МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ДУТЧАК ІГОР ВАСИЛЬОВИЧ

УДК 004.75

МЕТОДИ ТА ЗАСОБИ ВСТАНОВЛЕННЯ ОСОБИСТИХ КЛЮЧІВ ШИФРУВАННЯ КОРИСТУВАЧІВ У ХМАРНОМУ СЕРЕДОВИЩІ

123 «Комп’ютерна інженерія»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2018

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, професор, професор кафедри комп'ютерних систем та мереж
Лупенко Сергій Анатолійович,
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: доктор фізико-математичних наук, професор, професор кафедри фізики
Дідух Леонід Дмитрович,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 20 лютого 2018 р. о $10^{.00}$ годині на засіданні екзаменаційної комісії №34 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 46, навчальний корпус №1, ауд.603

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Сучасні потреби та стан розвитку електронного цифрового світу, надання транскордонних електронних довірчих послуг та у цілому обробки інформації у інформаційно-телекомунікаційних системах різного призначення вимагає суттєвого підвищення швидкодії та здешевлення надання фізичним та юридичним особам різних послуг.

Забезпечення контролю та управління доступом клієнтів до ресурсів хмари, надання криптографічних послуг з захисту інформації для клієнтів в середовищі хмари, а також управління хмарною інфраструктурою провайдером хмарних послуг, вимагає створення сервісу з управління ключами. Головною проблемою сервісу управління ключами для клієнтів є його розгортання в інфраструктурі, що контролюється постачальником хмарних послуг. Тобто користувач хмарного сервісу потребує додаткових гарантій постачальника хмарних послуг, що розташовані в хмарі особисті чи таємні ключі не будуть скомпрометовані.

Результати роботи надають можливість підвищити рівень довіри до хмарних сервісів.

Мета і задачі дослідження. Метою є розробка моделей, методів і засобів забезпечення безпеки в хмарних обчисленнях в частині управління ключами для різних моделей розгортання хмари (приватна, публічна, громадська та гібридна) та на різних рівнях надання послуг (IaaS, PaaS, SaaS).

Для досягнення поставленої мети необхідно вирішувалися наступні часткові задачі:

- побудова та аналіз моделі загроз для різних варіантів розгортання хмари та управління ключами;
- побудова та аналіз складених механізмів управління ключами для кінцевих користувачів в середовищі хмари;
- обґрунтування вимог та побудова протоколів та засобів КЗІ для встановлення ключів при хмарних обчисленнях;
- програмне моделювання та експериментальні дослідження застосування ключів в хмарі.

Об'єкт досліджень – процеси безпечного управління ключовими даними користувачів хмарних сервісів для надання безпечних транскордонних електронних послуг: конфіденційності, цілісності, доступності, справжності, неспростовності в умовах протидії та постановки загроз зі сторони порушника 2 рівня.

Предмет досліджень – методи та механізми управління ключами користувачів хмарних сервісів в умовах різних моделей розгортання та надання послуг в хмарі.

Наукова новизна полягає в тому, що отримали подальший розвиток методи оцінки ефективності механізмів управління ключовими даними користувача в середовищі хмари, що дозволяє оцінити ефективність реалізації механізму та провести його оптимізацію за рахунок використання теорії систем масового обслуговування за такими показниками, як середній час відповіді, середній час

очікування обробки запиту, середня довжина черги запитів та середня кількість запитів в системі.

Практичне значення. Запропоновано метод оцінки та вибору механізму управління ключовими даними користувача в середовищі хмари на основі сукупності організаційних, правових, технічних вимог та вимог інформаційної безпеки, показників продуктивності, інтероперабельності, технічних та економічних показників. Запропонований метод дозволяє вирішити задачу вибору механізму управління ключами з використанням системного підходу.

Апробація результатів дипломної роботи. Окремі результати роботи доповідались на VI Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій», 16-17 листопада 2017 року(ТНТУ, Тернопіль, Україна);

V науково-технічна конференця «Інформаційні моделі, системи та технології» 1-2 лютого 2018 року (ТНТУ, Тернопіль, Україна).

Публікації. Дутчак І.В. Встановлення особистих ключів шифрування в хмарних середовищах. VI Міжнародна науково-технічна конференція молодих учених та студентів. Актуальні задачі сучасних технологій. 16-17 листопада 2017 р.: тези доп. - Тернопіль, 2017. – С.60-61;

Дутчак І.В. Встановлення ключів шифрування в хмарних середовищах. V науково-технічна конференція. Інформаційні моделі, системи та технології . 1-2 лютого 2018 р.: тези доп. Тернопіль, 2018. – С 67.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 6 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 124 арк. формату А4, графічна частина – 8 аркушів формату А1

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми, сформовані об’єкт, предмет, мета та задачі дослідження, описана наукова новизна та практичне значення отриманих результатів.

У першому розділі проведено аналіз стану досліджень в області забезпечення безпеки хмарних обчислень, складу, функціонального призначення компонентів моделі хмари визначеної в NIST SP 500-292, а також формальної моделі безпеки хмари визначеної в стандарті NIST SP 500-293.

У другому розділі обґрунтовано та розроблено модель загроз ключовим даним ІТС хмарних обчислень. Проводиться класифікація та аналіз основних моделей механізмів управління ключами.

