УДК 681.3.06

КОМПЛЕКСНИЙ МЕТОД ПОРІВНЯННЯ, ОЦІНКИ ТА ВИБОРУ МЕХАНІЗМІВ УПРАВЛІННЯ КЛЮЧОВИМИ ДАНИМИ КОРИСТУВАЧІВ У ХМАРНИХ ІТС

І.Ф. АУЛОВ

Запропоновано методику, що дозволяє провести комплексне порівняння механізмів управління ключовими даними користувачів у хмарних ІТС за сукупністю критеріїв та показників. Наводиться обґрунтування критеріїв та показників оцінки механізмів управління ключовими даними користувачів у хмарі.

Ключові слова: механізми управління, ключові дані, хмарні ІТС, порівняльний аналіз.

ВСТУП

Сьогодні в ході використання хмарної інфраструктури користувачами, особливо при переході на її з власних інфраструктурних рішень виникає проблема управління ключовими даними користувачів. У першу чергу ця проблема пов'язана з необхідністю довіри користувача до постачальника хмарних послуг.

Аналогічна проблема існує і у випадку використання приватної хмари. Кінцевим користувачам необхідно надавати зручний доступ та можливості гнучкого управління їх ключовими даними безпосередньо в середовищі хмари при цьому забезпечуючи гарантії, щодо неможливості отримання несанкціонованого доступу до їх ключових даних іншими користувачами, в першу чергу обслуговуючим персоналом хмари [1–3].

На сучасному етапі розвитку хмарних технологій пропонується декілька механізмів з управління ключовими даними користувачів у середовищі хмарних обчислень. Метою дослідження є розробка методики, яка дозволить проводити комплексну оцінку та порівняння існуючих та перспективних механізмів управління ключовими даними користувачів у хмарі. Для досягнення мети було вирішено такі задачі: формалізація задачі управління ключовими даними користувача в хмарі, обґрунтування та вибір критеріїв та показників, вибір та обґрунтування методики порівняння, визначення обмежень до застосування методики.

1. СУЧАСНИЙ СТАН ДОСЛІДЖЕНЬ

Аналіз зарубіжних публікацій та патентів в області хмарних обчислень показав, що для управління ключами користувача існує 6 базових механізмів [4–13]:

– механізм управління ключами з використанням сертифікатів відкритих ключів;

– механізм управління ключами на основі паролів;

– механізм управління ключами з використанням HSM хмарного ЦОД;

– механізм управління ключами з використанням HSM користувача;

– механізм управління ключами з використанням криптографічного сервісу та захищеного сховища ключів;

– комбінований механізм управління ключами.

В першу чергу дослідники механізмів управління ключами приділяють увагу розробці нових, а також адаптації до вимог хмари та впровадженню існуючих рішень для управління ключами в середовищі хмарних обчислень.

Також суттєва увага дослідників приділяється питанням захисту та управління ключами в хмарі. До них відносяться такі [1–3]:

1. Встановлення таємних чи особистих ключів користувачів на об'єктах хмари з забезпеченням їх конфіденційності, цілісності, справжності, доступності, неспростовності та надійності.

2. Розповсюдження та встановлення чи отримання доступу до відкритих ключів користувачів з забезпеченням їх цілісності, справжності, доступності, неспростовності та надійності.

3. Оперативне виявлення фактів компрометації таємних та особистих ключів користувачів та виведення їх з дії з подальшим захищеним відновлення.

4. Дистанційне блокування чи знищення таємних та особистих ключів користувачами чи уповноваженими особами.

5. Захист таємних та особистих ключів користувачів від несанкціонованого доступу від внутрішніх та зовнішніх порушників, включаючи спеціалістів служб безпеки.

6. Створення, впровадження та застосування інфраструктур відкритого ключа (ІВК) в частині виготовлення та обслуговування сертифікатів відкритих ключів для надання електронних довірчих транскордонних послуг.

7. Забезпечення відносно особистих та відкритих ключів ІВК різних періодів чинності, наприклад чинність відкритих ключів має бути не менше періоду зберігання захищеної інформації архівів тощо.

