Вінницький національний технічний університет
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах
рукопису

ТИТАРЧУК ЄВГЕНІЙ ОЛЕКСАНДРОВИЧ

УДК 004.056.55

ДИСЕРТАЦІЯ
ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ СИСТЕМ ПРИ ВИКОРИСТАННІ ПУБЛІЧНИХ ХМАРНИХ СЕРВІСІВ

05.13.05 – комп’ютерні системи та компоненти
Технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____Є. О. Титарчук

Науковий керівник:
Квєтний Роман Наумович
доктор технічних наук, професор

Вінниця – 2018

АНОТАЦІЯ

Титарчук Є. О. Захист персональної інформації користувачів комп'ютерних систем при використанні публічних хмарних сервісів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Вінницький національний технічний університет. – Вінниця, 2018.

У дисертаційній роботі поставлена та вирішена актуальна задача захисту персональної інформації користувачів комп'ютерної системи, одним із компонентів якої є публічний хмарний сервіс, шляхом удосконалення моделі взаємодії компонентів комп'ютерної системи.

Наукова новизна одержаних результатів і положень, що виносяться на захист, полягає в подальшому розвитку теоретичних засад побудови захищених інформаційних систем, що виконують обчислення у публічних хмарних сервісах, які дозволили знизити ризик втрати персональної інформації користувачів даних інформаційних систем.

В роботі отримано такі наукові результати:

1. Запропоновано та розроблено нову математичну модель сервісу деперсоналізації користувачів, 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.

2. Запропоновано новий 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 (141.4 оп/с проти

119 оп/с алгоритму Пейє), а його довжину ключа – меншою (256 біт проти 2048 біт алгоритму Пейє)

3. Запропоновано метод кодування чисел точками еліптичної кривої з попередньою побудовою таблиці відповідності, що на відміну від існуючих аналогів включає етап попередньої генерації n-точок еліптичної кривої (де n – максимальне число, яке необхідно декодувати), що дозволяє виконувати операцію декодування числа, при відомому його максимальному розмірі.

Практичне значення одержаних результатів роботи полягає у створенні, на основі розроблених моделей та методів, алгоритмічного та програмного забезпечення інформаційної системи забезпечення анонімності користувачів з використанням частково гомоморфного шифрування на еліптичних кривих.

Обґрунтовано метод захисту інформації користувачів, в основу якого покладено перетворення моделі виконання обчислень у комп'ютерній системі та використання алгоритмів частково гомоморфного шифрування. Пропонується використання частково гомоморфного алгоритму шифрування на основі еліптичних кривих, що гомоморфний відносно операції додавання. Процес побудови захищеної комп'ютерної системи полягає у перенесенні ресурсовитратних задач, що складаються з послідовності операцій арифметичного додавання, у публічний хмарний сервіс з подальшим використанням алгоритму частково гомоморфного шифрування.

В якості алгоритму частково гомоморфного шифрування пропонується модифікований алгоритм шифрування на основі еліптичних кривих. Модифікація процесу шифрування та розшифрування точок еліптичної кривої надає алгоритму гомоморфних ознак відносно операції додавання.

Проведено аналіз криптографічної стійкості представленого алгоритму шляхом порівняння з не модифікованим алгоритмом шифрування на еліптичних кривих. Через те, що при виконання операцій гомоморфного

додавання, результуюча точка пов’язана з початковим приватним ключем шифрування, криптографічна стійкість запропонованого алгоритму нижча відносно початкової на кількість виконаних операцій додавання (при виражена стійкості у кількості операцій, що необхідна для розкриття приватного ключа шифрування).

Розроблено програмні засоби, які дають можливість визначити швидкість виконання операцій гомоморфного додавання та необхідну кількість тактів процесору комп`ютерної системи для програмної реалізації запропонованого методу та аналогічного алгоритму частково гомоморфного відносно операції додавання алгоритму Пейє.

Для перевірки швидкодії представленого алгоритму розроблено програмне забезпечення на мові програмування C#. Порівняння з відомим алгоритмом частково гомоморфного шифрування – Пейє показало перевагу представленого алгоритму у швидкості виконання операцій гомоморфного додавання при співвідносній по криптографічній стійкості довжині ключа шифрування. Загальний час виконання операції шифрування, 100 операцій гомоморфного додавання та операції розшифрування представленого алгоритму на 38% менший ніж у алгоритму Пейє.

До недоліків слід віднести необхідність попередньої генерації точок еліптичної кривої у області можливої суми доданків. У даному розділі було проаналізовано час генерації кількості точок, достатньої для кодування довільного цілого чотирьох байтного числа. Також було проаналізовано обсяг пам’яті, необхідний для збереження необхідної кількості точок.

Розроблено метод кодування та декодування чисел точками еліптичної кривої, що дозволяє виконувати математичні розрахунки з зашифрованими числами розміром до 4х байт. Представлений метод включає в себе етап генерації точок методом фіксованої точки застосованого відносно числа, що необхідно закодувати, та формування хеш-таблиці ключем якої є значення хеш функції з координат точки, а значеннями список точок та чисел, які вини кодують. Інформація необхідної для декодування може бути

представлена двома файлами – файлом з ключами хеш-таблиці, та файлом, що містить точки еліптичної кривої. Обсяг файлів складає 36 Гб та 256 Гб відповідно.

