Викладаються результати розробки та аналізу моделей загроз хмарних сервісів та ключовим даним. Пропонується модель та профіль порушника, загальні механізми захисту ключів, а також висуваються пропозиції з оцінки ризиків з використанням якісних та кількісних показників. В подальшому результати досліджень можуть бути використані при проведенні експертизи, оцінці безпеки та ризиків хмарних ІТС

Ключові слова: хмарне середовище, управління ключами, модель порушника, механізми захисту, оцінка ризиків

Излагаются результаты разработки и анализа моделей угроз облачных сервисов и ключевым данным. Предлагается модель и профиль нарушителя, общие механизмы защиты ключей, а также выдвигаются предложения по оценке рисков с использованием качественных и количественных показателей. В дальнейшем результаты исследований могут быть использованы при проведения экспертизы, оценки безопасности и рисков облачных ИТС

Ключевые слова: облачная среда, управление ключами, модель нарушителя, механизмы защиты, оценка рисков

УДК 004.75
DOI: 10.15587/1729-4061.2015.50912

ДОСЛІДЖЕННЯ МОДЕЛІ ЗАГРОЗ КЛЮЧОВИХ СИСТЕМ ХМАРИ ТА ПРОПОЗИЦІЇ ЗАХИСТУ ВІД НИХ

І. Ф. Аулов
Аспірант
Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
пр. Леніна, 16, м. Харків, Україна, 61166
E-mail: aulov@iit.kharkov.ua

1. Вступ

Нині до хмарних технологій та реалізації на їх основі хмарних обчислень проявляється велика зацікавленість, а технологічно розвинені держави їх уже реалізували та широко застосовують. Використання технологій хмарних обчислень дозволяє досягти ряд переваг, основними з них є такі, як [1]: гнучкість, обчислювальна потужність, великий обсяг файлового сховища, різноманітність програмного забезпечення; повсякчасна можливість доступу до ресурсів в хмарі та швидке розгортання сервісів, можливість збільшення навантаження в хмарі; простота масштабування, резервування та самовідновлення; можливість управління навантаженнями та здійснення моніторингу в реальному часі тощо.

З точки зору здійснення захисту інформації також маються переваги, основними з яких є такі, як [1]:

– практична можливість централізованого керування конфігурацією, рівнем безпеки та здійснення аудиту;

– можливість динамічного масштабування ресурсів системи, резервування та аварійного відновлення при збоях;

– як правило, наявність штатних підрозділів, які повинні забезпечувати безпеку інформації при хмарних обчисленнях;

– централізоване розміщення програмного та програмно-апаратного забезпечень захисту інформації та захисту даних відповідно прийнятих політик безпеки тощо.

До основних недоліків використання хмарних обчислень відносяться [1, 3]: неможливість роботи з сервісами хмари без постійного підключення до мережі Інтернет; неможливий або складний процес зміни постачальника хмарних послуг; недостатність єдиного міжнародного та національного правового регулювання в сфері хмарних обчислень та обробки інформації; необхідність високої довіри до постачальника послуг користувачів; складність надання користувачам основних послуг з безпеки інформації тощо.

Також при хмарних обчисленнях маються суттєві проблеми відносно гарантій надання послуг з безпеки інформації, основними з них є такі [1–3]:

– практично втрата контролю над механізмами захисту інформації та прикладного програмного забезпечення хмари;

– наявність привілегійованих користувачі та адміністраторів безпеки хмари, що можуть мати доступ до програмного забезпечення та даних користувачів;

– складність механізмів здійснення аналізу, оцінки ефективності та протидії загрозам;

– оскільки хмара є багатокористувацьким середовищем, то можливий виток конфіденційної інформації, порушення її цілісності, справжності, а також порушення прав власності;

– проблемність надання якісної послуги доступності при відсутності чи неякісному Інтернет з'єднанні;

– проблема управління конфіденційними та особистими ключовими даними, сертифікації та відновлення компрометованих ключових даних та ключової інформації.

2. Аналіз літературних джерел та постановка проблеми

Підвищений інтерес до впровадження хмарних сервісів та їх активне застосування зумовило появу

нових міжнародних та закордонних державних стандартів, роз'яснень та рекомендацій з використання хмарних сервісів та забезпечення безпеки в середовищі хмари. Окрім провідних державних організацій Європи та США: Європейського агентства мережевої та інформаційної безпеки (ENISA) і Національного інституту стандартів і технологій (NIST), питаннями стандартизації займається комітет міжнародної організації з стандартизації ISO/IEC JTC 1/SC 27, та об'єднання представників IT-індустрії в сфері хмарних технологій – Альянс безпеки в хмарі (Cloud Security Alliance, CSA).

Аналізу існуючих загроз, побудові моделей загроз та порушника в хмарі присвячено низку публікацій [2–4]. Так, в роботі [2], розглядає питання безпеки ключів, довіри до провайдера, управління ризиками, безпекою архітектури хмарного середовища, управління доступом, захисту даних та ізоляції програм. Подальший розвиток його робота знайшла в якості рекомендацій NIST SP 800-144 [3].

В статті [4], проводиться детальний аналіз існуючих загроз хмарних обчислень з урахуванням стандартів та рекомендації, що розробляються NIST, ISO\IEC, CSA.

В роботі [5] аналізуються доступні механізми захисту віртуального середовища в хмарі при використанні моделі розгортання IaaS. До розглянутих методів захисту відносяться: захист образів віртуальних машин від порушення цілісності, конфіденційності та доступності, налаштування захисту образів віртуальних машин від вірусів та шпигунського ПЗ, захист внутрішніх мереж. Аналіз питань безпеки управління ключами в хмарі проводиться в роботі [6].

Авторами роботи [7] робиться аналіз сучасного стану стандартизації в області забезпечення безпеки хмарних обчислень та пропонується підхід з аналізу ризиків, що дозволяє оцінити відповідність хмарного рішення заявленим рівням безпеки.