Аналіз показав, що наведені вище проблемні питання відносяться і до захисту ключових даних безпосередньо хмарних обчислень та службових ключових даних посадових осіб тощо.

2. ВИМОГИ ДО МЕХАНІЗМІВ УПРАВЛІННЯ КЛЮЧОВИМИ ДАНИМИ В ХМАРІ

Безумовною вимогою для гарантування належного рівня безпеки в хмарі є застосування загальноприйнятих та міжнародних практик з використання та управління ключами. Надання обов'язкових для хмари послуг, таких як самообслуговування на вимогу, забезпечення універсального доступу, об'єднання ресурсів, швидка еластичність та облік споживання, а також відсутність контролю з боку користувача над хмарним середовищем, одночасна обробка декількох потоків інформації з різним рівнем безпеки, неоднорідність системи та її розгалуженість висуває нові вимоги до механізмів управління ключовими даними.

Аналогічно існуючим ІТС, в середовищі хмарних обчислень висуваються вимоги з забезпечення конфіденційності, цілісності, доступності, спостережливості, неспростовності, криптоживучості та надійності ключів. Виконання цих вимог може бути досягнуто за рахунок технічних, організаційних та криптографічних методів захисту.

В середовищі хмарних обчислень існують значні проблеми в забезпеченні виконання цих вимог. Аналіз еталонної моделі хмари NIST США показав, що в процесі використання хмарних сервісів користувачам можуть надаватися три типи послуг – IaaS, PaaS та SaaS [1], а також необхідні засоби забезпечення безпеки та архітектурні рішення, що забезпечують реалізацію цих послуг.

Із [1–3] випливає, що управління ресурсами, які пов'язані з хмарними сервісами, є найважливішим аспектом хмарних обчислень та потребують забезпечення безпеки. При чому, на рівні з організаційними та технічними механізмами та методами забезпечення безпеки, криптографічні механізми та методи є обов'язковими для забезпечення безпечного управління ресурсами хмари. Окрім необхідності забезпечення безпеки управління хмарою та ресурсами, розглядаючи згідно з моделлю NIST роль користувача в хмарі, необхідно зазначити, що криптографічні перетворення необхідні також для безпечної взаємодії користувача хмари з різними сервісами хмари, а також для зберігання даних, що були генеровані та/або оброблені цими сервісами.

Таким чином система управління ключами, що необхідна для підтримки криптографічних перетворень для зазначених вище функцій, може бути складною, зважаючи на відмінності відносно контролю над рівнями інфраструктури хмари, в яких знаходяться KMS та ресурси, що захищаються.

Наприклад, хоча споживач і має право власності на дані, що знаходяться та обробляються в хмарі, дані фізично зберігаються на ресурсах, що контролюються провайдером хмарних послуг, і в багатьох випадках KMS, яка необхідна для управління ключами для захисту даних також буде розгорнута на ресурсах постачальника хмарних послуг. Це породжує проблему безпеки і довіри хмарних користувачів до криптографічних операцій, що виконуються в хмарі.

Хоча є деякі розбіжності в послугах, що надаються хмарними провайдерами, але можна визначити набір функцій для основних моделей надання послуг (IaaS, PaaS та SaaS). Грунтуючись на цьому наборі функції визначаються можливості щодо реалізації функцій захисту та архітектурних рішень для досягнення цих можливостей безпеки. Слід зазначити, що не залежно від реалізованих функцій безпеки та архітектурного рішення, у випадках, коли криптографічні ключі зберігаються в хмарі є обмеження на ступінь забезпечення безпеки, на яку може розраховувати споживач хмари при будь-якій моделі надання послуг, в зв'язку з тим, що логічні і фізичні ресурси повністю під контролем хмарного провайдера.

Проведений аналіз та враховуючи рекомендації [1] дозволяє визначити три основні групи вимог, що висуваються до механізмів управління ключами в хмарі: орагізаційні та правові, технічні та функціональні, інформаційної безпеки.

