2. Is Splitting off Resources for Your Database Right for You? URL: https://www.liquidweb.com/blog/is-splitting-off-resources-for-your-database-right-for-you/ (дата звернення: 01.11.2021)

Ключові слова: база даних, захист даних, безпека баз даних, ресурси баз даних, інформаційна система

Ключевые слова: база данных, защита данных, безопасность баз данных, ресурсы баз данных, информационная система

Keywords: database, data protection, database security, database resources, information system

Василенко Микола Дмитрович

Національний університет «Одеська юридична академія», професор кафедри кібербезпеки, доктор фізико-математичних наук, доктор юридичних наук, професор

Шевченко Тетяна Вікторівна

Державний університет «Одеська політехніка», доцент кафедри міжнародних відносин та права, кандидат юридичних наук

ШТУЧНИЙ ІНТЕЛЕКТ ТА ЙОГО БЕЗПЕКА В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ

Темпи розвитку штучного інтелекту (ШІ) дозволяють говорити про його суттєве використання в публічному адмініструванні. В Україні на виконавчому рівні задекларовано впровадження ШІ (високого порядку) в публічне управління і не тільки [1]. Однак ШІ такого порядку потребує відповідних інтелектуальних систем захисту інформації. Вони передбачають інтелектуалізації цих систем. При цьому все ж таки залишається відсутнім належне обґрунтування наслідків самих заходів щодо застосування ШІ в адміністративному управлінні щодо

мислення інтелекту машинного походження та його захисту, хоча вже відбулося затвердження плану заходів з реалізації Концепції розвитку ШІ в Україні на 2021-2024 роки [2].

Для розуміння можливостей ШІ вважають за можливе уявляти інтелект в цілому та використовувати його за подобою інтелекту та розробляти відповідні моделі та проводити їх навчання. В науці зі ШІ під інтелектом назагал вважається спроможність мозку до розумової діяльності, тобто до оперування знаннями для прийняття певних рішень стосовно конкретної задачі. Ця здатність мозку враховується при вирішуванні інтелектуальних задач шляхом придбання, запам’ятовування та цілеспрямованого перетворення знань у процесі навчання, отримання життєвого досвіду та адаптації до різноманітних зовнішніх та внутрішніх обставин. У цьому визначенні «інтелекту» під терміном «знання» мається на увазі не тільки та інформація, що поступає в мозок через органи чуття: вона інформація важлива, але недостатня для інтелектуальної діяльності. Річ у тім, що об’єкти навколишнього середовища володіють властивістю не тільки впливати на органи чуття, але і знаходитися один з одним в певних відносинах. Для того, щоб здійснювати в навколишньому середовищі інтелектуальну діяльність (або хоч би просто існувати), необхідно мати знання щодо моделі цього світу. У цій інформаційній моделі навколишнього середовища реальні об’єкти, їх властивості та відносини між ними не тільки відображаються і запам’ятовуються, але і можуть подумки цілеспрямовано перетворюватися. При цьому істотним є те, що формування моделі зовнішнього середовища відбувається у процесі навчання, отримання життєвого досвіду та адаптації до різноманітних обставин в системі середовища: природа – техніка – наука – суспільство.

Машинне навчання, яким користуються при створенні згаданих систем, становить підмножину технологій ШІ, яку можна описати як набір алгоритмів, що дозволяють комп'ютерам навчатися тому, на що вони з самого початку не запрограмовані. Іншими словами йдеться про алгоритмічну програму, яка сама може створювати програми для вирішення різних завдань. Алгоритм машинного навчання може навчатися на вибірці вже вирішених прикладів завдання (це

називається навчання з учителем), або він повинен самостійно виявити загальні риси і зв'язки в заданій множині об'єктів (навчання без вчителя). У разі навчання з учителем алгоритм може працювати в режимі навчання або в бойовому режимі. У режимі навчання алгоритм отримує навчальну вибірку, в якій об'єкти представлені своїми ознаками та мітками класів. З точки зору машинного навчання, нейронна мережа являє собою окремий випадок методів розпізнавання образів, дискримінантного аналізу, методів кластеризації тощо. Питання безпеки зазначеного ШІ розв’язується на програмно-технічному рівні інформаційної безпеки, який представляє собою рівень, у якому реалізуються різні програмно-технічні заходи, створені задля контроль працездатності устаткування й програмного забезпечення. Оскільки із загальної кількості загроз в останні роки все більшу питому вагу займають внутрішні загрози з боку персоналу, стосовно яких процедурні заходи не дають великого ефекту, саме на програмно-технічні заходи покладаються великі надії в силу, перш за все, великої різноманітності виконуваних ними функцій та способів їх реалізації [3 с. 13].