Суттєвий вплив на аналіз та оцінку ризиків в хмарі справила робота дослідників з організації ENISA, які розвинули їх ідеї [1]. Так в роботі [8] пропонується використовувати динамічну стратегію управління ризиками, в роботі [9] з запропонованих в стандарті ISO/IEC 31010 методів в якості динамічного методу пропонується байесовіський підхід. Подальший розвиток робота [8] знайшла в публікації [10] в якій автори розробили таксономію атак та оцінки ризиків для хмарних сервісів, що базується на ідентифікації, класифікації і пріоритетах.

Аналіз джерел показав, що найбільша увага приділяється аналізу, класифікації та побудові моделей загроз та порушника для хмари при цьому питання моделі загроз управління ключами та ключовими даним недостатньо розроблені.

В той же час нині застосування хмарних технологій користувачами, як показав аналіз, в суттєвій мірі залежить від довіри до управління ключовими даними в плані захисту від виявлених загроз.

3. Мета та задачі дослідження

Метою дослідження є аналіз стану безпечного управління ключовими даними та ключовою інформацією, обґрунтування та розробка моделі загроз компрометації ключів, а також обґрунтування, вибір та оцінка механізмів безпечного управління ключовою інформацією в хмарі.

Для досягнення поставленої мети в роботі вирішувалися наступні задачі:

– розробка моделі загроз відносно хмарних сервісів та управління ключовими даними;

– розробка моделі та профілю порушника хмарних сервісів та управління ключовими даними;

– вибір механізмів безпечного управління ключами;

– вибір методів оцінки ризиків для хмарних сервісів з використанням кількісних та якісних показників.

4. Матеріали та методи досліджень

4. 1. Вимоги до ключових даних в середовищі хмарних обчислень

Аналіз показав, що станом на сьогодні ряд закордонних держав підготували та опублікували низку стандартів та рекомендацій, в яких провідну роль відіграють США [7].

Хмарні обчислення – це модель забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню, наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів тощо. Вони можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера [11]. Основними моделями розгортання хмарних сервісів є такі: приватна, громадська, публічна та гібридна хмари. Ознакою такої класифікації є категорії користувачів, що мають доступ та можуть використовувати ресурс та дані хмари. При цьому постачальники хмарних ресурсів можуть надавати, а користувачі отримувати такі послуги, як [11]: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS).

Аналіз показує, що незалежно від моделі розгортання та обслуговування хмари, всі ключі, що використовуються в середовищі хмарних обчислень, можна поділити за призначенням та власником на такі два класи [6]:

– ключі, що використовуються провайдером хмарних послуг та є його власністю;

– ключі, що використовуються клієнтами провайдера хмарних послуг та є їх власністю.

Наприклад, якщо хмара розгорнута як публічна та надає послуги PaaS, то користувач хмари на основі сервісу, що надається провайдером, реалізує свої рішення, послугами якого користуються клієнти користувача. За цих умов користувач для своїх клієнтів буде виступати в якості провайдера хмарних послуг, а отже в цьому випадку будуть існувати також два класи ключів:

– клас ключів провайдера хмарних послуг, до якого відносяться ключі провайдера хмарних послуг публічної хмари, що надає послуги PaaS та ключі користувача хмари, по відношенню до клієнтів користувача;

– клас ключів користувача хмарних послуг, до якого відносяться по відношенню до провайдера хмарних послуг, ключі користувача хмарних послуг та ключі клієнтів користувача хмарних послуг.

Аналогічним чином можна виділити та показати існування лише двох класів ключів для інших моделей розгортання та надання послуг в хмарі [6]. Така модель хмари, у якій існує тільки дві ролі – користувач та провайдер, на відміну від моделі NIST, дозволяє зменшити складність аналізу безпеки управління ключами, включаючи крипто живучість. Це досягається за рахунок виключення ролі аудитора хмари, яка виступає в якості пасивного елементу хмари, та має доступ до хмари лише під час проведення аудиту з використанням строгого переліку доступних можливостей.

Вказане є справедливим і до посередника (брокера) хмарних послуг, який для провайдера хмарних послуг розглядається з точки зору клієнта, а для клієнта брокер є провайдером хмарних послуг. Теж саме можна прийняти і до транспортувальника хмарних послуг – в моделі безпеки його головною задачею повинно бути забезпечення доступності сервісів, забезпечення конфіденційність та цілісність даних, що передаються забезпечується тільки користувачем та провайдером хмарних послуг.

Ґрунтуючись на наведеному, розглянемо модель порушника хмарних обчислень, на основі якої побудуємо модель загроз відносно управління ключовими даними.

4. 2. Модель порушника ІТС хмарних обчислень

Побудові моделей порушника та загроз відносно хмарних сервісів присвячено ряд робіт [2–4]. При їх побудові застосовується методика, що ґрунтується спочатку на побудові моделі порушника, виявленні усіх можливих загроз та визначенні способів їх реалізації, а на останок – побудові моделі загроз. Побудовані моделі порушника та загроз дозволяють сформулювати вимоги до системи захисту інформації в середовищі хмарних обчислень.

Орієнтуючись на [3], під моделлю порушника будемо розуміти абстрактний формалізований чи неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії тощо.

Складність побудови моделі порушника для інформаційно-телекомунікаційної системи (ІТС) хмарних обчислень полягає в необхідності врахування моделі розгортання хмари, моделі надання послуг, власника та рівень контролю інформації, а також рівень контролю провайдера та користувачів над інфраструктурою хмари [3]. Також така модель має бути ще адекватною реальному порушнику.

Аналіз моделі хмари NIST (рис. 1) показує, що по відношенню до ІТС хмари порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи). Особливу небезпеку в середовищі хмарних обчислень становлять внутрішні порушники. Навіть при наданні послуг на рівні IaaS [3], внутрішня інфраструктура хмари, в тому числі і середовище передачі даних, контролюється провайдером хмарних послуг.

На рис. 2 наведена розроблена на основі рис. 1 модель порушника.

В табл. 1 наведено запропонований відносно хмарних сервісів на основі [3] та рис. 1 профіль порушника. Він включає такі основні категорії, як: категорія осіб; характер дій; рівень доступу та можливостей; рівень ознайомленості; методи та засоби, що використовуються, та мету дій.