До організаційних та правових вимог відносятся:

– відповідність міжнародним та державним стандартам та нормативним документам;

– проходження обов'язкової міжнародної та\або державної сертифікації;

– проведення аудиту впроваджених механізмів захисту;

– моніторинг, тестування та оновлення програмного та апаратного забезпечення;

– укладення договорів між користувачами та постачальниками;

– створення комплексної системи захисту для сервісу управління ключовими даними;

– забезпечення розмежування доступу та контролем над обслуговуючим персоналом;

– забезпечення безперебійної роботи, резервування та захист від відмов механізму управління ключами з причини стихійного лиха, збоїв в роботі сервісів хмари тощо;

– можливість зміни постачальника послуг.

До складу технічних і функціональних вимог, яким має відповідати механізм в першу чергу відносяться базові вимоги, що висуваються до хмари, а саме забезпечення:

– самообслуговування користувача на вимогу: функції пов'язані з підключенням та відключенням послуг сервісу управління ключами, безпосереднім управлінням ключами (генерацією, використанням, блокуванням, знищенням) мають надаватися автоматизовано;

– доступу до сервісу управління ключами за рахунок використання стандартних протоколів мережі та клієнтського програмного забезпечення для різних платформ;

– об'єднання ресурсів сервісу управління ключами в спільний пул та надаватися користувачам з нього залежно від їх запитів;

– надання та звільнення наданих ресурсів сервісу управління ключами має виконуватися автоматично за запитом від користувача з найбільшою швидкістю;

– вимірювання та контроль за обліком споживання ресурсів як користувачем, так і хмарним провайдером.

Окрім зазначених вище обов'язкових вимог існують такі, що можуть виконуватися частково залежно від потреб користувача:

– забезпечення функціонування та надання послуг сервісу управління ключами для моделей надання послуг IaaS, PaaS, SaaS;

– забезпечення функціонування та надання послуг сервісу управління ключами для різних моделей розгортання хмари;

– вимоги до технічних показників сервісу управління ключами, наприклад, такі як максимальна кількість клієнтів, що може одночасно обслуговуватися, середній час обробки запиту від клієнта, протоколи, алгоритми та формати ключових даних, що підтримуються, тощо.

Для задовільнення вимог інформаційної безпеки механізм має забезпечувати:

– автентифікацію сторін та перевірку дозволу при доступі до функцій управління ключовими даними окремого ключа;

– захист від підміни (автентифікація джерела має здійснюватися до виконання команд) та модифікації (забезпечення цілісності) команд управління ключами, результатів їх виконання, даних, що передаються;

– захист секретних та особистих ключів від несанкціонованого доступу;

– захист ключів та їх ключових даних від підміни;

– захист ключів та ключових даних від неявних та несанкціонованих модифікацій (забезпечення цілісності);

– стійкість криптографічних перетворень, що використовуються для захисту ключів не меншу, ніж стійкість ключів, що захищаються;

– захищений канал передачі (у випадках передачі ключів та ключових даних) з стійкістю не меншою, ніж стійкість ключів, що захищаються;

– виконання криптографічних перетворень, що застосовують ключі в довіреному середовищі.

3. КРИТЕРІЇ ТА ПОКАЗНИКИ МЕХАНІЗМІВ УПРАВЛІННЯ КЛЮЧОВИМИ ДАНИМИ В ХМАРІ

Окрім зазначених вище вимог, які висуваються до механізмів управління ключовими даними в хмарі під час проведення порівняння та вибору механізму серед інших пропонується використовувати групи критеріїв, що складаються з показників продуктивності (ПП), технічних показників (ТП), показників можливості розширення (ПМР), економічних показники (ЕП).

Як показники продуктивності пропонується використовувати:

– максимальна кількість сесій користувачів (ПП-1);

– щвидкість надання доступу до управління ключами, оп/с (ПП-2);

– швидкість криптографічних операцій за показником (ПП-3);

– швидкість генерації ключів, кл/с (ПП-4);

– швидкість захисту ключів, кл/с (ПП-5).

