

**ВИСНОВОК
ПРО НАУКОВУ НОВИЗНУ, ТЕОРЕТИЧНЕ ТА ПРАКТИЧНЕ
ЗНАЧЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ**

Гальченка Андрія Віталійовича на тему «Інструментальні засоби криптографічних систем на базі заперечуваного шифрування», що подана на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» (галузь знань 12 «Інформаційні технології»)

Дисертація Гальченка Андрія Віталійовича на тему «Інструментальні засоби криптографічних систем на базі заперечуваного шифрування», що подана на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» (галузь знань 12 – «Інформаційні технології»), виконана на кафедрі програмної інженерії математичного факультету Запорізького національного університету Міністерства освіти і науки України. Тема дисертації затверджена на засіданні науково-технічної ради Запорізького національного університету (протокол № 4 від 29 листопада 2016 р.).

Для підготовки висновку про наукову новизну, теоретичне та практичне значення результатів дисертації «Інструментальні засоби криптографічних систем на базі заперечуваного шифрування» Вченою радою Запорізького національного університету (протокол № 5-ДФ від 22 грудня 2020 року) визначено, що попередня експертиза дисертації проводитиметься на базі математичного факультету Запорізького національного університету, та призначено двох рецензентів:

1. Професора кафедри економічної кібернетики Запорізького національного університету, доктора фізико – математичних наук, професора Козіна Ігора Володимировича;
2. Доцента кафедри програмної інженерії Запорізького національного університету, кандидата фізико-математичних наук Кудіна Олексія Володимировича.

1. Ступінь актуальності теми дослідження

Дисертаційна робота присвячена вирішенню науково-практичної задачі – розробка ефективних моделей обчислень з використанням існуючих методів машинної обробки інформації. Вказане дозволить збільшити швидкість перетворення даних, які лежать в основі перспективних алгоритмів шифрування, а саме заперечуваного шифрування.

У сучасних автоматизованих і інформаційних системах програмні засоби захисту інформації, з-поміж інших, набули найбільшого поширення. Їх застосування дозволяє попередити можливість несанкціонованого доступу до інформації використовуються. Встановлено, що на практиці поширення набули криптографічні та стеганографічні схеми, і алгоритми перетворення даних. Їх надійність ґрунтується на застосуванні методів криптографії і стеганографії. Разом

з тим, зазначається, що на відміну від стеганографії, алгоритми криптографії дозволяють не лише приховати дані, а також захистити їх інформаційну складову від витоку. Таким чином, визначено, що розробка алгоритмів шифрування інформації з використанням алгоритмів, які мають обчислювальну та алгоритмічну стійкість, є перспективним напрямом досліджень. До вказаних алгоритмів автор відносить алгоритми заперечуваного шифрування даних, невирішеною проблемою яких є відсутність ефективної реалізації. Зазначено, що вказане унеможливорює їх практичну реалізацію. Незважаючи на це, з відкритих джерел встановлено, що імітуючи особливості механізмів заперечуваного шифрування, на сьогодні дослідники даної галузі знань створили велику кількість алгоритмів, стійких до обчислювальних атак. Однак вказані алгоритми мають обмеження та вразливості, які не перешкоджають використанню можливостей заперечуваного шифрування в повній мірі. Моделі перетворення та обробки даних, які викладені в дисертаційній роботі, ґрунтуються на комбінуванні елементів симетричної та асиметричної криптографії, а також використання методів прискорення обчислення. Поєднання вказаних напрямів ґрунтується на тому, що використання симетричної криптографії та окремих алгоритмів кодування дозволяє збільшити пропускну здатність алгоритмів заперечуваного шифрування, при цьому використання паралельних і розподілених обчислень дозволяє збільшити швидкість перетворення даних у короткий проміжок часу. Тим не менш, наукові праці з окремих питань проблематики щодо створення ефективних алгоритмів заперечуваного шифрування, жодним чином не применшуючи їх значення, не містять інформації щодо практичних обчислювальних досліджень присвячених алгоритмам заперечуваного шифрування, у контексті обґрунтування актуальності роботи не проведено.

