапів атаки, від розвідки та сканування вразливостей до використання слабких місць і запуску складного шкідливого ПЗ. За допомогою ботів на основі AI хакери можуть розширювати свої операції, адаптуючи свої стратегії та уникаючи традиційних заходів безпеки.

Крім того, AI можна використовувати для посилення атак соціальної інженерії. Аналізуючи величезну кількість особистих даних, доступних в Інтернеті, алгоритми AI можуть генерувати дуже переконливі фішингові електронні листи, повідомлення або голосові дзвінки, призначені для обману окремих людей або навіть систем безпеки. Таке поєднання AI та соціальної інженерії створює серйозну загрозу зловживання вразливостями людини з безпрецедентною точністю й ефективністю.

Ще одним викликом є поява зловмисного AI, коли порушники використовують методи AI, щоб підірвати або обійти захист, який власне й базується на технологіях AI. Такі порушення передбачають маніпулювання або обману моделей AI шляхом введення зловмисних даних або використання вразливостей у процесах прийняття рішень. Це може призвести до помилкових спрацьовувань або помилково негативних результатів, дозволяючи зловмисникам уникнути виявлення або отримати несанкціонований доступ до систем.

Крім цього, AI також може посилити вплив існуючих кіберзагроз, наприклад прискорити поширення зловмисних програм, автоматично генеруючи варіанти, які обходять традиційне антивірусне ПЗ. Це також може сприяти створенню діпфейк-контенту (Deepfake), де алгоритми AI генерують переконливі фейкові відео чи аудіо, що призводить до дезінформації, шкоди репутації або навіть політичних маніпуляцій.

Машинне навчання (ML) також стало трансформаційною технологією з широким застосуванням у різних галузях, включаючи кібербезпеку. Однак у міру того, як ML продовжує розвиватися, воно також відкриває нові шляхи для потенційних кібератак, створюючи значний виклик для майбутнього кібербезпеки. Кібератаки з використанням ML передбачають маніпулювання або використання вразливостей у моделях ML, щоб ввести в оману або змусити їх прийняти неправильні чи необдумані рішення. Зловмисники можуть вводити ретельно створені вхідні дані, часто непомітні для спостерігачів, щоб обманути алгоритми ML і змусити їх видавати неточні результати. Ці атаки можуть мати серйозні наслідки, наприклад обхід систем виявлення вторгнень, уникнення виявлення зловмисного ПЗ або маніпулювання результатами автоматизованих процесів прийняття рішень.

Як і у випадку штучного інтелекту, ML використовують для автоматизації й підвищення ефективності різних типів кібератак. Хакери можуть використовувати алгоритми ML для автоматизації ідентифікації вразливостей у системах або мережах, дозволяючи їм розширювати свої операції й ефективніше використовувати слабкі місця. Боти на базі ML можуть автономно сканувати мережі, виявляти вразливості й запускати цілеспрямовані атаки, потенційно переважаючи традиційні засоби захисту. Поєднання ML і автоматизації може значно збільшити швидкість і масштаб кібератак, ускладнюючи їх виявлення та протидію.

Ще одна проблемна сфера – потенційне зловживання ML для створення складних і переконливих фішингових атак. Використовуючи алгоритми ML, можна аналізувати величезні обсяги даних для створення персоналізованих фішингових повідомлень, які імітують стиль, тон і вміст законних повідомлень. Фішингові атаки на основі ML можуть обійти традиційні фільтри електронної пошти й заходи безпеки, збільшуючи шанси соціальної інженерії, компрометації конфіденційної інформації або отримання несанкціонованого доступу.

Крім того, ML також використовують для вироблення діпфейк-контенту, який передбачає створення дуже реалістичного, але підробленого аудіо або відео. Діпфейки можна використовувати для різних зловмисних цілей, включаючи поширення дезінформації, маніпулювання громадською думкою або навіть видавання себе за інших осіб у шахрайських діях. Алгоритми ML можуть аналізувати наявні дані та вчитися на них, щоб генерувати переконливі глибокі фейки, що ускладнює розрізнення справжнього вмісту від підробленого.

Отже, з огляду на те, що технології AI та ML продовжують розвиватися, майбутній потенціал кібератак із застосуванням цих методів викликає серйозне занепокоєння. Для подолання цих викликів необхідне впровадження проактивної та спільної відповіді, забезпечення постійної співпраці, формування кіберобізнаності, сприяння дослідженням і розробкам у сфері кібербезпеки новітніх технологій, а також заохочення їх відповідального використання у масштабах усього суспільства. Система кібербезпеки має спрямовувати свої зусилля на випередження нових загроз і захист цифрових екосистем організацій, установ та об’єктів критичної інфраструктури від дедалі складнішої й інтелектуальної природи кібератак, керованих AI та ML.

Література

1. Gallant B. The Future of “Smart” Cyber Threats. – Режим доступу до ресурсу: https://www.linkedin.com/pulse/future-smart-cyber-threats-brett-gallant.

2. Smart Technologies are Linked to Threats. – Режим доступу до ресурсу: https://www.trendmicro.com/vinfo/it/security/news/internet-of-things/smart-technologies-are-linked-to-threats.

Н.А. Святська, В.Б. Дендура
Державний університет інформаційно-комунікаційних технологій, м. Київ

АДАПТИВНА СИСТЕМА НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Адаптивне навчання являє собою освітній підхід, що використовує сучасні технології для персоналізації навчального процесу відповідно до потреб кожного співробітника організації. Цей підхід динамічно коригує зміст, темп і методи навчання на основі індивідуальних потреб, уподобань та успішності особи, з метою оптимізації результатів шляхом надання індивідуалізованого навчання та підтримки.

Адаптивне навчання надає значні переваги завдяки своїй персоналізації та адаптивності, гнучкості та масштабованості, а також завдяки унікальним характеристикам адаптивних систем. Основною перевагою адаптивного навчання є його здатність пристосовуватися до різних стилів навчання та здібностей працівників, забезпечуючи кожному належну підтримку. Системи адаптивного навчання динамічно коригують зміст та методи викладання, враховуючи індивідуальні вподобання та рівень підготовки кожної людини [1]. Це гарантує, що навчальний процес максимально відповідає потребам кожного учасника навчання, сприяючи ефективнішому засвоєнню знань та навичок.

Крім того, адаптивне навчання характеризується своєю гнучкістю та масштабованістю. Особи, що проходять курс, можуть отримувати доступ до систем адаптивного навчання в будь-який час та з будь-якого місця, використовуючи різноманітні пристрої, що робить навчання більш доступним та зручним. Такі системи також здатні масштабуватися для забезпечення великої кількості учнів персоналізованим навчанням та підтримкою, що є особливо корисним у великих навчальних закладах або організаціях.

Схема адаптивної системи навчання персоналу з інформаційної безпеки складається з п'яти ключових етапів: ідентифікація потреб у навчанні, розробка матеріалів, створення індивідуальних планів та платформи, проведення навчального процесу, моніторинг та оцінка ефективності [2].

На першому етапі, ідентифікації потреб у навчанні, здійснюється аналіз поточних знань і навичок персоналу в сфері інформаційної безпеки. Визначаються прогалини в знаннях, які необхідно заповнити, а також специфічні вимоги, що стосуються різних посад і ролей у компанії.

Рис. 1. Адаптивна система навчання з інформаційної безпеки

Другий етап, розробка матеріалів, передбачає створення навчальних ресурсів, що включають текстові матеріали, відео, інтерактивні завдання та практичні кейси. Ці матеріали повинні бути актуальними, легко зрозумілими та адаптованими до різних рівнів знань персоналу.

Наступний етап, створення індивідуальних планів та платформи, полягає у розробці персоналізованих навчальних планів для кожного співробітника, враховуючи результати аналізу їхніх потреб. Для цього використовується платформа для онлайн-навчання (LMS), яка забезпечує доступ до матеріалів з будь-якого місця та у будь-який час. Платформа також дозволяє відстежувати прогрес кожного співробітника.

Четвертий етап, проведення навчального процесу, включає організацію та проведення тренінгів, вебінарів та практичних занять. Важливо забезпечити інтерактивність навчання та можливість для співробітників застосовувати отримані знання на практиці.

Останній етап, моніторинг та оцінка ефективності, передбачає регулярне тестування знань персоналу та аналіз їхніх успіхів [3]. Зібрані дані використовуються для подальшого коригування навчальних програм і матеріалів, що забезпечує безперервне вдосконалення системи навчання.

Впровадження адаптивної системи навчання сприяє не тільки підвищенню рівня знань та навичок співробітників, але й формуванню культури інформаційної безпеки в організації. Це, у свою чергу, знижує ризики виникнення інцидентів, пов'язаних з інформаційною безпекою, та сприяє загальному зміцненню захисту інформаційних ресурсів. Таким чином, адаптивне навчання є невід'ємною частиною стратегії інформаційної безпеки будь-якої сучасної організації.

Література

1. An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work / F. Ben Salamah et al. // Applied Sciences, 2023. – Vol. 13. – N.17. – P.9595. – Режим доступу до ресурсу: https://doi.org/10.3390/app13179595.

2. Adaptive security awareness training using linked open data datasets / Z. Tan et al. / Education and Information Technologies, 2020. – Vol. 25, – N.6. – P.5235-5259. – Режим доступу до ресурсу: https://doi.org/10.1007/s10639-020-10155-x.

3. Zamiri M., Esmaeili A. Methods and Technologies for Supporting Knowledge Sharing within Learning Communities: A Systematic Literature Review // Administrative Sciences, 2024. – Vol. 14. – N.1. – P.17. – Режим доступу до ресурсу: https://doi.org/10.3390/admsci14010017.