На основі наведеного відносно хмарних сервісів профілю порушника розроблено та запропоновано модель загроз (рис. 2), у якій у формалізованій формі також міститься модель порушника. У ній формалізація зроблена на основі даних табл. 1.

В табл. 2 наведено запропонований основний перелік загроз для середовища хмари, модель якої наведено на рис. 1, та порушника, профіль якого наведено в табл. 1.

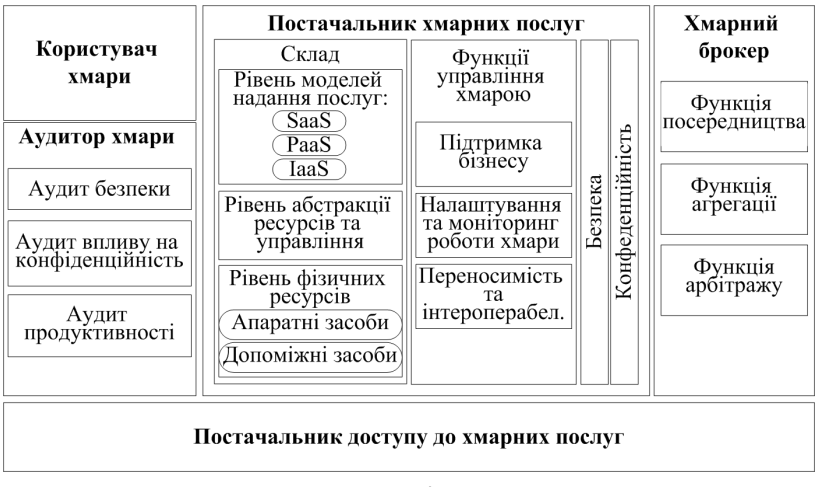

Рис. 1. Модель хмарних обчислень (сервісів) NIST

Наведена на рис. 1 модель визначає:

– категорії осіб, з числа яких може бути порушник;

– припущення про рівень можливостей, кваліфікацію, рівень ознайомлення з системою, характер дій порушника;

– методи та засоби, що може використовувати порушник;

– мета, яку перед собою ставить порушник;

– елементи системи, які порушник буде атакувати.

За категорією осіб порушниками можуть бути [2]:

– внутрішні порушники: працівники провайдера хмарних послуг, працівники користувача, сторонні особи, що отримують доступ до ресурсів ІТС хмари. Для їх визначення слід детально розглянути можливості несанкціонованого доступу до ресурсів ІТС кожного із працівників провайдера та користувача, а також можливості сторонніх осіб щодо несанкціонованого доступу до ресурсів ІТС з урахуванням наявної системи організаційного обмеження їх доступу;

– зовнішні порушники: інші особи, що не мають безпосереднього доступу до ресурсів ІТС хмари. Для їх визначення слід детально розглянути можливі канали витоку інформації та вразливі місця системи.

За рівнем можливостей порушників, згідно [2], розділимо на чотири класи:

– перший рівень припускає можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням ІТС хмари, тобто впливом на базове програмне забезпечення системи, на склад і конфігурацію її устаткування;

– четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів ІТС хмари, з можливістю включення до складу ІТС хмари власних засобів з новими функціями обробки інформації.

Таблиця 1

Профіль порушника відносно хмарних сервісів

№	Категорія	Значення (Позначення)
1	Категорія осіб	внутрішній (В)
		зовнішній (З)
2	Характер дій	випадковий (В)
		пасивний (П)
		активний (А)
3	Рівень доступу та можливостей	перший рівень (1)
		другий рівень (2)
		третій рівень (3)
		четвертий рівень (4)
4	Рівень ознайомленості	користувач (К)
		спеціаліст (С)
		адміністратор системи (А)
		спеціаліст з найвищим рівнем знань (Н)
		адміністратор безпеки (Б)
5	Методи та засоби	агентурні (Р)
		штатні (Ш)
		пасивні (П)
		активні (А)
6	Мета дій порушника	отримання атрибутів доступу персоналу чи користувачів АС (О)
		отримання несанкціонованого доступу до обчислювальних ресурсів хмари (НСД)
		проникнення на територію хмарного ЦОД з метою впливу на фізичне обладнання (ВФ)
		зміна режимів функціонування чи виводу з ладу фізичних ресурсів АС (М)
		встановлення засобів технічної розвідки (ТР)
		встановлення технічних засобів нав'язування (ТЗН)
		встановлення програмних закладок розвідки (ПЗР)
		встановлення програмних засобів нав'язування (ПЗН)

За рівнем ознайомлення з системою, порушників будемо класифікувати за такими рівнями, як [2, 11]:

– що не володіють спеціальними знаннями з обчислювальної техніки та програмування, проектування та експлуатації хмарної ІТС, а є лише користувачами сервісу;

– що володіють базовим або високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації хмарних ІТС, а також базовим або високим рівнем знать про системи захисту хмарних ІТС;

– що володіють інформацією про функціональні особливості визначеної ІТС хмари, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– що володіють високим рівнем знань та досвідом роботи з технічними засобами системи хмари та їхнього обслуговування;

– що володіють інформацією про функції та механізм дії засобів захисту в визначеній ІТС хмари.

Аналіз показує, що незалежно від моделі розгортання хмари та моделі надання послуг найнебезпечнішими порушниками в ІТС хмари є адміністратори хмари та адміністратори безпеки хмари. Порушення з боку цих осіб можуть бути як ненавмисними, так і зловмисними. При цьому якщо «випадковий порушник» здійснює загрози ІТС під час виконання своїх функціональних обов'язків внаслідок помилкових дій, за рахунок неуважності чи недбалості, то порушник, що здійснює зловмисне порушення, чітко розуміє свої дії та має змогу проаналізувати їх вплив. Також необхідно брати до уваги, що порушник в середовищі хмари може здійснювати активні чи пасивні загрози ресурсам ІТС чи АС. Під активною загрозою слід розуміти навмисні та не навмисні несанкціоновані дії порушника, що призвели до зміни стану ІТС (АС), а під пасивною загрозою – дії, що призвели до несанкціонованого проникнення в систему без зміни її стану.

