**ISSN 2519-2310**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені В. Н. КАРАЗІНА

# КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА

==========

# COMPUTER SCIENCE AND CYBERSECURITY

**Випуск 2 (24)**
**ISSUES 2 (24)**

**Заснований 2015 р.**

Харків
Kharkiv
2023

The journal publishes research articles on theoretical, scientific and technical problems of effective facilities development for computer information communication systems and on information security problems based on advanced mathematical methods, information tech-nologies and technical means.

Journal is published quarterly.

The Journal is a professional publication in the field of science:
12 Information Technologies by specialties: 122 Computer Science, 125 Cybersecurity.
MES Ukraine Order № 409 of 17/03/2020

Approved for placement on the Internet by by the decision of the Academic Council of V.N. Karazin Kharkiv National University

(Minutes Nr 23, dated December 25, 2023)

Editor-in-Chief: **Azarenkov Mykola**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
Deputy Editor: **Rassomakhin Serghii**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
Executive Editor: **Kuznetsov Alexandr**, V.N., Karazin Kharkiv National University, Ukraine;
Secretary: **Malakhov Serghii**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine.

***The Editorial Board***

**Alekseychuk Anton**, DSc (Computer Science), National Technical University of Ukraine "Kyiv Polytechnic Institute", Ukraine;
**Alexandrov Vassil Nikolov**, PhD (Computer Science), Barcelona Supercomputing Centre, Spain;
**Biletsky Anatoliy**, DSc (Computer Science), Institute of Air Navigation, National Aviation University, Ukraine;
**Bilogorskiy Nick**, V.N., Director Trust and Safety at Google,USA;
**Borysenko Oleksiy**, DSc (Computer Science), Sumy State University, Ukraine;
**Brumnik Robert**, PhD (Computer Science), GEA College,Metra Engineering Ltd, Slovenia:
**Dempe Stephan**, PhD (Computer Science), Technical University Bergakademie Freiberg, Germany;
**Geurkov Vadim**, PhD (Computer Science), RyersonUniversity, Canada;
**Iusem Alfredo Noel**, PhD (Computer Science), Instituto Nacional de Matemática Pura e Aplicada (IMPA), Brazil;
**Kalashnikov Vyacheslav**, PhD (Computer Science), Tecnológico University de Monterrey, México;
**Karpiński Mikołaj**, DSc (Computer Science), WSB-NLU, Poland;
**Kazymyrov Oleksandr**, PhD (Computer Science), EVRY Norge AS, Norway;
**Kemmerer Richard**, PhD (Computer Science), University of California in Santa Barbara (UCSB), USA;
**Kharchenko Vyacheslav**, DSc (Computer Science), Zhukovskiy National Aerospace University (KhAI), Ukraine:
**Khoma Volodymyr**, DSc (Computer Science), Institute "Automatics and Informatics", The Opole University of Technology, Poland;
**Kovalchuk Ludmila**, DSc (Computer Science), National Technical University of Ukraine "Kyiv Polytechnic Institute", Ukraine;
**Krasnobayev Victor**, DSc (Computer Science), V.N.Karazin Kharkiv National University, Ukraine;
**Kuklin Volodymyr**, PhD (Computer Science), Karazin Kharkiv National University, Ukraine;
**Kolovanova Ievgeniia**, PhD (Computer Science) Karazin Kharkiv National University, Ukraine;
**Khruslov Maksym**, PhD (Computer Science), Karazin Kharkiv National University, Ukraine;
**Lazurik Valentin**, PhD (Computer Science), Karazin Kharkiv National University, Ukraine;
**Lisitska Irina**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
**Mashtalir Volodymyr**, DSc (Computer Science), Kharkiv National University of Radio Electronics, Ukraine;
**Melkozerova Olha**, PhD (Computer Science), Karazin Kharkiv National University, Ukraine;
**Murtagh Fionn**, PhD (Computer Science), University of Derby, University of London, UK;


Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.