Д.В. Примаченко, З.Т. Доброжан
Державний університет інформаційно-комунікаційних технологій, м. Київ

ТЕХНОЛОГІЇ ТА МЕТОДИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ В МЕРЕЖІ ІНТЕРНЕТ

Інтернет став невід'ємною частиною життя мільярдів людей, забезпечуючи доступ до інформації, комунікаційних послуг та розваг. Однак, разом із зростанням ролі Інтернету, зростає і кількість загроз конфіденційності, які можуть поставити під сумнів безпеку особистих даних користувачів. Втрата конфіденційності може мати серйозні наслідки як для окремих осіб, так і для організацій.

Одним із ключових інструментів для забезпечення конфіденційності в Інтернеті є шифрування. Шифрування даних під час передачі та зберігання дозволяє захистити інформацію від несанкціонованого доступу. Протоколи SSL/TLS, які використовуються для захисту веб-сайтів, забезпечують безпечний обмін даними між користувачем і сервером.

Віртуальні приватні мережі (VPN) також широко використовуються для забезпечення конфіденційності. VPN створюють зашифровані тунелі між пристроєм користувача та Інтернетом, що дозволяє приховати IP-адресу та місцезнаходження користувача, а також забезпечити захист даних під час їх передачі.

TOR (The Onion Router) є ще одним потужним інструментом для захисту конфіденційності. TOR мережа дозволяє користувачам анонімно переглядати Інтернет, приховуючи їхні дії та місцезнаходження через багатошарове шифрування та переспрямування трафіку через численні вузли [1].

Окрім традиційних методів, існують також новітні технології та підходи, які спрямовані на підвищення рівня конфіденційності:

- шифрування від кінця до кінця (End-to-End Encryption);
- засоби захисту конфіденційності на основі блокчейну;
- анонімізація даних;
- диференціальна конфіденційність;
- Zero-Knowledge Proofs (ZKP);
- псевдонімізація.

Кіберзлочинність є однією з основних загроз конфіденційності в Інтернеті. Зловмисники використовують фішинг, шкідливе програмне забезпечення та інші методи для отримання доступу до особистих даних користувачів. Витоки даних є ще однією серйозною проблемою, яка може призвести до розголошення конфіденційної інформації мільйонів людей.

Слід також відзначити ризики, пов'язані з використанням соціальних мереж та мобільних додатків, які часто збирають і зберігають великі обсяги особистих даних, іноді без належного інформування користувачів або їхньої згоди.

Одним із найбільших викликів у сфері забезпечення конфіденційності є швидкий розвиток технологій, які можуть змінювати правила гри. Наприклад, зростання використання Інтернету речей (IoT) створює нові загрози для конфіденційності, оскільки ці пристрої часто мають слабкий захист і можуть бути зламані для отримання доступу до особистих даних [2].

Перспективи розвитку технологій захисту конфіденційності включають використання штучного інтелекту для виявлення та запобігання загрозам, а також розвиток нових методів шифрування, таких як квантове шифрування, яке може забезпечити ще більш надійний захист даних.

Забезпечення конфіденційності в мережі Інтернет є надзвичайно важливим і водночас складним завданням, яке потребує комплексного підходу. Сучасні технології, такі як шифрування, VPN та TOR, надають потужні інструменти для захисту даних, проте залишаються значні виклики, пов'язані з кіберзлочинністю, витоками даних та розвитком нових технологій.

Правове регулювання відіграє важливу роль у захисті конфіденційності, але потребує постійного оновлення та адаптації до нових загроз [3]. Інтеграція новітніх технологій, таких як штучний інтелект і квантове шифрування, може значно підвищити рівень захисту конфіденційності в майбутньому.

Успішне забезпечення конфіденційності в Інтернеті вимагає співпраці між урядами, технологічними компаніями та користувачами. Освіта користувачів щодо загроз та методів захисту їх особистих даних є ключовим елементом у боротьбі за конфіденційність. Лише спільними зусиллями можна забезпечити безпечне та конфіденційне середовище в Інтернеті для всіх користувачів.

Література

1. Безпека в інтернеті та захист персональних даних. – Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/50166/1/Bezpeka_v_Interneti_2022.pdf.
2. Сабадаш В.П. Деякі аспекти проблеми розповсюдження шахрайства в Інтернеті // Держава і право, 2005. – Вип. 30. – С. 452-457.
3. Гадомський Д.В. Сучасні тенденції захисту авторських прав у мережі Інтернет // Порівняльно-правові дослідження, 2008. – № 1. – С.139-141.

І.О. Черноус, Д.С. Сало, О.М. Трофимович
Державний університет інформаційно-комунікаційних технологій, м. Київ

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗКРИТТЯ ЗЛОЧИНІВ

Робота правоохоронних органів потребує вміння бачити неочевидні закономірності та зіставляти різнорідні докази. Але людина-слідчий не завжди може відстежити логіку дій злочинця або впізнати його почерк. В таких ситуаціях їй можуть допомогти цифрові інструменти [1] загалом та штучний інтелект (ШІ) зокрема.

Доведено, що 90% даних у світі є неструктурованими, і без технологій обробки великих даних проаналізувати їх неможливо. ШІ може об'єднати структуровані та неструктуровані дані з внутрішніх і зовнішніх джерел та застосувати до них різноманітні інструменти аналізу, серед яких – прогностична аналітика, розпізнавання облич, машинне навчання та аналітика когнітивних даних, тому ШІ-рішення надзвичайно корисні для поліцейських та детективів, щоб краще прочитати «почерк» злочинців у величезній кількості неструктурованих зібраних даних – відео, зображеннях, електронних доказах тощо. І це не мрії на майбутнє, а реальність: наприклад, наразі 70% поліцейських відділків світу мають доступ до тієї чи іншої форми інструментів розпізнавання облич.

Ось як вони використовують штучний інтелект у своїй роботі:

1. Аналіз місця злочину.

Злочинці завжди залишають сліди на місці злочину або недалеко від нього. Задача поліцейських – знайти їх та пов'язати в єдину систему, яка наблизить до розкриття злочину. ШІ може допомогти в пошуку закономірностей та збігів у цих даних.

Наприклад, дослідники з Університету Леона (Іспанія) навчили нейронні мережі виявляти докази, залишені на місці злочину [2]. Спочатку слідчі роблять детальну фотозйомку всього навколо, а потім передають ці дані нейромережі, яка їх аналізує.

Як саме це працює: спочатку нейромережу навчили на основі даних про попередні злочини – щоб ШІ-інструменти могли створити певні патерни поведінки зловмисників. Окрім того, їй пропонували можливі шаблони, які злочинці використовують у різних ситуаціях. Отримавши цей набір даних для аналізу, нейромережа навчилася не лише допомагати у визначенні злочинця, але й зіставляти декілька злочинів. Таким чином, наприклад, можна розкрити серію грабежів у певному районі, здійснених одним зловмисником.

2. Ідентифікація підозрюваних.

Один з найефективніший напрямків використання штучного інтелекту в кримінальних розслідуваннях, який уже порівняно давно та активно використовується, – це ідентифікація (впізнавання) злочинців. Для цього застосовують інструменти розпізнавання облич. Задача розпізнавання образів загалом і розпізнавання облич зокрема – це фундаментальні завдання теорії інтелектуальних систем, над розв'язанням яких вчені працюють давно з різним рівнем успішності.

Найвідоміша сфера використання цієї технології – сучасні *OCR-системи (optical character recognition – системи оптичного розпізнавання символів)*, які вже давно успішно можуть ідентифікувати текст на зображенні (почасти навіть рукописний) і перетворювати його на текстовий документ [3]. Людина вручну ніколи не зможе переглянути й проаналізувати велику кількість знімків або відеофрагментів, порівняти їх з оригіналом і дійти правильних висновків. Натомість системи розпізнавання вміють робити це з великою точністю. Цей показник може досягати 99,7%, а Facebook DeepFace може визначити, чи належать два сфотографовані обличчя одній людині, з точністю 97%. Крім того, автоматизовані інструменти вміють аналізувати контент, недоступний у так званому «відкритому вебі». Вже існують інструменти аналізу осіб, що працюють із контентом глибинного (deep) вебу і темного сегмента мережі (dark web). Технології розпізнавання облич активно застосовуються правоохоронними органами в усьому світі – не лише за фото підозрюваного, але й для аналізу відеопотоку. Відомий приклад

ефективності подібних систем – історія про те, як репортер BBC провів експеримент і перевірив, чи дійсно ці інструменти такі успішні. Його цікавило, наскільки швидко його ідентифікують системи розпізнавання, що використовуються в Китаї. Щоб його знайти, поліції знадобилося 7 хвилин – від моменту потрапляння його фото в базу даних до власне затримання.

3. Профілактика злочинів та оперативна реакція на критичні події.

Інструменти штучного інтелекту також значно спрощують інші задачі правоохоронців, у тому числі допомагають оперативніше реагувати на критичні ситуації. На приклад, поліція може швидко відреагувати на вчинення злочину, як-от випадок стрілянини в місті: датчики в місцях скупчення людей можуть оперативно повідомити чергових поліцейських про вчинення злочину ще до того, як про це сигналізують свідки. Ба більше, такі датчики в поєднанні з камерами з розпізнаванням облич зможуть відстежити переміщення підозрюваного у великому місті та допомогти визначити найімовірніше місцеперебування стрілка.

Підбиваючи підсумки: Користь від ШІ превалює над пересторогами та ризиками. Нагальним є регулювання «всього життєвого шляху ШІ», починаючи з ідеї його створення, котра повинна відповідати етичним критеріям та слідувати із домінанти антропоцентричного підходу. «Зарегульовувати» ШІ на шкоду його розвитку теж не слід. Відшукання стану цієї рівноваги є надважливим.