Представлено метод генерації спільного ключа симетричного алгоритму шифрування на основі еліптичних кривих, що може бути використаний у комп'ютерній системі, що складається з декількох компонентів, кожен з яких має доступ до єдиного хмарного сховища даних. Особливістю методу є можливість формування симетричного ключа шифрування для групи компонентів комп'ютерної системи, що запобігає необхідності у повторному шифруванні інформації для кожного окремого компоненту.

Представлено методику захисту комп'ютерних систем та мереж з використанням системи деперсоналізації користувачів на основі частково гомоморфного алгоритму шифрування, що полягає у перетворенні моделі обчислень комп'ютерної системи з винесенням ресурсовитратних операцій у публічний хмарний сервіс, який оперує лише зашифрованими даними.

На основі запропонованих алгоритмів та моделей розроблено програмний модуль, що реалізує схему частково гомоморфного шифрування відносно операції додавання на основі еліптичних кривих.

Реалізовано програмне забезпечення, що реалізує ядро системи деперсоналізації користувачів при використанні інформаційної системи, що виконує обчислення на стороні хмарного сервісу публічного типу.

Представлено підхід до створення комп'ютерної системи електронного голосування з використанням частково гомоморфного алгоритму шифрування для захисту принципів таємності вибору учасників. Наведено приклад роботи математичної моделі системи та час виконання затратної операції генерації таблиці кодування цілих чисел точками еліптичної кривої. Перевагою даного підходу є неможливість відслідковування вибору користувачів на стороні хмарного сервісу навіть після завершення голосування та розкриття кількості виборів кожного окремого варіанту.

Таким чином, на відміну від існуючих аналогів, інформація про вибір окремої людини є недосяжною не тільки для сторонніх осіб, а і для власників обчислювальних ресурсів на яких працює система.

Було розроблено та впроваджено інформаційно захищену комп’ютерну систему для створення відгуків для мобільного додатку. Перевагою даної системи над існуючими аналогами є неможливість доступу до приватної інформації користувачів та загальної статистичної інформації додатку. У ході роботи було виконано експериментальне дослідження, результати якого показали перевагу у швидкодії запропонованого алгоритму шифрування над існуючими аналогами.

Результати проведених досліджень впроваджено в інтелектуальні програмні засоби забезпечення анонімності на основі алгоритму частково гомоморфного шифрування користувачів комп’ютерної системи «Liquidity» ТОВ "СКАЙСОФТТЕК" (Код реєстрації 40524859, м. Вінниця) для збору анонімних відгуків та параметрів використання мобільного додатку. Акт впровадження №5 від 14 грудня 2017 року.

Ключові слова: публічний хмарний сервіс, частково гомоморфне шифрування, еліптична крива, гібридне шифрування, кодування чисел точками еліптичної кривої.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Сучасні технології комп`ютерних систем і мереж дають розвиток великій кількості нових інформаційних сервісів та служб. Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури, привели до значного розвитку хмарних сервісів, що дають можливість користувачам виконувати обчислення та зберігати дані на віддалених інтернет-серверах. Захист інформації від несанкціонованого доступу – одна з головних задач по забезпеченню конфіденційності, цілісності та автентичності даних, що передаються.

В останні роки, «хмарні» сервіси стають одним з основних компонентів сучасних комп’ютерних систем. Проте, при їх використанні, конфіденційна інформація стає доступною третій стороні – провайдеру хмарного рішення, адже такі сервіси оперують приватною інформацією користувачів комп’ютерної системи.[1]

Хмарні обчислення – це модель забезпечення зручного доступу на вимогу через мережу до розподіленого стеку обчислювальних ресурсів (мереж, серверів, місць для зберігання, додатків та сервісів), які можуть бути налаштовані, оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера. [2]

Економічна сторона використання хмарних сервісів добре відома. Завдяки своєму досвіду, провайдери хмарних сервісів можуть побудувати великі дата центри з відносно низькою собівартістю, а використання віртуалізації дозволяє оптимально розподілити навантаження на розгорнутому обладнанні. Цим досягається збільшення доходів постачальників обчислювальних ресурсів та зниження витрат для їх користувачів. Результуюча модель обчислень на вимогу дозволяє

провайдерам хмарних рішень досягти кращого використання ресурсів за допомогою статистичного мультиплексування, а також дозволяє користувачам уникати витрат на перевищення ресурсів за рахунок динамічного масштабування [3].

Сучасні комп’ютерні системи все частіше містять у своєму складі відразу декілька компонентів представлених публічними чи приватними хмарними сервісами. Використання компонентів, що представлені сторонніми хмарними сервісами, дозволяє значно спростити розробку комп’ютерної системи та покращити її характеристики за рахунок гнучкого масштабування обчислювальних ресурсів, збору статистики використання, вибір місця фізичного розташування серверів, тощо. [1], [2]

Проте в цьому проявляється головний недолік хмарних сервісів – приватна інформація користувача фактично стає доступна третій стороні – провайдеру, крім цього, данні можуть стати вразливими під час їх передачі каналами зв'язку, обробці та зберіганні. [4]

Одним з основних засобів для забезпечення захисту інформації, при використанні таких служб, є криптографічні алгоритми. Вони призначені для захисту прикладного рівня каналів комп`ютерних мереж. Класи криптографічних алгоритмів і крипто аналітичних атак наведені в літературі [5].

