УДК 004.75
DOI: 10.15587/2313-8416.2016.72701

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ УПРАВЛІННЯ ОСОБИСТИМИ КЛЮЧАМИ КОРИСТУВАЧІВ В ХМАРІ

© І. Ф. Аулов

Наводяться результати порівняння та рекомендації з застосування існуючих механізмів з управління особистими ключами користувачів в хмарному середовищі. Запропоновано новий механізм генерації та встановлення єдиної ключової пари між N-засобами управління ключами в хмарі за рахунок використання модифікованого протоколу Діффі-Хелмана
Ключові слова: *механізми управління ключами, апаратні засоби захисту, хмара, протокол Діффі-Хелмана*

The results of comparison and recommendations on the use of existing user key management mechanisms in the cloud environment are given. New generation and installing mechanism of a private key pair between the N-means of key management in the cloud by using a modified Diffie-Hellman protocol is proposed
Keywords: *key management mechanisms, hardware protection, cloud, Diffie-Hellman protocol*

1. Вступ

Міжнародні та українські дослідження в області хмарних обчислень виявили ряд проблем, які стосуються надання користувачам послуг з безпеки інформації в першу чергу з управління ключами користувачів в хмарі [1, 2]. Зважаючи, що кабінетом міністрів України в 2013 році було прийнято розпорядження «Про схвалення Стратегії розвитку інформаційного суспільства в Україні», якою було передбачено створення та застосування суперкомп'ютерних систем, зокрема на основі «хмарних» технологій, а також законопроекту Верховної Ради України від 24 березня 2016 року «Закон про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень» для України є актуальним задача дослідження механізмів та засобів управління ключами користувача.

2. Аналіз літературних джерел та постановка проблеми

За тематикою побудування та аналізу механізмів управління ключами в хмарному середовищі існує ряд закордонних публікації, в яких розглядаються протоколи [3–5] моделі [6, 7], засоби та методи [8, 9] управління ключами в хмарному середовищі. В публікаціях [1, 3, 4] розглядаються питання безпеки ключів в хмарі, та їх життєвий цикл. Окрім цього існує ряд патентів, що визначають базові моделі механізмів управління ключами в хмарі.

Аналіз джерел показав, що найбільша увага приділяється побудові механізмів управління ключами в хмарному середовищі. В той же час запропоновані моделі управління ключовими даними користувачів не в повній мірі відповідають вимогам хмарного середовища та вимогам захисту ключів.

Окремо слід відзначити відсутність публікацій в області оцінки ефективності механізмів управління ключами.

3. Мета та задачі дослідження

Метою дослідження є вдосконалення механізмів управління ключами, та аналізу їх ефективності.

Для досягнення мети було вирішено наступні задачі:

– обрано та обґрунтовано методи аналізу, критерії та показники оцінки ефективності механізмів, визначенні обмежень до застосування цих методів;

– проведено аналіз існуючих механізмів з використанням системного підходу;

– запропоновано новий механізм встановлення особистих ключів в хмарному середовищі між N-вузлами в хмарі, який за рахунок вдосконалення протоколу Діффі-Хелмана дозволяє генерувати та встановлювати особисті ключі користувача за рахунок передачі тільки відкритих даних каналами зв'язку.

4. Аналіз існуючих моделей механізмів управління ключами

Під криптографічним механізмом захисту інформації будемо розуміти конкретний процес, метод, криптографічний протокол або криптографічний алгоритм, що використовується для реалізації певних послуг та/або функцій криптографічного захисту інформації та інформаційних ресурсів [10].

Аналіз закордонних публікацій [3–9] та патентів в області хмарних обчислень, а також проведені дослідження показали, що для управління ключами зі сторони користувача можна застосовувати 7 основних механізмів (Keys management mechanism, KMM):

– механізм управління ключами з використанням сертифікатів відкритих ключів (KMM-1);

– механізм управління ключами на основі паролів (KMM-2);

– механізм управління ключами з використанням апаратного модулю захисту (Hardware secure module, HSM) хмарного ЦОД (KMM-3);

– механізм управління ключами з використанням HSM користувача (KMM-4);

– механізм управління ключами з використанням криптографічного сервісу та захищеного сховища ключів (КММ-5);

– механізм управління ключами з використанням хмарного HSM та криптографічного сервісу (КММ-6);

– механізм управління ключами з використанням розподілених апаратних засобів захисту ключів (КММ-7).

