ЗАТВЕРДЖУЮ
Голова комісії з реорганізації
Національного авіаційного
університету, в. о. ректора

_____Ксенія СЕМЕНОВА

«_25_» ____06____ 2024 року

ВИСНОВОК

Національного авіаційного університету (далі – НАУ) про наукову новизну, теоретичне та практичне значення результатів дисертації Проскуріна Дмитра Петровича на здобуття ступеня доктора філософії з галузі знань 12 "Інформаційні технології" за спеціальністю 122 "Комп'ютерні науки" на тему: "Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання"

ВИТЯГ

із протоколу № 10 розширеного засідання
кафедри комп'ютерних інформаційних технологій
Національного авіаційного університету від 29 травня 2024 року

Присутні на засіданні науково-педагогічні працівники кафедри комп'ютерних інформаційних технологій:

Савченко А.І., д.т.н, професор, завідувач кафедри;
Віноградов М.А., д.т.н., професор кафедри;
Воронін А.М., д.т.н., професор кафедри;
Зіатдінов Ю.К., д.т.н., професор кафедри;
Гнатюк С.О., д.т.н., професор кафедри;
Василенко В.А., к.т.н., доцент кафедри;
Харченко О.Г., к.т.н., доцент кафедри;
Моденов Ю.Б., к.т.н., доцент кафедри;
Райчев І.Е., к.т.н., доцент кафедри;
Холявкіна Т.В., к.т.н., доцент кафедри;
Климова А.С., к.т.н., доцент кафедри;
Чуба І.В., к.т.н. доцент кафедри;
Колісник О.В., к.т.н. доцент кафедри;
Зудов О.М., к.т.н., доцент кафедри;
Прокопенко К.І., к.т.н., доцент кафедри;
Сінько Ю.І., к.пед.н., доцент кафедри;
Толстікова О.В., к.т.н., доцент кафедри;
Сидоренко В.М., к.т.н., доцент кафедри;

Водоп’янов С.В., к.т.н., доцент кафедри;

Охріменко Т.О., к.т.н., ст. дослідник, доцент кафедри, п.н.с. НДЛ протидії кіберзагрозам в авіаційній галузі;

Фесенко А.О., к.т.н., доцент кафедри, в.о. декана ФКНТ;

Єрмачков Ю.О старший викладач кафедри;

Остапенко О.С., старший викладач кафедри;

Шевченко О.П., старший викладач кафедри;

Горіна В.В., старший викладач кафедри;

Рибасова Н.О., старший викладач кафедри;

Охремчук О.С., асистент кафедри;

Мельниченко П.І., асистент кафедри.

Присутні на засіданні науково-педагогічні працівники інших кафедр НАУ:

Одарченко Р.С. д.т.н., професор, в.о. декана факультету аеронавігації, електроніки та телекомунікацій НАУ;

Нечипорук О.П., д.т.н., професор, професор кафедри інтелектуальних кібернетичних систем НАУ;

Павленко П.М., д.т.н., професор, професор кафедри організації авіаційних перевезень НАУ.

Слухали:

Доповідь аспіранта кафедри комп’ютерних інформаційних технологій Національного авіаційного університету Проскуріна Дмитра Петровича на тему: “Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання”, поданої на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології”, за спеціальністю 122 “Комп’ютерні науки”.

Тему дисертаційного дослідження “Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання”, затверджено на засіданні Вченої ради Факультету комп’ютерних наук та технологій 11 грудня 2023 року, протокол №8.

Наукові керівники – д.т.н., професор Гнатюк С.О., професор кафедри комп’ютерних інформаційних технологій Національного авіаційного університету та PhD, професор Явіч М.П. професор Кавказького університету (Тбілісі, Грузія).

Доповідач обґрунтував актуальність обраної теми, визначив мету, завдання, методи дослідження, охарактеризував об’єкт та предмет дисертації, виклав основні наукові положення та висновки, що виносяться на захист, вказав науково-практичну значущість роботи, зазначив про впровадження результатів дослідження.

