AISE 2024

1-2.03.2024

ШТУЧНИЙ ІНТЕЛЕКТ У НАУЦІ ТА ОСВІТІ

ЗБІРНИК МАТЕРІАЛІВ МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

ARTIFICIAL INTELLIGENCE IN SCIENCE AND EDUCATION

PROCEEDINGS OF THE INTERNATIONAL SCIENTIFIC CONFERENCE

ОФІС ПІДТРИМКИ ВЧЕНОГО

ІНСТИТУТ ЦИФРОВІЗАЦІЇ ОСВІТИ НАПН УКРАЇНИ

ЖИТОМИРСЬКА ПОЛІТЕХНІКА ДЕРЖАВНИЙ УНІВЕРСИТЕТ

INNOVATIVE UNIVERSITY AND LEADERSHIP 10|5 PROJECT & NGO INNOVATIVE UNIVERSITY

Державна наукова установа «Український інститут науково-технічноїекспертизи та інформації»,
Інститут цифровізації освіти НАПН України,
Київський столичний університет імені Бориса Грінченка,
Державний заклад «Південноукраїнський національний педагогічний університет імені К.Д. Ушинського»,
Державний університет «Житомирська політехніка»,
Офіс підтримки вченого,
ADA University (Azerbaijan),
ВГО «Інноваційний університет»,
Центр інформаційно-аналітичного та технічного забезпечення моніторингу об'єктів атомної енергетики НАН України

ШТУЧНИЙ ІНТЕЛЕКТ У НАУЦІ ТА ОСВІТІ (AISE 2024)

ЗБІРНИК МАТЕРІАЛІВ МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ

1-2 березня 2024 року

КИЇВ, 2024

УДК 378: 044 : 001.37

Штучний інтелект у науці та освіті (AISE 2024): збірник матеріалів міжнародної наукової конференції (Київ, 1-2 березня 2024 р.). / [упоряд: А. Яцишин, В. Матусевич, В. Ковалеко]. К.: УкрІНТЕІ, 2024. – 604 с.

ISBN 978-966-479-141-7

Рекомендовано до опублікування та поширення через мережу інтернет
Вченими радами Державної наукової установи «Український інститут науково-технічної експертизи та інформації» (протокол № від …2024) та
Інституту цифровізації освіти НАПН України (протокол №7 від 26.04.2024)

Збірник матеріалів містить наукові статті та тези доповідей поданих на Міжнародну наукову конференцію «Штучний інтелект у науці та освіті» (AISE 2024), що відбулася 1-2 березня 2024 року. Матеріали подані на конференцію були розглянуті під час роботи таких секцій: Штучний інтелект в освіті; Штучний інтелект у науці; Штучний інтелект в економіці; Нейронні мережі та машинне навчання. В рамках конференції було проведено майстер-клас «GPT-store. ШІ-сервіси в навчанні».

Збірник адресовано всім хто цікавиться питаннями застосування штучного інтелекту для освіти та науки.

Подяка. Організатори конференції та автори публікації вдячні захисникам України за можливість продовжувати працювати та займатися науковою і викладацькою діяльністю у період війни.

З вдячністю Збройним силам України!
З вірою у перемогу України!

ISBN 978-966-479-141-7

***

СИМБІОЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

Ярослав Дорогий[1], Василь Цуркан[2]
[1]Донецький національний технічний університет, Київ, Україна
[2]КПІ ім. Ігоря Сікорського, Київ, Україна
E-mail: cisco.rna@gmail.com

АНОТАЦІЯ. Проаналізовано процес захищання інформації об'єктів критичної інформаційної інфраструктури. Виокремлено заходи забезпечення непорушності властивостей конфіденційності, цілісності та доступності. Продемонстровано форми співжиття окремих різновидів систем захисту інформації. Крім того акцентовано увагу на можливості їхнього інтегрування розробленням і впровадженням гібридних систем захисту, запропонованих штучним інтелектом на базі певного набору критеріїв.

КЛЮЧОВІ СЛОВА: штучний інтелект, набір критеріїв, система захисту, ОКІ, симбіоз.

I. Вступ

Порушення безпеки критичної інфраструктури в Україні є серйозною загрозою для життєво важливих національних інтересів. З метою ефективного протидії таким порушенням необхідно вживати заходів на об'єктовому рівні управління, зокрема, забезпечуючи безпеку об'єктів критичної інформаційної інфраструктури в критичних сферах держави [1].

II. Основна частина (назва)

Розв'язання цього завдання включає в себе розроблення та впровадження комплексних систем захисту інформації [2], систем інформаційної безпеки [3], а також систем управління інформаційною безпекою [2].

Характер упровадження таких систем полягає в орієнтації на інформаційно-комунікаційну систему як об'єкт захисту інформації [2–4] та певну специфіку сектору критичної інфраструктури, для якого такі системи розгортаються [5]. При цьому гарантування непорушності властивостей конфіденційності, цілісності та доступності може бути досягнуте за допомогою комплексних систем захисту інформації, систем інформаційної безпеки та систем управління інформаційною безпекою. Вибір між цими системами визначається необхідністю виконання вимог щодо захисту державної таємниці, службової інформації, а також державних і єдиних реєстрів [2], вимог стандартів [6] та певною специфікою сектору критичної інфраструктури.

Враховуючи вищезазначене, представляє інтерес розробка набору критеріїв вибору типу системи захисту, який можна застосувати в алгоритмах штучного інтелекту для автоматизації цього вибору або пошуку варіантів цих систем, які представляють собою певний симбіоз позитивних характеристик окремо взятих типів вказаних систем захисту.

III. Висновки

Таким чином, захист об'єктів критичної інформаційної інфраструктури конкретного сектору критичної інфраструктури може бути реалізований шляхом розроблення однієї чи комбінації систем захисту інформації, або певних гібридних варіантів, запропонованих штучним інтелектом на базі визначеного набору критеріїв.

IV. Список використаних джерел

[1] Закон України від 16.11.2021 №1882-IX "Про критичну інфраструктуру". URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 14.01.2024).

[2] Закон України від 05.07.1994 №80/94-ВР "Про захист інформації в інформаційно-комунікаційних системах". URL: https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80 (дата звернення: 14.01.2024).

[3] Постанова Кабінету міністрів України від 19.06.2019 № 518 "Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури". URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 14.01.2024).

[4] НД ТЗІ 3.6-004-21 "Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці". URL: https://cip.gov.ua/services/cm/api/attachment/download?id=53375 (дата звернення: 10.05.2023).

[5] Постанова Кабінету міністрів України від 09.10.2020 №943 "Деякі питання об'єктів критичної інформаційної інфраструктури". URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF (дата звернення: 14.01.2024).

[6] ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection. Information security management systems. Requirements". [Valid from 2022-10-25]. URL: https://www.iso.org/standard/27001 (accessed on: 14.01.2024).

SYMBIOSIS OF INFORMATION PROTECTION SYSTEMS FOR CRITICAL INFRASTRUCTURE OBJECTS BASED ON ARTIFICIAL INTELLIGENCE

FirstName, LastName

ABSTRACT. The process of securing information for critical information infrastructure objects has been analyzed. Measures to ensure the integrity of confidentiality, integrity, and availability properties have been highlighted. The coexistence forms of individual types of information security systems have been demonstrated. Additionally, emphasis has been placed on the potential for their integration through the development and implementation of hybrid protection systems, proposed by artificial intelligence based on a specific set of criteria.

KEYWORDS: artificial intelligence, set of criteria, protection system, CI objects, symbiosis.