За характером дій порушників можна класифікувати на [2, 3]:

– «випадковий порушник» – це користувачі, обслуговуючий персонал, які не навмисно подолали засоби управління (адміністрування) доступом до об'єкту захисту, виконали непередбачені дії відносно цього об'єкту, чим спричинили порушення політики безпеки до об'єкта захисту;

– «пасивний порушник» – авторизований користувач, або обслуговуючий персонал хмари, який навмисно порушив політику безпеки послуги, але не вживає рішучих дій. З метою прихованого подолання засобів управління (адміністрування), використовує атрибути доступу інших користувачів;

– «активний порушник» – порушник, який не приховує своїх дій та може використовувати всі доступні методи та засоби для порушення властивості захищеної інформації. До таких дій відносяться дії, що спрямовані на подолання організаційного обмеження доступу, охоронної сигналізації, управління доступом до фізичних ресурсів, фізичний доступ до засобів оброблення, зберігання чи передавання інформаційних об'єктів з метою виведення їх з ладу, зміни режимів функціонування, крадіжки чи пошкодження носіїв тощо;

– «віддалений порушник» – порушник, що використовує засоби віддаленого доступу до інформаційних об'єктів: виток інформації технічними каналами, спеціальний вплив на інформацію по технічним каналам, мережне обладнання локальних чи розподілених мереж, в тому числі і засоби телекомунікаційних мереж.

За методами та засобами, що використовує порушники, їх можна класифікувати як таких, що використовують [2, 3]:

– виключно агентурні методи одержання відомостей;

– пасивні технічні засоби перехоплення інформаційних сигналів;

– для реалізації спроб НСД виключно штатні засоби АС або недоліки проектування КСЗІ;

– способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

Також при подальших дослідженнях будемо вважати, що метою зловмисника, при здійсненні порушення, може бути наступне [1–3]:

– авторизація та отриманні атрибутів доступу з найбільшими правами до ресурсів ІТС з метою їх використання для ознайомлення з конфіденційною інформацією, її модифікації чи знищення, використання обчислювальних ресурсів хмари в своїх власних цілях;

– пошук та/або здобуття атрибутів доступу особи з персоналу чи користувачів АС, які мають атрибути доступу з найбільшими правами, з метою заволодіння їх атрибутами доступу. Здобуття атрибутів особи може бути реалізовано шляхом використання технічних засобів, крадіжок, купівлі, чи отримання іншим шляхом;

– проникнення на місця розміщення тих чи інших компонентів, елементів чи ресурсів АС (обчислювальних ресурсів, інформаційних ресурсів, базового, прикладного програмного забезпечення та програмного забезпечення системи ТЗІ, включаючи носії резервних копії, ресурсів вводу/виводу, телекомунікаційного обладнання, включаючи мережу передачі даних) шляхом подолання перешкод (огорожі, елементів будівельних конструкцій, охорони чи охоронної сигналізації та ін.) та нанесення збитків шляхом знищення матеріальних та інформаційних цінностей;

– зміна режимів функціонування чи виводу з ладу ресурсів АС;

– установка фізичних засобів (апаратурних закладок) чи інших засобів технічної розвідки в місцях розміщення елементів АС (в тому числі і віддалених, наприклад в елементах комунікаційної мережі зв'язку) для знімання інформації;

– установка фізичних чи інших засобів (апаратурних закладок) в місцях розміщення елементів АС (в тому числі і віддалених, наприклад, в елементах комунікаційної мережі зв'язку) для генерації несправжніх сигналів, інформаційних символів чи повідомлень;

– установка програмних засобів (програмних закладок) знімання інформації з метою її того чи іншого використання;

– установка програмних засобів (програмних закладок чи вірусів) для модифікації як програмних засобів, так і інформації АС, шляхом генерації (впровадження) програмних вірусів, несправжніх сигналів, інформаційних символів чи повідомлень з метою перевантаження систем АС і порушення, таким чином, доступності компонентів АС чи АС в цілому;

– здійснення спроб несанкціонованого доступу до обчислювальних ресурсів, інформаційних ресурсів, базового та прикладного програмного забезпечення та програмного забезпечення системи ТЗІ як власне АС, так і її телекомунікаційної підсистеми шляхом подолання системи управління доступом.

Важливим також є визначення та використання в моделі того, яким чином загрози можуть бути реалізовані при хмарних обчисленнях. Грунтуючись на [3, 11], будемо вважати, що вони реалізуються наступними способами:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, віброакустичні, акустоелектричні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів, як на стороні користувача так і провайдера хмарних послуг.

4. 3. Модель загроз відносно хмарних сервісів

Наведені вище в п. 4. 2 потенційні можливості порушника дозволили розробити модель загроз відносно хмарних сервісів (обчислень). Детально опис такої моделі загроз наведена в табл. 2. В ній на основі рис. 2 вказується об'єкт, для якого реалізується загроза, мета порушника, ймовірність загрози та мета здійснення захисту.