В механізмах, що розглядаються, захищений канал між користувачем та хмарним ЦОД реалізується з використанням асиметричної пари ключів провайдера та, за наявності, користувача. Будемо також вважати, що він реалізується у відповідності до криптографічних протоколів згідно стандарту ISO\IEC 11770-3.

В якості результату аналізу механізмів управління ключами, наводиться табл. 1 з результатами порівняння.

Таблиця 1

Порівняння механізмів управління ключами

Характеристики механізму	Механізм 2 3 4 5 6 7						
	1	2	3	4	5	6	7
1. Попередні налаштування							
$(d_{Ksign}, Q_{Ksign,} Certifiacate_{Ksign})$	+	–	–	–	–	+	–
$(d_{Kkep}, Q_{Kkep}, Certifiacate_{Kkep})$	+	–	–	–	–	+	–
$(d_{Пsign}, Q_{Пsign,} Certifiacate_{Пsign})$	+	–	–	–	–	+	–
$(d_{Пkep}, Q_{Пkep}, Certifiacate_{Пkep})$	+	+	+	+	+	+	+
$(d_{HSMkep}, Q_{HSMkep}, Certifiacate_{HSMkep})$	–	–	+	+	–	+	+
2. Взаємодіючі сторони							
Хмарний ЦОД	+	+	+	+	+	+	+
Користувач	+	+	+	+	+	+	+
ЦСК	+	–	–	–	–	+	–
3. Елементи системи							
HSM	–	–	+	+	–	+	+
Захищене сховище ключів	–	–	–	–	+	–	–
4. Сервіси							
Реєстрації події	+\–	+\–	+\–	+\–	+	+	+
Криптографічний сервіс	–	–	–	–	+	+	+
Сервіс ідентифікації та автентифікації	+	+	+	+	+	+	+
Сервіс управління ключами	–	–	–	–	+	+	+
5. Функції управління ключами в хмарі							
реєстрація користувача в системі	+	+	+	+	+	+	+
генерація, розподіл та введення ключів до засобів захисту	–	+	+	–	+	+	+
контроль над використанням ключів	+	–	–	+	–	+\–	+\–
зміна та знищення ключів	+	–	–	+	–	+\–	+\–
архівування, зберігання та відновлення ключів	+	–	–	+	–	+\–	+\–
6. Модель розгортання хмари							
Приватна	+	+	+	+	+	+	+
Публічна	+	–	+	+	+\–	+	+
Гібридна	+	–	+	+	+\–	+	+
7. Модель надання послуг хмари							
IaaS	+\–	+	+	+\–	+	+	+
PaaS	+\–	+	+	+\–	+	+	+
SaaS	+	+	+	+	+	+	+
8. Вразливі елементи							
Носій особистого ключа	+	–	–	–	–	+	+
БД з ключами	–	+	–	–	–	–	–
HSM	–	–	+	+	–	+	+
Захищене сховище	–	–	–	–	+	+	+
Криптографічний сервіс	–	–	–	–	+	+	+
Сервіс управління	–	–	–	–	+	+	+
Сервіс ідентифікації та автентифікації	+	+	+	–	+	+	+

Аналіз табл. 1 дозволив визначити перелік вимог та обмежень до механізмів з управління ключами. Головними вимогами при синтезі механізму управління ключами в хмарі є реалізація функції з управління ключами безпосередньо в хмарі для забезпечення інтероперабельності з високим рівнем захисту. Високий ступінь захисту в хмарі може бути реалізований за рахунок використання спеціалізованого обладнання для зберігання або управління ключами. У випадках коли відсутня необхідність безпосередньо в хмарі реалізовувати обробку даних, найбільш оптимальною є механізм KMM-1.

5. Вибір механізмів управління ключами з використанням системного підходу

Порівняння механізмів, що виконують функції управління ключами користувачів в хмарному середовищу, пропонується за рахунок застосування системного підходу. Пропонується застосовувати 4 основні групи показників, за якими буде відбуватися порівняння механізмів, а саме продуктивності (ПП), технічні (ТП), інтероперабельності (ПІ), економічні (ЕП). До зазначених груп показників відносяться часткові показники, що зазначені в табл. 2.