До технічних показників відносяться:

– максимальна кількість ключів, що можуть зберігатися (ТП-1);

– клас захищеності (ТП-2);

– захищеність сховища ключів (ТП-3);

– функції управління ключами в хмарі (ТП-4);

– моделі розгортання хмари, що підтримуються (ТП-5);

– моделі надання послуг у хмарі, що підтримуються (ТП-6);

– криптографічні алгоритми, що підтримуються (ТП-7);

– механізм автентифікації користувача (ТП-8).

До показників можливості розширення відносяться:

– функції криптографічного сервісу (ПМР-1);

– функції реєстрації подій (ПМР-2);

– функції ідентифікації та автентифікації (ПМР-3);

– функції сервісу управління ключами (ПМР-4);

– підтримка розподілених вузлів (ПМР-5);

– підтримка архівування, зберігання та відновлення ключів (ПМР-6);

– максимальна кількість розподілених вузлів (ПМР-7);

– гнучкість, щодо розширення та оновлення (ПМР-8).

До економічних показників відносяться:

– вартість рішення, у.о. (ЕП-1);

– вартість супроводження, у.о./рік (ЕП-2);

– вартість навчання відповідального персоналу, у.о./рік (ЕП-3).

4. АНАЛІЗ ЕФЕКТИВНОСТІ МЕХАНІЗМІВ УПРАВЛІННЯ КЛЮЧАМИ НА ОСНОВІ ЕКОНОМІЧНОГО ПОКАЗНИКА

Під час проведення аналізу механізмів та методів забезпечення безпеки в АС на практиці прийнято використовувати формалізовані моделі та методики аналізу ефективності систем захисту. Загальноприйнятим є твердження, що при синтезі механізмів захисту в першу чергу необхідно користуватися принципом розумної достатності [17], що передбачає застосовування формального критерію відповідності побудова-

ного механізму цьому принципу. В літературі як критерій ефективності захисту прийнято використовувати «комплексу оцінку захищеності», яка є сукупністю оцінок з ефективністю застосування програного-апаратних та організаційно-правових засобів захисту [17].

Вирішення задачі такого роду засновано на застосуванні теоретико-графового підходу у вигляді моделі системи з повним перекриттям загроз безпеці [17]. Модель системи захисту для механізмів управління ключами розглядається у вигляді дольного графа (рис. 1).

Кожне ребро графа G(P, O, Z, E, H) визначає дію конкретної загрози на конкретний об'єкт або нейтралізацію певним механізмом захисту загрози безпеки.

Отримання кількісного показника граф G(P, O, Z, E, H) зважується і еквівалентно представляється такою сукупністю векторів і матриць:

– вектор $P(p_1, p_2, \ldots p_N)$, де p_i – ймовірність реалізації загрози;

– вектор $O(o_1, o_2, \ldots o_L)$, де o_i – вартість об'єкту захисту;

– матриця $E\{e_{ij}\}$ розмірністю $N\times L$, де $e_{ij}=1$ якщо реалізується i-та загроза на j-й об'єкт, та $e_{ij}=0$, в іншому випадку;

– вектор $Z(z_1, z_2, \ldots z_M)$, де z_i – вартість механізму або засобу захисту;

– матриця $H\{h_{ij}\}$ розмірністю $N\times M$, де h_{ij} ймовірність усунення i-ї загрози від застосування j-го механізму або засобу захисту.

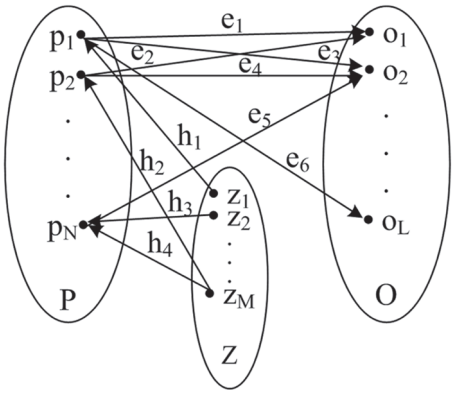

Рис. 1. Модель системи захисту системи управління ключами у вигляді тридольного графа