Література

1. Basysta I.V., Udovenko Zh. V. Review of trends regarding artificial intelligence and its prospects for procedural decisions during criminal proceeding // Uzhhorod National University Herald, 2024. – No. 81. – P.19-38. – Режим доступу до ресурсу: https://doi.org/10.24144/2307-3322.2024.81.3.3.

2. Ковтун В.О., Рвачов О.М. Огляд та перспективи використання технологій штучного інтелекту в правоохоронній діяльності / Використання технологій штучного інтелекту у протидії злочинності: матеріали науково-практичного онлайн-семінару, 5 листопада 2020 р., 2020. – Харків. – С.44-51.

3. Babuta A., Oswald M. Data Analytics and Algorithms in Policing in England and Wales Towards A New Policy Framework / Royal United Services Institute for Defence and Security Studies: Occasional Paper. – London, February 2020. – 49 p.

М.М. Запорожченко, К.В. Рубель
Державний університет інформаційно-комунікаційних технологій, м. Київ

ТЕЙЛГЕЙТИНГ ЯК ТЕХНІКА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ: АНАЛІЗ МЕТОДІВ, НАСЛІДКІВ ТА ЗАХОДІВ ПРОТИДІЇ

Соціоінженерні атаки експлуатують людську психологію, а не технічні вразливості для отримання доступу до конфіденційної інформації або зон з обмеженим доступом. У всьому спектрі соціоінженерних атак виділяється своєю простотою та ефективністю техніка «тейлгейтинг» (англ. «tailgating»), яка в традиційному розумінні передбачає

ситуацію, коли порушник отримує доступ до зони з обмеженим доступом, слідуючи за уповноваженою особою, не маючи при цьому належної ідентифікації або дозволу.

Хоча здебільшого «тейлгейтинг» стосується фізичного середовища, подібні атаки можуть бути здійснені і у віртуальному середовищі, наприклад, у захищених мережах або комп'ютерних системах.

У фізичному контексті ця техніка зазвичай передбачає, що несанкціонована особа слідує за уповноваженою особою через двері або ворота, не будучи зупиненою чи запитаною службою безпеки або охороною організації. Це може статися, якщо уповноважена особа притримує двері для сторонньої особи або якщо співробітники служби безпеки не перевіряють посвідчення тих, хто входить. Також зловмисник може вступити з уповноваженою особою в розмову, представляючись працівником, підрядником або кур'єром (їжа, посилки, документи), щоб увійти в довіру, при цьому він може використовувати різноманітні способи маскування. І, нарешті, зловмисник може спробувати потрапити у захищені зони організації під час високого трафіку, наприклад, під час зміни, коли охорона може бути менш пильною, і багато людей заходять одночасно.

Наслідки реалізації такої атаки можуть включати несанкціонований доступ до конфіденційних даних, крадіжки обладнання (USB-накопичувачі, SSD-накопичувачі, сервери, ноутбуки, ПК), шпигунство або навіть фізичну шкоду. У таких середовищах, як корпоративні офіси, центри обробки даних та урядові об'єкти з обмеженим доступом, ризики є особливо відчутними.

«Тейлгейтинг» у віртуальному середовищі передбачає, що неавторизований користувач може отримати доступ до захищеної мережі або комп'ютерної системи, використовуючи облікові дані авторизованого користувача. Це може статися, якщо авторизований користувач ненавмисно дозволяє неавторизованій особі використовувати свої облікові дані, свій пристрій або якщо неавторизована особа перехоплює автентифікаційну інформацію за допомогою фішингових атак чи в інший спосіб [1].

«Тейлгейтинг» використовує кілька психологічних принципів. По-перше, люди зазвичай дотримуються соціальних норм, таких як ввічливість і доброзичливість, що робить їх менш схильними до того, щоб ставити запитання тому, хто йде слідом за ними. По-друге, зловмисники можуть видавати себе за авторитетну особу, що не дає іншим ставити під сумнів їхню легітимність. По-третє, у місцях скупчення людей люди можуть припустити, що хтось інший перевірив повноваження зловмисника, що призводить до колективної втрати пильності.

Таким чином, ризик стати об’єктом успішної реалізації такої атаки зростає, якщо організація має багато працівників, які часто входять і виходять із зон з обмеженим доступом; якщо організація має декілька точок входу до зон з обмеженим доступом; якщо організація регулярно отримує доставки; якщо в організації працює багато підрядників; якщо для персоналу організації не проводилася належна підготовка з фізичної та кібербезпеки.

Для ефективного захисту від несанкціонованого доступу до зон з обмеженим доступом необхідний комплексний підхід, що включає фізичні, організаційні та технічні заходи безпеки [2]:

- слід встановити камери відеоспостереження на входах і виходах, щоб контролювати потік людей, які входять і виходять з будівлі або охоронюваних зон. Окрім

того, що безперервне спостереження допомагає виявити підозрілу діяльність, встановлені камери слугують стримуючим фактором для потенційних зловмисників;

- варто розмістити персонал охорони на входах для візуальної перевірки документів/посвідчень та спостереження за поведінкою осіб, які заходять до будівлі;
- слід використовувати електронні системи контролю доступу, такі як картки-ключі або біометрична автентифікація, щоб гарантувати, що доступ до будівель або захищених зон буде обмежений лише уповноваженими особами;
- доцільно впровадити системи виявлення обхідних шляхів, що використовують такі технології, як відеоаналітика, датчики руху та RFID, для виявлення та сповіщення персоналу служби безпеки, коли неавторизована особа слідує за авторизованою особою в зону з обмеженим доступом;
- обов'язковим є забезпечення навчання співробітників, щоб вони були здатні розпізнавати підозрілу поведінку та повідомляти про неї, і були повідомлені про важливість дотримання належних заходів безпеки, наприклад, тримати двері зачиненими, не дозволяти входити незнайомцям тощо;
- як більш доступну альтернативу СКУД можна встановити захисні фізичні бар'єри, такі як турнікети або двері, що обертаються, для контролю доступу до захищених зон, які запобігають несанкціонованому доступу та гарантують, що за один раз туди може увійти лише одна особа;
- слід впровадити суворі протоколи безпеки для роботи з відвідувачами, кур'єрами або підрядниками, включаючи ретельну перевірку для підтвердження особи та постійний супровід уповноваженим персоналом.

Таким чином, хоча команди з кібербезпеки в першу чергу зосереджені на виявленні та зменшенні ризиків цифрової безпеки, дуже важливо визнати, що фізичні вразливості також можуть поставити під загрозу безпеку даних і конфіденційність. Фізичні пристрої, що містять конфіденційну інформацію, є потенційними цілями для кіберзлочинців, що робить фізичну безпеку важливим компонентом комплексних стратегій кіберзахисту. Розуміючи механізми та психологічні принципи, що лежать в основі «тейлгейтингу», та інтегруючи перелічені превентивні заходи, організації можуть значно посилити свій захист від несанкціонованого доступу, захистивши як фізичні, так і цифрові активи від потенційних порушень безпеки.

Література

1. Tailgating Attack: Examples and Prevention. Fortinet. – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/tailgating-attack.

2. What Are Tailgating Attacks and How to Protect Yourself From Them. McAfee. – Режим доступу до ресурсу: https://www.mcafee.com/blogs/internet-security/what-are-tailgating-attacks.

О.А. Порохницький, Я.М. Яресько
Державний університет інформаційно-комунікаційних технологій, м. Київ

ЗАСТОСУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ТА ШТУЧНОГО ІНТЕЛЕКТУ В ЛОГІСТИЧНІЙ СФЕРІ: ПЕРСПЕКТИВИ ТА ПРОБЛЕМАТИКА

Швидкий розвиток технологій призвів до глобального питання серед багатьох країн та компаній по всьому світу. В даному випадку це оптимізації усіх процесів для прискорення обробки тієї великої кількості процесів та даних що людина самостійно не може обробити. Але вихід був знайдений у напрямку розвитку інтелектуальних систем.

Крім того, за допомогою штучного інтелекту(ШІ) або інтелектуальної системи (ІС) можна відстежувати найменші зміни у поведінці споживачів, логістичному питанні та відповідно у тому числі роздрібних покупців. Це дає змогу роздрібним торговцям поліпшувати увесь ланцюг постачання [1].

Перспективи застосування ІС та ШІ в логістиці

Зв'язок "транспортний засіб з усіма" (V2X) – це передача інформації від транспортного засобу до будь-якого пристрою, який може вплинути на транспортний засіб, і навпаки. За словами Ван Ліна, директора групи інтелектуальних мобільних рішень служби IoT в Advantech, "реалізація інтелектуального транспорту включає не тільки розвиток автобусів, метро і залізниць, а й людей, навколишнє середовище та інше пов'язане обладнання. Поєднання 5G, ШІ, граничних обчислень, LiDAR та IoT є ключем до реалізації цього розвитку. Advantech та її клієнти будуть впроваджувати інтелектуальне майбутнє зв'язку V2X та отримувати з нього вигоду" [2].

Прикладом даного покращення може слугувати розвиток 5G та штучного інтелекту що сприяли в свою чергу на еволюцію різних інтелектуальних додатків саме для залізничного транспорту що і призвело до покращення та оптимізації даного процесу. Кунхонг Чен, менеджер транспортного сектору групи промислового IoT компанії Advantech, зазначив, що у минулому операційні цілі метрополітену Тайбея були зосереджені на збільшенні пропускної здатності. Проте зараз їх цілі змінились на підвищення безпеки та якості для користувача та відповідно сами працівників. Відповідно, метрополітен Тайбея активно займається модернізацією своїх систем, зокрема, систем руху та сигналізації. Так, оцінка електронних систем, пов'язаних з безпекою (Safety Integrity Level, SIL), була підвищена з SIL 2 до SIL 4. Аналогічно, система сигналізації та обробки даних (European Train Controlling System/ETCS) була підвищена з ETCS 2 до ETCS 4. Ці удосконалення роблять значний внесок у підвищення безпеки. Крім того, використовуючи програми штучного інтелекту та LiDAR, а також автоматичне керування поїздами, оператори можуть будувати моделі керування, орієнтовані на інтелектуальні операції [2].