Зведемо доступні характеристики криптографічних засобів, що застосовуються в хмарних рішеннях від Amazon, а саме носія особистого ключа SafeNet Smart Card 400, рішення з зберігання в базі даних та управління ключами SafeNet Virtual KeySecure, апаратного модуля захисту SafeNet Luna Network HSM 1700, захищеного сховища ключів SafeNet KeySecure k250, OpenSSL до табл. 3. Значення економічних показників обирається відповідно до вартості спеціалізованих криптографічних пристроїв та їх обслуговування.

Таблиця 2

Групи показників механізмів управління ключами

Група показника	Показник	Скорочення
Продуктивності	максимальна кількість сесій користувачів	ПП-1
	швидкість криптографічних операцій	ПП-2
	швидкість генерації ключів	ПП-3
Технічні	максимальна кількість ключів, що можуть зберігатися	ТП-1
	клас захищеності	ТП-2
	криптографічні алгоритми, що підтримуються	ТП-3
	сертифікати відповідності стандартам	ТП-4
	функції сервісу управління ключами	ТП-5
	функції криптографічного сервісу	ТП-6
Інтероперабельності	інтерфейси взаємодії, що підтримуються	ПІ-1
	операційні системи, що підтримуються	ПІ-2
	максимальна кількість розподілених вузлів	ПІ-3
	моделі розгортання хмари, що підтримуються	ПІ-4
	моделі надання послуг в хмарі, що	ПІ-5
	підтримка розподілених вузлів	ПІ-6
Економічні	вартість рішення	ЕП-1
	вартість супроводження	ЕП-2

Таблиця 3

Показники механізмів управління ключами

Показник	Механізми					
	1	2	3	4	5	7
1Показники продуктивності						
1.1 ПП-1	1	500	800	800	100	800
1.2 ПП-2, Підпис (RSA-2048), оп\с	0,45	450	350	350	250	350
1.3 ПП-3 (RSA-2048), с	90	10	20	20	30	20
2Технічні показники						
2.1 ТП-1	10	25000	2000	2000	25000	2000
2.2 ТП-2	3	1	3	3	1	3
2.3 ТП-3	5	24	24	24	11	24
2.4 ТП-4	2	1	6	6	2	6
2.5 ТП-5	-	-	-	-	+	+
2.6 ТП-6	-	-	-	-	+	+
3 Показники інтероперабельності						
3.1 ПІ-1	6	6	7	7	7	7
3.2 ПІ-2	3	3	11	11	11	11
3.3 ПІ-3	1	1	1	1	1	16
3.4 ПІ-4	3	2	3	3	1	3
3.5 ПІ-5	1	3	3	1	3	3
3.6 ПІ-6	–	–	–	–	–	+
4 Економічні показники						
4.1 ЕП-1, у. о.	10	1	5000	29500	1	10000
4.2 ЕП-2, у. о.\рік	1	4700	18576	10000	31700	37152

Так як механізм КММ-6 за обраними показниками відповідає механізму КММ-3, в табл. 3 механізм КММ-6 не включено.

5. 1. Вибір механізмів управління ключами з використанням методу аналізу ієрархій

За запропонованими критеріями та показниками у відповідності до методу аналізу ієрархій [11] побудуємо дерево цілей (рис. 1).

На першому рівні дерева знаходиться головна ціль – найбільш ефективний метод управління ключами. На другому – групи показників, на третьому – показники. На четвертому рівні будуть знаходитися альтернативи методів управління ключами з яких, за допомогою методу ієрархій, буде обрано найбільш ефективний.

Рівень значущості показника, визначався з залученням експертів, рівень узгодженості яких не перевищував 0.1, що означає що при заповненні матриці попарних порівнянь не було допущено грубих помилок.

В табл. 4 наведемо значення векторів вкладів за кожною групою показників, а також вектор вкладу критеріїв до головної цілі – вибору найбільш ефективного та якісного механізму управління ключами.