З використанням розглянутої моделі, можна провести аналіз ефективності системи захисту системи управління ключами на основі кількісного критерію, що відображає вплив застосованих методів і засобів захисту на зміну величини збитків від загроз безпеці. Як такий критерій зокрема, можна використовувати наступний показник економічної ефективності застосування механізму захисту:

$$T = \frac{U - U`}{\sum_{i=1}^{L} o_i + \sum_{k=1}^{M} z_k}, \qquad (1)$$

де U – оцінка величини збитку від загроз безпеки за відсутності засобів і механізмів захисту; $U`$ – оцінка величини залишкового збитку в ході застосування засобів і механізмів захисту.

Значення U та U` може бути розраховано таким чином:

$$U = \sum_{i=1}^{L} o_i (1 - \prod_{j=1}^{N} e_{ij}(1 - p_j)), \qquad (2)$$

$$U` = \sum_{i=1}^{L} o_i (1 - \prod_{j=1}^{N} e_{ij}(1 - p_j(\prod_{k=1}^{M}(1 - h_{jk})))). \qquad (3)$$

Залишкова ймовірність реалізації всіх загроз у системі може бути обчислена таким чином:

$$P`_{\text{залиш.}} = 1 - \prod_{i=1}^{N}(1 - p_i(\prod_{k=1}^{M}(1 - h_{ik}))). \qquad (4)$$

Практичне застосування наведених співвідношень потребує застосування експертних методів оцінки ймовірностей реалізації загроз безпеці та значення h_{ij}.

Реалізація системного підходу щодо аналізу ймовірності загроз, рівню збитків, що вони завдають, а також ефективності застосованих механізмів управління ключами потребує долучення компетентних експертів, які добре знайомі з предметом експертизи, а також володіють достатнім досвідом і здатні виносити об'єктивні судження. Для зменшення впливу суб'єктивного фактора, що існує при долученні експертів до аналізу, пропонується використовувати підхід до нормування отриманих оцінок від експертів за рахунок коефіцієнта їх компетентності – $K_j^{(l)}$ [16]. Оцінка рівня компетентності експертів може бути проведена з використанням документального методу, який передбачає оцінку компетентності на основі таких документальних даних, як число наукових праць в області оцінюваної проблеми, науковий ступінь, стаж практичної роботи, займана посада, тестовий метод – оцінка компетентності формується на підставі вирішення експертами тестових задач, у яких відбита специфіка предмета експертизи, а також метод взаємної і самооцінки експертів – сутність якого полягає в оцінці компетентності експертом кожного з своїх колег, а також своєї власної компетентності [16].

5. ПОРЯДОК ЗАСТОСУВАННЯ МЕТОДИКИ

Запропонована методика направлена на отримання комплексної оцінки механізмів управління ключами в середовищі хмари та складається з таких кроків:

– збір та визначення вхідних даних;

– визначення переліку необов'язкових вимог на основі вхідних даних;

– визначити модель загроз та модель порушника для ключів та ключових даних у системі хмарних обчислень;

– з урахуванням наявних статистичних даних та оцінок експертів визначити ймовірності реалізації загроз;

– визначити можливі збитки та їх вартість;

– визначення відповідності механізмів висунутим обов'язковим та визначеним необов'язковим вимогам;

– визначити ефективність застосування механізмів управління ключами;

– критерії та показники механізмів управління ключами та їх значущість;

– враховуючи отримані результати обрати найбільш ефективний механізм управління ключовими даними.

З метою вирішення задачі оцінки та обрання механізму управління ключами, скористаємося системним підходом.

Вхідними даними під час проведення аналізу є такі:

– об'єкт де розташовані потужності, що забезпечують функціонування та розгортання механізму управління ключовими даними;

– модель розгортання хмари (приватна, публічна, гібридна) та модель надання послуг (SaaS, PaaS, IaaS);

– характеристики механізмів управління ключами, а саме показники продуктивності (ПП), технічні показники (ТП), показники можливості розширення (ПМР), економічні показники (ЕП);

– вартість ресурсу, що захищається.

