

РЕЦЕНЗІЯ

на дисертацію Шапрана Олександровича
на тему “Методика підвищення захищеності персональних даних
користувачів системи дистанційного навчання
Збройних Сил України”, подану на здобуття ступеня доктора філософії
з галузі знань 12 “Інформаційні технології”
за спеціальністю 125 “Кібербезпека”

Важливим напрямком розробки та впровадження як систем кібербезпеки взагалі, так і систем захисту персональних даних користувачів системи дистанційного навчання є можливість підвищення їх ефективності за рахунок розвитку математичного та програмного забезпечення. Результати дослідження доводять, що актуальним в цьому напрямку є використання моделей та методів штучного інтелекту, а саме, нечіткої логіки та гіbridних мереж. У кібербезпеці використовується кілька різних методів та моделей штучного інтелекту, а саме, нечітка логіка, генетичні алгоритми, нейронні мережі та машинне навчання.

Незважаючи на стрімкий розвиток теорії штучного інтелекту взагалі, актуальним є завдання удосконалення існуючого та розробки нового математичного та програмного забезпечення системи захисту персональних даних користувачів системи дистанційного навчання на основі нечіткого виведення.

Подана на розгляд дисертаційна робота на тему “Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України” присвячена розв'язанню актуального наукового завдання по підвищенню захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України.

Дисертант обґрунтує вибір теми дослідження, завдання, що сформульовані відповідно поставленої мети, об'єкт та предмет дослідження, а також комплекс використаних взаємопов'язаних методів на основі системного підходу з застосуванням моделей і методів кібербезпеки, математичної логіки, теорії множин, штучного інтелекту: нечіткої логіки та нечітких нейронних мереж. Для вирішення наукового завдання використано системний підхід. Методика проведення експерименту та перевірки достовірності розроблених наукових положень реалізована на основі методів комп'ютерного моделювання.

Найбільш вагомими результатами дисертаційного дослідження Шапрана Олександровича є:

вперше запропонована методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України, яка забезпечує своєчасне реагування на потік загроз та базується на основі впровадження моделей та методів нечіткої логіки та гіbridних мереж;

удосконалено модель оцінки стану системи захисту персональних даних, яка на відміну від існуючих базується на нечіткому логічному виведенні (алгоритм Мамдані);

вперше запропоновано метод прогнозування стану системи захисту персональних даних з метою попередження шкідливого впливу загроз, який побудований на основі технології адаптивної нейронної нечіткої мережової системи виведення ANFIS (Adaptive Neuro-Fuzzy Inference System).

Дисертаційне дослідження пов'язане з науково-дослідними роботами Національного університету оборони України за темами “Обґрунтування доцільного варіанту побудови системи дистанційного навчання вищого військового навчального закладу” (номер державної реєстрації № 0120U103270) та “Удосконалення системи дистанційного навчання Збройних Сил України: цифровізація та інтелектуалізація” (номер державної реєстрації № 0122U200401).

Структура роботи логічно продумана, збалансовані складові частини і підпорядкована реалізації основних завдань дослідження та складається з анотації, чотирьох розділів, загальних висновків, списку використаних джерел і додатків. На основі проведеного аналізу, а також теоретичних знань у сфері кібербезпеки, глибокого розуміння сучасної ситуації у системі захисту персональних даних користувачів системи дистанційного навчання Збройних сил України дисертантом запропонована методика, обґрунтованість якої підтверджується змістом дослідження.

Зміст і структура роботи відповідають основним положенням дисертаційного дослідження.

У *першому розділі* проаналізовано наукову літературу щодо існуючих технологій захисту інформації та персональних даних систем дистанційного навчання, результати засвідчили існування потреби у запровадженні ефективних змін для забезпечення ефективного захисту персональних даних користувачів у зв'язку з підвищенням рівня використання інструментів штучного інтелекту в кіберзлочинах та підвищенням загального рівня кіберзагроз і кількості кібератак з початком війни.

У *другому розділі* дисертантом були обґрунтоване провадження штучного інтелекту в методи, засоби та процедури кібербезпеки та захисту персональних даних, обґрунтована концепція підвищення захищеності персональних даних на основі штучного інтелекту, розроблені методика підвищення захищеності персональних даних на основі моделей та методів нечіткої логіки та гіbridних мереж і модель оцінки стану системи захисту персональних даних.

