

Міністерство освіти і науки України
Український державний університет залізничного транспорту



МАТЕРІАЛИ

двадцять першої науково-практичної міжнародної конференції
*«Міжнародна транспортна інфраструктура,
індустріальні центри та корпоративна логістика»*
(5-6 червня 2025р. м. Харків, Україна)



MT.KART.EDU.UA

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО ІНФРАСТРУКТУРИ УКРАЇНИ
ТРАНСПОРТНА АКАДЕМІЯ УКРАЇНИ
АТ «УКРАЇНСЬКА ЗАЛІЗНИЦЯ»
CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS (FRANCE)
INSTITUTE OF AUTOMATIC CONTROL TELEMATICS OF
TRANSPORT (POLAND)
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО
ТРАНСПОРТУ
ІНСТИТУТ ЕКОНОМІКИ ПРОМИСЛОВОСТІ НАН УКРАЇНИ

Матеріали

*Двадцять першої науково-практичної
міжнародної конференції*

**«МІЖНАРОДНА ТРАНСПОРТНА
ІНФРАСТРУКТУРА,
ІНДУСТРІАЛЬНІ ЦЕНТРИ ТА
КОРПОРАТИВНА ЛОГІСТИКА»**

(5 - 6 червня 2025р. м. Харків)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: *Панченко С.В.*, д.т.н., проф., ректор Українського державного університету залізничного транспорту (Харків).

Заступники голови: *Каграманян А.О.*, к.т.н., доц., проректор з науково-педагогічної роботи .Українського державного університету залізничного транспорту (Харків);
Дикань В.Л., д.е.н., проф., завідувач кафедри економіки та управління виробничим і комерційним бізнесом Українського державного університету залізничного транспорту (Харків).

Секретаріат:

Толстова А.В. к.е.н., доц., доцент кафедри економіки та управління виробничим і комерційним бізнесом Українського державного університету залізничного транспорту (Харків).

Шановал Г.В. к.т.н., доц., заступник декана з денної форми навчання Факультету УПП Українського державного університету залізничного транспорту (Харків).

Примаченко Г.О. к.т.н., доц., доцент кафедри транспортних систем та логістики Українського державного університету залізничного транспорту (Харків).

УДК 004.8:005.8:336:338.2

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ КІБЕРЗАХИСТІ ФІНАНСОВОЇ СКЛАДОВОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

THE ROLE OF AI IN CYBER DEFENCE OF THE FINANCIAL COMPONENT OF THE STATE ECONOMIC SECURITY

*В.А. Янковський, аспірант,
ДВНЗ «Донецький національний технічний університет» (м. Дрогобич)*

*V.A. Yankovskyi, postgraduate student,
SHEI «Donetsk National Technical University» (Drogobych)*

В умовах стрімкої цифровізації фінансового сектору зростає потреба у надійному кіберзахисті як ключовій складовій економічної безпеки та національних інтересів держави. Ефективне протистояння кіберзагрозам потребує впровадження інноваційних технологій, зокрема штучного інтелекту (далі – ШІ), здатного оперативно виявляти загрози та мінімізувати фінансові ризики, що в свою чергу не лише підсилює захист фінансової системи, а й сприяє сталому розвитку цифрового суспільства та зміцненню довіри громадян до державних інституцій.

Відповідно до статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII [1], кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Інтереси національної безпеки держави потребують більш інтенсивного впровадження цифрової економіки, функціонування якої відбувається здебільшого у кіберпросторі, який виконує роль місця взаємодії інформаційних потоків та проявів глобалізаційних процесів. Панченко О. та Гнатенко В. зазначають [2, с. 26], що система національної безпеки у кіберекономічному розрізі складається з наступних елементів: цифрова економіка, економічна кібербезпека та кіберпростір.