Автором проведено аналіз існуючих підходів до генерування та оцінювання якості послідовностей псевдовипадкових чисел. Дослідником визначено існуючі методології та стандарти в сфері аналізу генераторів псевдовипадкових послідовсностей, ідентифіковано основні недоліки та області для покращення.

Дослідником розроблено та досліджено модель ідентифікації джерела послідовностей псевдовипадкових чисел, для виявлення генераторів (якими були

сформовані послідовності) в умовах обмеженої кількості вхідних даних.

Дослідником удосконалено та дослідити модель передбачення наступної послідовності псевдовипадкових чисел з високою точністю.

Дослідником розвинуто та дослідити метод оцінювання якості послідовностей псевдовипадкових чисел з використанням алгоритмів штучного інтелекту для застосувань в галузі комп'ютерних наук.

Дослідником розроблено інформаційну технологію для комплексного оцінювання якості генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних.

Дослідником проведено верифікацію розроблених методів з використанням розробленого програмного забезпечення з метою підтвердження їх ефективності та придатності для практичного застосування.

Структура та обсяг дисертації зумовлена метою і логікою дослідження та складається з анотації, вступу, чотирьох розділів, які об'єднують 20 підрозділів, висновків, списку використаних джерел, додатків.

Запитання до здобувача:

1. **Савченко А.С.,** д.т.н., професор, завідувач кафедри комп'ютерних інформаційних технологій

Запитання: Де можна використовувати створену інформаційну технологію та які переваги вона надає по часу чи точності?

Відповідь: Створена інформаційна технологія буде корисна як для криптографії, стільникових мереж LTE / 5G / 6G, технологій на основі UAV, так і паралельно з існуючими тестами для аналізу генераторів псевдовипадковостей. Наші моделі успішно виявили недолікі у статистично високоякісному генераторів ACORN, як це вказано на слайді 28, а метод аналізу працює на 40% швидше за аналогічний статистичний тест, як це вказано на слайді 27.

2. **Савченко А.С.,** д.т.н., професор, завідувач кафедри комп'ютерних інформаційних технологій

Запитання: Чи не буде процес аналізу повільніший при застосувані даної інформаційнох технології? Так як потрібен час для тренування та оптимізації. Чи не буде вона уповільнювати процес аналізу?

Відповідь: Так, наша інформаційна технологія вимагає підготовки, тренування та навчання, але цей процес має бути завершеним до практичної імплементації. Таким чином час для аналізу не має зазнати сильних змін при використанні нашої інформаційнох технології.

3. **Нечипорук О.П.,** д.т.н., професор, професор кафедри інтелектуальних кібернетичних систем НАУ

Запитання: Наскільки підвищилася точність аналізу послідовностей з використанням вашої інформаційної технології?

Відповідь: Прошу звернути Вашу увагу на слайд 28. Ми провели базові статистичні тести для виявлення якості генераторів. Наша інформаційна технологія, змогла передбачити послідовності для низькоякісних генератори (LSFR, BBS). Але вона також змогла передбачити послідовності для генератора, який вважається статистично сильним – ACORN. Таким чином, використання нашої інформаційної

технології паралельно з існуючими тестами підвищить якість аналізу та допоможе краще ідентифікувати низькоякісні генератори.

4. **Нечипорук О.П.**, д.т.н., професор, професор кафедри інтелектуальних кібернетичних систем НАУ

Запитання: Які рекомендації ви надаєте після аналізу генераторів? Наприклад, чи визначаєте ви сферу використання для генератора або його практичне застосування?

Відповідь: Ми не надаємо рекомендації по використанню генераторів, так як це залежить від цілі його застосування, сфери, команди тощо. Наша інформацйна технологія визначає тільки якість генератора (висока чи низька).

5. **Нечипорук О.П.**, д.т.н., професор, професор кафедри кафедри інтелектуальних кібернетичних систем НАУ.

Запитання: Якщо ваша інформацйна технологія виявила неякісний генератор, чи надаєте ви рекомендація по його використанню? Чи по вибору наступної послідовності? Яка практична мета вашого дослідження?

