МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами IX Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:

ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

10 листопада 2023 року

Полтава 2023

Потенціал аміаку як альтернативного чистого енергоносія ще тільки починає розкриватися. Але вже зараз ціла низка машинобудівних компаній у всьому світі створюють великі та середні установки з виробництва аміаку для промисловості, енергозабезпечення важкого обладнання, морського судноплавства. Зараз найбільш очевидні напрями застосування аміаку в енергетиці – його спалювання безпосередньо на електростанціях та двигунах різних видів транспортних засобів.

Особливу цінність мають останні практичні технічні рішення програмно-керованих аміачних адсорберів для відокремлення азоту від водню та отримання водню високої чистоти для паливних елементів різних типів методом адсорбції при змінному тиску (PSA) та використанні пористих матеріалів сепараторів, таких як молекулярні сита або цеоліт.

INNOVATIVE ASPECTS OF ENERGY EFFICIENCY OF CONVERSION, STORAGE AND TRANSPORTATION TECHNOLOGIES IN THE FIELD OF RENEWABLE ELECTRICITY

***O. Dryuchko**, Ph.D., Associate Professor,*
***V. Halai**, Ph.D., Associate Professor,*
***A. Tretiak**, Ph.D.,*
***A. Burda**, student,*
***E. Oshkodyorov**, student*
National University «Yuri Kondratyuk Poltava Polytechnic»

УДК 004.89

***С.Г. Кислиця**, к.т.н., доцент,*
***А.С. Боровик**, аспірант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасні комп'ютерні системи та мережі перебувають у стані постійного розвитку та модифікації, а обсяги аналізованих даних у світі подвоюються щороку. Тому для забезпечення необхідного рівня захисту інформації необхідно гнучко і оперативно реагувати на умови, що змінюються, забезпечувати надійний захист з урахуванням постійної зміни вхідних впливів, попереджати дії зловмисників, тобто мати адаптивну систему захисту інформації (СЗІ).

Метою даної роботи є розробка методики застосування інтелектуального аналізу даних для побудови адаптивної системи захисту інформації, в корпоративних системах. Необхідність використання інструментарію інтелектуального аналізу даних у СЗІ корпоративних систем випливає з різнорідності структур інформаційних просторів цих систем; складності отримання аналітичної інформації із баз даних значного обсягу; великої кількості користувачів, що одночасно працюють у системі; вимог постійного

контролю функціонування та прийняття обґрунтованих управлінських рішень, що залежать від багатьох факторів.

Передумовами використання інтелектуального аналізу даних (ІАД) у корпоративних інформаційних системах (КІС) є клієнт-серверна технологія, розподілені бази даних, наявність сховищ інформації, застосування сучасних мережевих технологій та різноманітного інструментарію, що використовується для збирання, обробки, візуалізації та аналізу даних. Особливістю систем захисту в корпоративних системах є комбінація як мінімум трьох проблем: захист інформації в комп'ютерних мережах; забезпечення безпеки баз даних; забезпечення безпечної роботи систем автоматичного оброблення інформації [1].

До інтелектуальних засобів, що часто використовуються в комп'ютерних мережах, відносять бази знань у складі експертних систем, нечіткі логічні системи, нейронні мережі, еволюційні методи та гібридні інтелектуальні системи. Основними завданнями, які вирішуються інтелектуальними засобами забезпечення інформаційної безпеки комп'ютерної мережі, є класифікація та кластеризація.

З інтелектуальними засобами безпеки баз даних (БД) можна познайомитися в [2]. Вказано, що система інформаційної безпеки баз даних має використовувати засоби та об'єкти застосовуваної системи управління базами даних (СУБД), об'єкти та засоби бази даних, набір правил та подій, що характеризують дії користувачів. У [3] зазначено, що саме фіксація подій дозволяє скласти уявлення про те, чим цікавиться кожен із користувачів, складено перелік основних подій, що реєструються. До засобів забезпечення безпечної роботи систем обробки інформації відносяться механізми запобігання вторгненням, авторизація, розмежування прав доступу, криптозахист (на носіях інформації, мережах, парольний захист), управління повноваженнями користувачів.