2. Об'єкт, предмет, мета та завдання роботи

Об'єктом дослідження є схеми перетворення даних, в основі яких лежить використання сучасних засобів криптографічного захисту інформації, зокрема алгоритмів заперечуваного шифрування.

Предметом дослідження є способи і методи ефективного перетворення даних, використання яких не призводить до внесення змін у вихідні алгоритми заперечуваного шифрування.

Метою роботи є розробка способів ефективно організації обчислень, які лежать в основі існуючих алгоритмів заперечуваного шифрування інформації.

Для досягнення мети в роботі, на основі систематичного огляду та аналізу літературних джерел, що розкривають сучасний стан досліджень в обраній області, поставлені та вирішені наступні завдання:

1) **дослідити** проблемну область щодо методів підвищення швидкодії криптографічних алгоритмів шляхом застосування алгоритмів кодування, паралельних і розподілених обчислень;

2) розробити модель ефективної реалізації обчислень, які лежать в основі алгоритмів заперечуваного шифрування;

3) удосконалити модель обчислень заперечуваного шифрування у частині використання паралельних комп'ютерних систем зі спільною пам'яттю;

4) удосконалити модель обчислень заперечуваного шифрування у частині використання паралельних комп'ютерних систем з розділеною пам'яттю та статичним балансуванням навантаження;

5) розробити прототип програмного забезпечення, яке реалізує перетворення закладені у вихідну, паралельні та розподілену моделі заперечуваного шифрування.

3. Методи дослідження

З метою досягнення вказаної мети і виконання завдань дисертаційного дослідження використано: науковий метод; формальні математичні методи; існуючі програмні та математичні рішення опубліковані у відкритих джерелах; декомпозицію і аналіз існуючих алгоритмів шифрування, кодування та обробки даних; моделювання процесів перетворення даних і пошуку вузлів, які потребують оптимізації обчислювального процесу; оцінку витрат обчислювальних ресурсів системи з використанням спеціалізованих програмних модулів; оцінку ефективності запропонованих рішень шляхом аналізу експериментальних результатів; методи та мови програмування; методи планування, виконання та аналізу обчислювальних експериментів.

4. Рівень обізнаності здобувача про сучасний стан досліджень у контексті роботи

Визначено, що науковим підґрунтям для виконання дисертаційної роботи стали систематичне дослідження та аналіз наукових праць вітчизняних і закордонних фахівців. Досліджувався сучасний світовий науковий доробок у наступних галузях знань та наступних авторів, що достатньо покриває існуючий стан наукових досліджень у контексті дисертації:

– криптографічні методи захисту даних (Adleman L. M., Alvila M., Anderson R., Biham E., Brown L., Chou T., Diffie W., ElGamal T., Hellman M. E., Knudsen L., Krishnamurthy G. N., Menezes A. J., Moriai S., Orlandi C., Orschot P. V., Piessens F., Rabin M. O., Ramaswamy Dr. V., Rives R. L., Shamir A., Stallings W., Vanhoef M., Vanstone S. A., Williams H. C., Yiqun L. Y., Болотов А. А., Гашков С. Б., Евсютин О. О., Йона Л. Г., Калинин Д. А., Козина Г. Л., Конев А. А., Онацкий А. В., Пестунов А. И., Петухов М., Трунова А. А., Фомина И. А., Фролов А. Б., Шелупанов А. А., Шнайер Б., Яппаров Р. М.);

– стеганографічні методи захисту даних (Гнатюк С. О., Довгич Н. І., Євсєєв С. П., Конахович Г. Ф., Король О. Г., Кузнецов О. О., Літош М. С., Навроцький Д. О., Пузыренко А. Ю., Стасюк О. І.);

– комутативне шифрування даних (Березин А. Н., Молдовян А. А., Паутов П. А., Рыжков А. В.);