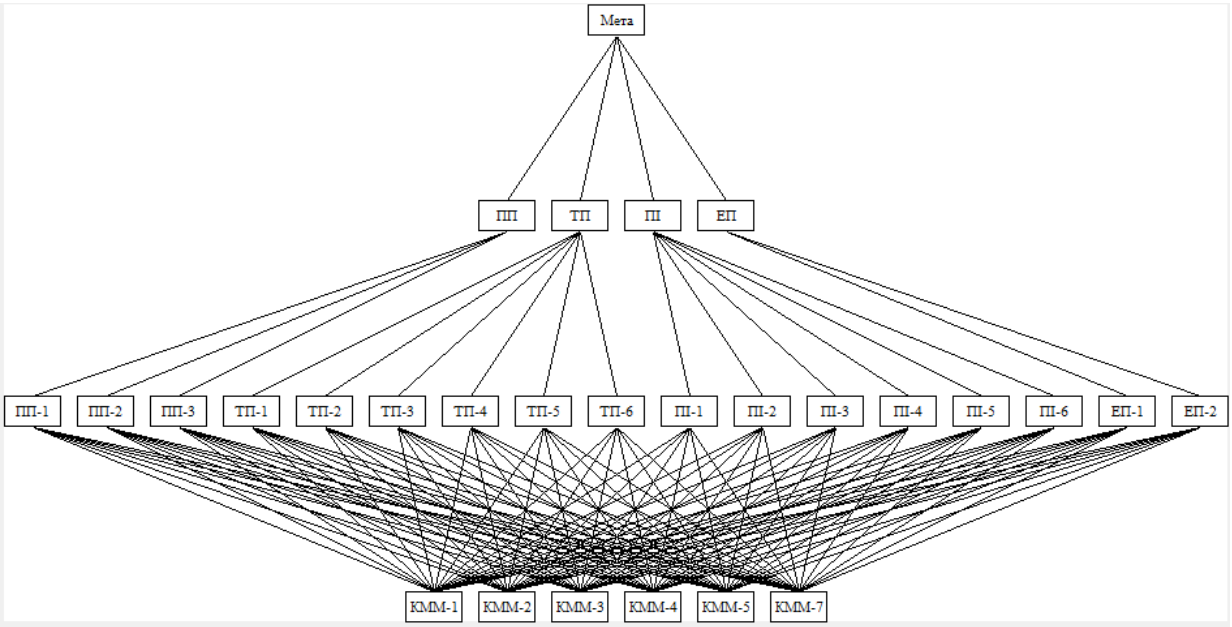

Рис. 1. Дерево цілей для обрання механізму управління ключами

Таблиця 4

Значення векторів вкладів альтернатив до головної цілі

	ПП	ТП	ПІ	ЕП		Вектор вкладу	Результат
КММ-1	0,45	0,22	0,25	0,04		0,16	0,15
КММ-2	0,06	0,17	0,24	0,05		0,13	0,09
КММ-3	0,09	0,13	0,11	0,17	*	0,09	0,15
КММ-4	0,09	0,13	0,12	0,36		0,62	0,27
КММ-5	0,18	0,11	0,14	0,10			0,12
КММ-7	0,09	0,07	0,08	0,25			0,18

Таким чином за сукупністю показників у результаті обрання механізму з використанням методу аналізу ієрархій було обрано механізм КММ-4. На другому місці опинився механізм КММ-7. Основною перевагою механізму КММ-4 над іншими стала його менша ціна порівняно з іншими.

5. 2. Вибір механізмів управління ключами за допомогою методу визначення вагових коефіцієнтів на основі функції втрат ефективності системи

Якщо необхідно виконати обрання механізму на основі тільки формальних показників, доцільно використовувати метод вибору на основі функції втрат ефективності системи [10].

Для обрання механізму з застосуванням методу визначення вагових коефіцієнтів на основі функції втрат ефективності системи з табл. 3 було обрано тільки числові показники та у відповідності до [10] побудовано графіки функції розкиду (рис. 2)

Таблиця 5

Узагальнена оцінка механізму управління ключами

$\hat{\Gamma}^{(k)}$	1	2	3	4	5	7
	0,32	0,56	0,42	0,39	0,41	0,60

Узагальнена оцінка механізму управління ключами $\hat{\Gamma}^{(k)}$ визначалася у відповідності до [10], та результати занесені до табл. 5.