Проте, існуючі методи захисту інформації не враховують специфіки використання хмарних сервісів, а саме необхідності виконання додаткових обчислень на даними, що до них передаються.

Тому, останнім часом, все більше зростає потреба в системах, які здатні не лише виконувати обчислення чи зберігати дані у хмарних сервісах, але й забезпечувати належний інформаційний захист приватної інформації користувачів. Одним з таких методів захисту може стати використання різноманітних схем гомоморфного шифрування у складі програмних засобів, що виконують обчислення на стороні хмарного сервісу.

Повністю гомоморфне шифрування (FHE) – це така схема шифрування, яка дозволяє виконувати арифметичні операції над зашифрованим текстом, без використання ключа шифрування. Очевидно, що, така алгебраїчна схема дозволяє виконувати будь-які операції над вхідними бітами публічно. Цей потужний математичний апарат став темою активних досліджень протягом останніх п’яти років.

Задачам забезпечення інформаційної безпеки хмарних сервісів комп’ютерних обчислень, а також засобам захисту приватної інформації користувачів, зокрема, застосуванню гомоморфного шифрування, приділена велика увага в роботах Дж. Риза [6], П. Фингара [7], В. Романченко [8], Крейга Джентрі [9], [10]

Не дивлячись на значну кількість серйозних наукових досліджень, теоретичних робіт і численних публікацій, задача захисту приватної інформації користувачів на сучасному етапі розвитку науково-дослідної бази стосується в основному проблем захисту від доступу до конфіденційної інформації з боку осіб, що є сторонніми до обчислювального процесу, чи її зберігання. Проте, залишається недослідженим механізм захисту інформації користувачів від неправомірного доступу до неї зі сторони провайдеру хмарного сервісу, а саме, не виявлені особливості застосування гібридної криптографії для захисту інформації під час її зберігання у хмарному сховищі, і, особливо, захист інформації під час виконання обчислень на стороні хмарного сервісу. Більшість сучасних хмарних сервісів створені саме для обробки інформації. Можливим універсальним рішенням задачі могло б стати саме гомоморфне шифрування, проте його надзвичайно низька продуктивність обмежує можливість застосування таких систем [11], [12]. Таким чином, наразі не існує універсальних та досконалих підходів до захисту інформації під час виконання обчислень над даними на боці хмарного сервісу.

Тому, є актуальною не тільки задача аналізу недоліків існуючих інформаційних систем та побудови нових, що організовують обчислення у

публічному хмарному сервісі, але й створення нових методів шифрування, що дозволять реалізувати захист даних при виконанні обчислень у таких сервісах з високою ефективністю.

Зв'язок роботи з науковими програмами, планами, темами. 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 складають наукові дослідження, що були проведені на кафедрі автоматики та інформаційно-вимірювальної техніки Вінницького національного технічного університету в 2012-2017 роках.

Мета і завдання дослідження. Метою роботи є підвищення ефективності захисту інформації в комп`ютерних системах, що використовують у своєму складі публічні хмарні сервіси, на основі розробки та впровадження нових методів і засобів шифрування.

Основними задачами дослідження є:

1. Аналіз задач пов'язаних з використанням публічних хмарних технологій у складі комп'ютерної системи: огляд існуючих моделей та стратегій розгортання хмарних сервісів; аналіз сучасних методів захисту інформації, під час її передавання, зберігання та оброблювання у публічному хмарному сервісі.

2. Розроблення методу захисту інформації користувачів у комп'ютерній системі, що містить у своєму складі публічні хмарні сервіси комп'ютерних обчислень, на основі частково гомоморфного алгоритму шифрування.

3. Визначення критерію ефективності методу частково гомоморфного шифрування, що орієнтований на використання у складі комп'ютерної системи, один або декілька компонентів якої представлені публічними хмарними сервісами.

4. Розроблення теоретично обґрунтованої модифікації методу криптографії на основі еліптичних кривих з метою надання їй гомоморфних властивостей відносно операції додавання.

5. Розроблення математичної моделі комп’ютерної системи з обмеженням доступу до інформації, що в ній обробляється, зі сторони провайдеру хмарного сервісу з використанням частково гомоморфного алгоритму шифрування на основі еліптичних кривих.

6. Реалізація розробленого алгоритму частково гомоморфного шифрування на основі еліптичних кривих з використанням обчислювальних потужностей технічних засобів.

7. Розроблення алгоритмічного забезпечення та програмного моделювального комплексу.

8. Забезпечення практичного впровадження результатів роботи.

Об'єктом дослідження є процес оброблення даних публічним хмарним сервісом у складі комп’ютерної системи.