Світові лідери в галузі баз даних, такі як SAP, Microsoft, Oracle і IBM, інтегрують штучний інтелект у свої пропозиції. То ж в цьому напрямку почався розвиток та відповідно оновлення наявного ПЗ та алгоритмів для оптимізації та автоматизації виконання. Штучний інтелект використовується для управління автоматичними штабелерами (AGV) та складними дронами на складах, що дозволяє зменшити людський фактор в даній ситуації та бачити чіткі дані стосовно всіх процесів [3].

У плануванні автопідприємств алгоритми програмного забезпечення, які враховують погодні та дорожні умови в реальному часі, щоб оптимізувати маршрутизацію транспорту. Технології штучного інтелекту зменшують потребу у великій кількості транспортних засобах та ефективно розраховувати витрати та доходи, пов'язані із замовленнями клієнтів. [3]

У сучасних вантажних транспортних засобах штучний інтелект використовується для ідентифікації дорожніх знаків та розміток, а також реагування на погоду та дорожні умови, забезпечуючи комфортне керування. Компанія HERE розробила цифрову програму, яка контролює безпеку на дорозі за допомогою аналізу зображень із фронтальних камер, смартфонів та відеореєстраторів [3].

У майбутньому ШІ зможе керувати автономними вантажівками та обробляти дані з інших транспортних засобів та інфраструктури. Вже зараз вантажівки оснащуються пристроями, що відслідковують стан та знос вузлів автомобіля, що дозволяє знизити ризики поломок та прогнозувати терміни технічного обслуговування на основі реального стану машини [3].

Проблематика застосування ІС та ШІ в логістиці

Проблеми і ризики використання ШІ в транспортуванні логістиці

Хоча технологія штучного інтелекту широко використовується в різних сферах, вона не є повністю безпечною і має своїх критиків. Однак, є беззаперечним фактом, що технології ШІ будуть все більше впроваджуватися в майбутньому [3].

Існують ризики зменшення трудової зайнятості в контексті широкого застосування ШІ. Економісти не мають єдиного погляду на те, скільки робочих місць може бути замінено штучним інтелектом, оцінки коливаються від 5% до 35%. Також виникають дискусії щодо морально-етичних аспектів використання цієї технології. Група експертів, створена в рамках Європейської комісії, займається етичною та моральною відповідальністю машиною, що вимагає ШІ [3].

Поставлені запитання дають кілька прикладів: якщо автономний автомобіль під керуванням штучного інтелекту стикається із ситуацією, де наїзд на людей неминучий, яким чином вибрано, кого врятувати – двох людей похилого віку або групу дітей? Навіть людям було важко прийняти правильне рішення в такій ситуації, а як зробити це машині? Хто бере на себе відповідальність, коли застосування ШІ зазнає невдачі [3]?

Підсумовуючи все вище наведене можна зазначити що інтеграція ШІ та ІС в логістичній сфері – це не варіативність, а висока потреба. Що в свою чергу зменшує помилки, людський фактор, прискорює доставку та обробку даних та надає інформацію стосовно реального стану речей як на підприємстві так його логістичних процесів. Тобто оптимізує усі процеси та автоматизує роботу. Відповідно навіть наявні проблеми в цій сфері можна цілком вирішити, створивши відповідні умови контролю, за устаткування та самою системою, створити нові безпечні вакантні посади для працівників та постійне покращення алгоритмів.

Література

1. Перспективи застосування штучного інтелекту в логістиці. Lading – вантажні перевезення. – Режим доступу до ресурсу: https://lading.ua/news/perspektivi-zastosuvannya-shtuchnogo-intelektu-v-logistici/ (дата звернення: 28.05.2024).

2. Розвиток інтелектуального транспорту за допомогою штучного інтелекту, 5G та граничних обчислень. ПРОКСИС™ – промислові комп'ютери та системи. – Режим доступу до ресурсу: https://www.proxis.ua/uk/show-article/531/ (дата звернення: 28.05.2024).

3. Використання штучного інтелекту в управлінні транспортними потоками та логістичними реакціями. Транспортная компания Cargofy.ua: Послуги перевезення автомобільнимтранспортом в Україні. – Режим доступу до ресурсу: https://cargofy.ua/uk/blog/vikoristannya-shtuchnogo-intelektu-v-upravlinni-transportnimi-potokami-ta-logistichnimi-reakciyami (дата звернення: 28.05.2024).

O.V. Budzynskyi
State University of Information and Communication Technologies, Kyiv

MAIN DIRECTIONS FOR THE APPLICATION OF INTELLIGENT SYSTEMS TO PROTECT CORPORATE DATABASES

Modern corporate databases store a vast amount of sensitive information, which is a valuable target for cybercriminals. Traditional protection methods often prove insufficient in the face of the increasing complexity of threats and require the development of new approaches to database security, aimed at the intellectualization of the methods being developed.

The field of intelligent systems (IS) has phenomenally expanded over the years, starting from the 1940s, both in terms of the range of methods and the number of applications where they have often provided a competitive advantage compared to other approaches [1].

IS encompasses a range of methods that work synergistically to provide flexible data processing capabilities in various forms. Intelligent systems based on machine learning and artificial intelligence (AI) technologies offer new opportunities for detecting and preventing attacks, adapting to changes in the cyber environment.

As noted in scientific research [2-4], the current promising directions for the application of intelligent systems to protect corporate databases include: anomaly detection and threat prediction; automation of incident response; protection against insider threats; use of blockchain technologies for ensuring integrity, and threat intelligence analysis.

For anomaly detection and prediction, models of normal user behavior in databases are created based on historical data, which, through comparison, detect unusual activity (e.g., accessing data during non-working hours), non-standard database queries, and suspicious network activity that may indicate threats. Analyzing behavior patterns and using IS to identify signs of attack preparation allows for proactive measures to protect databases.

Intelligent SOAR (Security Orchestration, Automation, and Response) systems automate the processes of responding to security incidents. Using AI for orchestrating actions enables quick responses to threats, minimizing the human factor. Examples include automatic blocking of suspicious accounts or isolating compromised systems. Intelligent bots can perform routine monitoring and incident response tasks. They are capable of quickly analyzing large volumes of data and identifying threats in real time, which significantly enhances the effectiveness of database protection.

AI-based systems can monitor user actions within an organization, detecting anomalies that may indicate internal threats. This includes unauthorized attempts to access confidential data or changes to database settings. User profiling using machine learning allows for the creation of individual behavior models for each user. This helps to detect even slight deviations from normal behavior, which may indicate account compromise.

The use of blockchain technology for storing audit logs ensures their immutability and integrity, making it impossible to tamper with records and allowing for an accurate reconstruction of all actions that have occurred in the database. Blockchain technology can be used to create distributed protection systems that provide reliable data storage and make unauthorized access more difficult.

IS can automatically enrich threat data from various intelligence sources. This approach allows for the quick acquisition of up-to-date information about new vulnerabilities and attacks, helping to take appropriate protective measures. IS are capable of correlating data from different sources and identifying links between various incidents. This provides a complete picture of an attack and a better understanding of its mechanisms, which helps to protect databases more effectively.

Data protection is a key issue during the implementation of cloud services [5]. The project "RestAssured – Secure Data Processing in the Cloud," funded by the European Union's Horizon 2020 research and innovation program, aims to protect data in the cloud through innovative security solutions, data lifecycle management methods, runtime adaptation, and automated risk management. Secure cloud computing is crucial for business success and the adoption of decentralized cloud services by end-users, and thus it is vital for fostering the growth of Europe's Digital Single Market. RestAssured is expected to provide solutions to specific technical challenges in cloud data protection (such as geolocation restrictions on personal data) imposed by the dynamic, multi-stakeholder, and decentralized nature of federated cloud systems. RestAssured will ensure the protection of sensitive business and citizen data in the cloud by combining four pillars of innovation: integrating fully homomorphic encryption for processing data without decryption with cloud inclusion of SGX hardware for secure data processing; stringent policies for decentralized lifecycle data management; models@runtime to ensure data protection; automated risk management to protect data during execution. The primary impact of RestAssured will be to ensure the free and seamless movement of data within the EU while complying with data protection regulations such as the EU Data Protection Directive and its successor, the General Data Protection Regulation (GDPR).

Conclusion

Intelligent systems based on machine learning and artificial intelligence offer new opportunities for protecting corporate databases. They allow for the detection of anomalies and threat prediction, automation of incident response, protection against insider threats, and the use of threat intelligence to enrich threat data. Integrating these technologies into database security systems helps to enhance security levels and effectively counter modern cyber threats.

References

1. Hines E., Leeson M., Llobet E., Iliescu D., Yang J. Intelligent Systems: Techniques and Applications. Printed in the Netherlands. – 2008. – 561 p.

2. Bayamlıoğlu, E., Leenes, R. The ‘rule of law’ implications of data-driven decision-making: a techno-regulatory perspective // Law, Innovation and Technology, 2018. – № 10(2). – P.295-313. – URL: https://doi.org/10.1080/17579961.2018.1527475.