Відповідь: Наша інформаційна технологія визначає лише якість генератора без додаткових рекомендація. Вона допоможе чітко виявити невипадкові послідовності, що покращить захист системи, де протестований генератор використовується. Як і коли використовувати неякісний генератор вже залежить від команди, сфери та ситуації.

6. **Нечипорук О.П.**, д.т.н., професор, професор кафедри кафедри інтелектуальних кібернетичних систем НАУ.

Запитання: Повіторіть, будь ласка, критерії оцінки якості, які ви застосували.

Відповідь: Ми використовуємо показники інформаційної моделі на кожному етапі як наші критерії якості. Якщо ми подивимося на слайд 28, то побачимо наші результати. Наприклад, запропонована інформаційна технологія видає точність ідентифікації джерела та точність передбачення наступної послідовності, що і є показником якості – точність менше 85% озаначає високу якість генератора, точність більше – низьку.

7. **Сидоренко В.М.**, к.т.н., доцент, доцент кафедри комп’ютерних інформаційних технологій

Запитання: Чи у вас є акти впровадження вашої інформаційної технології?

Відповідь: Результати були впроваджені в навчальний процес кафедри комп’ютерних інформаційних технологій Факультету комп’ютерних наук та технологій і в наукову діяльність Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Національного авіаційного університету і Головного управління розвідки Міністерства оборони України.

8. **Сидоренко В.М.**, к.т.н., доцент, доцент кафедри комп’ютерних інформаційних технологій

Запитання: Скільки входить методів та моделей в вашу інформаційну технологію?

Відповідь: До нашої інформаційної технології входить дві моделі та один метод, відображені в науковій новизні роботи.

9. **Одарченко Р.С.** д.т.н., професор, в.о. декана факультету аеронавігації,

електроніки та телекомунікацій НАУ

Запитання: На вашу думку, які перспективи практичного застосування вашої інформаційної технології?

Відповідь: Наразі в багатьох галузях є потреба застосування різноманітних технологій на основі теорії випадкових процесів – це і безпека (паролі й ключі), і фінанси, і телекомунікації. Застосування ж методів машинного навчання робить цю технологію гнучким і адаптивним інструментом, що дозволяє забезпечити необхідну точність оцінювання і збільшити швидкість.

10. **Фесенко А.О.**, к.т.н., доцент кафедри, в.о. декана ФКНТ

Запитання: Чим відомі підходи і стандарти оцінювання генераторів послідовностей псевдовипадкових чисел вас не влаштовують?

Відповідь: Відомі підходи типу NIST STS чи DIEHARD потребують значних обчислювальних ресурсів, не є гнучкими і не дозволяють в комплексі зробити оцінювання генераторів, передбачаючи їх. Ми проаналізували багато сучасних підходів синтезу машинного навчання та криптографії, проте отримані нами результати є оригінальними і ефективними, як показали експерименти.

Проскурін Д.П. докладно відповів на всі поставлені запитання, обґрунтувавши свою авторську позицію.

Висновки наукових керівників

Після відповідей на запитання було озвучено висновок наукового керівника Гнатюка Сергія Олександровича, д.т.н., професора кафедри комп'ютерних інформаційних технологій Національного авіаційного університету.

Зазначено, що дисертант успішно виконав індивідуальний план наукової роботи та індивідуальний навчальний план. Підготовлена дисертація готова до захисту. У роботі опрацьовано досить багато різноманітного матеріалу, дуже багато наукових праць – англомовні видання, які дозволили узагальнити досить широкий світовий досвід.

У процесі виконання роботи дисертант показав необхідну кваліфікацію для самостійного вирішення поставлених наукових задач, постійно працює над підвищенням свого освітнього і професійного рівня. Вміє проводити наукові дослідження, приймає участь у науково-дослідних роботах, має наукові публікації та доповіді у наукових конференціях.

Проскурін Дмитро Петрович працює над способами покращення аналізу псевдовипадкох послідовностей з використанням технологій машинного навчання протягом усього періоду навчання в Національному авіаційному університеті з 2020 року. За цей час продемонстрував себе як старанний та цілеспрямований здобувач, а наукові результати висвітлено та обговорено під час численних доповідей на науково-практичних конференціях та наукових форумах, отримав дипломи ступеня бакалавр та магістр з відзнакою.