**Niskanen Vesa**, PhD (Computer Science) University of Helsinki, Finland;
**Oliynikov Roman**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
**Rassomakhin Serhii**, DSc (Computer Science), Universal Research & Development Enterprise, USA;
**Raddum Håvard**, PhD (Computer Science), Simula Research Laboratory, Norway;
**Rangan C. Pandu**, PhD (Computer Science), Indian Institute of Technology, India;
**Romenskiy Igor**, PhD (Computer Science), GFaI Gesellschaft zur Förderung angewandter Informatik e.V., Deutschland;
**Świątkowska Joanna**, PhD (Cybersecurity), CYBERSEC Programme, Kosciuszko Institute, Poland;
**Tolstoluzka Olena**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
**Toliupa Serhii**, DSc (Computer Science), Taras Shevchenko National University of Kiev, Ukraine;
**Velev Dimiter**, PhD (Computer Science), University of National and World Economy, Bulgaria;
**Watada Junzo**, DSc (Computer Science), The Graduate School of Information, Production and Systems (IPS), Waseda University, Japan;
**Zadiraka Valeriy**, DSc (Computer Science), Glushkov Institute of Cybernetics of National Academy of Sciences of Ukraine, Ukraine;
**Zholtkevych Grygoriy**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
**Yesin Vitalii**, DSc (Computer Science), Karazin Kharkiv National University, Ukraine;
**Yanovsky Volodymyr**, PhD (Computer Science), "Institute for Single Crystals" of National Academy of Sciences of Ukraine, Ukraine;
**Yesina Marina**, PhD (Computer Science), Karazin Kharkiv National University, Ukraine

Editorial Board Adress: Svobody Sq., 6, office 315a, Kharkiv, 61022, Karazin Kharkiv National University, North building of University, 3th floor
tel. (057) 705-10-83, e-mail: cscsjournal@karazin.ua
Web-page: http://periodicals.karazin.ua/cscs (OJS)

Double-blind peer review was conducted.
The authors of the published materials are solely responsible for the selection, accuracy of the facts, proper names, etc.

*© V.N. Karazin Kharkiv National University, publishing, design, 2015/2019*


Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.

***ЗМІСТ***




Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.

***CONTENTS***




Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.

ISSN 2519-2310

КОМП'ЮТЕРНІ НАУКИ ТА КІБЕРБЕЗПЕКА, 2023, Вип. 2 (24)

COMPUTER SCIENCE AND CYBERSECURITY, 2023, Iss. 2 (24)

*Оригінальна стаття*

DOI: https://doi.org/10.26565/2075-3810-2023-50-02
УДК 004.8:342.9

# ПРОБЛЕМНІ ПИТАННЯ ТЕХНОЛОГІЇ МАШИННОГО НАВЧАННЯ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

**Дмитро Узлов[1], Володимир Струков[2], Владислав Гуділін[3], ОлексійВласов[4]**

*[1]Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна, e-mail: dmytro.uzlov@karazin.ua, ORCID: https://orcid.org/0000-0003-3308-424X*
*[2]Харківський національний університет внутрішніх справ, пр. Льва Ландау, 27, Харків, 61080, Україна, e-mail: struk_vm@ukr.net, ORCID: https://orcid.org/0000-0003-4722-3159*
*[3]Харківський національний університет внутрішніх справ, пр. Льва Ландау, 27, Харків, 61080, Україна, e-mail: vgudilin7@gmail.com, ORCID: https://orcid.org/0000-0002-3844-1448*
*[4]Харківський національний університет радіоелектроніки, пр. Науки, 14, Харків, 61166, Україна, e-mail: moonreactor@gmail.com, ORCID:https://orcid.org/0000-0003-1619-0032*

Надійшла до редакції та переглянута: Листопад 2023. Прийнята до друку :Грудень 2023.