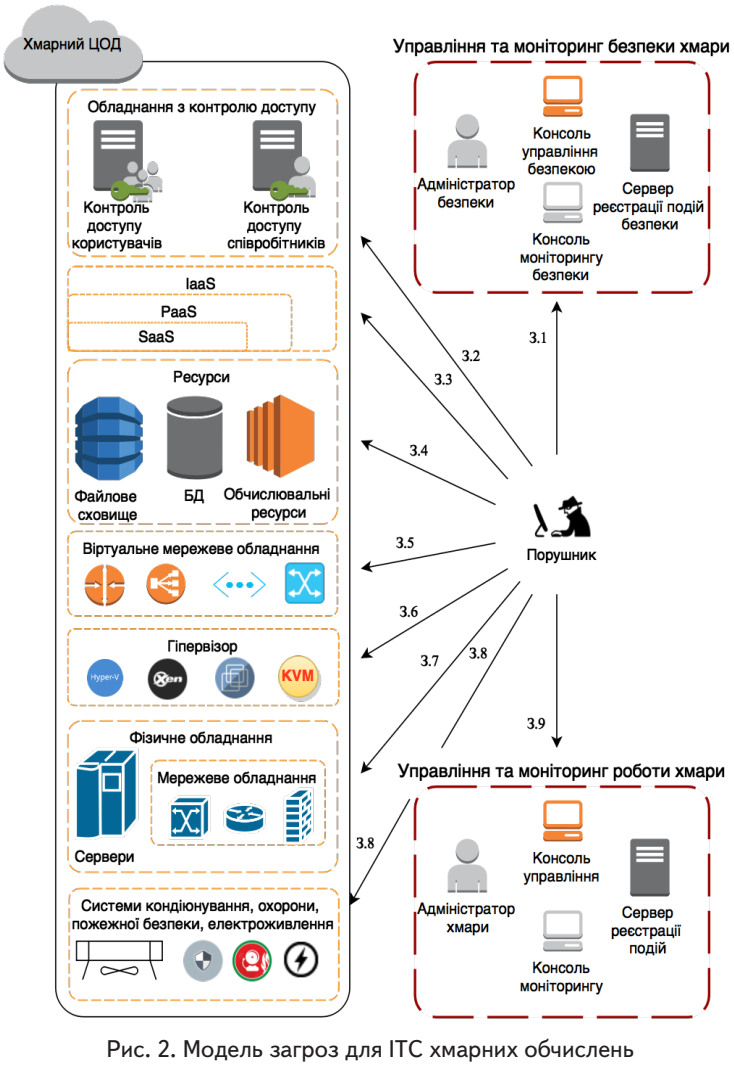

Рис. 2. Модель загроз для ІТС хмарних обчислень

Таблиця 2

Загрози в середовищі хмари

Загроза	Об'єкт для якого реалізується загроза	Мета	Ймовірність загрози	Методи захисту
З.1	Управління та моніторинг безпеки хмари	Отримання несанкціонованого доступу до хмари	низька	Використання систем з контролю доступу, політики безпеки, атестація персоналу
З.2	Обладнання з контролю доступу	Отримання несанкціонованого доступу до хмарних ресурсів чи управління хмарою	висока	Використання захищених носіїв ключа для автентифікації
З.3	Середовище хмари: сервіси, додатки та інфраструктура	Порушення сервісами, додатками та об'єктами інфраструктури прав доступу. Несанкціонований доступ до функцій управління інфраструктурою, даних сервісів та додатків користувача хмари. Зараження шпигунським ПЗ та вірусами	висока	Використання технологій розмежування та обмеження доступу, контроль над цілісністю об'єктів та їх моніторинг
З.4	Ресурси хмари	Отримання несанкціонованого доступу до файлів, записів БД або використання обчислювальних ресурсів	висока	Впровадження механізмів обмеження доступу, шифрування даних, моніторинг роботи
З.5	Віртуальні мережі в межах хмарної інфраструктури	Прослуховування трафіку, порушення цілісності, доступності, організація атак DDoS, несанкціоноване підключення до мережі	висока	Використання засобів захисту даних в мережі, систем виявлення та протидії мережевим атакам, моніторинг роботи
З.6	Гіпервізор	Повний контроль над розгорнутим віртуальним середовищем	низька	Захист гіпервізора та контроль доступу до його налаштувань
З.7	Фізичне обладнання	Встановлення засобів несанкціонованого доступу, модифікації та знищення інформації. Порушення доступності ЦОД	низька	Використання систем контролю доступу, політики безпеки, атестація персоналу. Встановлення контрольованої зони
З.8	Допоміжні системи (живлення, охорони, безпеки, охолодження)		низька	
З.9	Управління та моніторинг роботи хмари	Отримання несанкціонованого доступу до налаштувань хмари	середня	Використання технологій розмежування та обмеження доступу, моніторинг дій адміністраторів
З.10	Зв'язки між хмарними ЦОД	Порушення доступності ЦОД, отримання несанкціонованого доступу до інформації, що передається мережею	низька	Використання надійних протоколів з стійкими криптограф. алгоритмами

Класифікація загроз за ймовірністю була проведена з урахуванням рекомендацій [1]. Згідно цих рекомендацій, найбільшу ймовірність мають загрози, що здійснюються на компоненти хмарної інфраструктури, які мають інтерфейси доступу з зовні та/або знаходяться в віртуалізованому середовищі.

Аналіз моделі загроз, зображеної на рис. 2, показав, що найбільшу небезпеку становлять загрози управління хмарою (З.9) та її безпекою (З.1), а також загрози гіпервізору (З.6).

5. Результати досліджень моделі загроз та порушника відносно ключів

5. 1. Модель загроз відносно ключів та ключової інформації

На основі розроблених моделей хмарних обчислень, порушника та загроз ІТС хмарних обчислень(сервісів) з суттєвим урахуванням [2–4, 6] визначено, що найбільш проблемними з точки зору перекриття є загрози відносно ключів та ключової інформації.

На рис. 3 наведено визначений в процесі досліджень та даних табл. 1, 2, а також рис. 1, 2, перелік загроз ключовим даним (ключам), які необхідно застосовувати для криптографічного захисту інформації в процесі хмарних обчислень. Детально опис моделі загроз наведений в табл. 3.

Враховуючи в аналізі наведенні дані в роботі [6], приймемо що в середовищі хмари відносно ключових даних можуть існувати та реалізовуватись зі сторони порушника такі загрози:

– компрометація ключів та ключової інформації;

– несанкціоноване знищення ключів та ключової інформації;

– перехоплення та запам'ятовування ключів та ключової інформації;

– нав'язування помилкових або хибних ключів та ключової інформації;

– нав'язування слабких ключів або напів слабких ключів;

– підміна ключів або ключової інформації;

– отримання несанкціонованого доступу до ключів чи ключової інформації;

– отримання можливості несанкціонованого використання ключів тощо.

Зважаючи на пропозиції та визнані критерії, що наведені в [1, 3, 6], приймемо в якості основного критерію ймовірність реалізації загрози. Також приймемо, що вона може оцінюватись як: низька, середня та висока.