З метою контролю стану системи використовують бази сигнатур відомих атак, а як основні джерела інформації – системні журнали та файли, аналізують вміст мережного трафіку та файлів. При традиційному підході до побудови системи захисту із застосуванням інструментарію ІАД використовуються штучні нейронні мережі, алгоритми класифікації, методи нечіткої кластеризації, асоціативні правила, алгоритми обмеженого перебору та кластерний аналіз. Нейронні мережі використовуються для контролю трафіку локальної мережі, пошуку прихованих закономірностей в масивах первинних даних, виявлення вторгнень.

Для прогнозування значення цільового показника використовуються набори вхідних змінних, математичних функцій активації та вагових коефіцієнтів вхідних параметрів. Виконується ітеративний навчальний цикл, нейронна мережа модифікує вагові коефіцієнти доти, доки передбачуваний вихідний параметр відповідає дійсному значенню. Після навчання нейронна мережа стає моделлю, яка застосовується під час прогнозування.

Інтелектуальний аналіз даних є необхідним та сучасним доповненням такої великої інформаційної структури, як корпоративна система. Однією з її складових є система захисту. Засоби захисту повинні постійно

вдосконалюватися і розвиватися, через що запропонований у роботі механізм побудови адаптивної СЗІ є актуальним, а використання поряд з ІАД швидких алгоритмів збільшить ефективність системи.

ЛІТЕРАТУРА:

1. Han J. Data Mining: Concepts and Techniques / J. Han, M. Kamber // Morgan Kaufmann. – 2000.

2. Маслова Н.А. Інформаційна безпека систем управління базами даних / Маслова Н.А. // Комп'ютерна математика. Оптимізація обчислень : зб. наук. праць. – Київ : ІК НАН України, 2001. – Т. 1. – С. 271-280.

3. Задірака В.К. Т-ефективні алгоритми наближеного розв'язування задач обчислювальної математики / В.К. Задірака, М.Д. Бабич, А.І. Березовський та ін. – К., 2003. – 216 с.

INTELLIGENT DATA ANALYSIS IN ENSURING INFORMATION SECURITY

***S. Kyslytsia**, Ph.D., Associate Professor,*
***A. Borovyk**, postgraduate student*
National University «Yuriy Kondratyuk Poltava Polytechnic»

УДК 004.93'14

***Н.В. Єрмілова**, доцент,*
***Ю.Р. Зоураб**, аспірант,*
***Р.О. Єрмілов**, аспірант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ПОРІВНЯЛЬНИЙ РОЗГЛЯД МЕТОДІВ РОЗПІЗНАВАННЯ ОБРАЗІВ

Розпізнавання образів — важливе завдання систем комп'ютерного зору, яке використовується для виявлення візуальних об'єктів певних класів (наприклад, людей, тварин, предметів, автомобілів та будівель) у цифрових зображеннях, таких як фотографії чи відеокадри. Метою виявлення об'єктів є розробка обчислювальних моделей, які надають найбільш фундаментальну інформацію, необхідну програмам комп'ютерного зору [1]. Розглянемо основні сучасні моделі розпізнавання та порівняємо їх за допомогою оцінки максимуму апостеріорної імовірності (mAP), що застосовується для отримання точкової оцінки неспостережуваної величини на базі емпірічних даних і пов'язана з методом максимальної правдоподібності.

Одним із перших методів вибіркового пошуку є метод R-CNN, розроблений Дж. Р. Уйлінгсом та ін. (2012), він є альтернативою повному пошуку на зображенні для фіксації розташування об'єкта. Метод ініціалізує невеликі області зображення та поєднує їх у ієрархічну групу. Таким чином, остання група є блоком, що містить все зображення. Недоліком методу є те, що навчання