ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного технічного
університету України
"Київський політехнічний інститут
імені Ігоря Сікорського"
к.філос.н., проф.
Анатолій МЕЛЬНИЧЕНКО

" 18 " березня 2024 р.

ВИТЯГ

з протоколу № 11 від 13.03.2024 р. розширеного засідання
кафедри програмного забезпечення комп'ютерних систем
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"

БУЛИ ПРИСУТНІ:

- з кафедри програмного забезпечення комп'ютерних систем:
професор, д.т.н., професор Легеза В. П.; доцент, к.т.н., доцент Заболотня Т. М.; доцент, к.т.н., доцент Онай М. В.; доцент, к.т.н., доцент Олещенко Л. М.; доцент, к.т.н., доцент Юрчишин В. Я.; доцент, к.т.н., доцент Нещадим О. М.; доцент, к.т.н., доцент Люшенко Л. А.; доцент, к.т.н., доцент Саяпіна І. О; асистент, доктор філософії Юсин Я. О.; доцент, к.е.н., доцент Ткаченко К. О.
- з системного програмування і спеціалізованих комп'ютерних систем:
завідувач кафедри, д.т.н., професор Романкевич В. О.; доцент, к.т.н., доцент Клятченко Я. М.; доцент, к.т.н., доцент Петрашенко А. В.
- з кафедри інформаційних систем та технологій:
професор, д.ф.-м.н., професор Дорошенко А. Ю.
- з кафедри інженерії програмного забезпечення в енергетиці:
завідувач кафедри, д.т.н., професор Коваль О. В.
- інші запрошені:
декан факультету прикладної математики, д.т.н., професор Дичка І. А.

Запрошені з інших організацій:
- з Національного університету «Запорізька політехніка», д.т.н., професор, завідувач кафедри програмних засобів факультету комп'ютерних наук і технологій Субботін С. О.;

- з Харківського національного університету радіоелектроніки, к.т.н., доцент, доцент кафедри штучного інтелекту факультету комп'ютерних наук Золотухін О. В.

СЛУХАЛИ:

1. Повідомлення аспіранта кафедри програмного забезпечення комп'ютерних систем Северіна Андрія Івановича за матеріалами дисертаційної роботи "Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації", поданої на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення.

Освітньо-наукова програма Інженерія програмного забезпечення.

Тему дисертаційної роботи "Методи захисту приватних наборів даних для вирішення задач класифікації й кластеризації" затверджено на засіданні Вченої ради факультету прикладної математики (протокол № 4 від "23" листопада 2020 року) та перезатверджено на тему "Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації" на засіданні Вченої ради факультету прикладної математики (протокол № 2 від "25" вересня 2023 року).

Науковим керівником затверджений к.т.н., доцент Онай М. В.

2. Запитання до здобувача.

Запитання по темі дисертації ставили:

д.т.н., професор, Субботін С. О.; д.т.н., професор, Коваль О. В.; д.т.н., професор Романкевич В. О.; доцент, к.т.н., доцент Клятченко Я. М.; доцент, к.т.н., доцент Петрашенко А. В.; доцент Олещенко Л. М.

3. Виступи за обговореною роботою.

В обговоренні дисертації взяли участь:

д.т.н., професор, Субботін С. О.

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження:

1. Актуальність теми дослідження

Впровадження систем аналізу даних і штучного інтелекту набуває все більшого поширення у різних аспектах людського життя. Окрім звичних випадків застосування таких систем у електронній комерції та соціальній сфері, такі інструменти стрімко поширюються й для персонального використання (наприклад, чатботи ChatGPT, Google Bard, Microsoft Copilot).

В основі систем, що використовують методи машинного навчання, лежать дані. Вони є необхідним елементом як для навчання систем аналізу

даних і штучного інтелекту, так і для їх тестування. Чим більше різнопланових даних, аналізується, тим точнішою є побудована програмна система. Незважаючи на те, що кількість створюваних та оброблюваних даних стрімко зростає, дані досить часто містять щонайменше частину приватної інформації, що обмежує їх використання для систем аналізу даних і штучного інтелекту. Приватні дані – інформація, яка є конфіденційною, чутливою або секретною. Збереження приватності даних є вкрай важливим, адже втрата приватності може призвести до негативних наслідків (передусім різноманітних злочинів).

Таким чином, вище описані задачі визначають актуальну науково-технічну задачу вдосконалення алгоритмічного та програмного забезпечення захисту приватних наборів даних у системах з використанням штучного інтелекту, яка вирішується у дослідженні для задачі класифікації.

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

Дослідження за темою дисертаційної роботи провадились на кафедрі програмного забезпечення комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» в рамках виконання ініціативної науково-дослідної роботи «Розроблення та дослідження засобів зберігання секретності приватних наборів даних при побудові систем аналізу даних і штучного інтелекту» (номер державної реєстрації 0121U109925).