У третьому розділі було проведено аналіз загроз та ефективності систем управління ключами ІТС хмарних обчислень. Відповідно до механізмів, що розглянуті в 3 розділі було визначено ймовірність несанкціонованого доступу до ключів, що зберігаються на захищеному носії ключів, в HSM та захищеному засобі ключів. Наведені результати дослідження основних технологій реалізації криптографічних бібліотек, що застосовуються для надання базових послуг з

захисту інформації користувачам в середовищі хмарних обчислень в моделі надання послуг SaaS за допомогою веб-браузера.

У четвертому розділі «Обгрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

У п'ятому розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання безпеки при роботі з комп'ютером та оглянуті фактори що впливають на стан користуваців ПК.

У шостому розділі «Екологія» проаналізовано енергозбереження і його ролоь у вирішення екологічних проблем і статистику екології об'єктів природного серидовища.

ВИСНОВКИ

Дослідження моделей, методів і засобів забезпечення безпеки в хмарних обчисленнях в частині управління ключами для різних моделей розгортання хмари (приватна, публічна, громадська та гібридна) та різних рівнях надання послуг (IaaS, PaaS, SaaS). Результати досліджень дали можливість проаналізувати існуючи механізми управління ключами користувача в хмарі, виконати їх порівняння за різними показниками та визначити перелік вимог до них. Запропонований механізм встановлення спільного особистого ключа користувача між модулями захисту, дозволяє виконати узгодження ключа без його передачі відкритими каналами зв'язку.

Удосконалено модель загроз хмарних обчислень, яка дозволяє оцінити ефективність засобів захисту та мінімізувати втрати за рахунок оцінки ризиків та використання методів оцінки ефективності. Запропонована модель відрізняється від моделі NIST SP 500-299 тим, що загрози розглядаються з використанням профілю порушника, мети, що досягається при реалізації загрози, та ймовірності виникнення загрози.

Отримали подальший розвиток методи оцінки ефективності механізмів управління ключовими даними користувача в середовищі хмари, що дозволяє оцінити ефективність реалізації механізму та провести його оптимізацію за рахунок використання теорії систем масового обслуговування за такими показниками, як середній час відповіді, середній час очікування обробки запиту, середня довжина черги запитів та середня кількість запитів в системі.

Запропоновано метод оцінки та вибору механізму управління ключовими даними користувача в середовищі хмари на основі сукупності організаційних, правових, технічних вимог та вимог інформаційної безпеки, показників продуктивності, інтероперабельності, технічних та економічних показників. Запропонований метод дозволяє вирішити задачу вибору механізму управління ключами з використанням системного підходу.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

Дутчак І.В. Встановлення особистих ключів шифрування в хмарних середовищах. VI Міжнародна науково-технічна конференція молодих учених та

студентів. Актуальні задачі сучасних технологій. 16-17 листопада 2017 р.: тези доп. - Тернопіль, 2017. – С.60-61;

Дутчак І.В. Встановлення ключів шифрування в хмарних середовищах. V науково-технічна конференція. Інформаційні моделі, системи та технології . 1-2 лютого 2018 р.: тези доп. Тернопіль, 2018. – С 67.

АНОТАЦІЯ

Дутчак І.В. Метод та засоби встановлення особистих ключів шифрування користувачів у хмарному середовищі.

В дипломній роботі запропонована модель загроз ключовим даним користувачів хмарних сервісів, що враховує об'єкти хмарного середовища, для якого реалізується загроза, мету реалізації загрози та її ймовірність. Запропоновано механізм генерації та встановлення загальної ключової пари між N-апаратними засобами захисту в хмарі, що дозволяє встановлювати ключі без передавання особистих ключів через недовірений канал зв'язку. Запропонована модель системи масового обслуговування для механізму управління ключовими даними в середовищі хмари, дозволяє оцінити ефективність реалізації механізму та провести його оптимізацію за такими показниками, як середній час відповіді, середній час очікування обробки запиту, середня довжина черги запитів та середня кількість запитів в системі. Розроблена практична реалізація кросплатформеної криптографічної бібліотеки для надання послуг з захисту інформації кінцевим користувачам в браузері з використанням мови програмування JavaScript.

Ключові слова: хмарні обчислення, механізми управління ключами, модель загроз, апаратні модулі захисту, системи масового обслуговування.

ANNOTATION

Dutchak I.V. Methods and means of user personal code keys setting in cloud environment

In the thesis proposed the user`s key data threat model for cloud services considering objects of the cloud environment for which threat, the purpose of realization of threat and its probability is realized is offered.

The mechanism of generation and installation the general key pair between N-hardware secure modules in the cloud is proposed. It allows to establish keys without transfer private keys through not entrusted communication channel by using a modified Diffie-Hellman algorithm.

For the mechanism of key management in the cloud environment in the thesis proposed the model of mass service system. It allows to estimate efficiency of realization of the mechanism and to perform its optimization on such indicators as average time of the answer, average time of expectation of processing of inquiry, average length of turn of inquiries and average amount of inquiries in system.

The method of assessment and selection mechanism for management of key user data among cloud-based set of organizational, legal, technical requirements and information security requirements, performance metrics, interoperability, technical and

economic indicators. The proposed method can solve the problem selection mechanism key management using a systematic approach.

Keywords: cloud computing, key management mechanisms, the threat model, hardware secure modules, queuing theory.