Дисертаційна робота є завершеною науковою працею, яка націлена на вирішення актуальної наукової задачі, відповідає спеціальності 122 "Комп'ютерні науки", а її автор Проскурін Дмитро Петрович заслуговує присудження ступеня доктора філософії, на підставі Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої

ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, який затверджено Постановою Кабінету Міністрів України № 44 від 12 січня 2022 року.

Науковий керівник запропонував затвердити позитивний висновок про наукову новизну, теоретичне та практичне значення результатів зазначеної дисертації та рекомендувати до захисту на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології”, за спеціальністю 122 “Комп’ютерні науки”.

Після відповідей на запитання було озвучено висновок наукового керівника Явіча Максима Павловича, професора, професора Кавказького університету (Тбілісі, Грузія).

Відзначено, що дисертант завершив виконання всіх вимог індивідуального плану наукової роботи та індивідуального навчального плану. Дисертаційна робота містить глибокий аналіз великої кількості літературних джерел, зокрема фахових рецензованих англомовних журналів, що дозволило здобувачеві розглянути міжнародний досвід у відповідній галузі.

Протягом виконання дисертації дисертант проявив здатність самостійно вирішувати наукові завдання, постійно працював над підвищенням своєї професійної компетенції. Він здатен проводити наукові дослідження, активно залучений до науково-дослідних проектів (у т.ч. міжнародних), має публікації в наукових журналах та виступи на конференціях.

Проскурін Дмитро Петрович протягом свого навчання в аспірантурі Національного авіаційного університету працював над покращенням аналізу та оцінювання псевдовипадкових послідовностей із застосуванням технологій машинного навчання. Він зарекомендував себе як наполегливий та цілеспрямований дослідник, а його наукові результати були представлені на численних конференціях та форумах.

Дисертаційна робота є завершеною науковою працею, яка націлена на вирішення актуальної наукової задачі, відповідає спеціальності 122 “Комп’ютерні науки”, а її автор Проскурін Дмитро Петрович заслуговує присудження ступеня доктора філософії, на підставі Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, який затверджено Постановою Кабінету Міністрів України № 44 від 12 січня 2022 року.

Науковий керівник запропонував затвердити позитивний висновок про наукову новизну, теоретичне та практичне значення результатів зазначеної дисертації та рекомендувати до захисту на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології”, за спеціальністю 122 “Комп’ютерні науки”.

Обговорення дисертаційного дослідження

Савченко А.С.

Зазначила, що доповідь дисертанта та власне дослідження свідчать про його високий рівень як науковця і фахівця в галузі інформаційних технологій. Підтримала дисертаційне дослідження з урахуванням виправлення озвучених зауважень і пропозицій.

Нечипорук О.П.

Зазначила, що необхідно чітко вказати критерії для аналізу генераторів та послідовностей, що дозволить визначити переваги над аналогами.

Павленко П.М.

Відмітив актуальність теми і інноваційність підходу, що полягає в поєднання методів шифрування і штучного інтелекту, а також в мультидисциплінарності цього наукового дослідження.

Сидоренко В.М.

Підтримала дисертацію і відзначила необхідність допрацювання презентації і доповіді на захист із урахуванням озвучених зауважень.

Охріменко Т.О.

Підтримала дисертацію, відмітила що здобувач давно вже сформувався як науковець, а також відзначила активну співпрацю Д. Проскуріна з НДЛ протидії кіберзагрозам в авіаційній галузі НАУ в рамках дослідницьких проєктів.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації на тему: “ Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання ”, поданої на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології” за спеціальністю 122 “Комп’ютерні науки”

Актуальність теми дослідження та її зв’язок із планами науково-дослідних робіт.

У сучасному світі стійкість інформаційних систем є критично важливою, особливо в контексті зростаючої кількості кіберзагроз та необхідності захисту критичної інфраструктури. Генератори послідовностей псевдовипадкових чисел (ГППВЧ) є ключовими компонентами в багатьох протоколах безпеки, що використовуються в різних галузях, включаючи телекомунікації, фінансові послуги та державні служби.