3. Наукова новизна отриманих результатів

У дисертації вперше одержані такі нові наукові результати:

1. **Уперше** запропоновано архітектуру програмної системи для вирішення задачі класифікації на основі приватних даних, характерною особливістю якої є захист приватних наборів даних, шляхом функціонального шифрування, що відбувається на стороні клієнта, і дозволяє збільшити кількість наборів даних для навчання загальнодоступних систем аналізу даних і штучного інтелекту.
2. **Уперше** запропоновано модифікацію програмної моделі шифрування даних, яка відрізняється від існуючої використанням двовимірних згорткових нейронних мереж, замість одновимірних, і дозволяє застосовувати модель шифрування з використанням нейронних мереж до даних, що представлені набором пікселів, з яких складається зображення.
3. **Уперше** розроблено алгоритмічно-програмний метод функціонального шифрування наборів даних, особливістю якого є можливість використання приватних наборів даних в загальнодоступних системах аналізу даних та штучного інтелекту шляхом зменшення їх розмірності й функціонального шифрування отриманих даних з використанням приватного ключа.
4. **Уперше** розроблено алгоритмічно-програмний метод пошуку нормальних поліномів серед незвідних, який відрізняється від існуючого використанням простих чисел у десятковому представленні замість поліномів, що дозволяє зменшити обчислювальні витрати алгоритму

пошуку незвідних многочленів з $O(n^3)$ до $O(n \log(\log n))$ і, як наслідок, спростити міжбазисні перетворення у бінарних скінченних полях з метою пришвидшення виконання операцій над елементами поля у методах гомоморфного шифрування даних.

5. **Уперше** розроблено модифікований спосіб побудови матриці переходу між поліноміальним та нормальним базисами скінченного поля, який полягає у використанні рекурентної формули $\alpha_{i+1} = t^{p^{i+1}} = t^{p^i \cdot p} = (\alpha_i)^p$ замість обчислення остачі від ділення елемента $t^{p^{i+1}}$ на незвідний поліном, що дозволяє зменшити кількість використовуваної пам'яті з $n p^i$ до $n \cdot p$, а також обчислювальну складність з $O(m^{p^i})$ до $O(m^p)$.

4. Теоретичне та практичне значення результатів роботи

Теоретичне значення результатів роботи полягає в удосконаленні процесу оброблення приватних наборів даних для програмних систем інтелектуального аналізу даних.

Практичне значення одержаних результатів полягає у спрощенні процесу розроблення загальнодоступних систем аналізу даних і штучного інтелекту на основі приватних даних, яке передбачає застосування розроблених методів захисту приватних наборів даних.

Розроблене алгоритмічне та програмне забезпечення для захисту приватних наборів даних, яке застосовано при виконанні ініціативної науково-дослідної роботи «Розроблення та дослідження засобів зберігання секретності приватних наборів даних при побудові систем аналізу даних і штучного інтелекту» (номер державної реєстрації 0121U109925) для шифрування даних, з метою їх подальшого використання в загальнодоступних системах штучного інтелекту.

5. Апробація/використання результатів дисертації

Основні результати дисертаційного дослідження доповідалися та обговорювалися на наукових конференціях:

1. Тринадцята наукова конференція магістрантів і аспірантів «Прикладна математика та комп'ютинг» (ПМК' 2020), Київ, 18 - 20 листопада 2020 р., Київ, Україна.
2. XII Міжнародна науково-практична конференція молодих учених та студентів «Актуальні задачі сучасних технологій», 6-7 грудня 2023, Тернопіль, Україна.
3. XI науково-технічно конференція «Інформаційні моделі, системи та технології», 13-14 грудня 2023 р., Тернопіль, Україна.

6. Дотримання принципів академічної доброчесності

За результатами науково-технічної експертизи дисертація Северіна А. І. визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 7 наукових публікацій, у тому числі:

- 2 статті у наукових фахових виданнях України категорії Б за спеціальністю, 121 Інженерія програмного забезпечення;
- 1 статтю у закордонному фаховому виданнях третього квартиля (Q3), яке проіндексоване в базі даних Scopus;
- 1 статтю у фаховому виданні, яке проіндексоване в базі даних Web of science;
- 3 тези виступів на наукових конференціях.