3. Curry E. The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches. New Horizons for a Data-Driven Economy // Springer, Cham, 2016. – P.29-37. – URL: https://doi.org/10.1007/978-3-319-21569-3_3.

4. Zheng W. Opaque: An oblivious and encrypted distributed analytics platform / 14th USENIX Symposium on Networked Systems Design and Implementation (NSDI 17), 2017. – P.283-298.

5. Mann Z.Á. Secure data processing in the cloud. Advances in Service-Oriented and Cloud Computing / Workshops of ESOCC 2017, Oslo, Norway, September 27-29, 2017, Revised Selected Papers 6. – Springer International Publishing, 2018. – P.149-153. – URL: https://doi.org/10.1007/978-3-319-79090-9_10.

К.О. Папук, С.В. Галун
Державний університет інформаційно-комунікаційних технологій, м. Київ

СТВОРЕННЯ МЕДИЧНОГО ГУМАНОЇДА-ЛЯЛЬКИ SAMANTA ДЛЯ ПРАКТИКИ СТУДЕНТІВ МЕДИКІВ

Постановка задачі. Використання штучного інтелекту в медичній освіті та тренуванні стає все більш поширеним, але існує прогалина між теоретичними знаннями та практичними навичками. Ця проблема може бути вирішена за допомогою інноваційного тренувального робота-гуманоїда, який імітує реалістичні медичні сценарії [1]. Наразі у медицині використовуються лише застарілі польські аналоги [2], при цьому зберігається великий попит на розробку більш інноваційний варіант. Такий робот-гуманоїд використовує передові технології для створення реалістичних сценаріїв, що дозволяють медичним працівникам набувати практичних навичок в безпечному та контрольованому середовищі.

Мета дослідження: Головною метою цього дослідження є розробка алгоритмів штучного інтелекту, які можуть аналізувати медичні дані для створення реалістичних і складних тренувальних сценаріїв, а також створення натуралістичної ляльки гуманоїда, на яких і будуть практикуватись молоді фахівці. Потрібні алгоритми використовують великі обсяги медичних даних для генерації реалістичних сценаріїв [1], що відображають різноманітність медичних станів та ситуацій, з якими можуть зіткнутися медичні працівники. Сам робот являтиме собою практично повну імітацію людини [3]: наближені до реальних органи, кровообіг, можливість змінювати температуру, та вологість окремих ділянок тіла. Робота з великою кількістю даних дає змогу задавати різні показники на ляльці, а також оптимізувати роботу персоналу, оскільки все буде проводитись автоматизовано.

Результати дослідження: Надання інформації від фахівців медиків дало змогу створити базу даних на сервері. Дані звіти, використовуються для навчання нейронної мережі, сутність якої – надавати симптоми за визначеною хворобою які далі будуть відображатися вже на медичній ляльці. Робот-гуманоїд був розроблений таким чином,

що його частини (кінцівки, торс, голова) легко замінюються та модифікуються для відтворення різних медичних станів. Використання передових сенсорів дозволяє відстежувати взаємодію між роботом-гуманоїдом та медичним персоналом, збираючи дані про ефективність виконання процедур. Ці сенсори можуть відстежувати різні параметри, включаючи силу, швидкість та точність рухів, що дозволяє медичним працівникам отримувати відгук про свої навички та вдосконалювати їх. Для роботи за даними в нейромережі будуть використовуватись технологія CRUD, бази на PSQL, нейромережі моделі GLM, та інші джейнерики [4].

CRUD – це абревіатура, що означає Create (Створити), Read (Прочитати), Update (Оновити) та Delete (Видалити). Це чотири основні операції, які програмне забезпечення повинно виконувати. Кожна літера в абревіатурі CRUD відповідає методу HTTP-запиту: “Створити” відповідає POST, “Прочитати” – GET, “Оновити” – PUT або PATCH, “Видалити” – DELETE. Ці операції є основними для будь-якої програми, що працює з базами даних. Вони дозволяють користувачам створювати дані, мати доступ до даних, оновлювати або редагувати дані та видаляти дані.

Узагальнена лінійна модель (GLM) – це фундаментальний фреймворк який використовують у нейронауці для моделювання активності нейронів. Наприклад, в одному з туторіалів Neuromatch Academy метою було моделювання потягу спайків ретинальної ганглійської клітини шляхом налаштування временного рецептивного поля спочатку з лінійно-гаусової GLM (також відомої як модель регресії за методом найменших квадратів), а потім з Пуассоновою GLM (також відомою як модель “ Лінійно-нелінійно-Пуассон”).

Висновки та перспективи: Це дослідження підкреслює важливість використання штучного інтелекту в медичній освіті. Використання робота-гуманоїда може забезпечити доступ до широкого спектру медичних випадків, які можуть бути рідкісними або складними для відтворення в реальному житті, підвищуючи рівень підготовки медичних працівників, знижуючи медичні помилки та покращуючи якість пацієнтського догляду. В майбутньому ці технології можуть бути використані для створення більш складних і реалістичних сценаріїв, що дозволить медичним працівникам набувати навичок, необхідних для роботи в надзвичайних ситуаціях.

Література

1. Робота з базою даних на PQSL з використанням CRUD. – Режим доступу до ресурсу: How to Create a CRUD API Using Node, PostgresSQL, and Express (makeuseof.com).

2. Medical Crash Kelly. – Режим доступу до ресурсу: https://laerdal.com/products/simulation-training/emergency-care-trauma/crash-kelly/shop.

3. General Language Model Pretraining with Autoregressive Blank Infilling. – Режим доступу до ресурсу: [2103.10360] GLM: General Language Model Pretraining with Autoregressive Blank Infilling (arxiv.org).

4. Work with GLM, GAM. – Режим доступу до ресурсу: 5.3 GLM, GAM and more Interpretable Machine Learning (christophm.github.io).

Є.Є. Кузьменко
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ОБЛІКУ ТА АНАЛІЗУ ДАНИХ

Актуальність проблеми.

В часи економічної нестабільності, бізнесу важливо максимально розширити свою присутність на ринку.

Постановка задачі.

Задачею дослідження є розробка програмного забезпечення для обліку та аналізу даних.

Мета дослідження.

Метою дослідження є автоматизація процесу обліку та аналізу даних рейтингу викладачів.

Результати дослідження.

Об'єкт дослідження – процес розробки програмного забезпечення для обліку та аналізу даних рейтингу викладачів. Предмет дослідження – технології розробки програмного забезпечення для обліку та аналізу даних рейтингу викладачів

Для створення концепції майбутнього продукту було обрано метод проектування «wireframing». Wireframe – це прототип, який демонструє, які елементи інтерфейсу мають бути присутні на сторінці [4]. Схема розробленої бази даних показана на рис. 1.

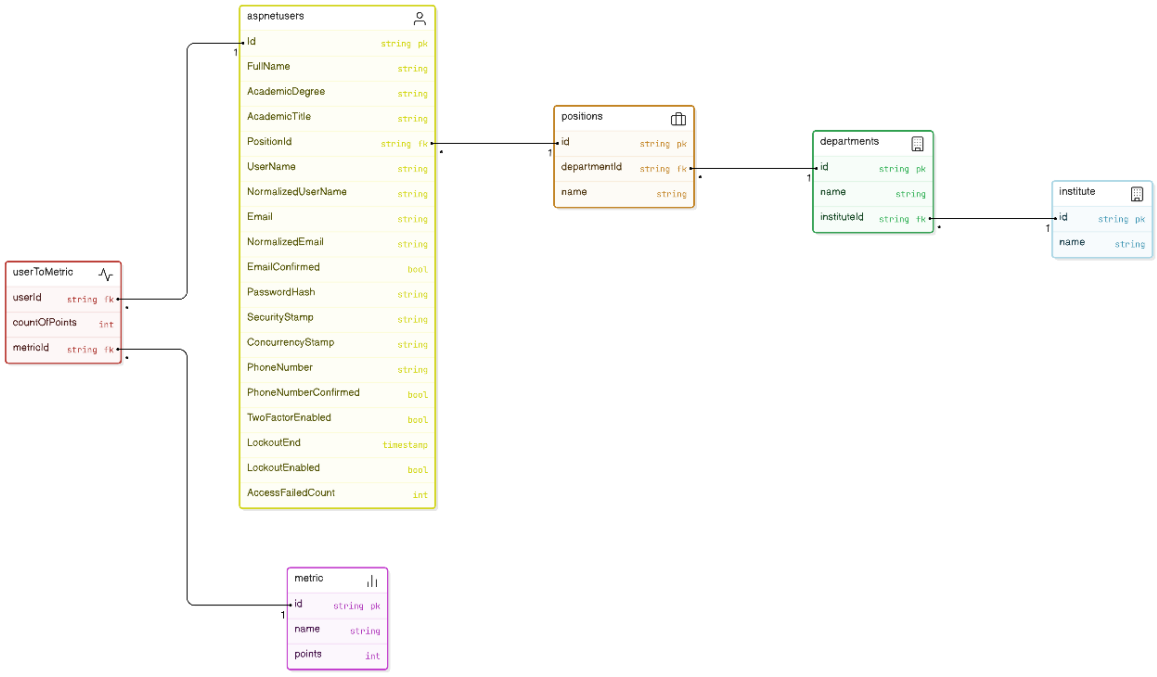

Рис. 1. Схема баз даних

Після створення прототипу сторінки було складено критерії вибору технологічного стеку.

Вибір майбутнього стеку мав задовольняти такі критерії:

- Легкість знаходження нових розробників
- Можливість переходу на інші сторінки без повного перезавантаження сторінки

• Детальна документація по використанню

З урахуванням цих критеріїв вибір пав на екосистему мови програмування JavaScript.

