ВІДГУК

Офіційного опонента – доктора технічних наук, професора, завідувача кафедри захисту інформації Національного університету «Львівська політехніка» Опірського Івана Романовича на дисертаційну роботу Проскуріна Дмитра Петровича на тему «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання», представлену на здобуття ступеня доктора філософії в галузі знань 12 – «Інформаційні технології» за спеціальністю 122 – «Комп'ютерні науки»

Актуальність теми дисертації

Дисертаційна робота Проскуріна Дмитра Петровича на тему "Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання" є надзвичайно актуальною в сучасному світі, де кіберзагрози постійно зростають, а вимоги до надійності та безпеки інформаційних систем стають дедалі жорсткішими.

Генератори послідовностей псевдовипадкових чисел (ГППВЧ) відіграють ключову роль у криптографічних алгоритмах, що використовуються в різних критично важливих сферах, таких як телекомунікації, фінансові послуги та державні служби. Надійність цих алгоритмів безпосередньо залежить від якості використовуваних ГППВЧ, що робить оцінювання їхньої якості критично важливим завданням для забезпечення безпеки та захисту інформації.

Сучасні методи оцінювання якості ГППВЧ часто потребують великих обсягів даних і значних обчислювальних ресурсів, що ускладнює їх застосування в умовах обмежених ресурсів. Це створює необхідність у розробці нових підходів, які б дозволили ефективно оцінювати якість ГППВЧ за умов обмеженої кількості вхідних даних і обчислювальних можливостей.

Запропонована в дисертації інформаційна технологія, яка базується на методах машинного навчання, таких як гібридні та згорткові нейронні мережі, спрямована на підвищення точності та швидкості оцінювання якості ГППВЧ.

Використання методів машинного навчання дозволяє адаптивно та ефективно аналізувати послідовності псевдовипадкових чисел, навіть за умов обмеженого обсягу вхідних даних, що є надзвичайно важливим для реальних умов застосування.

Удосконалення методів оцінювання якості ГППВЧ забезпечує нові можливості для використання генераторів у різних практичних додатках, де доступ до великих обсягів даних може бути обмеженим, і гарантує високий рівень надійності та безпеки інформаційних систем. Це особливо актуально для таких сфер, як криптографія, стільникові мережі LTE/5G/6G, технології на основі безпілотних авіаційних систем (UAV) та захист критичної інформаційної інфраструктури.

Таким чином, дана дисертаційна робота є важливим внеском у розвиток методів оцінювання якості генераторів псевдовипадкових чисел, сприяючи підвищенню рівня безпеки та надійності інформаційних систем у сучасному світі, що постійно змінюється.

Оцінка обґрунтованості та достовірності наукових положень

Обґрунтованість наукових положень, висновків та практичних рекомендацій обумовлена аналізом та теоретичним узагальненням широкого кола наукових праць вітчизняних та закордонних авторів. Використання достатньої кількості результатів наукових та практичних публікацій у їх поєднанні з задіяними коректними методами досліджень мають позитивний вплив на достовірність наукових положень, висновків та практичних рекомендацій, що подані в роботі.

Для розв'язання конкретних завдань дослідження автор сучасні методи штучного інтелекту, включаючи гібридні та згорткові нейронні мережі, що дозволяє суттєво підвищити точність та швидкість оцінювання якості генераторів навіть за умови обмеженої кількості вхідних даних. Це відкриває нові можливості для їх застосування в реальних умовах, де доступ до великої кількості даних може бути обмеженим, і забезпечує високий рівень стійкості та безпеки інформаційних систем.

Оцінка новизни наукових результатів дисертаційного дослідження

У дисертаційній роботі одержані наступні нові наукові результати.

1. *Вперше* розроблено модель ідентифікації джерела послідовностей псевдовипадкових чисел, що за рахунок використання гібридної нейронної мережі та обмеженої кількості вхідних даних для навчання та оптимізації, дає можливість виявляти генератори, якими були сформовані послідовностей псевдовипадкових чисел.

2. *Вперше* розроблено малоресурсну інформаційну технологію, яка за рахунок використання моделей ідентифікації джерела послідовності псевдовипадкових чисел і передбачення наступної послідовності, а також методу оцінювання якості послідовностей псевдовипадкових чисел, дає можливість здійснювати комплексне оцінювання якості генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних, виявляти неякісні, ненадійні і скомпроментовані генератори.

3. *Удосконалено* модель передбачення наступної послідовності псевдовипадкових чисел, що за рахунок використання гібридної нейронної мережі та обмеженої кількості вхідних даних для навчання, дозволяє передбачати чергові послідовності для неякісних генераторів псевдовипадкових чисел.

4. *Отримав подальшого розвитку* метод оцінювання якості послідовностей псевдовипадкових чисел, який за рахунок використання одновимірної рекурентної нейронної мережі та датасетів, сформованих різними генераторами псевдовипадкових чисел, дозволяє більш швидко оцінювати якість генераторів для криптографічних та інших застосувань в галузі комп'ютерних наук.