1. Modified Change-of-Basis Conversion Method in $GF(2^m)$ / I. A. Dychka, V. P. Legeza, M. V. Onai, A. I. Severin. // Radio Electronics, Computer Science, Control. — 2020. — №2. — С. 117–128 — DOI: 10.15588/1607-3274-2020-2-12. (**Web of Science**, **категорія «А»**)
   Здобувачем розроблено метод пошуку нормальних поліномів для міжбазисних перетворень бінарних скінченних полів, незвідні поліноми у якому пропонується шукати як прості числа представлені у системі числення з основою 2.
2. Method of Performing Operations on the Elements of $GF(2^m)$ Using a Sparse Table / I. Dychka, M. Onai, A. Severin, C. Hu. // International Journal of Computer Network and Information Security (IJCNIS). — 2024. — Vol. 16, №1. — pp. 61-72 — DOI: 10.5815/ijcnis.2024.01.05. (**Scopus, Q3**)
   Здобувачем показано, як час виконання операцій над елементами розширеного поля Галуа залежить від базису, в якому представлені елементи.
3. Северін А.І. Методи збереження приватності в машинному навчанні. / М.В. Онай, А.І. Северін // Вісник Хмельницького національного університету Серія: «Технічні науки». — 2023. — №6. — С. 274-280 — DOI: 10.31891/2307-5732-2023-329-6-274-280. (**категорія «Б»**)
   Здобувачем проведено комплексний порівняльний аналіз методів збереження приватності в машинному навчанні.
4. A. Severin. Architecture of a software system for solving the classification problem based on private data. / M. Onai, A. Severin // Herald of Khmelnytskyi national university. Technical Sciences. — 2024. — №1. — pp. 244-247 — DOI: 10.31891/2307-5732-2024-331-36. (**категорія «Б»**)
   Здобувачем запропоновано архітектуру програмної системи для вирішення задачі класифікації на основі приватних даних, особливістю якої є захист приватних наборів даних шляхом функціонального шифрування, що відбувається на стороні клієнта.
5. Северін А.І. Метод захисту набору даних зображень для вирішення задачі класифікації. / М.В. Онай, А.І. Северін // Прикладна математика та комп'ютинг. ПМК-2020 : тринадцята наук. конф. магістрантів та аспірантів, Київ, 18-20 листопада 2020 р. : зб. тез доп. / [ред кол.: Дичка І.А. та ін.] . — К. : Просвіта, 2020. — С. 221-226.

Здобувачем розроблено метод функціонального шифрування наборів даних-зображень, особливістю якого є можливість використання приватних наборів даних в загальнодоступних системах для вирішення задачі класифікації.

6. Северін А.І. Комплексний порівняльний аналіз методів збереження приватності в машинному навчанні. / М.В. Онай, А.І. Северін // Актуальні задачі сучасних технологій : зб. тез доповідей XII міжнар. наук.-практ. конф. Молодих учених та студентів, (Тернопіль, 6-7 грудня 2023) / М-во освіти і науки України, Терн. націон. техн. ун-т ім. І. Пулюя [та ін.]. — Тернопіль: ФОП Паляниця В. А., 2023. — С. 406-407.
   Здобувачем проаналізовано загрози приватності в системах машинного навчання й розглянуто методи протидії їм.
7. Северін А.І. Модифікований підхід для побудови матриці міжбазисних перетвореннь у $GF(p^m)$. / М.В. Онай, А.І. Северін // Матеріали XI науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 13-14 грудня 2023 р.). — Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2023 — С. 110.
   Здобувачем розроблено спосіб побудови матриці переходу, шляхом пошуку базисних елементів нормального базису на основі рекурентної формули.

Якість та кількість публікацій відповідають "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 р. № 44".

ВВАЖАТИ, що дисертаційна робота Северіна А. І. "Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації", що подана на здобуття ступеня доктора філософії з галузі знань Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення за своїм науковим рівнем, новизною отриманих результатів, теоретичною та практичною цінністю, змістом та оформленням повністю відповідає вимогам, що пред'являють до дисертацій на здобуття ступеня доктора філософії та відповідає напрямку наукового дослідження освітньо-наукової програми КПІ ім. Ігоря Сікорського Інженерія програмного забезпечення зі спеціальності 121 Інженерія програмного забезпечення.

РЕКОМЕНДУВАТИ:

1. Дисертаційну роботу "Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації", подану Северіном Андрієм Івановичем на здобуття наукового ступеня доктора філософії, до захисту у разовій спеціалізованій вченій раді.

2. Вченій раді КПІ ім. Ігоря Сікорського утворити разову спеціалізовану вчену раду у складі:

Голова:

д.т.н., професор, завідувач кафедри інженерії програмного забезпечення в енергетиці Навчально-наукового інституту атомної та теплової енергетики КПІ ім. Ігоря Сікорського **Коваль Олександр Васильович**.

Члени:

Рецензенти:

д.ф.-м.н., професор, професор кафедри інформаційних систем та технологій факультету інформатики та обчислювальної техніки КПІ ім. Ігоря Сікорського **Дорошенко Анатолій Юхимович**;

к.т.н., доцент, доцент кафедри системного програмування і спеціалізованих комп'ютерних систем факультету прикладної математики **Клятченко Ярослав Михайлович**.

Офіційні опоненти:

д.т.н., професор, завідувач кафедри програмних засобів факультету комп'ютерних наук і технологій Національного університету «Запорізька політехніка» **Субботін Сергій Олександрович**;

к.т.н., доцент, доцент кафедри штучного інтелекту факультету комп'ютерних наук Харківського національного університету радіоелектроніки **Золотухін Олег Вікторович**.

Головуючий на засіданні
д.т.н., професор,
професор кафедри програмного
забезпечення комп'ютерних систем
КПІ ім. Ігоря Сікорського — Віктор ЛЕГЕЗА

Заступник завідувача кафедри
програмного забезпечення
комп'ютерних систем,
к.т.н., доцент — Оксана ШКУРАТ

Гарант освітньо-наукової програми,
д.т.н., доцент — Євгенія СУЛЕМА

Вчений секретар
кафедри програмного
забезпечення комп'ютерних систем
к.т.н., доцент — Любов ОЛЕЩЕНКО