Проте, існуючі методи оцінювання якості ГППВЧ часто вимагають великих обсягів даних і значних обчислювальних потужностей, що може бути проблематичним в умовах обмежених ресурсів. У цьому контексті розробка нових методів, моделей та інформаційних технологій на основі машинного навчання для швидкого і точного оцінювання якості ГППВЧ набуває особливої актуальності.

Запропонована у роботі інформаційна технологія використовує 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.

Результати роботи пов’язані з НДР №0122U002361 «Інтелектуалізована система захищеного передавання пакетних даних на базі розвідувально-пошукового безпілотного літального апарату», що фінансується МОН України і

виконується згідно планів НДР Національного авіаційного університету протягом 2022-2024 років, а також дослідницьким грантом NFR-22-14060 «AI-based multilayer 5G security assurance methodology for the needs of special groups of subscribers in Georgia», що фінансується Shota Rustaveli National Foundation of Georgia.

Тема дисертації відповідає освітньо-науковій програмі "Комп'ютерні науки" за спеціальністю 122 "Комп'ютерні науки" галузі знань 12 "Інформаційні технології" в Національному авіаційному університеті.

Формулювання наукового завдання, вирішення якого отримано в дисертації

Метою роботи є забезпечення швидкого та точного оцінювання генераторів послідовностей псевдовипадкових чисел на основі розроблених методів, моделей та інформаційної технології із застосуванням машинного навчання.

Для цього сформульовано комплекс наступних науково-технічних задач:

1. Аналіз існуючих підходів до генерування та оцінювання якості послідовностей псевдовипадкових чисел, визначення ефективності методів і засобів штучного інтелекту в контексті вирішення зазначених завдань;
2. Розробити та дослідити модель ідентифікації джерела послідовностей псевдовипадкових чисел, для виявлення генераторів (якими були сформовані послідовності) в умовах обмеженої кількості вхідних даних;
3. Удосконалити та дослідити модель передбачення наступної послідовності псевдовипадкових чисел з високою точністю;
4. Розвинути та дослідити метод оцінювання якості послідовностей псевдовипадкових чисел з використанням алгоритмів штучного інтелекту для застосувань в галузі комп'ютерних наук;
5. Розробити інформаційну технологію для комплексного оцінювання якості генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних

Об'єкт дослідження – процес оцінювання якості генераторів послідовностей псевдовипадкових чисел.

Предмет дослідження – методи, моделі та інформаційні технології оцінювання якості генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних на основі машинного навчання.

У дисертаційній роботі вирішено науково-прикладну задачу щодо забезпечення комплексного оцінювання якості генераторів послідовностей псевдовипадкових чисел в умовах обмеженої кількості вхідних даних із застосуванням машинного навчання.

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 послідовностей 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;

Обґрунтованість і достовірність наукових положень, висновків, рекомендацій, які захищаються.

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 мсти 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.

Наукове значення роботи полягає у вирішенні актуальної науково-технічної задачі щодо комплексного аналізу статистичних характеристик генераторів послідовностей псевдовипадкових чисел на основі машинного навчання.

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. 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 викладення матеріалів дисертації в публікаціях та особистий внесок у них автора. Дисертація «Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання» Проскуріна Дмитра Петровича є самостійною науковою працею, в якій наведено теоретичні і практичні положення, висновки, власні ідеї та розробки автора, які дають змогу вирішити поставлені завдання. Усі висновки та практичні рекомендації, винесені на захист, розроблені дисертантом особисто.

Найважливіші ідеї, висновки, рекомендації, отримані в дисертації, оприлюднені на наукових та науково-практичних конференціях, у тому числі міжнародних, всеукраїнських та за міжнародною участю: Міжнародна науково-технічна конференція «ABIA» (Київ, 2021), «Information, Communication, Society», (Зозулі, 2023), «Інформаційно-комп'ютерні технології: стан, досягнення та перспективи розвитку», (Житомир, 2021), «IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS» (Дортмунд, 2023), «Proceedings of the Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023) co-located with International Conference on Problems of Infocommunications. Science and Technology (PICST 2023)» (Kyiv, 2023), «Modern Machine Learning Technologies and Data Science Workshop, (MoMLeT&DS)» (Львів, 2021), «Modern Machine Learning Technologies and Data Science Workshop, (MoMLeT&DS)» (Львів, 2023), «Eastern European Machine Learning Summer School» (Кошице, 2023).