Таблиця 3

Загрози ключам в середовищі хмари

Загроза	Об'єкт для якого реалізується загроза	Мета	Ймовірність загрози	Методи захисту
З.1	Користувач	Компрометація, знищення, отримання несанкціонованого доступу чи несанкціоноване використання ключів	висока	Використання захищених носіїв ключа
З.2	Канал зв'язку між користувачем та хмарою	Перехоплення, нав'язування, підміна ключів	висока	Використання захищеного каналу зв'язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються
З.3	Сервіс ідентифікації, автентифікації, авторизації та керування правами доступу	Отримання несанкціонованого доступу до ключів; Отримання можливості несанкціонованого використання ключів.	висока	Використання надійних протоколів автентифікації з стійкими криптографічними алгоритмами. Використання багатофакторної автентифікації
З.4	Хмарне середовище: сервіси додатки, інфраструктура	Компрометація, знищення, підміна, нав'язування, отримання несанкціонованого доступу чи несанкціоноване використання ключів	висока	Використання HSM для здійснення криптографічних операцій
З.5	Криптографічний сервіс	Компрометація, знищення, підміна, нав'язування, отримання несанкціонованого доступу чи несанкціоноване використання ключів	середня	Використання HSM для здійснення криптографічних операцій
З.6	Адміністратор ЦОД та адміністратор безпеки	Компрометація, отримання несанкціонованого доступу чи несанкціоноване використання ключів адміністраторів з метою отримання вищих повноважень в системі	низька	Використання захищених носіїв ключа
З.7	Канал зв'язку між відокремленими хмарними ЦОД	Перехоплення, нав'язування, підміна ключів	середня	Використання захищеного каналу зв'язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються
З.8	Менеджер ключів користувачів	Компрометація, знищення, підміна, нав'язування, отримання несанкціонованого доступу чи несанкціоноване використання ключів	середня	Використання надійного сервісу автентифікації
З.9	Засоби зберігання ключів	Компрометація, знищення, підміна, отримання несанкціонованого доступу до ключів	низька-середня	Використання захищених апаратних модулів зберігання ключів та/або HSM
З.10	Канал зв'язку між хмарним ЦОД та ЦСК	Перехоплення, нав'язування, підміна ключів та результатів перевірки ключів	низька	Використання надійних протоколів з стійкими криптографічними алгоритмами
З.11	ЦСК	Компрометація, отримання несанкціонованого доступу чи несанкціоноване використання ключів з метою компрометації сервісів, що надаються ЦСК	низька	Створення КСЗІ для ЦСК, проходження експертизи та відповідність державним та міжнародним стандартам

На основі аналізу переліку загроз та моделі загроз ключовим даним можна зробити висновки про те, що порушник може з високою ймовірністю здійснювати:

– компрометацію, знищення, отримання несанкціонованого доступу чи несанкціоноване використання ключів відносно користувача;

– перехоплення, нав'язування та підміну ключів через канали зв'язку між користувачем та хмарою;

– отримання несанкціонованого доступу до ключів через сервіси ідентифікації, автентифікації, авторизації та керування правами доступу;

– отримання несанкціонованого доступу чи несанкціоноване використання ключів через хмарне середовище – сервісів додатків та, інфраструктуру;

– найбільшу небезпеку в середовищі хмарних обчислень для ключових даних користувача представляють адміністратори хмарних сервісів, які мають

доступ до середовища в якому розгорнуто хмарні додатки користувача.

Для захисту від вказаних загроз на рівні користувача необхідно використовувати захищені з необхідним рівнем носії ключів.

На рівні каналів зв'язку між користувачем та хмарою використовувати захищені канали зв'язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються.

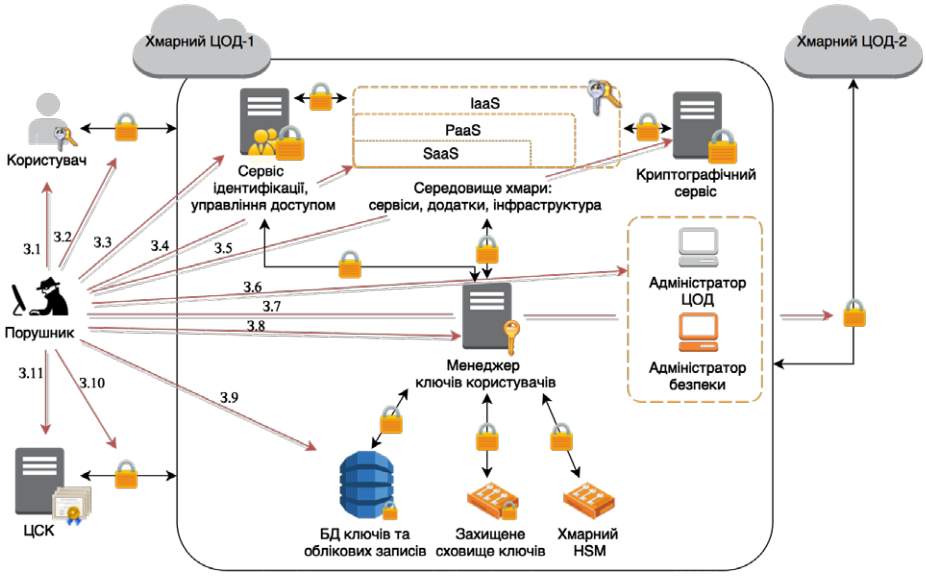

Рис. 3. Загрози ключам в середовищі хмари

На рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом використовувати надійні протоколи автентифікації з стійкими криптографічними алгоритмами, також методи багатофакторної автентифікації.

На рівні хмарного середовища, тобто сервісів додатків та інфраструктури – використовувати для здійснення криптографічних операцій захищені відповідним чином криптографічні модулі – HSM.

Також на основі табл. 3 можна визначити методи та механізми криптографічного та іншого захисту в середовищі хмарних обчислень для середнього та низького рівнів ймовірностей реалізації загроз.

