

## **ВІДГУК**

офіційного опонента

доктора технічних наук, професора

Фауре Еміля Віталійовича

на дисертаційну роботу Проскуріна Дмитра Петровича

на тему «Інформаційна технологія оцінювання якості генераторів

послідовностей псевдовипадкових чисел на основі машинного навчання»,

подану на здобуття ступеня доктора філософії

за спеціальністю 122 «Комп'ютерні науки»

галузі знань 12 Інформаційні технології

### **1. Актуальність теми дисертаційного дослідження.**

На сьогоднішній день забезпечення високого рівня надійності та безпеки інформаційних систем є однією з найважливіших задач в умовах зростання кіберзагроз. Генератори послідовностей псевдовипадкових чисел (ГППВЧ) є ключовими компонентами криптографічних алгоритмів, що використовуються в комунікаційних технологіях, фінансових послугах і державних службах. Сучасні методи оцінювання якості ГППВЧ вимагають великих обсягів даних, значних обчислювальних і часових ресурсів, що ускладнює їх застосування в умовах, коли ці ресурси є обмеженими. Разом з тим, з огляду на швидкий розвиток інформаційних технологій, постійне збільшення обсягу оброблюваних даних, а також на потребу в забезпеченні визначеного рівня безпеки комунікаційних систем призводить до необхідності підвищення ефективності та точності оцінювання якості ГППВЧ.

Таким чином, удосконалення методів оцінювання якості ГППВЧ є необхідним компонентом підтримки високого рівня безпеки, особливо в умовах обмежених обчислювальних ресурсів, а актуальність теми дисертаційного дослідження Проскуріна Дмитра Петровича «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання» не викликає жодних сумнівів.

### **2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність.**

Основні наукові результати дослідження: розроблена модель ідентифікації ГППВЧ, удосконалена модель передбачення наступної послідовності, розвинутий метод оцінювання якості послідовностей псевдовипадкових чисел і розроблена малоресурсна інформаційна технологія – чітко сформульовані, достатньо обґрунтовані та не викликають сумнівів. Достовірність наукових положень дисертації забезпечено:

- коректним використанням у процесі досліджень методів теорії ймовірностей і математичної статистики, машинного навчання, статистичного аналізу, комбінаторики;
- відповідністю чисельних розрахунків теоретичним висновкам;
- адекватністю структурно-логічної схеми дослідження визначеній меті: кожен наступний розділ чи підрозділ органічно пов'язаний із попереднім і доповнює його;
- використанням широкої бази наукових джерел за темою дисертації й достатнім масивом аналітичних даних.

### **3. Наукова новизна отриманих результатів:**

- *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 послідовності псевдовипадкових чисел;
- *вперше розроблено* малoresурсну 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;
- *удосконалено* модель передбачення наступної послідовності псевдовипадкових чисел, що за рахунок використання гібридної нейронної мережі та обмеженої кількості вхідних даних для навчання дозволяє передбачати наступні послідовності для неякісних генераторів псевдовипадкових чисел;
- *набув подальшого розвитку* метод оцінювання якості послідовностей псевдовипадкових чисел, який за рахунок використання одновимірної рекурентної нейронної мережі та датасетів, сформованих різними генераторами псевдовипадкових чисел, дозволяє швидше оцінювати якість генераторів для криптографічних та інших застосувань у галузі комп'ютерних наук.

**4. Практична цінність результатів** полягає в можливості використання отриманих результатів відповідними органами для ефективного оцінювання генераторів псевдовипадкових послідовностей.

Автором роботи показано, що:

- 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 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  $\chi^2$ -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 ГППВЧ 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. Результати впроваджено в навчальний процес кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій (акт впровадження №03 від 09.05.2024), в наукову діяльність Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Національного авіаційного університету (акт впровадження від 30.11.2024) і Головного управління розвідки Міністерства оборони України.

## **5. Повнота викладу в наукових публікаціях, зарахованих за темою дисертації.**

Наукові результати дисертації висвітлені у 13 наукових публікаціях, серед яких 3 статті в наукових виданнях, включених до переліку наукових фахових видань України, та 5 публікацій у виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus. Результати дослідження апробовано на 5 наукових конференціях та реалізовано в науково-технічних розробках. Усі публікації відповідають вимогам щодо наукового рівня та академічної доброчесності, що підтверджує високу наукову цінність дисертаційної роботи.

## **6. Мова та стиль викладення результатів**

Дисертаційну роботу написано українською мовою. Вона характеризується високим рівнем системності та логічною структурою викладення, що дозволяє легко розуміти розвиток дослідження та логічні зв'язки між розділами. Представлення інформації чітке та зрозуміле, що сприяє засвоєнню основних понять та методів, які використовуються в дослідженні. У роботі використано загальноприйняті терміни та поняття, що робить її зрозумілою для широкого кола фахівців у галузі інформаційних технологій.

## **7. Дотримання норм академічної доброчесності.**

Дисертаційна робота є завершеною науковою працею та демонструє наявність особистого внеску здобувача в науковий напрям.

Аналіз дисертації Проскуріна Д.П. свідчить про дотримання автором норм і правил академічної доброчесності та наукової етики. Звіт подібності свідчить про відсутність ознак елементів фальсифікації чи плагіату. Некоректно оформлених запозичень чи інших ознак неправомірного використання результатів інших авторів без зазначення авторства в роботі не виявлено. Використані ідеї та результати інших авторів мають належні посилання на джерела.