Предметом дослідження є методи та засоби побудови системи для реалізації анонімності користувачів у хмарному сервісі комп’ютерних обчислень.

Методи дослідження. В роботі використано методи абстрактної алгебри для визначення точок еліптичної кривої, системного аналізу схем частково гомоморфного шифрування для визначення їх переваг та недоліків, комп’ютерне моделювання та експериментальне дослідження описуваних схем шифрування для аналізу та перевірки достовірності отриманих теоретичних результатів. Реалізації алгоритму частково гомоморфного шифрування виконувалося за допомогою середовища програмування Microsoft Visual Studio 2015. Оброблення експериментальних даних виконувалося за допомогою програми Microsoft Excel пакету MS Office.

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних засад побудови захищених інформаційних комп’ютерних систем, що виконують обчислення у публічних хмарних

сервісах, які дозволили знизити ризик втрати персональної інформації користувачів даних інформаційних систем.

− Запропоновано та розроблено нову 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.

− Запропоновано новий 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 (141.4 оп/с проти 119 оп/с алгоритму Пайє), а його довжину ключа – меншою (256 біт проти 2048 біт алгоритму Пайє)

− Запропоновано метод кодування чисел точками еліптичної кривої з попередньою побудовою таблиці відповідності, що на відміну від існуючих аналогів включає етап попередньої генерації n-точок еліптичної кривої (де n – максимальне число, яке необхідно декодувати), що дозволяє виконувати операцію декодування числа, при відомому його максимальному розмірі.

Практичне значення отриманих результатів. На основі розроблених моделей та методів створено алгоритмічне та програмне забезпечення інформаційної системи забезпечення анонімності користувачів з використанням частково гомоморфного шифрування на еліптичних кривих.

− Розроблено методику інформаційного захисту комп'ютерних систем, що використовують публічні хмарні сервіси, на основі алгоритму частково гомоморфного шифрування.

− На основі запропонованих алгоритмів та моделей розроблено програмний модуль, що реалізує схему частково гомоморфного шифрування відносно операції додавання на основі еліптичних кривих.

− Реалізовано програмне забезпечення, що реалізує ядро системи деперсоналізації користувачів при використанні інформаційної системи, що виконує обчислення на стороні хмарного сервісу публічного типу.

− Результати проведених досліджень впроваджено в інтелектуальні програмні засоби забезпечення анонімності на основі алгоритму частково гомоморфного шифрування користувачів комп'ютерної системи «Liquidity» ТОВ "СКАЙСОФТТЕК" (Код реєстрації 40524859, м.Вінниця) для збору анонімних відгуків та параметрів використання мобільного додатку. Акт впровадження №5 від 14 грудня 2017 року.

Особистий внесок здобувача у роботах, які виконані у співавторстві, полягає в наступному: [13] – виконано аналіз основних напрямів атак на публічний хмарний сервіс; [14] – розроблено алгоритм та програмний засіб, що його реалізує для шифрування інформації користувача, при використанні хмарного сервісу DropBox; [15] – розроблено математичну модель протоколу обміну ключами серед груп користувачів без використання центрального серверу; [16] – розроблено протокол взаємодії елементів системи голосування, що дозволяє інформаційно захистити персональні дані користувачів; [17] – розроблено математичну модель алгоритму шифрування на основі еліптичних кривих та модель деперсоналізації користувачів з використанням алгоритму частково гомоморфного шифрування на основі еліптичних кривих; [18] – проведено аналіз криптографічної стійкості алгоритму частково гомоморфного шифрування на еліптичних кривих; [19] – розроблено протокол взаємодії елементів фінансової системи, що дозволяє захистити персональні дані користувачів.

Апробація матеріалів дисертації. Основні результати та положення дисертаційної роботи доповідались та обговорювались на міжнародних наукових конференціях [20]–[26]:

– Всеукраїнському конкурсі наукових робіт з напрямку «Інформатика та кібернетика», де робота була нагороджена дипломом переможця ІІІ ступеня;
– XLI, XLII, XLIII, XLIV регіональні науково-технічні конференції професорсько-викладацького складу, співробітників та студентів ВНТУ з участю працівників науково-дослідних організацій та інженерно-технічних працівників підприємств м. Вінниці та області. – м. Вінниця, 2013, 2014, 2015, 2016;
– І Міжнародна конференція Infocom Advanced Solution 2015 присвячена 70-річчю кафедри автоматики та управління в технічних системах НТУУ "КПІ". – м. Київ, 2015
– Міжнародна науково-практична Інтернет-конференція. Наукові дослідження і їх практичне застосування. Сучасний стан та шляхи розвитку;
– ІХ Міжнародна науково-практична конференція «Інтернет-Освіта-Наука. ІОН2014». – м. Вінниця, 2014;
– XII Міжнародна конференція «Контроль і управління в складних системах. КУСС 2014». – м. Вінниця, 2014;
– XIII міжнародна конференція «Контроль і управління в складних системах. КУСС-2016». – м. Вінниця, 2016;
– IV Міжнародна наукова конференція «Вимірювання, контроль та діагностика в технічних системах». – м. Вінниця, 2017;

Публікації. За результатами виконаних досліджень опубліковано 14 наукових праць: 4 статті [15], [16], [18], [19] у виданнях, що входять до переліку фахових видань України, 1 стаття у журналі, що входить до науко метричної бази Scopus [17], 2 статі у інших виданнях, що не входять до переліку ВАК [13], [14], 7 тез доповідей.

