РЕЦЕНЗІЯ
на дисертацію
Асєєвої Людмили Анатоліївни
«Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки»,
подану на здобуття наукового ступеня доктора філософії з галузі знань 12 - Інформаційні технології за спеціальністю 125 - Кібербезпека

Актуальність теми дисертації.

Управління інформаційною безпекою є важливою складовою комплексної системи управління будь-якого сучасного підприємства чи установи, що особливо актуально для вітчизняних підприємств в умовах збройної агресії та загального зростання рівня кіберзлочинності. Організації приділяють багато уваги розробці систем управління інформаційною безпекою, що призначені для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки. Враховуючи постійний розвиток кіберзлочинцями засобів атак на інформаційні системи, задачі розвитку та удосконалення методів та технологій забезпечення інформаційної безпеки підприємств є актуальними.

Застосування методів машинного навчання є ефективним при вирішенні задач в багатьох галузях, в тому числі при ідентифікації атак в кібербезпеці. Нечітка логіка дозволяє моделювати невизначеність та розмитість даних, дає змогу побудувати алгоритми управління та класифікації даних на основі лінгвістичних змінних й наборів правил бази знань.

Таким чином, тема «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки» дисертації Асєєвої Людмили Анатоліївни є актуальною і присвячена вирішенню важливого для науки і практики наукового завдання з розробки моделей, методів та алгоритмів системи управління інформаційною безпекою у складі інформаційної системи підприємства на основі підходів машинного навчання та нечіткої логіки.

Також слід відмітити, що актуальність теми дисертаційного дослідження додатково підтверджується її безпосереднім зв'язком із Стратегією кібербезпеки України від 26 серпня 2021 року №447/2021.

Оцінка обгрунтованості наукових положень, висновків і рекомендацій дисертації.

Обгрунтованість наукових положень, висновків і рекомендацій дисертації визначається якісним аналізом та узагальненням значного числа наукових праць вітчизняних та закордонних авторів, коректним застосуванням загальнонаукових та емпіричних методів дослідження, перевіркою теоретичних результатів дисертації на наборах тестових даних з використанням комп'ютерного моделювання та результатами їх застосування в практичній діяльності підприємств, які підтверджені актами впровадження.

Оцінка новизни наукових результатів дисертації.

У дисертації одержані наступні нові наукові результати.

1. Вперше розроблено гібридний метод виявлення вторгнень до корпоративної мережі, новизна якого полягає у використанні ансамблевого підходу на базі алгоритмів нечіткої логіки для поєднання результатів класифікації даних окремими моделями машинного навчання, що забезпечило більш високу точність у порівнянні з існуючими методами.

2. Отримав подальший розвиток метод обрання набору ознак для навчання класифікаторів вторгнень, який на відміну від інших базується на ансамблевому підході з використанням нечіткої логіки для оцінки важливості ознаки, що дало можливість підвищити надійність та зменшити розмірність набору ознак.

3. Отримала подальший розвиток модель оцінки ризиків інформаційної безпеки документів підприємства за рахунок формалізації їх структури, операцій над ними та факторів порушення їх цілісності, конфіденційності та доступності на основі нечіткої логіки і методу аналізу ієрархій, що дало можливість врахувати невизначеність та розмитість інформації щодо складових небезпеки.

Практична цінність одержаних результатів.

Практичне значення одержаних результатів полягає в збільшенні швидкодії та точності роботи аналітичного блоку системи управління інформаційною безпекою у складі інформаційної системи підприємства. Застосування запропонованого методу обрання набору ознак для навчання моделей класифікації вторгнень дозволило зменшити час навчання на 50-60% та скоротити час виявлення можливого вторгнення на 30-40% за рахунок підвищення надійності та зменшення розмірності набору ознак. Використання результатів дослідження дозволяє збільшити точність виявлення вторгнень до корпоративної мережі підприємства у порівнянні з існуючими методами на 3-5%. Результати дисертаційної роботи прийнято до впровадження в ТОВ "Хуавей Україна", в ТОВ "РЕНТСОФТ", в навчальному процесі Державного університету інформаційно-комунікаційних технологій.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

Метою дисертації є збільшення швидкодії і точності роботи аналітичного блоку системи управління інформаційною безпекою у складі інформаційної системи підприємства за рахунок розробки відповідних моделей, методів та алгоритмів на основі підходів машинного навчання та нечіткої логіки. Ознайомлення зі змістом дисертації, основними публікаціями та анотацією дозволяє визнати, що мету дослідження досягнуто.