5. 2. Оцінки ризиків та потенційних втрат за рахунок ключових даних

Під час розробки комплексної системи захисту для хмари, в процесі аналізу моделі загроз виникає необхідність отримати значення ризику виникнення загроз з метою використання найбільш оптимальних методів захисту, а також оцінки використаних методів в побудованій системі.

В загальному випадку існує два показники, які отримують в процесі аналізу ризиків: якісний та кількісний.

За визначення стандарту ISO/IEC 27005 під ризиком розуміється вплив невизначеності на цілі, що характеризується комбінацією ймовірності подій та їх наслідків. Значення ризику R може бути задано наступним виразом:

$$R = P_i \cdot C_j, \quad (1)$$

де P_i – ймовірність успішної реалізації і-й загрози, C_j – оцінка збитку викликаного впливом інциденту ІБ на активи при успішній реалізації і-й загрози.

Під загрозою розуміється будь-які обставини або події, що виникають у середовищі хмарних обчислень, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі.

Стандарт ISO/IEC 31010 описує основні методи з оцінки ризиків, сферу їх застосування та можливості, вхідні та вихідні дані, а також переваги та недоліки цих методів.

На сьогодні існує декілька методологій та підходів по оцінці ризиків. В першу чергу оцінка ризиків може бути виконана використовуючи кількісний (ISAMM, Mehari), якісний (EBIOS, Octave, IT-Grundshutz) або змішаний підхід (CRAMM, MEGERIT). Кількісні методи використовують вимірні, об'єктивні дані для визначення вартості активів, імовірність втрати і пов'язаних з ними ризиків. В ході оцінки з використанням кількісного підходу обчислюються числові значення для кожного з компонентів, зібраних в ході оцінки ризиків та аналізу витрат і переваг. В свою чергу, якісні методи ґрунтуються на використанні відносного показнику ризику або вартості активу на основі рейтингу або поділу на категорії, такі як низький, середній, високий, не важливо, важливо, дуже важливо, чи за шкалою від 1 до 10. Якісна модель дозволяє оцінити дії й імовірності виявлених ризиків більш швидким та дешевшим способом порівняно з кількісним. Якщо вимагається більш детальний та точний аналіз на основі окремих отриманих якісних оцінок можна провести кількісний аналіз. Такий аналіз з комбінації якісного та кількісного підходів являє собою змішаний підхід з сукупністю переваг і недоліків вище згаданих методів.

Окремих стандартів, що описують аналіз ризиків ключових систем в хмарі станом на 2015 не існує, але в якості керуючих документів по аналізу ризиків в середовищі хмарних обчислень можуть бути застосовані наступні стандарти: ISO 27001, ISO 27005, ISO 17799. В цих стандартах теоретично описуються і даються методичні вказівки процесу оцінки ризиків, в тому числі і для ключових систем. В наведених стандартах не визначено та не дається конкретних технологій з проведення оцінок, тому в якості інструментів для проведення аналізу можуть бути використані різні програмні додатки, наприклад такі як Cobra (Великобританія), RiskWatch (США), ГРИФ (Росія).

Окрім зазначених вище стандартів існує публікація NIST NISTIR 7956, що розглядає питання та проблеми управління ключами в хмарних сервісах.

Низка закордонних та вітчизняних публікацій [8–10] відзначають наступні особливості при проведенні оцінки ризиків хмарних обчислень:

– загалом існуючи підходи до оцінки ризиків можуть бути використанні в середовищі хмарних обчислень, за умови урахування особливостей функціонування та інфраструктури хмари;

– розробка та використання методів оцінки повинна будуватися на принципах адаптивності, тобто враховувати принцип невизначеності складу хмарної інфраструктури та можливості її динамічної зміни;

– невизначеність та динамічна зміна конфігурації хмари потребує методик з поточного аналізу вразливостей хмари;

– суттєвим недоліком існуючих методик є ускладнене отримання прогнозів про стан середовища хмарних обчислень, що в умовах високої невизначеності є важливим фактором, в результаті знижується загальний рівень захищеності хмарної ІТС;

– також недоліком існуючих методик є складність їх застосування до каналів НСД в хмарі, через їх відмінність для кожної з реалізації моделі хмарних обчислень;

– наявність можливості користувачами використання своїх власних пристроїв для взаємодії з середовищем хмари призводить до розмиття поняття контрольована зона;

– при проведенні аналізу ризиків у хмарній ІТС, відповідно до традиційних підходів, часто відсутня можливість отримання будь-яких кількісних експертних оцінок про ймовірність реалізації загроз, через незнання географії, умов функціонування та рівня захищеності ресурсів.

Задачу вибору методу з аналізу ризиків в середовищі хмари ускладнюють такі особливості хмарного середовища, як: розподілена складна архітектура, наявність адміністраторів, які контролюють обслуговуюче обладнання та розгорнуту інфраструктуру, конфігурація системи, що складається з різних вузлів та може динамічно змінюватися, відсутність контролю середовища користувачами тощо. Керуючись зазначеними вище особливостями середовища хмари, а також відсутністю статистичних даних з реалізації загроз, з широкого кола методів було обрано два, що найбільш повно дозволяють провести аналіз та отримати оцінки з ризиків інформаційної безпеки в хмарному середовищі.

В якості методів, що дозволяють провести аналіз та класифікацію загроз, пропонується використовувати метод попереднього аналізу небезпек (PHA), що дозволяє провести аналіз на попередніх стадіях проектування з недостатньою кількістю інформації, ранжування небезпек та ризику або метод CHAZOP, який виконує всебічний та систематичний аналіз на завершальному етапі розробки системи або коли вона вже побудована. По причині складності використання методу CHAZOP його доцільно застосовувати тільки у випадках, коли необхідно виконати повний аналіз системи. В якості кількісного методу оцінки ризиків пропонується до застосування використання байесовського підходу, який дозволяє отримати апостеріорну ймовірність на основі апріорних ймовірностей, при цьому є можливість уточнення результатів при отриманні нових даних, що важливо при динамічній зміні кількості вузлів в системі та її архітектури [9].