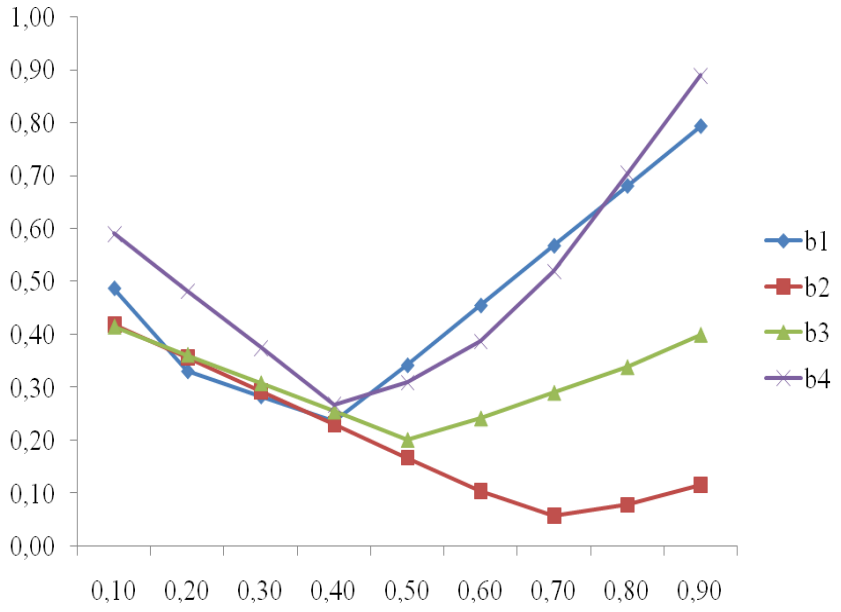

Рис. 2. Графік функції розкиду

З урахуванням того, що найкращим механізмом буде вважається той, для якого значення $\hat{\Gamma}^{(k)}$ є максимальним, маємо, що за сукупними показниками, найкращим механізмом управління ключами вважається КММ-7. Механізми КММ-3, КММ-4 та КММ-5 мають практично однаковий результат, що пов'язано з практично однаковою ціною їх застосування та характеристиками апаратних пристроїв, що застосовуються.

6. Механізм генерації та встановлення спільної пари особистих ключів між *N*-засобами управління ключами

За результатами аналізу публікацій в області механізмів управління ключами та проведеного порівняння існуючих механізмів управління з використанням системного підходу, було визначено, що істотним недоліком існуючих механізмів є необхідність передачі особистих ключів користувача відкритими каналами зв'язку.

Для розв'язання цієї задачі пропонується застосовувати механізм, що реалізується засобом виконання захищеного криптографічного протоколу та складається з наступних кроків:

1. Налаштування засобів захисту: обрання та встановлення загальносистемних параметрів у всіх *N*-модулях.

2. Вироблення спільної системної ключової пари (k_{HSM}, Q_{HSM}).

3. Підпис отриманого відкритого ключа Q_{HSM}, ключем підпису модуля захисту та відправлення на сертифікацію до ЦСК.

Протокол вироблення спільної системної ключової пари може бути реалізований при застосування криптографічних перетворень в групі точок еліптичних кривих, а також за необхідності в скінченному полі.

6. 1. Протокол генерації та встановлення спільного ключа в групі точок еліптичної кривої

Налаштування

Перед застосуванням протоколу між двома засобами повинні бути узгодженні наступні загальносистемні параметри: еліптична крива (ЕК) - E, базова точка ЕК - G, порядок базової точки ЕК - n, розмір поля, що визначає базове кінцеве поле – $F(p)$. За один прохід передбачається генерація спільної пари ключів тільки між двома засобами. Для більшого числа засобів спочатку виконується генерація спільної пара для двох вузлів, після чого спільна пара генерується між вузлами, де її згенеровано, та новим вузлом.

Протокол встановлення ключа

1. Генерується випадкове число $d_i\,(1 \le d_i < n)$, та обчислює відкритий ключ Q_i, кожним з засобів захисту:

$$Q_i = d_i G (\mathrm{mod}\ p). \qquad (1)$$

2. Виконується підпис відкритого ключа Q_i кожного з засобів за допомогою особистого ключа засобу захисту.