JavaScript - це мова програмування, яка дозволяє реалізувати складні функції на веб-сторінках. [3] Вона також є найвживанішою мовою програмування у світі [2].

Фреймворком був вибраний Next.js. Next.js - це React фреймворк для створення веб-додатків повного стеку (backend + frontend) [1].

На цей вибір вплинуло багато факторів, такі як перехід на інші сторінки без перезавантаження, довготривала підтримка, відкритий код та велика спільнота розробників які його використовують.

Для зберігання даних була використана реляційна база даних MySQL через можливість роботи з великими обсягами даних та зручність у використанні.

Аутентифікація за допомогою паролю була реалізована за допомогою бібліотеки NextAuth.js.

Висновки та перспективи.

Метод прототипування інтерфейсів «Wireframe» значно прискорює розробку користувацьких інтерфейсів.

При виборі майбутнього технологічного стеку потрібно враховувати

особливості кожного окремого проекту.

Популярні мови програмування мають багату екосистему яка створювалася роками та використання якої може сильно пришвидшити розробку продукту.

Література

1. What is wireframing?. Experience UX. – Режим доступу до ресурсу: https://www.experienceux.co.uk/faqs/what-is-wireframing/ (дата звернення: 20.04.2024).

2. What is JavaScript?. MDN Web Docs. – Режим доступу до ресурсу: https://developer.mozilla.org/enUS/docs/Learn/JavaScript/First_steps/What_is_JavaScript (дата звернення: 20.04.2024).

3. JavaScript tutorial. W3Schools. – Режим доступу до ресурсу: https://www.w3schools.com/js/ (дата звернення: 20.04.2024).

4. Https://nextjs.org/docs. Docs Next.js. – Режим доступу до ресурсу: https://nextjs.org/docs (дата звернення: 20.04.2024).

Іг.І. Чичура, І.І. Туряниця
Ужгородський національний університет, м. Ужгород
Ів.І. Чичура
Інституту електронної фізики НАН України, м. Ужгород

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ВОЛОКОННО-ОПТИЧНИХ ДАТЧИКІВ ТЕМПЕРАТУРИ АМПЛІТУДНОГО ТИПУ У СУЧАСНИХ АВТОМАТИЗОВАНИХ СИСТЕМАХ КОНТРОЛЮ

Швидкий розвиток волоконно-оптичних технологій спонукає розвиток сучасних та ефективних датчиків фізичних величин на їх основі. Особливе місце серед значної

кількості волоконно-оптичних датчиків (ВОД) займають волоконно-оптичні датчики температури (ВОДТ) з амплітудною модуляцією оптичного сигналу, завдяки простоті їх конструкції, надійності та непоганим технічним характеристикам. Принцип роботи таких сенсорів базується на реєстрації зміни пропускання напівпровідника при зміні температури. Можливі дві схеми побудови ВОДТ з чутливим елементом з напівпровідника: прохідна (рис. 1 а) і відбиваюча (рис. 1 б).

В якості чутливого напівпровідникового елементу можуть бути використані кристали *GaAs, Si, Ge* та ін. [1-3], край поглинання яких знаходиться в ближній області інфрачервоного спектру. При конструюванні системи ВОДТ, останні потребують оптичного узгодження: спектр випромінювання світлодіода, область поглинання чутливого елементу і спектральна чутливість приймача випромінювання повинні знаходитись в одній спектральній області. Оскільки оптичні характеристики оптопари (світлодіод, фотодіод) практично задані, то для оптимізації оптичної узгодженості схеми залишається змінювати параметри чутливого елементу. У кристалічних напівпровідниках вони також незмінні.

Використання в якості чутливого елементу пластинки з напівпровідникового халькогенідного скла дає можливість варіювати властивостями матеріалу в широких межах, в тому числі і оптичними, змінюючи їх склад. При цьому також значно спрощується оптичне узгодження схеми, технологія виготовлення чутливих елементів, оптимізація їх інформаційних характеристик.

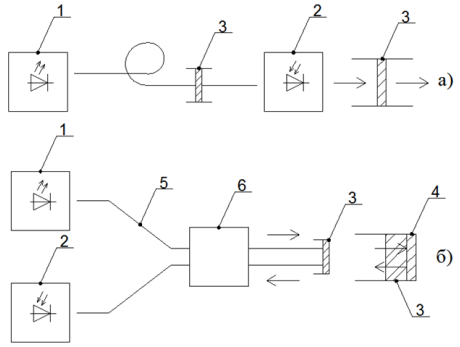

Рис. 1. Схеми ВОДТ прохідного (а) і відбиваючого (б) типів: 1 – світлодіод; 2 – фотодіод; 3 – чутливий елемент з напівпровідника; 4 – дзеркальна металева плівка (золото); 5 – оптичне волокно; 6 – волоконно-оптичний розгалужувач

Попередні наші дослідження показали, що оптимальна товщина чутливого елементу, для таких датчиків, знаходиться в межах 0,5 – 0,3 мм. Виготовлення таких пластинок традиційним методом шліфування і полірування є трудомістким, нетехнологічним. Враховуючи той факт, що запропоновані нами матеріали є аморфними напівпровідниками, в яких при збільшенні температури в'язкість зменшується. Тому при температурі близькій до температури розм'якшення *Tg* з'являється можливість формувати з крупинки такого скла пластинки чутливих елементів розчавлюючи її між двома прозорими пластинками із кварцового скла, слюди, оптичного волокна і ін. При стиковці одержаного таким способом чутливого елементу з оптичним волокном з невеликою площею поперечного перерізу (S = 0,1 ± 0,8 мм^2) робить таку технологію привабливою та простою.

Виготовлена за даною методикою пластинка з халькогенідного скла зі складом $As_{45}Se_{55}$ товщиною ≈0,6 мм була проаналізована на модифікованому спектрофотометрі

СФ-47 для дослідження зміни краю фундаментального поглинання при зміні температури. На основі цих даних була обрана робоча довжина хвилі оптичної схеми та побудована залежність пропускання чутливого елементу від температури, що приведено на рис. 2.

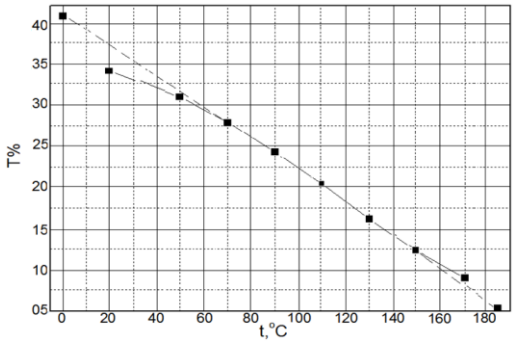

Рис. 2. Залежність пропускання пластини $As_{45}Se_{55}$ товщиною d = 0,6мм на λ_p = 0,808 мкм від температури

Висновки: Розроблена нами технологія отримання пластинок ХСН для використання їх в якості активного елементу ВОДТ суттєво спрощує процес виготовлення оптичних трактів для датчиків температури. Дані елементи можуть бути застосованими для дистанційного моніторингу температури у різних складних умовах роботи: нафтові та газові шахти, зона дії сильних радіаційних та електромагнітних полів та при ректифікації чи перегонці спиртів. Волоконно-оптичні датчики добре зарекомендували себе у різних автоматизованих системах контролю на виробництві та у промисловості і стали незамінними засобами вимірювання у складних та високоточних лабораторних установках.

Література

1. Yong Zhao, Min Rong, Yanbiao Liao. Fiber-optic temperature sensor used for oil well based on semiconductor optical absorption // IEEE Sensor Journal, 2003. – V.3. – No.4. – P.400-403.

2. Yuhan Ding X. Dai, T. Zhang. Low cost fiber-optic temperature measurement system for high voltage electrical power equipment // IEEE Transactions on instrumentation and measurement, 2010 – V.59. – is.4. – P.923-933.

3. Min Li, Yulin Li. Fiber-optic temperature sensor based on interaction of temperature-dependent refractive index and absorption of germanium film // Applied optics, 2011. – Vol. 50. – No.2. – P.231-236.

В.В. Цигика
Ужгородський національний університет, м. Ужгород

ЗАХИСТ ТЯГОВИХ ДВИГУНІВ РЕЙКОВОГО ЕЛЕКТРОТРАНСПОРТУ

Сучасна мікропроцесорна техніка та інформаційні технології спричиняють революційні зміни, в тому числі, і в рейковому електротранспорті, що ілюструє, зокрема, перехід на застосування асинхронного електроприводу з частотним керуванням.

Тенденція активного впровадження асинхронних тягових електродвигунів з частотно-регульованим керуванням спостерігається як на рухомому складі метрополітену, так і на залізничному транспорті [1, 2].

Проте, незважаючи на значні переваги інноваційних технологій, в електротранспорті широко застосовуються колекторні електродвигуни послідовного збудження, які характеризуються наявністю м'якої механічної характеристики n(M), що дозволяє плавно і в широких межах регулювати частоту обертання n, забезпечує належний пусковий момент $M_П$.

Як відомо, особливістю двигунів послідовного збудження є неможливість застосування для приводу механізмів, що працюють в режимі холостого ходу. Оскільки споживаний струм I, отже, відповідно, і магнітний потік Ф при малих навантаженнях сильно зменшується, частота побертання n різко зростає і може перевищити максимально допустиме значення (двигун «іде в рознос»). Зазвичай мінімально допустиме значення струму якоря для колекторних двигунів великої і середньої потужності становить $(0,2 \div 0,25)\cdot I_{ном}$.