Основні положення та результати дисертаційного дослідження викладено

у 11.5 наукових працях, у тому числі: 1.5 статті, опубліковані у наукових виданнях, включених до переліку фахових видань України, 5 – в зарубіжних наукових виданнях, включених до наукометричної бази Scopus; 5 – у матеріалах тез доповідей на науково-практичних конференціях різного рівня.

Праці, в яких опубліковані основні наукові результати дисертації:

Статті у наукових фахових виданнях:

1. Рябий М., Кінзерявий О., Проскурін Д., Сорокопуд В. An advanced method of compressing digital images as part of a video stream to pre-process the data before encrypting, Проблеми інформатизації та управління. 2023. Т. 1, № 73. С. 128-137.

Особистий внесок Проскуріна Д.: проведено аналіз датасетів шифрування інформації на основі технологій машинного навчання.

Особистий внесок Рябого М.: проведено аналіз способів обробки інформації до моменту шифрування.

Особистий внесок Кінзерявого О.: проведено аналіз датасетів шифрування інформації різнох якості.

Особистий внесок Сорокопуда В.: створено загальний датасет шифрування інформації.

2. Гнатюк С.О., Поліщук Ю.Я., Кінзерявий В.М., Горбаха Б.М., Проскурін Д.П. Формування датасету криптоалгоритмів для забезпечення конфіденційності даних, які передаються з розвідувально-пошукового БПЛА, Кібербезпека: освіта, наука, техніка. 2023. № 4 (20). С. 205–219.

Особистий внесок Проскуріна Д.: проведено аналіз датасетів шифрування інформації на основі технологій машинного навчання.

Особистий внесок Поліщук Ю.: проведено аналіз способів обробки інформації з використанням БПЛА.

Особистий внесок Кінзерявого В.: проведено аналіз датасетів шифрування інформації різнох якості.

Особистий внесок Гнатюка С.: проведено аналіз способів забезпечення конфіденційності даних з використанням БПЛА.

Особистий внесок Горбахи Б.: створено загальний датасет шифрування інформації.

3. Проскурін Д.П., Явіч М.П., Гнатюк С.О. Модель ідентифікації джерела послідовностей псевдовипадкових чисел на основі гібридної нейронної мережі, Проблеми інформатизації та управління. 2024. Т. 1, № 73. С. 54-62.

Особистий внесок Проскуріна Д.: створено модель ідентифікації джерала послідовності.

Особистий внесок Гнатюка С.: проведено аналіз генераторів псевдовипадкових чисел.

Особистий внесок Явіча М.: проведено аналіз нейронних мереж різних типів.

Статті у виданнях, які включено до міжнародних наукометричних баз:

1. Proskurin D., Gnatyuk S., Okhrimenko T., Iavich M. ML-Based Cryptographic Keys Quality Assessment for 5G / 6G Networks Privacy and Security, Proceedings of the IEEE International Conference on Intelligent Data Acquisition

and Advanced Computing Systems: Technology and Applications, IDAACS. 2023. С. 1025-1030.

Особистий внесок Проскуріна Д: створення методу аналізу псевдо-випадкових послідовностей на основі технологій машинного навчання.

Особистий внесок Гнатюка С.: проведено аналіз генераторів псевдовипадкових чисел.

Особистий внесок Явіча М.: проведено аналіз нейронних мереж різних типів.

Особистий внесок Охріменко Т.: проведено аналіз підходів шифрування стільникового зв'язку.

2. Gnatyuk S., Okhrimenko A., Navrotskyi D., Proskurin D., Horbakha B. Dataset of Cryptographic Algorithms for UAV Image Encryption based on Artificial Neural Networks, CEUR Workshop Proceedings. 2023. Вип. 3504. С. 63-71.

