ВІДГУК

офіційного опонента на дисертаційну роботу Титарчука Євгенія Олександровича "Захист персональної інформації користувачів комп'ютерних систем при використанні публічних хмарних сервісів" на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Актуальність теми дисертації.

Дисертаційна робота Титарчука Євгенія Олександровича присвячена розробці нової методики захисту приватної інформації користувачів на основі методу частково гомоморфного шифрування та спрямована на підвищення ефективності захисту інформації в комп'ютерних системах, що використовують у своєму складі публічні хмарні сервіси. Необхідність розробки такої методики обумовлена тим, що завдяки збільшенню пропускної здатності сучасних мереж, зниженню загальної вартості комп'ютерної техніки та пристроїв зберігання даних, значному впровадженню технологій віртуалізації та набуттю популярності мікро-сервісної архітектури – окремі компоненти системи все частіше замінюють публічними хмарними сервісами. Це дозволяє пришвидшити час розробки таких систем, зручність їх налаштування та спростити підтримку. Проте, використання сторонніх модулів, інфраструктурою яких керує третя сторона – провайдер хмарного рішення, робить вразливим персональну інформацію користувачів, що обробляється у таких модулях. Застосування методів перетворення моделі обчислення комп'ютерної системи та методів частково гомоморфного та гібридного шифрування дозволяють захистити інформацію користувача під час її зберігання та обробки на стороні публічного хмарного сервісу.

Таким чином, актуальність теми дисертаційної роботи здобувача обумовлена необхідністю підвищення ефективності захисту інформації в комп'ютерних системах, що використовують у своєму складі публічні хмарні сервіси шляхом розробки нової методики захисту приватної інформації

користувачів на основі методу частково гомоморфного шифрування, використання якого дозволить виконувати обчислення у сторонніх сервісах без ризику втрати приватної інформації користувачів.

Робота виконувалася відповідно до Указу Президента України «Про Положення про технічний захист інформації в Україні» (у редакції від 11.04.2008) та згідно положенню «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації.» Державної служби спеціального зв'язку та захисту інформації України (НД ТЗІ 1.1-005-07).

Основний зміст роботи.

У вступі обґрунтовано актуальність дисертації, визначено мету, об'єкт та предмет дослідження. Сформульовано завдання дослідження та наведено основні наукові та практичні результати. Відзначено особистий внесок здобувача, апробацію результатів дисертаційної роботи на конференціях, наведено відомості про публікації та структуру роботи.

У першому розділі здобувачем проаналізовано актуальні недоліки та небезпеки при використанні публічних хмарних сервісів обробки та зберігання інформації. Також проаналізовано сучасні методи захисту інформації, та визначено їх основний недолік – неможливість застосування при виконанні обчислень з даними, що необхідно захистити. На основі цього аналізу обрано напрямок та сформульовано завдання дослідження.

У другому розділі дисертаційної роботи формалізовано компоненти комп'ютерної системи, що використовує хмарний сервіс. Наведено математичну модель гомоморфного відносно операції додавання алгоритму шифрування на основі еліптичних кривих, та виконано його перевірку на криптографічну стійкість. Створений алгоритм дозволяє гомоморфно додати два зашифрованих числа без їх розшифрування. У цьому розділі також запропоновано алгоритм формування спільного ключа для алгоритму симетричного шифрування між багатьма учасниками.

Третій розділ присвячено розробці загальної методики для побудови

комп'ютерних систем, що використовують публічні хмарні сервіси, з захистом приватної інформації користувача від провайдерів хмарного рішення, побудованому на основі запропонованого у другому розділі алгоритму частково гомоморфного шифрування. У цьому ж розділі запропоновано алгоритм кодування та декодування чисел точками еліптичної кривої. Також, здобувачем розроблено програмні засоби, які дають можливість визначити швидкість виконання операцій гомоморфного додавання та виконано порівняння розробленого алгоритму з аналогічним.

Четвертий розділ дисертаційної роботи присвячений проведенню експериментальних досліджень запропонованої інформаційної технології при розв'язанні прикладних задач. Представлено підхід до створення комп'ютерної системи електронного голосування, комп'ютерної системи накопичення та обробки відгуків мобільного додатку, та систему обміну електронними грошима. Зроблено порівняльний аналіз результатів розв'язання розглянутих прикладних задач за допомогою запропонованого та існуючих методів частково гомоморфного шифрування. У даному розділі також описано розроблене програмне забезпечення, що реалізує функції шифрування та розшифрування.

Наукова новизна дисертаційної роботи. В результаті виконаних теоретичних і експериментальних досліджень, які в сукупності формують поставлену в дисертаційній роботі науково-прикладну задачу, вирішені і, зокрема, отримані наступні нові найбільш суттєві наукові результати:

– запропоновану математичну модель взаємодії компонентів комп'ютерної системи, яка на відміну від існуючих, використовує метод частково гомоморфного шифрування на основі еліптичних кривих, що дозволяє захистити інформацію користувача від несанкціонованого доступу до неї зі сторони провайдера хмарного сервісу, враховуючи необхідність її обробки.