## **8. Зауваження та недоліки:**

- 1) у оглядовій частині дисертації (зокрема, в підрозділі 1.2 Аналіз методів оцінювання якості послідовностей псевдовипадкових чисел) автор обмежився тільки короткою згадкою про тест  $\chi^2$ -квадрат, натомість детальний аналіз саме цих методів є одним з базових і необхідних для вирішення задач дисертаційного дослідження. Як наслідок, автор обмежується порівнянням результатів аналізу оцінювання ГППВЧ за розробленою технологією тільки з результатами застосування тесту  $\chi^2$ -квадрат для рівномірного розподілу, хоча існує значна кількість інших статистичних критеріїв (параметричних і непараметричних), а також статистичних тестів, наприклад, з наборів NIST, DIEHARD, TestU01, які оперують розподілами, що відрізняються від рівномірного;
- 2) автор у роботі змішує та сумісно оцінює генератори різної природи – випадкових і псевдовипадкових чисел. Натомість, варто було чітко їх класифікувати та досліджувати групами в залежності від сфери застосування. Крім того, зазначене на стор. 28 дисертації твердження «Генератори псевдовипадкових чисел (PRNG) і квантові генератори випадкових чисел (QRNG) є двома основними типами генераторів

випадкових чисел» не є коректним і є прямим наслідком відсутності проведеного якісного аналізу генераторів випадкових і псевдовипадкових чисел у оглядовій частині. Тільки в п. 2.4.4 для дослідження «Прогнозування виходу PRNG за допомогою послідовного аналізу» автор використовує чотири широко відомі ГППВЧ: лінійний конгруентний, MiddleSquare, Xorshift і Mersenne Twister;

- 3) у тексті роботи відсутнє формалізоване представлення розробленої моделі ідентифікації джерела послідовностей, удосконаленої моделі передбачення наступної послідовності псевдовипадкових чисел, розвинутого методу оцінювання якості послідовностей псевдовипадкових чисел, що значно ускладнює можливість їх використання. Крім того, було б корисно більш детально описати ступінь новизни, об'єкт наукової новизни, відмінність від існуючих підходів та досягнутий ефект;
- 4) у таблицях на сторінках 54-65 автор використовує «Середній бал» як показник оцінювання результатів експериментів, проте не наводить правила його обчислення. Це ускладнює якісне оцінювання запропонованих автором рішень і отриманих результатів. Крім того, підписи назв, значень і діапазонів координатних осей на наведених на сторінках 54-66 графіках відсутні або представлені невдало, що ускладнює розуміння отриманих результатів;
- 5) у підрозділі 3.5 дисертації автор виконує порівняльне оцінювання ефективності тесту хі-квадрат і CNN для сформованих наборів даних. Разом з тим, умови та параметри експерименту описано недостатньо, що не дозволяє повною мірою оцінити справедливність отриманих результатів;
- 6) у підрозділі 4.5 автором розглянуто оцінку продуктивності системи, що формується через метрики точності та швидкості аналізу, проте не наведено відповідні показники застосування розробленої інформаційної технології для оцінювання якості генераторів послідовностей псевдовипадкових чисел;
- 7) автором зазначено, що реалізація одновимірної згорткової нейронної мережі (1D-CNN) підтвердила можливість аналізу менших за довжиною послідовностей (п. 3 практичної цінності), проте чисельних підтверджень цьому не наведено;
- 8) зауваження щодо структури й оформлення дисертації:
  - назви деяких структурних елементів не відповідають їх змісту: зокрема, це стосується розділу 2, підрозділів 1.1, 2.2, 3.1, 3.2, 3.3, 3.4;
  - обсяг анотації необхідно було б збільшити та навести її англійською, частина чисельних показників, наведених у пункті вступу «Структура

та обсяг дисертації», помилкові, два останніх абзаци вступу є зайвими;

- дисертація не містить посилань на додатки, зокрема, на додаток зі списком публікацій здобувача за темою дисертації та відомостями про апробацію результатів дисертації;
- у роботі зазначено про наявність актів впровадження результатів дисертації, проте самі акти в роботі не наведено;
- робота містить орфографічні, пунктуаційні, стилістичні помилки.

Наведені зауваження не впливають на загальну позитивну оцінку дисертаційної роботи.

## 9. Висновок.

Дисертація Проскуріна Дмитра Петровича представляє собою завершену наукову працю на актуальну тему, а отримані результати вирішують важливу науково-технічну задачу забезпечення швидкого та точного оцінювання генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних.

Представлена до розгляду дисертація відповідає освітньо-науковій програмі «Комп'ютерні науки» та спеціальності 122 Комп'ютерні науки, вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, а її автор – Проскурін Дмитро Петрович – заслуговує на присудження ступеня доктора філософії за спеціальністю 122 Комп'ютерні науки галузі знань 12 Інформаційні технології.

### Офіційний опонент:

проректор з науково-дослідної роботи  
та міжнародних зв'язків  
Черкаського державного  
технологічного університету  
доктор технічних наук, професор



Еміль ФАУРЕ

Чесний секретар



Триша Меркелєва