**Анотація:** Правоохоронні органи все частіше використовують технології прогнозування та автоматизації, де основною технологією часто є застосування методів машинного навчання (ML). У статті розглядається проблема підзвітності та відповідальності правоохоронних органів і посадових осіб в контексті застосування моделей машинного навчання ML. Автори вказують, що підзвітність є ключовим елементом демократичної правоохоронної діяльності, але використання прогнозного програмного забезпечення може створювати проблеми у забезпеченні цієї підзвітності. Стаття обговорює, що застосування ML може призвести до завуалювання відповідальності та ускладнення підзвітності у «мультиагентних структурах», що об'єднують людей і обчислювальні інструменти. Особлива увагу приділяється непрозорості алгоритмів прикладних прогнозних моделей та автоматизованих систем прийняття рішень, що стає джерелом непорозумінь і обережності щодо їх використання. Автори висувають питання щодо того, як можна забезпечити ефективний контроль та повну звітність, коли ключові компоненти процесу прийняття рішень залишаються невідомими для широкої громадськості, посадових осіб та навіть розробників моделей. У статті стверджується, що важливі питання, пов'язані з моделями рішень ML, можуть бути розглянуті без детального знання алгоритму навчання, що дає змогу експертам правоохоронної діяльності, які не займаються ML, вивчати їх у формі інтелектуального контролю. Експерти, які не займаються ML, можуть і повинні переглядати навчені моделі ML. Автори надають «набір інструментів» в формі запитань про три елементи моделі прийняття рішень, які можуть бути якісно досліджені експертами, які не є спеціалістами з машинного навчання: навчальні дані, навчальна мета та антиципаційна оцінка



Computer Science and Cyber Security Journal
Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.

результатів. Такий підхід розширює можливості цих експертів у вигляді об’єктивної оцінки використання моделей ML у правоохоронних завданнях. Основна ідея полягає в тому, що навіть без глибоких технічних знань експерти можуть аналізувати та переглядати моделі ML, розкриваючи їхню ефективність через призму власного досвіду. Даний підхід сприяє порозумінню використання технологій машинного навчання в рамках правоохоронної діяльності, розширюю-чи потенціал відповідних експертів, не пов’язаних з ML.

**Ключові слова:** *машинне навчання, штучний інтелект, аналіз даних*

**Як цитувати**: Узлов Д.Ю., Струков В.М., Гуділін В.О., Власов О.В.. Проблемні питання технології машинного навчання в правоохоронній діяльності. Комп’ютерні науки та кібербезпека. 2023; 24(2):6–15. https://doi.org/10.26565/2075-3810-2023-50-02

**Incites:** Uzlov D., Strukov V., Hudilin V., Vlasov O.. Problematic issues of machine learning technology in law enforcement. Computer science and cybersecurity. 2023; 24(2):6–15. https://doi.org/10.26565/2075-3810-2023-50-02

**Open Access**. This article is licensed under a Creative Commons Attribution 3.0 http://creativecommons.org/licenses/by/3.0/

## Вступ

Правоохоронні органи все частіше застосовують досягнення інформаційних технологій та штучного інтелекту, щоб намагатися передбачити події та автоматизувати обробку даних що виникають в процесі правоохоронної діяльності. У цьому правоохоронна діяльність схожа на багато інших галузей управління авто, прогнозування погоди, вирішення заявок на кредит тощо. Прогностична аналітика підтримує управління ризиками у сфері управління безпекою[1]. Лондон, Лос-Анджелес, Мюнхен, Новий Орлеан, Філадельфія, Цюрих та Харків це приклади міст, де поліція використовує або тестувала інтелектуальне поліцейське програмне забезпечення, яке має на меті або передбачити, де можуть статися злочини, або хто, ймовірно, вчинить злочин у майбутньому. Машинне навчання (ML) є ключовою технологією, яка лежить в основі багатьох із цих програм. Програмне забезпечення для машинного навчання може раціоналізувати трудомісткі завдання обробки даних, таких як аналіз великого обсягу документів, оприлюднених у ході розслідування, та класифікація їх за категоріями[2]. Разом з цим підзвітність поліції викликала занепокоєння що використання моделей ML робить людей неспроможними відповідати за рішення що були прийняті на їх основі[3]. Щоб спростувати подібні занепокоєння, необхідно зробити процеси прийняття рішень, що ґрунтуються на результатах використання моделей ML, доступними для контролю.