На сучасному етапі розвитку цифрових процесів, існує багато кіберзагроз які несуть велику шкоду першочергово для фінансового сектору кожної країни, що в свою чергу впливає на загальний рівень економічної безпеки держави. До основних кіберзагроз для фінансового сектору можна віднести: фішинг (використання фальшивих сайтів або направлення різних повідомлень, з метою отримання конфіденційної

інформації людини (паролі, інформація щодо платіжних засобів)); DDos-атаки (хакерські атаки на вебсайти та сервери державних і фінансових установ з метою їх перевантаження та зробити недоступними, та отримання конфіденційної інформації); розвідка (отримання конфіденційної інформації щодо фінансової установи та громадян з метою здійснення кібератаки); кібершпигунство (отримання конфіденційної інформації про фінансові операції, інтелектуальну власність тощо); шахрайство з кредитними картками (попереднє отримання конфіденційної фінансової інформації про платіжні засоби громадян та проведення шахрайських транзакцій); розповсюдження шкідливого програмного забезпечення (використання вірусного програмного забезпечення для які можуть пошкодити або зруйнувати технологічні системи державних інституцій та отримати доступ до конфіденційної інформації) та інше.

Одним із дієвих інструментів по мінімізації ризиків та боротьбі з кіберзагрозами та розвитку і оптимізації фінансових процесів у фінансовому секторі є ШІ, так його вже використовують за наступними напрямками:

- автоматизація бізнес-процесів (наприклад використовується при здійсненні фінансового моніторингу та автоматизації транзакцій);
- аналіз Big Data (використання машинного навчання аналізу даних, для покращення прогнозування, управління ризиками та розробки нових продуктів та послуг);
- фінансове консультування та інвестування (автоматизовані системи при формуванні інвестиційних стратегій);
- виявлення шахрайства та мінімізація ризиків (аналіз транзакцій для виявлення шахрайських операцій та оцінки фінансових ризиків, що в свою чергу підвищує безпеку та мінімізує фінансові втрати);
- кредитний скоринг (аналіз поведінкових моделей та архівних даних, що дозволяє досягти об'єктивного кредитного рішення).

Таким чином, можна стверджувати, що використання інструментів ШІ у фінансовому секторі України є доволі активним, але варто зазначити, що для подальшого розвитку впровадження елементів ШІ, державі потрібно провести зміни у нормативно-правових актах, з метою встановлення чітких правил та стандартів при використанні ШІ, зокрема з дотриманням високих стандартів безпеки персональних даних та етичних норм. Зазначені зміни зроблять фінансовий сектор України більш розвиненим та підвищать рівень економічної безпеки держави в цілому.

[1] Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII URL: [Про основні засади забезпе... | від 05.10.2017 № 2163-VIII](#) (Дата звернення 28.05.2025).

[2] Панченко О.А., Гнатенко В.С. (2021). Економічна кібербезпека в державній системі національної безпеки. *Публічне урядування*. 2021. (2 (27), С. 22-31. DOI: [https://doi.org/10.32689/2617-2224-2021-2\(27\)-3](https://doi.org/10.32689/2617-2224-2021-2(27)-3) (Дата звернення 28.05.2025).

МАТЕРІАЛИ
ДЕВ'ЯТЬ ПЕРШОЇ НАУКОВО-ПРАКТИЧНОЇ
МІЖНАРОДНОЇ КОНФЕРЕНЦІЇ
«МІЖНАРОДНА ТРАНСПОРТНА ІНФРАСТРУКТУРА,
ІНДУСТРІАЛЬНІ ЦЕНТРИ ТА КОРПОРАТИВНА ЛОГІСТИКА»
(5-6 ЧЕРВНЯ 2025 РОКУ)

Відповідальний за випуск А.В. Толстова

Підписано до друку 25 червня 2025р.
Формат паперу 60X84 1/16. папір писальний.
Умовн.-друк. Арк. **25,45.** Обл.— вид. арк.. **26,1.**
Замовлення № Тираж 300. Ціна договірна

Видавництво УкрДУЗТу, свідоцтво ДК № 6100 від 21.03.2018 р.