

Голові разової спеціалізованої вченої ради
Національного авіаційного університету
доктору технічних наук, професору
Нечипорук Олені Петрівні

РЕЦЕНЗІЯ

рецензента Андрія Олексійовича Фесенка

на дисертацію Проскуріна Дмитра Петровича «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання», представлену на здобуття наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертаційного дослідження

У сучасних умовах зростання кіберзагроз та постійного збільшення обсягу оброблюваних даних забезпечення надійності інформаційних систем стає критично важливим завданням. Генератори послідовностей псевдовипадкових чисел є основою для багатьох криптографічних алгоритмів, що застосовуються в різних сферах, включаючи телекомунікації, фінансові послуги та державне управління. Вдосконалення методів оцінювання якості ГППВЧ дозволить підвищити рівень безпеки цих систем та забезпечити їх ефективне функціонування навіть за умов обмежених ресурсів.

Запропонована інформаційна технологія оцінювання якості ГППВЧ з використанням методів машинного навчання відповідає сучасним вимогам до надійності та безпеки інформаційних систем. Використання машинного навчання для аналізу та оцінювання ГППВЧ забезпечує нові можливості для підвищення точності та ефективності оцінювання, що особливо важливо в умовах обмежених ресурсів та даних. Це дослідження має потенціал значно

покращити захист інформаційних систем і є важливим внеском у галузь інформаційних технологій.

2. Зв'язок роботи з науковими програмами, планами, темами

Дослідницький грант NFR-22-14060 «AI-based multilayer 5G security assurance methodology for the needs of special groups of subscribers in Georgia», фінансований Shota Rustaveli National Foundation of Georgia, також підтверджує зв'язок роботи з міжнародними науковими програмами. Цей грант передбачає розробку методологій забезпечення безпеки для спеціальних груп абонентів у мережах 5G з використанням методів штучного інтелекту. Дисертація Проскуріна Дмитра є невід'ємною частиною цих наукових програм і вносить вагомий внесок у їх реалізацію.

3. Наукова новизна отриманих результатів

Наукові положення, розроблені особисто здобувачем, та їх новизна полягають у тому, що:

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;
- 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;

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;

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;

4. Практичне значення, отриманих результатів

Практичне значення та використання результатів дисертаційного дослідження полягає у тому, що отримані результати можуть бути використані відповідними органами для ефективного оцінювання генераторів псевдовипадкових 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 χ^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 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. 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.

5. Мова та стиль викладення результатів

Дисертація написана українською мовою, сформована послідовно та доступно, з використанням загальноприйнятої термінології та врахуванням наукових проблем і тенденцій галузі. Автор демонструє високу культуру наукового викладу, що сприяє легкому сприйняттю матеріалу навіть для читачів, які не є фахівцями у вузькій сфері дослідження.

Стиль викладу є чітким та логічним, що дозволяє легко прослідкувати основні ідеї та результати дослідження. Використання графіків, таблиць та інших візуальних засобів ілюстрації сприяє кращому розумінню та сприйняттю наукових положень. Це підвищує загальну якість роботи і робить її доступною для широкого кола читачів.

6. Повнота оприлюднення результатів та дисертаційної роботи

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.

7. Загальна характеристика структури роботи та змісту дисертаційного дослідження

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Вступ містить обґрунтування актуальності, мету, задачі дослідження, наукову новизну та практичну цінність результатів. Кожен розділ логічно пов'язаний з попереднім і доповнює його, що забезпечує послідовність та цілісність наукового дослідження.

У першому розділі здійснено аналіз існуючих підходів до генерування та оцінювання якості послідовностей псевдовипадкових чисел, визначено ефективність методів і засобів штучного інтелекту в контексті вирішення зазначених завдань. У другому розділі розроблено та досліджено модель ідентифікації джерела послідовностей псевдовипадкових чисел, що дозволяє виявляти генератори навіть за умов обмеженої кількості вхідних даних. Третій розділ присвячено розробці та дослідженню методу оцінювання якості послідовностей псевдовипадкових чисел з використанням алгоритмів штучного інтелекту. У четвертому розділі розроблено інформаційну

технологію для комплексного оцінювання якості генераторів у реальних умовах.

8. Недоліки та зауваження по роботі

1. В роботі не завжди чітко вказано межі застосування розробленої інформаційної технології, що могло б бути доповнено прикладами з реальних проектів. Більш детальне описання реальних прикладів застосування підвищило б практичну цінність роботи та зробило б її більш зрозумілою для практиків.
2. У розділі, присвяченому практичному застосуванню, доцільно було б навести більше порівнянь з існуючими методами оцінювання ГППВЧ. Це дозволило б більш повно оцінити переваги та недоліки запропонованого підходу та показати його ефективність у порівнянні з іншими методами.
3. У дисертації представлено показники ефективності впровадження результатів дослідження в роботу науково-дослідних лабораторій та навчальний процес, але було б корисно більш детально описати процес впровадження та отримані результати. Це підвищило б переконливість роботи та показало б реальний вплив отриманих результатів на практику.

Вважаю, що висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та значимість одержаних результатів. Вони спрямовані на підвищення якості та зрозумілості роботи, але не впливають на її позитивне оцінювання.

9. Висновки

Дисертаційна робота Проскуріна Дмитра Петровича на тему «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання» виконана на високому науковому рівні, не порушує принципів академічної доброчесності

та є закінченою цілісною роботою. Отримані результати мають вагомe значення для галузі знань 12 «Інформаційні технології».

Автором розроблено нові методи та моделі, які дозволяють значно підвищити точність та ефективність оцінювання якості ГППВЧ, що має важливе значення для безпеки інформаційних систем у різних галузях. Результати дослідження вже впроваджені в навчальний процес та діяльність науково-дослідних лабораторій, що підтверджує їх практичну цінність та високу наукову значущість.

Таким чином, дисертаційна робота відповідає вимогам до робіт такого типу, а її автор заслуговує присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки.

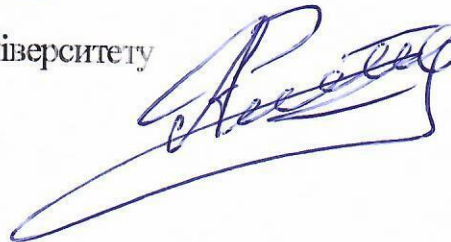
РЕЦЕНЗЕНТ

в.о. декана факультету

комп'ютерних наук та технологій

Національного авіаційного університету

к.т.н., доцент



Андрій ФЕСЕНКО

«15» 08 2024 року