Прогнозну правоохоронну діяльність можна розглядати як окрему техніку під ширшою парасолькою правоохоронної діяльності, керованої аналітикою (ILP). ILP виник як практична управлінська програма для прийняття рішень,щодо правоохоронних послуг на основі об’єктивного аналізу даних [4]. Систематичний збір і аналіз розвідувальних даних мають на меті підвищити як ефективність протидії злочинності, забезпечуючи як більш точне


Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.

визначення цілей, так і економічну ефективність [5]. У правоохоронній діяльності з прогнозуванням, як і в ILP, аналіз і рішення централізовані та раціоналізовані; прогностична правоохоронна діяльність підкреслює об'єктивний, науковий вибір стратегій та тактик і надає перевагу централізованому, раціоналізованому прийняттю рішень на основі аналізу даних.

## Підзвітність правоохоронних органів

Підзвітність та відповідальність правоохоронних організацій і посадових осіб є ключовим компонентом демократичної правоохоронної діяльності, і вже давно є предметом занепокоєння дослідників і практиків правоохоронних органів [6]. З точки зору позиції правоохоронних сил у демократичній системі, підзвітність може означати політичний контроль над поліцією або співпрацю між поліцією та урядом, згідно з якою поліція повинна надавати пояснення про прийнятті рішення.

Застосування прогнозного програмного забезпечення або програмного забезпечення для автоматизації для підтримки прийняття рішень може фундаментально поставити під сумнів здатність посадових осіб та організацій звітувати про процеси прийняття рішень, а також завуалювати відповідальність у «мультиагентних структурах», що складаються з людей і обчислювальних інструментів. Непрозорість «алгоритмів» прикладних прогнозних моделей або автоматизованих систем прийняття рішень залишається основною причиною занепокоєння щодо їх використання [7]. Існує занепокоєння, що алгоритми «є непрозорими» в тому сенсі, що одержувачі вихідних даних роботи алгоритму ML (класифікація, кластеризація, прогноз), рідко мають конкретне уявлення про те, як і чому конкретна класифікація, кластеризація або прогноз були отримані на основі вхідних даних [7].

Коли один або більше елементів процесу прийняття рішень незрозумілі, будь-яка з вищезгаданих концепцій підзвітності ставиться під сумнів. Модель ML, як правило, вбудована в програмне забезпечення, працює як «чорна скринька», де вхідні дані (наприклад, геопросторові дані, щодо злочинності та/чи демографії) обробляються у вихідні дані (наприклад, прогноз чи класифікацію) за допомогою обчислень, які залишаються невидимими для кінцевого користувача. Незважаючи на те, що цей процес, по суті, не є незрозумілим, він практично незрозумілий для не експертів, і може зробити основу незрозумілості щодо обґрунтування прийняття рішень.

Виникають питання: як може існувати ефективний політичний контроль над прийняттям рішень, якщо ключовий компонент у формуванні прийняття рішень фактично невідомий? Як поліція може повністю звітувати про свої рішення, якщо вони частково спиралися на аналіз, який вони самі не в змозі пояснити? В цьому сенсі прозорість розглядається як частина ідеального вирішення проблем використання ML для підзвітного прийняття рішень. Для досягнення прозорості інформація має бути доступною та зрозумілою [8]. Однак це складно, коли йдеться про напівавтоматизовані інтелектуальні системи. Разом з цим, підзвітність може бути можливою без повної прозорості (наприклад, розкриття вихідного коду) шляхом розробки підзвітності в програмному забезпеченні.


Downloaded from periodicals.karazin.ua/cscs. For personal use only.
No other uses without permission. Copyright © Karazin Kharkiv National University 2024. All rights reserved.