1. **Структура та обсяг дисертації.** Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Робота містить 108 сторінок основного друкованого тексту, 29 рисунків, 9 таблиць, список використаних джерел із 110 найменувань та сім додатків. Загальний обсяг роботи – 160 сторінки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Y. Jadeja і K. Modi, «Cloud computing - Concepts, architecture and challenges», *2012 Int. Conf. Comput. Electron. Electr. Technol. ICCEET 2012*, no November, pp 877–880, 2012.

[2] P. Mell і T. Grance, «The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology», *Natl. Inst. Stand. Technol. Inf. Technol. Lab.*, vol 145, p 7, 2011.

[3] Y. Chen, V. Paxson, і R. H. Katz, «What's New About Cloud Computing Security?», *Electr. Eng. Comput. Sci. Univ. Calif. Berkeley*, vol 20, no 2010, pp 1–8, 2010.

[4] D. Hubbard і M. Sutton, «Top Threats to Cloud Computing», *Cloud Secur. Alliance*, no March, pp 1–14, 2010.

[5] Н. Фергюсон і Б. Шнайер, «Практическая криптография.pdf». Диалектика, М., p 420, 2005.

[6] G. Reese, *Cloud Application Architectures*, 1st ed, no 1. Sebastopol, CA, 2009.

[7] Питер Фингар, *Dot.Cloud: облачные вычисления – бизнес-платформа XXI века*. М.: Аквамариновая Книга, 2011.

[8] В. Романченко, *Облачные вычисления на каждый день*. М.: Вільямс, 2009.

[9] Craig Gentry, «Fully homomorphic encryption using ideal lattices», *STOC*, pp 169–178, 2009.

[10] Craig Gentry, A. Sahai, і B. Waters, «Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based», *Adv. Cryptol.*, vol 8042, p 18, 2013.

[11] M. Tebaa, S. El Hajji, a El Ghazi, S. El Hajji, і A. El Ghazi, «Homomorphic Encryption Applied to the Cloud Computing Security», *Proc. World Congr. Eng.*, vol 1, pp 4–6, 2012.

[12] M. Naehrig, «Can homomorphic encryption be practical?», *ACM Comput.*

Commun. Secur., pp 113–124, 2011.

[13] Є. О. Титарчук, «Захист даних в хмарних технологіях комп'ютерних обчислень», *Придніпровський науковий вісник*, vol 5, no 152, pp 77–82, 2014.

[14] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридної криптографії в хмарних технологіях комп'ютерних обчислень», *Сборник научных трудов Sworld*, no 3, pp 63–67, 2014.

[15] Р. Н. Квєтний, Є. О. Титарчук, і А. А. Гуржій, «Метод та алгоритм обміну ключами серед груп користувачів на основі асиметричних шифрів ECC та RSA», *Інформаційні технології та комп'ютерна інженерія*, vol 3, no 37, pp 38–44, 2016.

[16] Р. Н. Квєтний і Є. О. Титарчук, «Використання частково гомоморфного алгоритму шифрування на еліптичних кривих у хмарній системі електронного голосування», *Оптико-електронні інформаційно-енергетичні технології*, vol 32, no 2, pp 14–22, 2016.

[17] R. N. Kvyetnyy, E. A. Titarchuk, O. N. Romanyuk, K. Gromaszek, і N. Mussabekov, «Usage of the hybrid encryption in a cloud instant messages exchange system», *Photonics Appl. Astron. Commun. Ind. High-Energy Phys. Exp.*, no 10031, p 8, 2016.

[18] Р. Н. Квєтний і Є. О. Титарчук, «Аналіз криптостійкості частково гомоморфного алгоритму шифрування на основі еліптичних кривих», *Інформаційні технології та комп'ютерна інженерія*, vol 1, no 38, pp 83–87, 2017.

[19] Р. Н. Квєтний і Є. О. Титарчук, «Хмарна система обміну електронними грошима на основі алгоритму частково гомоморфного шифрування», *Інформаційні технології та комп'ютерна інженерія*, vol 2, 2017.

[20] Є. О. Титарчук, «Захист даних в хмарних технологіях комп'ютерних обчислень», в *XLII регіональна науково-технічна конференція професорсько-викладацького складу, співробітників та студентів університету з участю працівників науково-дослідних організацій та*

інженерно-технічних працівників підприємств м. Вінниці та області, 2013, p 8.

[21] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридної криптографії в хмарних технологіях комп'ютерних обчислень», в *Міжнародна науково-практична Інтернет-конференція. Наукові дослідження і їх практичне застосування. Сучасний стан та шляхи розвитку '2014*, 2014, p 5.

[22] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридного шифрування в хмарних технологіях комп'ютерних обчислень», в *IX Міжнародна науково-практична конференція ІОН2014*, 2014, p 2.