Для запобігання можливості роботи двигуна без навантаження застосовують жорстке сполучення валу з приводним механізмом, наприклад, при з'єднанні з колісною віссю електровоза. Але в рейковому транспорті можливе явище так званого боксування, яке викликане зменшенням зчеплення між колесом і рейкою при реалізації тяги локомотива або моторного вагона і може виникати як при рушанні поїзда, так і в русі. Після зриву в боксування коефіцієнт тертя ковзання між колесом і рейкою різко знижується і спонтанний бокс важко зупинити. Для попередження боксування використовують модифікатори тертя (наприклад, подача піску) і автоматичне регулювання тягового моменту. Проте ці методи недостатньо ефективні для належного обмеження n, уникнення погіршення комутації та кругового іскріння на колекторі.

В даній роботі розглянуто пристрій захисту двигунів послідовного збудження від наслідків недовантаження, який, фактично, представляє собою реле мінімального струму. Застосовано безконтактний метод вимірювання сили струму якоря двигуна за допомогою датчика Холла. Сигнал з датчика подають на вхід компаратора, який порівнює його з опорною напругою і формує напругу управління. При величині струму $0,25\cdot I_{ном}$ транзисторний ключ розмикає нормально замкнений контакт контактора, який відключає живлення електродвигуна.

Література

1. Сулим А. Процедура вибору асинхронного тягового електроприводу для інноваційного рухомого складу метрополітену / Збірник наукових праць ДУІТ. Серія «Транспортні системи і технології», 2021. – Вип. 37. – С.97-118.

2. Хворост М.В., Шпіка М.І., Бесараб А.І. Тяговий асинхронний електропривод для міського електротранспорту // Енергозбереження, енергетика, енергоаудит, 2012. – № 03(97). – С.7-10.

А.Б. Петренко, О.В. Кочеткова
Національний авіаційний університет, м. Київ

АТАКА ПОРУШЕННЯ ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ДАНИХ У ВЕБ ЗАСТОСУНКАХ

Посилаючись на звіти спеціалістів з сайту Hackerone – платформи для пошуку вразливостей на відомих вебсайтах та провести аналіз недоліків у безпеці, які знаходять спеціалісти, то можна зробити висновок, що значна частина вебсайтів сьогодні все ще вразлива до атак, а забезпечення безпеки веб-додатків навіть у найбільших ресурсах не задовольняє всіх вимог для забезпечення цілісності інформації.

Посилаючись на рейтинг OWASP [1], то на восьмій позиції знаходиться категорія «Порушення цілісності програмного забезпечення та даних». Як і більшість позицій рейтингу, цей вектор є комплексним. Він складається з вразливостей, які зловмисники здатні використовувати під час оновлення програмного забезпечення користувачем. Вебдодатки не можуть бути повністю захищеними, це пов’язано з регулярними оновленнями різних програмних компонентів [2], які застосовуються для побудови системи.

Якщо програма оновлюється без перевірки цілісності, злочинці можуть завантажити своє підроблене оновлення та разом із ним шкідливий код. Також вразливість може реалізуватися, якщо зловмисник змінює код/структуру об'єкта таким чином, щоб зробити його вразливим для майбутніх атак.

Саме тому вони є потенційною мішенню для зловмисника, який може використовувати наявні вразливості для несанкціонованого доступу до інформації вебсервісів, впливу на роботу програм і сервісів, введення шкідливого коду у систему.

До категорії увійшли 10 видів збоїв та помилок [3], у тому числі пов'язаних з ненадійними джерелами веб-функцій (CWE-830), готовність програми десеріалізувати ненадійний потік байтів (CWE-502), активацію функцій з непідтверджених, ненадійних та/або сумнівних сфер CWE-829) та ряд інших.

В основному вразливості програмного забезпечення у веб-додатках виникають через логічні помилки та помилки програмного забезпечення.

Порушення цілісності веб-застосунків та даних у них стосуються коду та інфраструктури, які не захищають від порушень цілісності. Прикладом цього є ситуація, коли програма використовує плагіни, бібліотеки або модулі з ненадійних джерел, сховищ і мереж доставки вмісту (CDN). Незахищений конвеєр CI/CD може призвести до несанкціонованого доступу, зловмисного коду або компрометації системи. Також багато програм тепер включають функцію автоматичного оновлення, коли оновлення завантажуються без достатньої перевірки цілісності та застосовуються до попередньо довіреної програми. Зловмисники потенційно можуть завантажити власні оновлення для розповсюдження та запуску на всіх інсталяціях. Іншим прикладом є те, що об’єкти чи дані кодуються або серіалізуються в структуру, яку зловмисник може побачити та змінити, вразливу до незахищеної десеріалізації.

Приклад атаки: небезпечна десеріалізація: програма JS React викликає набір мікросервісів Spring Boot. Фахівці можуть намагатися забезпечити незмінність свого коду. Рішення, яке можна реалізувати, – це серіалізація стану користувача та передача

його вперед і назад з кожним запитом. Зловмисник помічає підпис об’єкта Java і використовує інструмент з експлуатації, щоб отримати віддалене виконання коду на сервері додатків.

Приклади вразливостей: CWE-830 Включення веб-функцій із ненадійного джерела, CWE-565 Використання файлів cookie без підтвердження та перевірки цілісності, CWE-353 Відсутня підтримка перевірки цілісності.

Основний спосіб завадити зловмисникам здійсненню атаки за вектором A08-2021 – контролювати одержувані із зовнішніх джерел оновлення та дані, перевіряти чи не зазнавали вони змін і чи дійсно приходять із очікуваних джерел. Для цього варто подбати про використання цифрових підписів чи інших подібних механізмів контролю [4].

Також можливо підвищити кіберзахищеність за вектором A08-2021 наступним чином [5]:

- Забезпечити надсилання незашифрованих серіалізованих даних клієнтам лише за умови наявності цифрового підпису або будь-якої форми перевірки цілісності. Так з'явиться можливість унеможливити повторне відтворення даних, що пройшли серіалізацію, і виявити підробки.
- Переконатися, що забезпечено цілісність коду, що проходить процеси серіалізації/десеріалізації. Для цього потрібно переконатися в тому, що використовуваний конвеєр CI/CD має необхідні налаштування, а доступ – контролюється.
- Перевірити наявність/працездатність процесу, в рамках якого перевіряються зміни коду та конфігурації. Такий процес дозволяє мінімізувати ризик потрапляння шкідливих даних в інформаційну інфраструктуру компанії.
- Забезпечити проведення перевірок програмного забезпечення, що поставляється, на предмет відсутності відомих вразливостей (це здійснюється шляхом застосування спеціальних інструментів безпеки).
- Переконатися у використанні бібліотеками та залежностями довірених репозиторіїв. За потреби розмістити внутрішній надійний репозиторій.

Література

1. OWASP Top Ten [Електронний ресурс] // OWASP. – 2023. – Режим доступу до ресурсу: https://owasp.org/www-project-top-ten/.
2. Total number of Websites [Електронний ресурс] // Internet Live Stats – Режим доступу до ресурсу: https://www.internetlivestats.com/watch/websites/.
3. An OWASP top ten driven survey on web application protection method / O. Ben Fredj, O. Cheikhrouhou, M. Krichen, H. Hamam // Springer, 2020. – №12528. – С.235.
4. Петренко А.Б. Програмне рішення із застосуванням ai/ml для пошуку вразливостей у вебдодатках / А.Б. Петренко, А.А. Мілінчук // Студентська конференція інформаційна, функційна і кібербезпека (СКІФіК): науково-технічна конференція, 30 листопада - 1 грудня 2022 р.: тези доповідей. – Х., 2022. – С.41-42.
5. Петренко А.Б. Сучасні методи та засоби виявлення вразливостей у вебзастосунках / А.Б. Петренко, О.В. Кочеткова // Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2024): XVII Міжнародна науково-практична конференція, 21 травня 2024: тези доп. – К., 2024.– С.464-465.

О.К. Довгаленко
Державний університет інформаційно-комунікаційних технологій, м. Київ

РОЗРОБКА ІНТЕЛЕКТУАЛЬНИХ АЛГОРИТМІВ ДЛЯ ОПТИМІЗАЦІЇ СПОЖИВАННЯ ЕНЕРГІЇ В МЕРЕЖАХ ЕНЕРГОПОСТАЧАННЯ

Вступ Останніми роками споживання енергії значно зросло, що ставить перед енергетичними компаніями завдання оптимізації використання ресурсів. Розумні мережі (smart grids) пропонують нові можливості для управління споживанням енергії завдяки інтеграції сучасних інформаційних технологій та методів штучного інтелекту. Оптимізація споживання енергії дозволяє не тільки знизити витрати, але й підвищити ефективність роботи енергетичних систем, сприяючи сталому розвитку.

Мета та завдання дослідження

Метою даного дослідження є розробка та впровадження інтелектуальних алгоритмів для оптимізації споживання енергії в мережах енергопостачання. Основні завдання включають:

1. Аналіз поточних методів оптимізації споживання енергії.
2. Розробка нових алгоритмів з використанням методів машинного навчання та штучного інтелекту.
3. Експериментальна перевірка та оцінка ефективності запропонованих рішень.

Огляд літератури

Сучасні дослідження в галузі розумних мереж демонструють значний інтерес до використання методів штучного інтелекту для управління споживанням енергії. Найпоширенішими підходами є нейронні мережі, генетичні алгоритми, алгоритми рою частинок і методи навчання з підкріпленням. Однак існуючі рішення часто стикаються з проблемами масштабованості та адаптивності в реальних умовах.

Теоретичні основи

Оптимізація споживання енергії в розумних мережах включає аналіз великого обсягу даних і прийняття рішень у реальному часі. Методи машинного навчання, такі як глибоке навчання і навчання з підкріпленням, надають інструменти для створення адаптивних і самонавчальних систем. Ці методи дозволяють прогнозувати споживання енергії, виявляти аномалії та оптимізувати управління ресурсами.