– гомоморфне шифрування даних (Астахова Л. В., Ашихмин Н. А., Варновский Н. П., Султанов Д. Р., Трубей А. И., Шокуров А. В.);

– заперечуване шифрування даних (Barakat T. M., Basu S., Canetti R., Caro A. D., Chen B., Deera N., Dwork C., Ereemeev A. E., Goldwasser S., Hong X., Howlader J., Ibrahim H., Iovino V., Klonowski M., Kubiak P., Kutylowski M., Mannan M., Meng B., Micali C., Moldovyan A. A., Moldovyan D. N., Naor M., O'Neill A., Ostrovsky R., Rjazhkova Z., Shcherbacov V. A., Skillen A., Wang B., Wang JQ., Биричевский А. Р., Вайчикаускас М. А., Молдовян Н. А., Мондикова Я. А., Морозова Е. В., Татчина Я. А.);

– паралельні обчислення (Берцун В. Н., Бугеря А. Б., Воеводин В. В., Воеводин Вл. В., Галаган П. В., Гергель В. П., Ким Е. С., Кормен Т., Лейзерсон Ч., Ривест Р., Соловьев М. А., Старченко А. В., Чудинов С. М., Штайн К.);

– кодування даних (Bryant D., Durgesh P., Kedarnath J. B., Motta G., Nur A. T., Rajawat A. S., Salomon D., Кулешов С. В., Лидовский В. В.);

– розподілені обчислення (Бугеря А. Б., Ван Стеен М., Варганян С. О., Десятирикова Е. Н., Ким Е. С., Лесная Н. С., Сокол В. В., Соловьев М. А., Таненбаум Э.).

У роботі використано елементи критичного мислення для пошуку та забезпечення повноти вибору релевантних публікацій для аналізу літературних джерел, що обґрунтовує систематичність та повноту обізнаності автора щодо сучасного стану науково-технічного доробку в контексті дисертаційного дослідження.

Разом з тим, враховуючи розмаїття наукових праць з окремих питань проблематики здобуття термінів та вимог щодо побудови описових теорій предметних областей, й жодним чином не применшуючи їх значення, варто зазначити, що комплексних наукових досліджень, безпосередньо присвячених алгоритмам заперечуваного шифрування даних, з експериментально обґрунтованими показниками продуктивності, дослідження впливу окремих характеристик даних і методів організації ефективного перетворення даних у комп'ютерних науках, які забезпечують можливість практичного застосування заперечуваного шифрування, не проведено, проведено у неповній мірі або проведено з неможливістю відтворення результатів експериментів. Тому, дисертаційна робота є обґрунтованою у даному науково-технічному напрямі, вищезазначені факти роблять актуальним представлені в дисертації дослідження та зумовлюють їх теоретичне та практичне значення.

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

Здобувач вірно визначає зв'язок роботи з науковими програмами, планами, темами, грантами, вказує на те, що дослідження проводились у рамках виконання

державної бюджетної програми «Розробка математичного забезпечення для інженерного аналізу об'єктів аерокосмічної техніки на базі хмарних технологій» (№ державної реєстрації 0117U007204). Науковий керівник: д.т.н., професор Чопоров С. В. Участь здобувача – виконавець.

6. Наукова новизна, теоретичне та практичне значення результатів дисертації

Наукова новизна результатів дослідження полягає у тому, що робота є одним з перших у вітчизняній галузі комп'ютерних наук комплексним дослідженням, присвяченим алгоритмам заперечуваного шифрування, їх розробки та пошуку практичних способів реалізації, що повно характеризують професійну предметну область. У результаті проведеного дослідження:

Розроблено:

1) **модель операцій** заперечуваного шифрування, удосконалення якої у частині кодування інформації дозволило скоротити час, необхідний на перетворення окремих типів даних, за рахунок зменшення кількості використаних у цьому процесі операцій;

2) **програмні модулі**, які реалізують запропоновану аналітичну модель, паралельні та розподілені методи заперечуваного шифрування.