– запропонований метод частково гомоморфного шифрування відносно операції додавання, що на відміну від існуючих аналогів використовує математичний апарат еліптичних кривих, який, при однаковій криптографічній

стійкості запропонованого алгоритму, робить його швидшим, ніж аналогічні алгоритми відносно часу виконання однакової кількості операцій гомоморфного додавання за секунду, а його довжину ключа – меншою.

– запропоновано метод кодування чисел точками еліптичної кривої з попередньою побудовою таблиці відповідності, що, на відміну від існуючих аналогів, включає етап попередньої генерації точок еліптичної кривої, який дозволяє виконувати операцію декодування числа при відомому його максимальному розмірі.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується коректним використанням відповідного математичного апарату і підтверджується співставленням з результатами експериментальних досліджень. Достовірність отриманих результатів також підтверджується їх успішним використанням у ТОВ «СКАЙСОФТТЕК» для збору анонімних відгуків та параметрів використання мобільного додатку, про що свідчить акт впровадження, наведений у додатку А.

Практична цінність роботи полягає у розробці програмного забезпечення, яке дозволяє розв'язувати прикладні задачі захисту приватної інформації користувачів комп'ютерної системи. З використанням цього програмного забезпечення, було розв'язано три прикладні задачі: 1) захист приватної інформації користувачів комп'ютерної системи електронного голосування; 2) захист інформації користувачів комп'ютерної системи «Liquidity» ТОВ «СКАЙСОФТТЕК»; 3) захист інформації користувачів комп'ютерної системи обміну електронними грошима.

Впровадження результатів роботи підтверджено відповідним актом.

Апробація результатів роботи та публікації.

Апробацію результатів роботи здійснено на 7 науково-технічних конференціях. За результатами дослідження опубліковано 14 наукових праць, серед яких 1 стаття у журналі, що входить до наукометричної бази Scopus, 4 статті у фахових журналах з переліку ВАК України, 7 робіт у матеріалах і тезах доповідей конференцій та 2 статі у виданнях, що не входять до переліку фахових. Основні публікації достатньо повно відображають зміст роботи.

Відповідність автореферату дисертації. Зміст автореферату є ідентичним до змісту дисертації й повною мірою відображає основні завдання, наукову новизну, практичне значення, висвітлює всі отримані результати, висновки та запропоновані рекомендації.

Зауваження по роботі:

1. В другому розділі доцільно було б навести схему з основними етапами формування спільного симетричного ключа для представленого алгоритму гібридного шифрування.
2. У другому розділі присутні звісні дані, що доцільно було б навести у першому розділі. Наприклад формули 2.7, 2.8, 2.9 доцільно перенести у перший розділ, лишивши посилання на них у пункті 2.2.
3. Під час визначення криптографічної стійкості представленого алгоритму гомоморфного шифрування припущення про зменшення стійкості на кількість операцій додавання є недостатньо обґрунтованим.
4. При визначенні коефіцієнта порівняння було б доцільно включити показники криптографічної стійкості – це б дозволило уникнути етапу попереднього порівняння алгоритмів по цьому показнику, а також порівнювати алгоритми з різною криптографічною стійкістю.
5. На рисунку 3.1 рівноправні компоненти системи показані різними елементами UML діаграми. Так, хмарний сервіс показано як систему, хоча,

було б доцільним виділення його, як окремого актора.

6. У третьому розділі було б доцільним додати опис до змінних використаних у блок-схемах на рисунках 3.3, 3.4, 3.8, 3.11 та співвіднести їх з відповідним формулами у розділі 2.

7. У тексті дисертації зустрічаються допущені автором термінологічні розбіжності. Так в назві дисертаційної роботи автор декларує за мету захист персональної інформації користувачів, у меті роботи що наведена у вступі, автор ставить завдання підвищення ефективності захисту інформації в комп`ютерних системах, предметом розробки автор пропонує розглядати методи та засоби побудови системи для реалізації анонімності користувачів, а в самій роботі автор вводить поняття «деперсоналізація». При цьому пояснень розбіжності цих термінів не надається. Крім цього автор допускає деякі термінологічні неточності, наприклад на рис. 3.1. невдало наведено термін «дешифрування» (потрібно було «розшифрування»).

Відзначені зауваження не ставлять під сумнів основні наукові та практичні результати, і суттєво не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок.

Дисертаційна робота Титарчука Є. О. представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково обґрунтовані результати, які дозволяють розвинути наукові методики та моделі, що застосовуються при захисті приватної інформації користувачів комп'ютерних систем.

Вважаю, що кандидатська дисертація Титарчука Є. О. за актуальністю теми, ступенем обґрунтованості наукових положень, рівнем апробації та публікацій, науковою новизною та практичною цінністю отриманих результатів відповідає вимогам, що висуваються до кандидатських дисертацій згідно п. 9, 11, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а сам автор заслуговує

на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – "Комп'ютерні системи та компоненти".

Офіційний опонент,
завідувач кафедри обчислювальної техніки
та програмування
Національний технічний університет
«Харківський політехнічний інститут»,
доктор технічних наук, старший науковий співробітник С. Г. Семенов