Особистий внесок Проскуріна Д.: проведено аналіз датасетів шифрування інформації на основі технологій машинного навчання.

Особистий внесок Охріменко Т.: проведено аналіз способів обробки інформації з використанням БПЛА.

Особистий внесок Навроцького Д.: проведено аналіз датасетів шифрування інформації різнох якості.

Особистий внесок Гнатюка С.: проведено аналіз способів забезпечення конфіденційності даних з використанням БПЛА.

Особистий внесок Горбахи Б.: створено загальний датасет шифрування інформації.

3. Hu Z., Ryabyy M., Prystavka P., Janisz K., Proskurin D. Advanced Method for Compressing Digital Images as a Part of Video Stream to Pre-processing of UAV Data Before Encryption, Lecture Notes on Data Engineering and Communications Technologies. 2023. Вип. 181. С. 371-381.

Особистий внесок Проскуріна Д.: проведено аналіз підходів до компресії зображень на основі технологій машинного навчання.

Особистий внесок Рябого М.: проведено аналіз способів обробки інформації до моменту шифрування.

Особистий внесок Приставки П.: проведено аналіз датасетів шифрування інформації різнох якості.

Особистий внесок Ху Ж.: створено загальний датасет способів оброки інформації.

Особистий внесок Яніш К.: проведена аналіз способів обробки інформації на основі БПЛА.

4. Proskurin D., Gnatyuk S., Okhrimenko T. Predicting Pseudo-Random and Quantum Random Number Sequences using Hybrid Deep Learning Models, CEUR Workshop Proceedings. 2023. Вип. 3426. С. 77-88.

Особистий внесок Проскуріна Д.: створення методу передбачення псевдовипадкових послідовностей на основі технологій машинного навчання

Особистий внесок Охріменко Т.: проведено аналіз квантумних генераторів даних.

Особистий внесок Гнатюка С.: постановка завдання дослідження.

5. Proskurin D., Gnatyuk S., Bauyrzhan M. Distributive Training Can Improve Neural Network Performance based on RL-CNN Architecture, CEUR Workshop Proceedings. 2021. Вип. 3187. С. 48-57.

Особистий внесок Проскуріна Д.: створення методу ідентифікації об'єктів на зображеннях на основі технологій машинного навчання.

Особистий внесок Бауиржан М.: проведена аналіз способів обробки інформації на основі БПЛА.

Особистий внесок Гнатюка С.: постановка завдання дослідження.

Наукові праці, які додатково відображають наукові результати дисертації:

1. Проскурін Д.П., Гнатюк С.О. Дистрибутивне навчання покращує роботу нейронних мереж на основі RL-CNN архітектури, ABIA-2021: XVI міжнар. наук.-техн. конф., 20-22 квітня 2021 р.: тези доп. Київ: НАУ, 2021. С. 16.14-16.17.

Особистий внесок Проскуріна Д.: створення методу ідентифікації об'єктів на зображеннях на основі технологій машинного навчання.

Особистий внесок Гнатюка С.: проведено аналіз нейроних мереж різного типу.

2. Гнатюк С.О., Проскурін Д.П. Імплементація дистрибутивного навчання покращує роботу RL-CNN архітектури для ідентифікації об'єктів на зображеннях // Всеукраїнська науково-практична інтернет-конференція здобувачів вищої освіти і молодих учених «Інформаційно-комп'ютерні технології: стан, досягнення та перспективи розвитку», 25-26 листопада 2021, Житомир, Україна.

Особистий внесок Проскуріна Д.: створення методу ідентифікації об'єктів на зображеннях на основі технологій машинного навчання.

Особистий внесок Гнатюка С.: постановка завдання дослідження.

3. Proskurin D. P. Assessing Randomness in Number Sequences in Cryptography: A Comparative Study of the Chi-Squared Test and Neural Network-Based Approaches, EEML 2023: Eastern European Machine Learning Conference, June 2023.

4. Проскурін Д.П., Гнатюк С.О. Підхід до оцінювання рівня випадковості бінарних послідовностей на основі одновимірної згорткової нейронної мережі, Information, Communication, Society (ICS-2023), 18-20 травня 2023 р., Зозулі (Львівська область), Україна.