[23] Р. Н. Квєтний і Є. О. Титарчук, «Захист даних в хмарних технологіях комп'ютерних обчислень», в *XII Міжнародна конференція. Контроль і управління в складних системах. КУСС 2014*, 2014, p 2.

[24] Р. Н. Квєтний і Є. О. Титарчук, «Використання гібридного шифрування в хмарній системі обміну миттєвими повідомленнями», в *InfoCom 2015: Матеріали 1-ї Міжнародної конференції присвяченої 70-річчю кафедри автоматики та управління в технічних системах*, 2015, p 2.

[25] Р. Н. Квєтний і Є. О. Титарчук, «Алгоритм частково гомоморфного шифрування на основі еліптичних кривих», в *XIII міжнародна конференція «Контроль і управління в складних системах (КУСС-2016)»*, 2016, p 2.

[26] Р. Н. Квєтний і Є. О. Титарчук, «Хмарна система обміну електронними грошима на основі алгоритму частково гомоморфного шифрування», в *Вимірювання, контроль та діагностика в технічних системах (ВКДТС-2017)*, 2017, p 2.

[27] Д. Мутур і В. А. Бхат, «Virtual computing lab», *IBM Dev.*, p 14, 2011.

[28] C. Hewitt, «ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing», *IEEE Internet Comput.*, vol 12, no 5, 2008.

[29] L. Columbus, «Roundup Of Cloud Computing Forecasts And Market

Estimates». [Online]. Available at: https://www.forbes.com/sites/louiscolumbus/2016/03/13/roundup-of-cloud-computing-forecasts-and-market-estimates-2016/#145e3a712187. [Accessed: 16-Жов-2017].

[30] «Dropbox», *Official site*. [Online]. Available at: https://www.dropbox.com/. [Accessed: 03-Лют-2018].

[31] «Google Drive», *Official site*. [Online]. Available at: https://www.google.com/drive/. [Accessed: 03-Лют-2018].

[32] Microsoft, «Office 365», *Official site*. [Online]. Available at: https://www.office.com/.

[33] «UniSender», *Official site*. [Online]. Available at: https://www.unisender.com/. [Accessed: 03-Лют-2018].

[34] «Twilio», *Official site*. [Online]. Available at: https://www.twilio.com/. [Accessed: 03-Лют-2018].

[35] «SalesForce», *Official site*. [Online]. Available at: https://www.salesforce.com. [Accessed: 02-Бер-2018].

[36] «Azure Portal», *Official site*. [Online]. Available at: https://portal.azure.com/. [Accessed: 02-Бер-2018].

[37] «Google App Engine», *Official site*. [Online]. Available at: https://cloud.google.com/appengine/. [Accessed: 03-Лют-2018].

[38] «Heroku», *Official site*. [Online]. Available at: https://www.heroku.com/. [Accessed: 03-Лют-2018].

[39] «Azure Virtual Machines», *Official site*. [Online]. Available at: https://azure.microsoft.com/services/virtual-machines/. [Accessed: 03-Лют-2018].

[40] «Amazon Web Services», *Official site*. [Online]. Available at: https://aws.amazon.com/. [Accessed: 03-Лют-2018].

[41] Microsoft, «Cloud computing terms», 2015. [Online]. Available at: https://azure.microsoft.com/en-us/overview/cloud-computing-dictionary/. [Accessed: 02-Бер-2018].

[42] «Hyper-V Technology Overview», 2016. [Online]. Available at: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-technology-overview. [Accessed: 03-Лют-2018].

[43] OpenTok, «OpenTok Basics». [Online]. Available at: https://tokbox.com/developer/guides/basics/.

[44] *Про захист персональних даних*. 2010.

[45] *Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»*. Україна, 1995.

[46] L. Wei *et al.*, «Security and privacy for storage and computation in cloud computing», *Inf. Sci. (Ny).*, vol 258, pp 371–386, 2014.

[47] Wikipedia, «Zeus (malware)», 2017. [Online]. Available at: https://en.wikipedia.org/wiki/Zeus_(malware). [Accessed: 16-Жов-2017].

[48] J. Kincaid, «Google Confirms That It Fired Engineer For Breaking Internal Privacy Policies», 2010. [Online]. Available at: https://techcrunch.com/2010/09/14/google-engineer-spying-fired/. [Accessed: 16-Жов-2017].

[49] J. Kincaid, «This Is The Second Time A Google Engineer Has Been Fired For Accessing User Data», 2010. [Online]. Available at: https://techcrunch.com/2010/09/14/google-engineer-fired-security/. [Accessed: 16-Жов-2017].

[50] InfoWatch, «InfoWatch представила дайджест главных утечек 2017 года», 2017. [Online]. Available at: http://www.cnews.ru/news/line/2017-12-27_infowatch_predstavila_dajdzhest_glavnyh_utechek. [Accessed: 03-Лис-2018].

[51] «Apple: The leaked iPhone source code is outdated», 2018. [Online]. Available at: https://www.cnet.com/news/apple-calls-leaked-iphone-source-code-outdated/. [Accessed: 03-Лис-2018].