3. Підписаний відкритий ключ передається іншим засобам.

4. За протоколом Діффі-Гелмана двома засобами обчислюється спільний секрет S:

$$S_1 = d_1 Q_2 (\mathrm{mod}\ p), \qquad (2)$$

$$S_2 = d_2 Q_1 (\mathrm{mod}\ p), \qquad (3)$$

$$S = d_1 d_2 G (\mathrm{mod}\ p). \qquad (4)$$

5. З використанням функції вироблення ключа H отриманий спільний секрет S, перетворюється в

псевдовипадкове число $d\left(1 \le d < n\right)$, яке є особистим ключем користувача.

6. Відкритий ключ користувача Q, обчислюється згідно виразу 1.

7. Кроки алгоритму 1–6 виконуються для усіх засобів захисту. Отримане значення особистого ключа користувача (d, Q) на останньому кроці – є спільною ключовою парою для всіх засобів. Відкритий ключ користувача Q підписується за допомогою особистого ключа одного з модулів захисту та відправляється на сертифікацію до ЦСК.

7. Обговорення результатів досліджень механізмів управління ключами користувача в хмарі

Керуючись результатами з порівняння та аналізу механізмів управління ключами, що наведені в табл. 1, користувачі хмарних сервісів можуть обрати механізм з управління, що в найбільшій ступені відповідає їх вимогам та середовищу застосування.

Результати, отримані при порівнянні механізмів управління ключами з використанням методу аналізу ієрархій та методу на основі функції втрати ефективності, дозволяють казати, що за сукупністю показників найбільш ефективними є механізми, що застосовують апаратні засоби захисту.

При вирішенні задачі вибору механізму захисту в умовах невизначеності, доцільно використовувати метод з аналізу ієрархій. Недоліком цього методу є необхідність визначення переліку показників та їх значень, а також залучення експертів.

В умовах коли необхідно отримати кількісну оцінку порівняння різних механізмів доцільно використовувати метод заснований на функції втрати ефективності. Недоліком методу є необхідність точного визначення переліку необхідних характеристик системи та їх значень за допомогою експертів.

У відповідності до набору критеріїв в [10], запропонований протокол забезпечує взаємну автентифікація суб'єктів, новизну ключів, захист від атак типу «маскарад» та «модифікація» для відкритих ключів, на спільний ключ впливають всі засоби захисту, що їм володіють. До недоліків протоколу можна віднести, що не передбачена автентифікація ключів, не забезпечується криптоживучіть ключів у випадках компрометації одного з засобів захисту або ключа генерації ключів, а також необхідність залуження третьої довіреної сторони.

8. Висновки

Для аналізу ефективності механізмів з управління ключами, що виконується при розробці технічних завдань на створення комплексної системи захисту інформації в хмарі, доцільно використовувати системний підхід, та методи, що засновані на аналізу ієрархій та функції втрати ефективності.

Застосування цих методів в першу чергу потребує залучення експертів, які мають достатній рівень компетентності та добре знайомі з предметом експертизи.

Запропонований механізм генерації та встановлення спільного ключа, усуває недолік передачі особистих ключів каналами зв'язку між N засобами захисту та дозволяє забезпечити архівування та відновлення особистого ключа.

Література

1. Chandramouli, R. Cryptographic Key Management Issues & Challenges in Cloud Services [Text] / R. Chandramoli, S. Chokhani, M. Iorga. – NIST, 2013. doi: 10.6028/nist.ir.7956

2. Аулов, І. Ф. Дослідження моделі загроз ключових систем хмари та пропозиції захисту від них [Текст] / І. Ф. Аулов // Восточно-Европейский журнал передовых технологий. – 2015. – Т. 5, № 2 (77). – С. 4–13. doi: 10.15587/1729-4061.2015.50912

3. Damgard, I. Secure key management in the cloud [Text]: conference / I. Damgard, T. P. Jakobsen, J. B. Nielsen, J. I. Pagter. – Springer Berlin Heidelberg, 2013. – P. 270–289.