Розробка алгоритмів

Пропонується розробка декількох алгоритмів:

1. Прогнозування споживання енергії: використання рекурентних нейронних мереж (RNN) і довгої короткострокової пам'яті (LSTM) для точного прогнозування споживання енергії на основі історичних даних.
2. Оптимізація управління: застосування алгоритмів навчання з підкріпленням (наприклад, Q-learning) для адаптивного управління споживанням енергії з урахуванням динамічних змін у мережі.
3. Виявлення аномалій: використання методів машинного зору і кластеризації для виявлення відхилень у споживанні енергії та запобігання нештатних ситуацій.

Експериментальна перевірка

Для перевірки запропонованих алгоритмів буде створено експериментальне середовище, що включає симуляцію роботи розумної мережі та реальні дані про

споживання енергії. Ефективність алгоритмів буде оцінюватися за наступними критеріями:

- Точність прогнозування споживання енергії.
- Зниження пікових навантажень і підвищення енергоефективності.
- Швидкість адаптації до змін у мережі і виявлення аномалій.

Очікувані результати

Розробка інтелектуальних алгоритмів дозволить значно поліпшити управління споживанням енергії в розумних мережах. Очікується, що запропоновані рішення забезпечать більш точне прогнозування, ефективний розподіл ресурсів і швидке реагування на зміни у мережі. Це призведе до зниження експлуатаційних витрат і підвищення стійкості енергетичних систем.

Висновок

Дослідження спрямоване на створення нових методів оптимізації споживання енергії, які можуть бути інтегровані в сучасні розумні мережі. Розробка і впровадження інтелектуальних алгоритмів має важливе значення для підвищення ефективності і стійкості енергетичних систем, що сприяє економічному зростанню і охороні навколишнього середовища.

В.П. Іваницький, Р.О. Мешко
Ужгородський національний університет, м. Ужгород

ОПТИМІЗАЦІЯ СИСТЕМ КЕРУВАННЯ НАЗЕМНИМИ ПРИСТРОЯМИ ОРІЄНТАЦІЇ НА СОНЦЕ

Питання визначення та оптимального застосування географічних і астрономічних величин залишаються актуальними при розв'язанні багатьох різноманітних практичних задач геодезії, метеорології, сонячної енергетики, маркшейдерської справи тощо. Їх використання лежить в основі нових поколінь електронних теодолітів, роботизованих геодезичних систем, автоматизованих систем орієнтування, автоматичних астрометричних приладів і пристроїв. Вони дозволяють підвищити як точність, так і продуктивність вимірювань та обробки їх результатів. Це вимагає створення нових ефективних систем керування та методів і алгоритмів автоматичних обчислень географічних і астрономічних величин для них. У той же час, для існуючих точних астрономічно-географічних моделей необхідно обчислювати велику кількість тригонометричних функцій. Тому такі системи керування досить складно розробляти з використанням мікроконтролерів, оскільки вони не мають достатньої обчислювальної потужності та об’ємів пам’яті для швидкого виконання таких математичних операцій в реальному часі. Для цього необхідно вводити в систему керування обчислювальні мікропроцесорні модулі, які суттєво ускладнюють пристрої орієнтації. Тому наукові дослідження можливості застосування значно простіших астрономічних моделей для мікроконтролерних пристроїв є важливими для розвитку сучасних наземних систем орієнтації.

У доповіді наводяться результати оптимізації систем керування наземними двовісними пристроями орієнтації на Сонце із швидкодіючим алгоритмом роботи

мікроконтролерів. У технічному відношенні у систему введено геомагнітний датчик для підвищення надійності контролю за позиціонування сонячних елементів. Інформаційним базисом алгоритму покладено спрощену астрономічно-географічну модель руху Сонця по небесній сфері. Відповідно з цією моделлю система керування автоматично відслідковує траєкторію руху Сонця та розраховує його кутові координати для текучого моменту часу в будь-який день року і для будь-якої точки земної кулі. Отримані рівняння спрощеної математичної моделі придатні для розрахунків кутів орієнтації на Сонце в реальному часі на 8-ми бітних мікроконтролерах з низькою обчислювальною потужністю. Дослідження оптимізованої системи керування на мікроконтролері AVR-328 показують, що її використання для двовісних систем орієнтації забезпечує високу стабільність та надійність процесу функціонування трекерів. Технічні параметри мікроконтролерів AVR-328 у випадку застосування створеного алгоритму забезпечують виконання системою керування одного кроку переорієнтації за проміжок часу, менший 2 с. Це забезпечує мінімальний технічний період процесу переорієнтації механізмами трекера біля 5 с. Відхилення розрахованого кута орієнтації від точного значення не перевищують 3°, що відповідає відносній похибці реєстрації інтенсивності сонячного випромінювання, меншій 0,3 %. Написана за спрощеним алгоритмом програма мікроконтролера займає біля 65 % його пам'яті. Тому використання такого оптимізованого алгоритму вивільняє ресурси мікроконтролерів AVR-328 для виконання додаткових операцій з обробки даних та автоматичного керування різними додатковими пристроями, пов'язаними із процесом орієнтації на Сонце. У випадку сонячної енергетики алгоритм забезпечує використання біля 98 % добового об'єму енергії сонячного випромінювання.

Т.В. Капелюшна
Державний університет інформаційно-комунікаційних технологій, м. Київ

ПРОПОЗИЦІЇ ЩОДО УПЕРЕДЖЕННЯ РИЗИКІВ ІНФОРМАЦІЙНИХ АКТИВІВ ЗАДЛЯ ЗАХИСТУ РЕПУТАЦІЇ ПІДПРИЄМСТВА

На сьогодні нематеріальні активи формують цінність на рівні із матеріальними, так, некодифіковані знання, інтелектуальні здібності, патенти, репутація відіграють важливу роль у формуванні результативних показників діяльності підприємств. Нині близько 80 % створеної ринкової вартості припадає саме на нематеріальні активи, в тому числі капітал бренду, інтелектуальну власність і гудвіл. Гудвіл є нематеріальним активом, що виникає при придбанні компанії та включає надбання, яке перевищує ринкову вартість активів за рахунок репутації, відгуків клієнтів, інформації, що поширюється серед постачальників, конкурентів, зацікавлених сторін, що призводять до приросту вартості компанії понад вартість його матеріальних активів. Капітал бренду визначається вартістю іміджу компанії та ступенем його сприйняття, обізнаності щодо компанії серед споживачів, формується передусім з взаємного поєднання емоційних та раціональних аспектів, що вимальовують уявний позитивний образ бренду та сприяють його успіху на ринку. Тож наразі захист інформаційного середовища компаній є важливим для збільшення їх ринкової вартості, оскільки впливає на збереження репутації,

конфіденційність даних, тим самим дозволяє утримувати конкурентні позиції за рахунок позитивного іміджу компанії та її сприйняття.

Взаємозв`язок репутаційних ризиків, інформаційної безпеки та вартості компанії логічно пояснюється тим, що, як вже зазначалося на початку, нині 70-80% ринкової вартості активів припадає на нематеріальні активи (капітал бренду, інтелектуальна власність, гудвіл), саме тому варто проводити захист інформаційного середовища, щоб уникнути репутаційних ризиків, що сприятиме укріпленню іміджу компанії, сприйняттю клієнтами підприємства, як надійного, і, як результат, забезпечення інформаційної безпеки сприяє формуванню нематеріальної вартості компанії (гудвілу). В додачу до матеріальної вартості, яка надає суттєві переваги компанії перед клієнтами, знижується їх відтік у разі невизначеностей, тому що компанія позиціонується, як надійна, з високим ступенем довіри. Рекомендаціями щодо упередження інформаційних ризиків є: рекламні заходи із підкресленням позитивних сторін компанії, щоб інформація спрацювала на користь підприємства; використання інформації щодо клієнтських вподобань з урахування культурних цінностей та звичаїв, традицій для формування нових продуктів та конкурентних переваг за рахунок клієнтоорієнтованості компанії; захист некодованих даних, інтелектуальних здібностей персоналу (патенти, реєстрація права власності); дотримання загальноприйнятих поглядів щодо безпекової ситуації в світі; пошук інформації щодо конкурентів з метою моніторингу їх переваг та використання компанією інформації для власного вдосконалення; дотримання стандартів безпеки, а також забезпечення прозорості у зборі та використанні персональних даних; активне співробітництво з регуляторами, попередження можливих проблем та вчасне вирішення регуляторних питань, стандартизація ISO 27000; моніторинг гармонізації інтересів персоналу за допомогою періодичного розрахунку коефіцієнта Фехнера; відстеження ландшафту кіберзагроз та інцидентів безпеки за допомогою інструментів аналізу кіберзагроз (Barracuda, F5 BIG-IP Advanced WAF, FogBugz, Fortinet FortiWeb WAF, GitHub, Imperva Web Application Firewall, Mattermost, Pivotal Tracker), доцільна взаємна Інтеграція DevSecOps, CI/CD, SDLC, що дозволить забезпечити гнучке та швидке усунення вразливостей безпеки інформаційних активів. Урахування даних рекомендацій дозволить суттєво покращити репутацію підприємства, а головне убезпечити від загроз порушення інформації, як активу підприємства.

З М І С Т

Надруковано в РВЦ
Державного університету
інформаційно-комунікаційних технологій
Формат 60х90/16. Папір друкарський.
Наклад 100 прим. Зам. 711.

Свідоцтво суб'єкта видавничої справи
ДК №7917 від 16.08.2023 р.

03110, м. Київ, вул. Солом'янська, 7.
Тел. (044) 249-25-76