[52] M. Lipp *et al.*, «Meltdown», 2018.

[53] «Meltdown and Spectre attack», 2017. [Online]. Available at:

https://meltdownattack.com/. [Accessed: 03-Лют-2018].

[54] «Число утечек конфиденциальной информации из организаций увеличилось на 80% в 2016 году», 2017. [Online]. Available at: https://www.infowatch.ru/presscenter/news/17498. [Accessed: 03-Лис-2018].

[55] В. Столлингс, *Криптография и защита сетей: принципы и практика*. М.: Издательский дом «Вильямс», 2002.

[56] J. Hoffstein, J. Pipher, і J. H. Silverman, *An Introduction to Mathematical Cryptography*, vol XVI. San Francisco, CA, USA: Mathematics Department of San Francisco State University, 2008.

[57] J. Daemen і V. Rijmen, «The Design of Rijndael. AES: The Advanced Encryption Standard», *Springer – Berlin*, vol 234, pp 24 – 28, 2002.

[58] R. Cramer і V. Shoup, «Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack», *SIAM J. Comput.*, vol 33, no 1, pp 167–226, 2003.

[59] R. L. Rivest, A. Shamir, і L. Adleman, «A method for obtaining digital signatures and public-key cryptosystems», *Commun. ACM*, vol 21, no 2, pp 120–126, 1978.

[60] W. Diffie, W. Diffie, і M. E. Hellman, «New Directions in Cryptography», *IEEE Trans. Inf. Theory*, vol 22, no 6, pp 644–654, 1976.

[61] Т. Г. Білова, «Проблеми та перспективи використання методів гомоморфного шифрування в хмарних обчисленнях», *Розвиток радіотехнічного забезпечення, АСУ та зв'язку Повітряних Сил*, vol 3, no 24, pp 115–118, 2016.

[62] Б. Шнейер, *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*, 2nd ed. Москва: Диалектика, 2003.

[63] С. Коутинхо, *Введение в теорию чисел Алгоритм RSA.pdf*. Москва: Постмаркет, 2001.

[64] T. Elgamal, «A public key cryptosystem and a signature scheme based on discrete logarithms», *Inf. Theory, IEEE Trans.*, vol 31, no 4, pp 469–472,

1985.

[65] D. Hankerson, S. Vanstone, і A. Menezes, *Guide to elliptic curve cryptography*. New York: Springer-Verlag, 2004.

[66] I. Blake, G. Seroussi, і N. Smart, *Elliptic Curves in Cryptography*. Cambridge: Cambridge University Press, 1999.

[67] T. Volkhausen, «Paillier Cryptosystem: A Mathematical Introduction», *J. Cryptol.*, vol 3, 2006.

[68] C. Jost, H. Lam, A. Maximov, і B. Smeets, «Encryption performance improvements of the Paillier cryptosystem», *Retrieved Febr.*, vol 8, p 2016.

[69] N. Koblitz, A. Menezes, і S. Vanstone, «The State of Elliptic Curve Cryptography», *Des. Codes Cryptogr.*, vol 193, no 2, pp 173–193, 2000.

[70] P. Longa, «Accelerating the Scalar Multiplication on Elliptic Curve Cryptosystems over Prime Fields», *Master's Thesis, Univ. Ottawa, June*.

[71] А. Е. Жуков, «Легковесная криптография», *Вопросы кибербезопасности*, vol 2, no 10, p 10, 2015.

[72] А. Кочубинский, «Принципы построения криптографических алгоритмов на эллиптических кривых», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, vol 6, pp 55–63, 2003.

[73] A. W. Knapp, *Elliptic Curves*, 1st ed. Princeton: Princeton University.

[74] NIST, *Recommended elliptic curves for federal government use*, no July. Maryland, USA: National Institute of Standards and Technology, 1999.

[75] В. Ковтун, «Криптопреобразования в группах точек эллиптических кривых», *Сборник Лекций*, 2011.

[76] Клод Шенон, *Теория связи в секретных системах*. М.: Связь, 1978.

[77] Н. Коблиц, *Курс теории чисел и криптографии.pdf*. М.: Научное издательство «ТВП», 2001.

[78] M. Mathur, «Comparison between DES , 3DES , RC2 , RC6 , BLOWFISH and AES», *Proc. Natl. Conf. New Horizons IT*, pp 143–148, 2013.

[79] F. Callegati, W. Cerroni, і M. Ramilli, «Man-in-the-Middle Attack to the

HTTPS Protocol», *IEEE Secur. Priv.*, vol 7, no 1, pp 78–81, 2009.

[80] В. Лужецький і Ю. Яремчук, «Використання рекурентних послідовностей для розповсюдження секретних ключів», *Вимірювальна та обчислювальна техніка в технологічних процесах*, vol 2, pp 16–23, 1999.

[81] К. Шеннон, *Работы по теории информации и кибернетике*. Москва: Издательство иностранной литературы, 1963.

[82] L. Morris, «Analysis of Partially and Fully Homomorphic Encryption», *IEEE Trans. Dependable Secur. Comput.*, 2013.

