ВІДГУК

офіційного опонента, начальника кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації ім. Героїв Крут, доктора технічних наук, старшого наукового співробітника Чевардіна Владислава Євгенійовича 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 дослідження

Дисертаційна робота Проскуріна Дмитра Петровича присвячена розробці інформаційної технології для оцінювання якості генераторів псевдовипадкових послідовностей (ГПВП) на основі машинного навчання. Це дослідження є важливим внеском у галузь інформаційних технологій, враховуючи постійне зростання потреби у безпечних криптографічних системах та виклики, пов'язані з оцінкою якості ГПВП.

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

Найбільш цікавою є ідея, яка полягає у використанні моделей нейронних мереж CNN, HNN та їх варіацій для ідентифікації джерел генерації псевдовипадкових послідовностей. Особливої важливості ця робота набуває в рамках виконання завдань щодо аналізу та дослідження систем захисту інформації противника та проведення тестування на проникнення власних систем захисту інформації та кіберзахисту.

Наукова новизна представлених в роботі результатів полягає 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 і оптимізації, дає можливість ідентифікувати 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.

Наукова обґрунтованість та достовірність отриманих результатів

Наукові положення, висновки й рекомендації, сформульовані в дисертації, відповідають вимогам до такого виду досліджень. Високий рівень обґрунтованості наукових положень, висновків, рекомендацій, сформульованих у дисертації, їхня достовірність забезпечені:

– професійним вирішенням автором низки наукових завдань, що сприяло реалізації поставленої мети дослідження, та 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.

Практичне значення отриманих результатів дисертаційної роботи полягає у тому, що отримані результати можуть бути використані відповідними органами для ефективного оцінювання генераторів псевдовипадкових послідовностей. Окрім цього:

– 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 вище 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 у сфері криптографічного захисту інформації та кіберзахисту, для стільникових мереж LTE / 5G / 6G, технологій на основі UAV. Результати були впроваджені в навчальний процес кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій (Акт впровадження від 09.05.2024 №03) і 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.

Обґрунтованість та достовірність результатів

Дисертаційна робота базується на сучасних методах машинного навчання та математичних моделях, що забезпечує високу обґрунтованість та достовірність отриманих результатів. Достовірність основних наукових результатів дисертаційного дослідження забезпечується обґрунтованим вибором та використанням відомих наукових методів дослідження. Теоретичні висновки підтверджені чисельними експериментами, що свідчить про їх практичну значимість та відповідність реальним умовам.

Оцінка структури та змісту дисертації

Дисертаційна робота 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.

Дотримання принципів академічної доброчесності

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.

Оприлюднення результатів дисертаційної роботи

Наукові результати дисертації висвітлені у 13 наукових публікаціях, серед яких 3 статті у наукових виданнях, включених до переліку наукових фахових видань України, та 5 статей 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.

Недоліки та зауваження до дисертаційної роботи

1. У вступі автор пропонує комплекс науково-технічних задач, хоча дисертація присвячена вивченню однієї науково-технічної задачі. Насправді "комплекс науково-технічних задач" є частковими завданнями дослідження.

2. Не зрозуміло, чому автором не проводились дослідження генераторів псевдовипадкових послідовностей з використанням відомих методик NIST STS, Diehard з використанням всіх тестів (Frequency, BlockFrequency, CumulativeSums, Runs, LongestRun, Rank, FFT та ін.) для врахування під час оцінювання якості псевдовипадкових послідовностей.

3. В дисертаційній роботі автор використовує шаблонні генератори BBS, ACORN, LCG та інші, проте генератори, що визначені в стандарті NIST SP 800-90A, а саме: CTR_DRBG, HMAC_DRBG, Hash_DRBG не були досліджені. Проведення експериментів для зазначених генераторів ПВП дозволило б посилити положення, що виносяться на захист.

4. У списку використаних джерел посилання 84 і 89 описують той самий документ, а саме NIST SP 800-22, який містить набір статистичних тестів для оцінки якості генераторів випадкових та псевдовипадкових чисел, що використовуються у криптографічних додатках.

Вказані недоліки не впливають на наукову новизну та практичну цінність отриманих результатів дослідження.

Висновок про відповідність дисертації встановленим вимогам

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.

Дисертація відповідає вимогам наказу Міністерства освіти і науки України від 12.01.2017 р. № 40 “Про затвердження вимог щодо оформлення дисертації”, що висуваються до дисертацій на здобуття ступеня доктора філософії.

За своєю актуальністю, внеском у науку, ступенем новизни та обґрунтованості, теоретичною та практичною значущістю отриманих результатів дисертація Проскуріна Д.П. на тему “Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання” відповідає вимогам пунктів 6, 7, 8 “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 року № 44 (зі змінами, внесеними згідно з Постановою КМ від 19.05.2023 р. № 502), а її автор заслуговує присудження наукового ступеня доктора філософії за спеціальністю 122 Комп’ютерні науки.

Офіційний опонент:
начальник кафедри кібербезпеки ВІТІ ім. Героїв Крут
д.т.н., с.н.с. Владислав ЧЕВАРДІН
“06” серпня 2024 року

Підпис Владислава Чевардіна
засвідчую ЗНВП та С студ-т В.Каминенко