Одним із центральних понять для програмно-технічного рівня стало поняття сервісу (функції безпеки). Найбільш поширеними сервісами безпеки вважають [3, с. 13]: ідентифікація та аутентифікація; керування доступом; протоколювання та аудит; шифрування; контроль цілісності; екранування; аналіз захищеності; забезпечення відмовостійкості; забезпечення безпечного відновлення; тунелювання; керування. Деякі з цих сервісів виступають як «майданчик» для реалізації відповідних функцій захисту за допомогою методів штучного інтелекту. Зміст кожної функції достатньо добре визначено (див. [4]). Передбачається, що основні функції, які виконує інформаційна система, відносяться до її основних сервісів, а сервіси безпеки належать до групи допоміжних сервісів (функцій) системи.

Для підвищення ефективності публічного адміністрування важливим стає те, яким чином закладений алгоритм в ШІ, впливатиме на рішення, що приймається адміністративними, судовими або будь-якими іншими органами державної влади. Нині лідером у використанні ШІ у судочинстві залишаються США, де залучаючи ШІ до розгляду цивільних та кримінальних справ, судді

отримують «асистента» під час обрання запобіжного заходу щодо підсудного, оскільки через суб'єктивність та людський фактор трапляються розбіжності у прийнятті рішень різними суддями у подібних чи навіть тотожних ситуаціях. Натомість ШІ, аналізуючи ризики неупереджено на основі попередньої практики, визначає необхідність у запобіжному заході. Хоча, звісно, актуальним у цій ситуації залишається питання об'єктивності самого масиву даних для аналізу, адже попередні рішення приймалися звичайними суддями. Технології ШІ в ЄС, як і в Україні, відстають від США. Однак системи ШІ вже застосовуються для цифрової ідентифікації та верифікації особистості, а також впроваджуються: менше – у галузі охорони здоров'я, більше – для аналізу, прогнозування та моделювання показників ефективності публічного управління, для виявлення недобросовісної діяльності чиновників. Наявність відкритих державних даних стає першою передумовою до використання можливостей ШІ для покращення якості державних послуг. Так, Government AI Readiness Index оцінює готовність до впровадження штучного інтелекту в публічних сервісах. Індекс включає три основні компоненти: урядову політику, спроможність технологічного сектору, потенціал даних та інфраструктури. Розвивати ШІ в Україні планують і в різних напрямках публічного адміністрування. Так, ведуться роботи з використання ШІ в наявних технологіях – Електронний суд, Єдиний реєстр досудових розслідувань і так далі. WINCOURT – модуль автоматичного аналізу на платформі Суд на долоні. Він оцінює подібність судових документів, які завантажує користувач, до тих, на основі яких були вже вирішені подібні справи, та надає прогноз стосовно успішності їх розгляду. Verdictum PRO – сервіс з аналогічним функціоналом та спеціалізацією в господарському судочинстві. Для вирішення завдань щодо публічного адміністрування необхідно ще прийняти відповідні законодавчі акти, що урегулюють суспільні відносини у визначеній сфері. Однак, законодавче забезпечення регулювання системи ШІ та їх безпеки, наприклад зміни у судовій системі, взагалі бачаться достатньо складними, у той час коли технології ШІ натепер розвиваються досить швидко.

Список використаних джерел:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. No 1556-р // Урядовий портал. URL: https://www.kmu.gov.ua/npas/pro-shvalennyakoncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220

2. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки. Розпорядження Кабінет Міністрів України від 12 травня 2021 р. № 438-р URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#

3. Васильев В. И. Интеллектуальные системы защиты информации: учеб. пособие. Машиностроение, 2013. 172 с.

4. Галатенко В. А. Основы информационной безопасности. Курс лекций: учеб. пособие. М.: ИНТУИТ.РУ. 2004. 264 с.

Ключові слова: штучний інтелект , машинне навчання, публічне адміністрування, програмно-технічні заходи, безпека

Ключевые слова: искусственный интеллект, машинное обучение, публичное администрирование, программно-технические мероприятия, безопасность

Keywords: risk, artificial intelligence, machine learning, public administration, software and hardware, security

Бойко Віктор Дмитрович

Національний університет «Одеська юридична академія»,

доцент кафедри кібербезпеки, кандидат технічних наук, доцент

ПРАКТИЧЕСКИЕ АСПЕКТЫ ПЕРЕХОДА НА СВОБОДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В СОВРЕМЕННОМ АКАДЕМИЧЕСКОМ ОБРАЗОВАНИИ

В предыдущем докладе была обоснована актуальность и необходимость перехода на открытое программное обеспечение [1]. Были рассмотрены