[83] S. D. Galbraith і P. Gaudry, «Recent progress on the elliptic curve discrete logarithm problem», *Des. Codes, Cryptogr.*, vol 78, no 1, pp 51–72, 2016.

[84] В. Ю. Лёвин і В. А. Носов, «Анализ повышения криптографической сложности систем при переходе на эллиптические кривые», *Интеллектуальные системы. Теория и приложения (ранее Интеллектуальные системы по 2014, № 2, ISSN 2075-9460)*, vol 12, no 1–4, pp 253–270, 2008.

[85] R. P. Gallant, R. J. Lambert, і S. a Vanstone, «Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms», *Crypto 2001 - Lncs*, no d, pp 190–200, 2001.

[86] L. Chen, «Microservices: Architecting for Continuous Delivery and DevOps», *IEEE Int. Conf. Softw. Archit.*, no April, 2018.

[87] R. Schoof, «Counting Points on Elliptic Curves over Finite Fields», *J. Theor. des Nombres Bordeaux*, vol 7, no 1, pp 219–254, 1995.

[88] Н. Вирт, *Алгоритмы и структуры данных*. М.: Мир, 1989.

[89] Т. Кормен і Ч. Лейзерсон, *Алгоритмы. Построение и анализ*. Вильямс.

[90] В. А. Лужецький і А. О. Олексюк, «Метод швидкого хешування на основі еліптичних кривих», *Інформаційні технології та комп'ютерна інженерія*, pp 156–157, 2013.

[91] T. Izu, B. Möller, і T. Takagi, «A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks», *Prog. Cryptology—INDOCRYPT*

2002, pp 296–313, 2002.

[92] Г. Тимур, «Под капотом у Stopwatch», 2014. [Online]. Available at: https://habrahabr.ru/post/226279/. [Accessed: 02-Бер-2018].

[93] MSDN, «Класс Stopwatch», 2016. [Online]. Available at: https://msdn.microsoft.com/ru-ru/library/system.diagnostics.stopwatch.

[94] Г. І. Шелудько, «Електронне голосування як різновид виборчих інформаційно - комунікативних технологій: зарубіжний та вітчизняний досвід», *Soc. Stud. Sci.*, pp 76–80, 2015.

[95] Wikipedia, «Електронне голосування». [Online]. Available at: http://uk.wikipedia.org/wiki/Електроннеголосування. [Accessed: 02-Бер-2018].

[96] R. Litan, «Law and Policy in the Age of the Internet», vol 50, no 4, pp 1045–1085, 2001.

[97] SwissInfo, «Hacking fears jeopardise e-voting rollout», 2016. [Online]. Available at: http://www.swissinfo.ch/directdemocracy/voting-with-a-click_hacking-fears-jeopardise-e-voting-rollout/41635672.

[98] SwissInfo, «Пряма демократія Швейцарії у цифрову еру», 2016. [Online]. Available at: http://www.swissinfo.ch/rus/detail/content.html?cid=36670692&link=cto. [Accessed: 25-Чер-2016].

[99] Wikipedia, «Elections in Brazil», 2012. [Online]. Available at: https://en.wikipedia.org/wiki/Elections_in_Brazil#The_Brazilian_voting_machines. [Accessed: 20-Чер-2016].

[100] D. Pons, R. Vallés, M. Abarca, і F. Rubio, «QR codes in use: the experience at the UPV Library», *Ser. J. Ser. Community*, vol 24, no 0, pp S47–S56, 2011.

[101] I. Ristić, *Bulletproof SSL and TLS*. London: Feisty Duck, 2015.

[102] S. A. Thomas і J. Wiley, «SSL and TLS Essentials - Securing the Web.pdf».

[103] O. N. Zdanov, *Methods and tools of cryptographic information protection*. Krasnoyarsk: SibHau, 2007.

[104] «Uservoice», *Official site*, 2017. [Online]. Available at: https://www.uservoice.com/product/. [Accessed: 05-Лют-2018].

[105] «HelpStack», *Official site*, 2017. [Online]. Available at: http://www.helpstack.io/. [Accessed: 05-Лют-2018].

[106] «Zendesk», *Official site*, 2017. [Online]. Available at: https://www.zendesk.com/. [Accessed: 05-Лют-2018].

[107] «SimpleFeedback», 2017. [Online]. Available at: http://www.simplefeedback.com/. [Accessed: 05-Лют-2018].

[108] «HappyFox», *Official site*, 2017. [Online]. Available at: https://www.happyfox.com/. [Accessed: 05-Лют-2018].

[109] «MPIR: Multiple Precision Integers and Rationals». [Online]. Available at: http://mpir.org/. [Accessed: 05-Вер-2018].

[110] J. Reynolds, «Mpir.NET». [Online]. Available at: http://wezeku.github.io/Mpir.NET/. [Accessed: 05-Вер-2018].

[111] «Paillier Library». .

[112] D. Chaum, «Blind Signatures for Untraceable Payments», *Advances in Cryptology*. University of California, Santa Barbara, pp 199–203, 1983.

[113] R. N. Kvyetnyy i E. A. Titarchuk, «Partially homomorphic encryption algorithm based on elliptic curves».