У *третьому розділі* була обґрунтована доцільність застосування методу прогнозування на основі нейро-нечіткого логічного виведення та розроблено метод прогнозування захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України на основі адаптивної системи

нейро-нечіткого виведення. Дослідження розробленого методу прогнозування стану системи захисту персональних даних дозволяє зробити висновок про високу ступінь його адекватності реальними вихідними даними та рекомендувати цей метод до практичного використання. Варто зазначити, що нечіткі моделі адаптивних систем нейронечіткого виведення можуть вважатися ефективним інструментом для інших розробок в кібербезпеці.

У четвертому розділі були висвітлені рекомендації щодо реалізації розроблених наукових результатів, проведено комп’ютерне моделювання елементів захисту системи дистанційного навчання і дослідження ефективності методики підвищення захищенності персональних даних в системі дистанційного навчання Збройних Сил України. Впровадження результатів дисертаційного дослідження дозволило підвищити ефективність захисту персональних даних в системі дистанційного навчання Збройних Сил України, а саме, захищеність під час кризових періодів покращилася на 26-28%, а час реагування на загрози захищенності даних зменшився на 28-30%. Що ще раз підтверджує досягнення мети наукового дослідження.

Практичне значення одержаних результатів полягає в тому, що їх реалізація доцільна в математичному та програмному забезпеченні, як складової системи управління захистом персональних даних.

Аналіз публікацій Шапрана О.О. засвідчив їхню відповідність вимогам до оприлюднення результатів дисертацій. Основні результати дослідження відображені у 23 наукових працях, серед яких: 11 статей, опублікованих у періодичних виданнях, що входять до переліку видань МОН України для публікацій результатів досліджень з технічних наук (з них 2 у виданнях, які індексуються у наукометричних базах Scopus та Web of Science, а також 1 у періодичному науковому виданні держави, яка входить до Європейського Союзу), 12 матеріалах науково-технічних конференцій (з яких 1 індексовані у наукометричній базі Scopus). Додатково матеріали та результати роботи опубліковані у двох звітах з НДР.

Дисертаційна робота є завершеною працею. Висновки відображають основні наукові досягнення проведеного дослідження, містять узагальнюючі і конкретні рекомендації.

Поряд із вказаними позитивними сторонами рецензована робота містить ряд моментів, які викликають зауваження та потребують уточнення, а саме:

1. На початку роботи варто було б навести загальну схему Системи дистанційного навчання Збройних Сил України, на якій позначити елементи підсистеми захисту персональних даних користувачів.

2. У роботі недостатньо приділено уваги аналізу існуючих методів нечіткого логічного виведення та обґрунтуванню вибору саме алгоритму Мамдані у якості основного методу.

3. Автор стверджує, що удосконалена модель оцінки стану системи захисту персональних даних забезпечує «оптимальний метод дефазифікації,

раціональні ваги та кількість правил, оптимальні параметри функцій належності». Разом з тим, у роботі не згадується за яким критерієм є оптимальним метод дефазифікації та параметри функцій належності і що саме мається на увазі, коли говориться про раціональні ваги та кількість правил.

Водночас, зазначені нами міркування та побажання не завадили загальному позитивному сприйняттю дисертації та переважно мають характер рекомендацій, оскільки у дисертації розв'язані всі поставлені дисертантом дослідницькі завдання.

Представлена дисертаційна робота Шапрана Олександра Олександровича є завершеною; сформульовані у ній положення, результати та висновки мають наукову новизну й практичну цінність.

При детальному розгляді дисертаційної роботи порушень академічної доброчесності не виявлено.

Висновок. У цілому дисертаційна робота Шапрана Олександра Олександровича “Методика підвищення захищеності персональних даних користувачів системи дистанційного навчання Збройних Сил України” є цілісною, самостійною, завершеною роботою на правах рукопису, яку виконано на актуальну тему з використанням широкого кола наукових методів дослідження. Робота характеризується чіткістю змісту, містить науково обґрунтовані науково-теоретичні результати, які мають наукову новизну, теоретичне та практичне значення, свідчать про особистий внесок здобувача та достатньо повно представлені у наукових працях. Дисертація відповідає спеціальності 125 – Кібербезпека та вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44), а також до оформлення дисертацій, затвердженим наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 (з наступними змінами), а її автор – Шапран Олександр Олександрович – заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Рецензент:

доктор технічних наук, професор, професор кафедри систем інформаційного та кібернетичного захисту Державного університету інформаційно-комунікаційних технологій

Володимир АХРАМОВИЧ

“ 03 ” 11 2023 року

Відпис Ахрамовича Володимира
засвідчено,
учений секретар Державного університету інформаційно-комунікаційних технологій