Особистий внесок Проскуріна Д.: створення моделі оцінювання рівня випадковості бінарних послідовностей.

Особистий внесок Гнатюка С.: постановка завдання дослідження.

5. Проскурін Д.П., Гнатюк С.О. Оцінювання випадковості бінарних послідовностей на основі одновимірної згорткової нейронної мережі 1D-CNN для криптографічних застосувань // Новітні дослідження культури і мистецтва: пошуки, проблеми, перспективи : матеріали Всеукр. наук.-практ. конф. / М-во культ. України та інформ. політики ; Нац. акад. кер. кадрів культ. і мистец. ;

Наук. тов. студ., асп., доктор. і молод. вч. (Київ, 18 травня 2023 р.). Київ : НАКККіМ, 2023. С. 27-32.

Особистий внесок Проскуріна Д.: створення моделі оцінювання рівня випадковості бінарних послідовностей.

Особистий внесок Гнатюка С.: постановка завдання дослідження.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертації становить 185 сторінок, із них 160 – основного тексту. Робота містить 45 рисунків, 20 таблиць, 10 додатків. Список використаних джерел налічує 80 найменувань.

Оцінка мови та стилю дисертації. Текст дисертації викладено грамотною мовою, логічно та послідовно. Матеріали дослідження викладені з дотриманням вимог наукового стилю. Дисертація оформлена згідно з вимогами Міністерства освіти і науки України.

Характеристика особистості здобувача. Під час підготовки дисертаційної роботи здобувач проявив себе як висококваліфікований та творчий дослідник, здатний самостійно вирішувати наукові та практичні завдання. Володіє сучасними методами аналізу та має глибокі знання у своїй галузі дослідження. Здобувач відповідальний, дисциплінований, активно бере участь у наукових заходах і демонструє високий рівень аналітичного мислення та комунікативних навичок.

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Проскуріна Дмитра Петровича на тему “Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання”.
2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Проскуріна Дмитра Петровича відповідає спеціальності 122 “Комп’ютерні науки” та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 року. № 261 (зі змінами і доповненнями від 03 квітня 2019 року № 283), вимогам пп. 6, 7, 8, 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 року № 44.
3. Рекомендувати дисертаційну роботу “Інформаційна технологія оцінювання якості генераторів послідовностей псевдовипадкових чисел на основі машинного навчання”, подану Проскуріним Дмитром Петровичем на здобуття ступеня доктора філософії з галузі знань 12 “Інформаційні технології”, за спеціальністю 122 “Комп’ютерні науки” до захисту у разовій спеціалізованій вченій раді.

4. Рекомендувати Вченій раді НАУ клопотати про призначення:

Головою разової спеціалізованої вченої ради:

Нечипорук Олену Петрівну, доктора технічних наук, професора, професора кафедри інтелектуальних кібернетичних систем НАУ.

Рецензентом:

– *Фесенка Андрія Олексійовича,* кандидата технічних наук, доцента, в.о. декана Факультету комп'ютерних наук та технологій;

Офіційними опонентами:

– *Чевардіна Владислава Євгенійовича,* доктора технічних наук, старшого наукового співробітника, начальника кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені Героїв Крут;

– *Опірського Івана Романовича,* доктора технічних наук, професора, завідувача кафедри захисту інформації Національного університету «Львівська політехніка»;

– *Фауре Еміля Віталійовича,* доктора технічних наук, професора, проректора з науково-дослідної роботи та міжнародних зв'язків Черкаського державного технологічного університету.

Головуючий на засіданні:
доктор технічних наук, професор,
завідувач кафедри комп'ютерних
інформаційних технологій НАУ Аліна САВЧЕНКО

Секретар засідання:
кандидат технічних наук, ст. дослідник,
п.н.с. НДЛ протидії кіберзагрозам
в авіаційній галузі НАУ Тетяна ОХРІМЕНКО

ПОГОДЖЕНО:
доктор технічних наук, професор,
в.о проректора з наукової роботи НАУ Сергій ГНАТЮК