4. Singh, K. Multi-Level Cryptographic Key Sharing For Secure Access and Authorization on Cloud Platforms [Text] / K. Singh, A. Kaur // International Journal of Science and Research (IJSR). – 2015. – Vol. 4, Issue 11. – P. 152–154. doi: 10.21275/v4i11.sub159266

5. Tysowski, P. K. Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds [Text] / P. K. Tysowski, M. A. Hasan // IACR Cryptology ePrint Archive. – 2011. – Vol. 2011. – 668 p.

6. Punia, J. Multi-Level Complex Key Sharing For Secure Access and Authorization on Cloud Platforms [Text] / J. Punia, R. K. Bawa // International Journal of Science and Research (IJSR). – 2015. – Vol. 4, Issue 5. – P. 2369–2372.

7. Lei, S. Research on key management infrastructure in cloud computing environment [Text]: conference / S. Lei, D. Zishan, G. Jindi. – IEEE, 2010. – P. 404–407. doi: 10.1109/gcc.2010.84

8. Bennani, N. Toward cloud-based key management for outsourced databases [Text]: conference / N. Bennani, E. Damiani, S. Cimato. – IEEE, 2010. – P. 232–236. doi: 10.1109/compsacw.2010.47

9. Lerman, L. Key Management as a Service [Text] / L. Lerman, O. Markowitch, Jr. J. Nakahara, P. P. Samarati // SECRYPT. – 2012. – P. 276–281.

10. Горбенко, І. Д. Прикладна криптологія: Теорія. Практика. Застосування [Текст]: монографія / І. Д. Горбенко, Ю. І. Горбенко. – вид. 2-ге, перероб. і доп. – Харків: Видавництво «Форт», 2012. – 880 с.

11. Саати, Т. Принятие решений: Метод анализа иерархий [Текст] / Т. Саати. – М.: Радио и связь, 1993. – 278 с.

References

1. Chandramouli, R., Iorga, M., Chokhani, S. (2013). Cryptographic Key Management Issues and Challenges in Cloud Services. NIST. doi: 10.6028/nist.ir.7956

2. Aulov, I. F. (2015). The research of the threat model of the cloud key systems and protection proposals against them. Eastern-European Journal of Enterprise Technologies, 5/2 (77), 4–13. doi: 10.15587/1729-4061.2015.50912

3. Damgard, I., Jakobsen, T. P., Nielsen, J. B., Pagter, J. I. (2013). Secure key management in the cloud. Springer Berlin Heidelberg, 270–289.

4. Singh, K., Kaur, A. (2015). Multi-Level Cryptographic Key Sharing For Secure Access and Authorization on Cloud Platforms. International Journal of Science and Research (IJSR), 4 (11), 152–154. doi: 10.21275/v4i11.sub159266

5. Tysowski, P. K., Hasan, M. A. (2011). Re-Encryption-Based Key Management Towards Secure and Scalable Mobile Applications in Clouds. IACR Cryptology ePrint Archive, 2011, 668.

6. Punia, J., Bawa, R. K. (2015). Multi-Level Complex Key Sharing For Secure Access and Authorization on Cloud Platforms. International Journal of Science and Research (IJSR), 4 (5), 2369–2372.

7. Lei, S., Zishan, D., Jindi, G. (2010). Research on key management infrastructure in cloud computing environment. IEEE, 404–407. doi: 10.1109/gcc.2010.84

8. Bennani, N., Damiani, E., Cimato, S. (2010). Toward cloud-based key management for outsourced databases. IEEE, 232–236. doi: 10.1109/compsacw.2010.47

9. Lerman, L., Markowitch, O., Nakahara, Jr. J., Samarati, P. P. (2012). Key Management as a Service. SECRYPT, 276–281.

10. Gorbenko, I. D., Gorbenko, U. I. (2012). Applied Cryptology: Theory. Practice. Application. Kharkiv: Publishing House "Fort", 880.

11. Saaty, T. (1993). Making decisions. Analytic Hierarchy Method. Moscwo: Radio and Communications, 278.

Рекомендовано до публікації д-р техн. наук, професор Горбенко І. Д.
Дата надходження рукопису 19.05.2016

Аулов Іван Федорович, молодший науковий співробітник, кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, пр. Науки, 14, м. Харків, Україна, 61166
E-mail: aulov@iit.kharkov.ua