Удосконалено:

1) метод заперечуваного шифрування у частині його роботи у **паралельних комп'ютерних системах зі спільною пам'яттю**, що дозволяє збільшити швидкість перетворення даних алгоритмами заперечуваного шифрування;

2) метод заперечуваного шифрування у частині його роботи у **паралельних комп'ютерних системах з роздільною пам'яттю (обчислювальних кластерах)** зі статичним балансуванням навантаження, що дозволило збільшити швидкість обробки даних великого обсягу.

7. Практичне значення результатів дисертації

Практичне значення отриманих наукових результатів полягає у програмній реалізації, що дозволяє більше ефективно використовувати заперечуване шифрування у паралельних комп'ютерних системах. Науково-технічний ефект полягає у зменшенні часу, необхідного на обробку даних при заперечуваному шифруванні.

8. Публікації, що висвітлюють основні результати дисертації, та особистий внесок здобувача

Наукові положення і результати, що представлені в дисертаційній роботі, отримані здобувачем особисто. Наукові публікації результатів дисертаційної роботи, написані у співавторстві. Нижче наведені ці публікації та вказано

особистий внесок здобувача і розділи дисертації, що висвітлюються цими публікаціями:

1. Гальченко А. В., Козіна Г. Л. Модифікація алгоритму заперечуваного шифрування Менга. *Радіоелектроніка. Інформатика. Управління*. 2016. № 2. С. 77–86.

Особистий внесок здобувача: аналіз структури алгоритму заперечуваного шифрування, визначення місця в якому можливо виконати атаку на обчислювальну схему алгоритму та пошук методів щодо підвищення стійкості обчислювальної схеми алгоритму.

Розділи дисертації: 2.1-2.4.

2. Гальченко А. В. Захист персональних даних з використанням алгоритмів неоднозначного шифрування. *Вісник ЗНУ*. 2017. № 2. С. 19–32.

Особистий внесок здобувача: презентація прототипу аналітичної моделі блокового перетворення даних на основі існуючого алгоритму заперечуваного шифрування.

Розділи дисертації: 2.1-2.4.

3. Гальченко А. В., Чопоров С. В. Заперечуване шифрування на основі застосування підходу гібридних криптографічних систем. *Радіоелектроніка. Інформатика. Управління*. 2019. № 1. С. 178–191.

Особистий внесок здобувача: розробка структури аналітичної моделі перетворення даних, побудова прикладної моделі заперечуваного шифрування на баз існуючого алгоритму перетворення даних, експериментальне дослідження моделі та окремих характеристик, які впливають на ефективність її роботи.

Розділи дисертації: 2.1-2.4.

4. Galchenko A., Choporov S. Block cipher modes in the deniable encryption. *Вісник ЗНУ*. 2019. № 1. С. 146–153.

Особистий внесок здобувача: розробка адаптивних моделей режимів шифрування даних та перевірка можливості їх практичного використання в алгоритмах заперечуваного шифрування, з урахуванням необхідності захисту вихідних даних і забезпечення високого рівня продуктивності обчислень.

Розділи дисертації: 2.1.2.

5. Гальченко А. В., Чопоров С. В. Кодування даних в алгоритмах заперечуваного шифрування. *Прикладні питання математичного моделювання*. 2020. Т. 3, № 2 (1). С. 72–79.

Особистий внесок здобувача: розробка механізму адаптованого кодування даних з можливістю прогнозування коефіцієнту компресії вихідних даних, експериментальне дослідження залежності продуктивності кодування даних від налаштувань програм для їх компресії.

Розділи дисертації: 4.1-4.5.

6. Гальченко А. В. Реалізація заперечуваного шифрування на базі розподілених обчислень. *Вісник ЗНУ*. 2020. № 1. С. 128–138.