Практична цінність отриманих результатів

Практичне значення та використання результатів дисертаційного дослідження полягає у тому, що отримані результати можуть бути використані відповідними органами для ефективного оцінювання генераторів псевдовипадкох послідовностей, крім цього було:

- Використання гібридної нейронної мережі (HNN) дало можливість дослідити 8 реалізованих генераторів та 4 000 згенерованих послідовностей (для

навчання та оптимізації) і ідентифікувати на основі нових для HNN даних з усередненою точністю 87,14% джерела послідовностей псевдовипадкових чисел;

- Використання гібридної нейронної мережі (HNN) дало можливість більш точно передбачати наступні послідовності псевдовипадкових чисел у порівнянні з рекурентною нейронною мережею (RNN) та згортковою нейронною мережею (CNN) – на 2,52% та 1,44% відповідно;
- Реалізація одновимірної згорткової нейронної мережі (1D-CNN) та генераторів псевдовипадкових чисел середовища розробки Python підтвердила можливість на 40% швидшого оцінювання якості генераторів у порівнянні з методом chi-квадрат (з незмінним рівнем точності P-value), а також можливість аналізу менших за довжиною послідовностей
- Зазначені результати лягли в основу малоресурсної інформаційної технології, що дозволяє здійснювати комплексне оцінювання якості генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних, виявляти неякісні, ненадійні і скомпроментовані генератори;
- Отримані результати будуть корисні для криптографії, стільникових мереж LTE / 5G / 6G, технологій на основі UAV, захисту критичної інформаційної інфраструктури держави.

Зв'язок роботи з науковими програмами, планами, темами

Результати були впроваджені в навчальний процес кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій (акт впровадження №03 від 09.05.2024) і в наукову діяльність Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Національного авіаційного університету (акт впровадження 30.11.2024) і Головного управління розвідки Міністерства оборони України.

Повнота викладу основних результатів дисертації в публікаціях

Наукові результати дисертації висвітлені у 13 наукових публікаціях, серед яких 3 статей у наукових виданнях, включених до переліку наукових фахових видань України, та 5 статті у виданнях, індексованих у базах даних Web of Science Core Collection та/або Scopus. Результати дослідження були апробовані на 5

наукових конференціях та реалізовані в науково-технічних розробках. Всі публікації відповідають вимогам щодо наукового рівня та академічної доброчесності, що підтверджує високу наукову цінність дисертаційної роботи.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення та дотримання принципів академічної доброчесності

Дисертаційна робота має добре структуровану побудову, що складається з чотирьох розділів, кожен з яких детально висвітлює окремі аспекти дослідження. Виклад матеріалу є логічним та послідовним, що сприяє легкому сприйняттю інформації. Автор демонструє високий рівень володіння спеціальною термінологією та глибоке розуміння предметної області, що свідчить про високий науковий рівень роботи.

Характеризуються логічним поданням наукового матеріалів і відповідають діючим вимогам щодо дисертацій на здобуття наукового ступеня доктора філософії передбаченим чинним «Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. №44.

Дисертаційна робота виконана з дотриманням принципів академічної доброчесності. Використані у роботі ідеї та результати інших авторів належним чином цитовані, що свідчить про високий рівень наукової етики. Звіт про подібність підтверджує оригінальність дисертації та відсутність плагіату, що є важливим показником академічної доброчесності здобувача.

Зауваження до проведеного дисертаційного дослідження

Аналіз змісту дисертаційної роботи, поданих в ній наукових та практичних результатів дисертаційного дослідження дозволи позитивно оцінити її зміст та визначити певні зауваження, що подані нижче:

1. В першому розділі варто було більш детальніше проаналізувати існуючі методи використання штучного інтелекту для оцінювання якості псевдовипадкових чисел. Наведений ґрунтовний аналіз методів узагальнив та

більш фундаментально обґрунтував проблематику та актуальність дисертаційного дослідження.

2. У розділі 2.1. автор приводить результати порівняння ефективності та продуктивності традиційних моделей (RNN, GRU, CNN, LSTM) і почергово наводить отримані результати описово та графічно, проте не наводить кількісно-якісні результати. Бажано б було представити отримані результати у вигляді таблиці з кількісно-якісними результатами порівняння, що б підтвердило недосконаліть існуючих моделей та більш ґрунтовніше довело б актуальність дисертаційного дослідження.

3. У розділі 3.5 автор наводить результати тренування своєї моделі і зазначає, що найвища точність і найменші втрати досягнуті через 100 епох, проте згідно наданої графічної ілюстрації на рис.34 кількість відображених результатів обмежувалось 100 епохами, що не дає повноцінної можливості підтвердити це твердження. Відображення більшої кількості епох тренування дало б змогу підтвердити дані результати або підвищити точність і втрати при більшій кількості епох тренування.

4. В розділі 4 автор пропонує технологію оцінювання якості генераторів псевдовипадкових чисел та стверджує, що вона дозволяє виявляти неякісні і ненадійні генератори, проте у самій роботі не надано детальної моделі чи методики щодо проведення такого типу тестування. Наявність обумовленої методики дозволило б підтвердити практичну цінність розробленої технології.

Приведені зауваження не впливають на наукову цінність та новизну поданих в дисертаційній роботі Проскуріна Дмитра Петровича результатів та висновків. Робота має важливе теоретичне і практичне значення.

Висновок

Дисертаційна робота здобувача ступеня доктора філософії Проскуріна Дмитра Петровича на тему «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання» є завершеним науковим дослідженням, що виконане на високому

науковому рівні. Робота відповідає всім вимогам щодо академічної доброчесності, актуальності та практичної цінності. Сукупність теоретичних та практичних результатів вирішує актуальне наукове завдання та має важливе значення для галузі інформаційних технологій.

За рівнем наукової новизни, якістю досліджень, достовірністю та обґрунтованістю висновків дисертація Проскуріна Дмитра Петровича на тему: «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання» відповідає спеціальності 122 – «Комп'ютерні науки» і чинним вимогам 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», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор – Проскурін Дмитро Петрович, заслуговує на присудження ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки».

Офіційний опонент:
доктор технічних наук, професор,
завідувач кафедри захисту інформації
Національного університету «Львівська політехніка»,
МОН України Іван ОПІРСЬКИЙ

Підпис д.т.н., професора Опірського І.Р. засвідчую
Вчений секретар Національного університету
«Львівська політехніка», к.т.н., доцент Роман БРИЛИНСЬКИЙ

07 серпня 2024 року