Якщо модель розгортання хмари не задана, рекомендується розглядати публічну хмару, яка має найбільшу кількість та ймовірність реалізації загроз, порівняно з іншими існуючими моделями, до яких можна перейти, зменшивши кількість загроз, що існує для публічної хмари. Аналогічно, якщо не задана модель надання послуг, слід розглядати можливості з надання послуги на різних рівнях.

Характеристики окремих елементів, що входять до складу механізмів управління ключами, мають бути обрані з урахуванням існуючих рішень в галузі захисту інформації.

Вартість ресурсу, що захищається, визначається на основі даних, отриманих від користувача хмарних послуг. Якщо в системі існує декілька користувачів, вартість ресурсів, що захищається, задається як набір значень вартості ресурсів. При цьому, якщо вартість ресурсу набагато вища, ніж сукупна вартість хмарного сервісу, користувачу необхідно розрахувати ефективність створення приватної хмари, що дозволяє суттєво знизити ризики виникнення загроз.

Ефективність механізмів управління ключами пропонується розраховувати за економічними показниками.

Як методи для вирішення задачі обрання механізму управління ключами, пропонується використовувати метод аналізу ієрархій [15] за рахунок використання кількісних та якісних показників, а також із застосуванням методу визначення вагових коефіцієнтів на основі функцій втрат ефективності системи з використанням тільки кількісних показників [16]. При подальшому прийнятті рішення з використання механізму управління ключами особа, що приймає рішення залежно від поставленої задачі має застосовуватись один з критеріїв прийняття рішень [16].

ВИСНОВКИ

Аналіз публікацій, стандартів та патентів в області хмарних обчислень, а також проведені дослідження показали, що для управління ключами зі сторони користувача можна застосовувати механізми управління ключами з використанням: сертифікатів відкритих ключів; паролів; HSM хмарного ЦОД; HSM користувача; криптографічного сервісу та захищеного сховища ключів.

Реалізація системного підходу до аналізу ймовірності загроз, які дорівнюють рівню збитків, що вони завдають, а також ефективності застосованих механізмів управління ключами потребує долучення компетентних експертів, які добре знайомі з предметом експертизи, а також володіють достатнім досвідом і здатні виносити об'єктивні судження. Для зменшення впливу суб'єктивного фактора, що існує при долученні експертів до аналізу, слід використовувати підхід, щодо нормування отриманих оцінок від експертів за рахунок коефіцієнта їх компетентності.

Ефективність механізмів управління ключами пропонується розраховувати за економічними показниками. Як методи для вирішення задачі обрання механізму управління ключами, пропонується використовувати метод аналізу ієрархій та метод на основі функцій втрат ефективності системи.

Література

[1] *Chandramouli, R.* NIST Cryptographic Key Management Issues & Challenges in Cloud Services. / R. Chandramoli, S. Chokhani, M. Iorga, // Режим доступу: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7956.pdf. http://dx.doi.org/10.6028/NIST.IR.7956

[2] *Damgård I.* Secure Key Management in the Cloud / I. Damgård, T. P. Jakobsen, J. B. Nielsen, J. I. Pagter // Cryptography and Coding Lecture Notes, Springer, v. 8306. – P. 270-289. – 2013.

[3] *Choo, K.* A Cloud Security Risk-Management Strategy. / K. Choo // Cloud Computing, IEEE, – 2014. – Vol. 1 (2). – P. 52–56.

[4] *Tysowski, P.K.* Cloud-hosted key sharing towards secure and scalable mobile applications in clouds / P.K Tysowski, M.A. Hasan // Networking and Communications, – 449-455 pp. – 2013.

[5] Tysowski, P.K. Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds, / P.K Tysowski, M.A. Hasan // IEEE Transactions on , vol. 1, – 172-186pp., – 2013.