Особистий внесок здобувача: розробка моделі обчислень визначенням критичних технічних характеристик кінцевих пристроїв, експериментальне дослідження запропонованої моделі шляхом проведення обчислювального експерименту.

Розділи дисертації: 5.1-5.4.

7. Гальченко А. В., Чопоров С. В. Використання методу розділяй та володарюй в алгоритмах заперечуваного шифрування. *Кібербезпека: освіта, наука, техніка*. 2020. Т. 2, № 10. С. 29–44.

Особистий внесок здобувача: розробка механізму автоматизованого поділу та відновлення даних, імплементація механізму у вихідну аналітичну модель та експериментальне дослідження ефективності запропонованого рішення у порівнянні зі звичайним паралелізмом.

Розділи дисертації: 3.1-3.5.

Таким чином, можна зазначити, що:

1. Здобувачем опубліковано 7 наукових робіт, що висвітлюють основний зміст дисертації, 2 з яких опубліковано у виданні, що проіндексовано у наукометричній базі Web Of Science.

2. Ці публікації достатньо повно розкривають основний зміст дисертації та відповідають умовам зарахування їх за темою дисертації відповідно пункту 11 Порядку проведення експерименту з присудження ступеня доктора філософії (*Постанова КМУ № 167 від 6.03.2019 р. із змінами згідно з Постановою КМУ № 979 від 21.10.2020р.*).

9. Відповідність дисертації вимогам, передбаченим пунктом 10 Порядку проведення експерименту з присудження ступеня доктора філософії

Дисертацію подано у вигляді спеціально підготовленої кваліфікаційної наукової праці на правах рукопису, що виконувалася здобувачем особисто. Дисертація містить наукові положення, нові науково обґрунтовані теоретичні та експериментальні результати проведених здобувачем досліджень, що мають істотне значення для галузей комп'ютерних наук і інформаційної безпеки. Це ґрунтовно підтверджено публікаціями, що розкривають основний зміст роботи. Дисертація свідчить про особистий внесок здобувача в науку та характеризується єдністю змісту.

Дисертацію оформлено у повній відповідності до вимог Міністерства освіти і науки України (Наказ №40 від 12.01.2017 із змінами, внесеними згідно з *Наказом Міністерства освіти і науки №759 від 31.05.2019*).

Дисертація написана грамотною українською мовою. Стиль викладення матеріалу відповідає прийнятому в науковій літературі з комп'ютерних наук, та характеризується точністю, логічністю, зрозумілістю, зв'язністю, цілісністю та завершеністю.

ВИСНОВОК

Ознайомившись із дисертацією Гальченка Андрія Віталійовича «Інструментальні засоби криптографічних систем на базі заперечуваного шифрування» та науковими публікаціями, у яких висвітлені основні наукові результати дисертації вважаємо, що:

1. Дисертація Гальченка Андрія Віталійовича «Інструментальні засоби криптографічних систем на базі заперечуваного шифрування» є науковим дослідженням з актуального питання, характеризується єдністю змісту, містить наукові результати, яким властива наукова новизна, теоретичне та практичне значення, а отже, свідчить про особистий внесок здобувача у розвиток перспективних алгоритмів перетворення та обробки даних, які використовуються на стику та є частиною галузі комп'ютерних наук.

2. Дисертація Гальченка Андрія Віталійовича «Інструментальні засоби криптографічних систем на базі заперечуваного шифрування» може бути рекомендована до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки» (галузь знань 12 – «Інформаційні технології») у разовій спеціалізованій вченій раді.

Рецензент:

професор кафедри економічної кібернетики
Запорізького національного університету,
доктор фізико-математичних наук, професор


(підпис)

I. В. Козін

«04» лютого 2021 р.

Рецензент:

доцент кафедри програмної інженерії
Запорізького національного університету,
кандидат фізико-математичних наук


(підпис)

О. В. Кудін

«04» лютого 2021 р.

Підпис
засвідчую

Козіна І. В.
Кудіна О. В.



А. Котелесова