Робота написана українською мовою, виконана на належному науковому рівні, є завершеною науковою працею, має практичне значення та відображає розв'язання актуального наукового завдання. Дисертація характеризується цілісністю та логічністю викладу матеріалів. Загальний обсяг роботи складає 189 сторінок, з яких 137 сторінок основного тексту. До структури дисертації входить вступ, чотири розділи, висновки, список використаних джерел зі 169

найменувань та три додатки.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

За своїм змістом дисертаційна робота здобувача Асєєвої Л.А. повністю відповідає тимчасовому стандарту освітньо-наукової програми підготовки докторів філософії з кібербезпеки Державного університету інформаційно-комунікаційних технологій МОН України.

Поставлене наукове завдання в дисертаційній роботі виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння та наукові публікації здобувача, можна зробити висновок, що дисертаційна робота Асєєвої Л.А. є результатом самостійних досліджень здобувача і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Оприлюднення результатів дисертаційної роботи

Результати дисертаційної роботи опубліковано у 14 наукових працях, у тому числі: 7 наукових статей, серед яких 1 стаття в іноземному науковому виданні, що індексується в наукометричній базі Scopus, та 6 наукових статей у періодичних виданнях України, що на момент публікації були включені до переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів. Автором також підготовлено 7 тез доповідей в матеріалах наукових конференцій. Кількість, обсяг та зміст друкованих праць відповідають вимогам МОН України щодо публікацій основного змісту дисертації на здобуття наукового ступеня доктора філософії та надають авторові право публічного захисту дисертації.

Проведений аналіз наукових праць здобувача показав, що основні результати дисертаційної роботи повноцінно відображені в публікаціях автора. Науковий рівень публікацій високий, принципи академічної доброчесності дотримано. Особистий внесок здобувача у зазначених наукових публікаціях є достатнім.

Недоліки та зауваження до дисертаційної роботи.

1. У списку використаних джерел дисертації зі 169 посилань лише близько 20% складають роботи українських дослідників, інші джерела є роботами закордонних колег. Бажано було б звернути більше уваги на дослідження українських науковців, які працюють у галузі кібербезпеки.

2. Автор приділив велику увагу способам збільшення швидкості навчання моделі та виконання класифікації даних для ідентифікації вторгнень. Доцільно було б розглянути можливість використання паралельних обчислень для підвищення швидкості навчання.

3. У тексті дисертаційної роботи (наприклад, на с. 97 та на с. 100) автор констатує, що використані набори даних є незбалансованими. Проте у роботі наведено результати багатокласової класифікації на основі цих даних. З тексту

роботи незрозуміло, яким чином навчалася модель класифікації для міноритарних класів.

Представлені вище зауваження не зменшують загальну наукову новизну та цінність результатів дисертації. Робота має вагоме теоретичне та практичне значення.

Висновок про дисертаційну роботу.

Дисертаційна робота здобувача наукового ступеня доктора філософії Асєєвої Людмили Анатоліївни на тему «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеним науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання з розробки моделей, методів та алгоритмів системи управління інформаційною безпекою у складі інформаційної системи підприємства на основі підходів машинного навчання та нечіткої логіки, що має істотне значення для галузі знань 12 Інформаційні технології. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п.6 – 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

Здобувач Асєєва Л.А. заслуговує на присудження ступеня доктора філософії за спеціальністю 125 - Кібербезпека.

Рецензент:
доктор технічних наук, професор,
директор Навчально-наукового інституту Захисту інформації
Державного університету інформаційно-комунікаційних технологій
МОН України

Віталій САВЧЕНКО

Підпис Віталія Савченка
засвідчую, учений секретар
Державного університету
інформаційно-комунікаційних
технологій

Анжела Тямина

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Ідентифікаційний код 38855376
УКРАЇНА, м. КИЇВ