[6] Cloud key management system: United States Patent Application Publication. / Pub. No.: US 2014/0050317 A1 / Authors: Jason Allen Sabin, Lehi, UT (US). Режим доступу: https://www.google.com/patents/US20140050317

[7] Cloud key management system: United States Patent Application Publication. / Pub. No.: US 20140019753

A1 / Authors: J John Houston Lowry, Jonathan A. Rubin. Режим доступу: https://www.google.com/patents/US20140019753

[8] Cloud-based hardware security modules: United States Patent Application Publication. / US 20130179676 A1 / Authors: Laurence Hamid. Режим доступу: https://www.google.com/patents/US20130179676

[9] Cloud key management: United States Patent Application Publication. / US 20140019753 A1/ Authors: John Houston Lowry, Jonathan A. Rubin. Режим доступу: http://www.google.com/patents/US20140019753

[10] Remote key management in a cloud-based environment: United States Patent Application Publication. / US 20140270178 A1 / Authors: Andy Kiang, Chris Byron, Jeffrey Queisser. Режим доступу: http://www.google.com/patents/US20140270178

[11] Secure Cloud Storage and Encryption Management System: United States Patent Application Publication. / US 20140281477 A1 / Authors: Alex Nayshtut, Edward Jimison, Omer Ben-Shalom, Michael Raziel. Режим доступу: http://www.google.com/patents/US20140281477

[12] Virtual key management and isolation of data deployments in multi-tenant environments: United States Patent Application Publication. / US 20140283010 A1 / Authors: Matthew Francis Rutkowski, Ronald W. Bassett, Thomas Alexander. Bellwood. Режим доступу: http://www.google.com/patents/US20140283010

[13] Cloud-based key management: United States Patent Application Publication. / US 20150172260 A1 / Authors: Stephan Brenner. Режим доступу: http://www.google.com/patents/US20150172260

[14] *Аулов І.Ф.* Дослідження моделі загроз ключових систем хмари та пропозиції захисту від них / І.Ф. Аулов // Восточно-Европейский журнал передовых технологий. – 2015. – № 5/2 (77). – С. 4–13.

[15] *Саати Т.* Принятие решений. Метод анализа иерархий. – М: Радио и связь, 1999. – 341 с.

[16] *Медіченко М.П., Потій О.В.* Основи теорії систем та системного аналізу. – Харків: ХВУ, 2002. – 258 с.

[17] *Гайдамакин, Николай Александрович*. Учебно-методический комплекс дисциплины «Теоретические основы компьютерной безопасности» [Электронный ресурс] / Н. А. Гайдамакин ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ «Информационная безопасность» [и др.]., Екатеринбург. – 2008.

Надійшла до редколегії 25.11.2015

Аулов Іван Федорович, молодший науковий співробітник кафедри БІТ ХНУРЕ. Наукові інтереси: дослідження безпеки хмарних обчислень.

УДК 681.3.06

Комплексный метод сравнения, оценки и выбора механизмов управления ключевыми данными пользователя в облачной ИТС / И.Ф. Аулов // Прикладная радиоэлектроника: научн.-техн. журнал. – 2015. – Том 14. – № 4. – С. 397–402.

Предложено методику, которая позволяет провести комплексное сравнение механизмов управления ключевыми данными пользователей в облачных ИТС по совокупности критериев и показателей. Приводится обоснование критериев и показателей оценки механизмов управления ключевыми данными пользователей в облаке.

Ключевые слова: механизмы управления, ключевые данные, облачные ИТС, сравнительный анализ.

Рис.: 1. Библиогр.:17 назв.

UDC 681.3.06

Complex method of comparison, assessment and selection of key data management mechanisms in a cloud ITS / I.F. Aulov // Applied Radio Electronics: Sci. Journ. – 2015. – Vol. 14. – № 4. – P. 397–402.

The paper proposes a technique, which allows to make complex comparative analysis of user key management mechanisms in a cloud ITS using a collection of criteria and indicators. The substantiation of criteria and indicators for assessing user key data management mechanisms in the cloud is given.

Keywords: control mechanisms, key data, cloud ITS, comparative analysis.

Fig.: 1. Ref.: 17 items.