6. Обговорення результатів досліджень моделі загроз та порушника відносно ключів

Запропоновані на основі аналізу сучасного стану стандартизації та застосування хмарних сервісів моделі хмарних обчислень, порушника та загроз ІТС хмарних сервісів дозволили встановити, що найбільш проблемними та такими, що вимагають вирішення в частині надання послуг конфіденційності, цілісності, справжності та доступності тощо, є задачі захисту ключів та ключової інформації. Для цього на основі аналізу стану встановлено, що в середовищі хмари відносно ключових даних існують та можуть бути реалізованими такі загрози як компрометація, несанкціоноване знищення, перехоплення та запам'ятовування, нав'язування слабких та несанкціоноване використання тощо ключів. При цьому встановлено, що найбільшу небезпеку в середовищі хмарних обчислень для ключових даних користувача представляють адміністратори хмарних сервісів, які мають доступ до середовища, в якому розгорнуто хмарні додатки користувача.

Також на основі детального аналізу стану та вимог відносно безпечності управління ключами зі сторони нормативно-правових документі та стандартів, включаючи проекти, обґрунтовані механізми захисту конфіденційних, особистих та відкритих ключів користувача від виявленої множини загроз. Вони зводяться до використання для забезпечення високого рівня безпеки, тобто високого рівня ймовірностей реалізації загроз в середовищі хмарних обчислень, комплексу технічних, організаційних та організаційно-технічних заходів та засобів, в тому числі до використання:

– на рівні користувача захищених з необхідним рівнем безпеки ключових носіїв;

– на рівні каналів зв'язку між користувачем та хмарою захищених каналів зв'язку з взаємною автентифікацією сторін та стійкістю вищою за стійкість ключів, що передаються;

– на рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом надійних протоколів автентифікації з стійкими криптографічними алгоритмами, а також методів багатофакторної автентифікації;

– для здійснення криптографічних операцій на рівні сервісів додатків та інфраструктури захищених відповідним чином модулів криптографічного захисту – HSM.

Необхідно відмітити, що наведені в табл. 3 дозволяють визначити методи та механізми криптографічного захисту і для середнього та низького рівнів безпеки (ймовірностей реалізації загроз) в середовищі хмарних обчислень.

При дослідженнях та аналізі загроз рекомендується використовувати метод попереднього аналізу небезпек (PHA). Він дозволяє провести аналіз на попередніх стадіях проектування, з недостатньою кількістю інформації, зробити ранжування небезпек та ризику. Також можна використовувати метод CHAZOP, якщо хмарному середовищу властиві такі особливості як розподілена складна архітектура, що складається з різних вузлів, наявність адміністраторів з високими можливостями щодо контролю над обслуговуючим обладнанням та розгорнутою інфраструктурою, кон-

фігурація системи та розгорнутої інфраструктури, що змінюється динамічно, відсутність контролю середовища користувачами, відсутність статистичних даних з реалізації загроз тощо. Але у зв'язку зі складності використання методу CHAZOP доцільно застосовувати тільки у випадках, коли необхідно виконати повний аналіз системи.

Для кількісної оцінки ризиків пропонується [9] використовувати байесовський підхід, який дозволяє отримати апостеріорну ймовірність на основі апріорних ймовірностей. При цьому є можливість уточнення результатів при отриманні нових даних, що важливо при динамічній зміні кількості вузлів в системі та її архітектури.

7. Висновки

1. Розроблена модель загроз хмарних сервісі дозволяє зробити висновок про те, що найбільшу ймовірність реалізації мають загрози, що здійснюються на компоненти хмарної інфраструктури, які мають інтерфейси доступу з зовні та/або знаходяться в віртуалізованому середовищі. С точки зору найбільшої небезпеки та найбільших втрат системи у разі реалізації загроз слід виділити згідно рис. 2 загрози управління хмарою (З.9) та її безпекою З.1, а також загрози гіпервізору (З.6).

2. Визначений в результаті аналізу перелік загроз та розроблена модель загроз ключовим даним дозволили зробити висновки про те, що порушник з високою ймовірністю може реалізовувати ряд наведених в підрозділі 5. 1. загроз, але найбільша небезпеку в середовищі хмарних обчислень для ключових даних користувача виникає при використанні їх в середині розгорнутою інфраструктури, без застосування криптографічних сервісів та HSM.

3. Розроблений профіль порушника, що включає категорію осіб, характер дій, рівень доступу та можливостей, рівень ознайомленості, методи та засоби, що використовуються та мету дій порушника. Його використання дозволяє формалізувати процес побудування моделі загроз хмари та аналіз можливостей порушника.

4. Результати аналізу моделі загроз ключовим даним дозволили запропонувати методи та механізми захисту, дані відносно яких наведені в табл. 3. До основних механізмів можна віднести використанням захищених сховищ ключів для безпечного зберігання ключів, та криптографічних сервісів та хмарних HSM для безпечного використання ключів в хмарі.

5. Проведені результати досліджень дозволили з урахуванням особливостей функціонування хмар обрати методи оцінки ризиків згідно стандарту ISO/IEC 31010, за рахунок яких досягається найбільша повнота та якість проведення оцінки.

Література

1. Haeberlen, T. Cloud Computing Benefits, risks and recommendations for information security [Electronic resource] / T. Haeberlen, L. Dupré // Available at: https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/at_download/file
2. Jansen, W. Cloud Hooks: Security and Privacy Issues in Cloud Computing [Text] / W. Jansen // 44th Hawaii International Conference on System Sciences (HICSS) – 2011. – P. 1–10. doi: 10.1109/hicss.2011.103
3. Jansen, W. Guidelines on Security and Privacy in Public Cloud Computing. [Electronic resource] / W. Jansen, F. Grance, J. Mao, R. Bohn, J. Messina, L. Badger, D. Leaf // Available at: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
4. Hashizume, K. An analysis of security issues for cloud computing [Text] / K. Hashizume, D. Rosado, E. Fernández-Medina, E. Fernandez // Journal of Internet Services and Application – 2013. – Vol. 4, Issue 5. – P. 15–28. doi: 10.1186/1869-0238-4-5
5. Chandramouli, R. Analysis of Protection Options for Virtualized Infrastructures in Infrastructure as a Service Cloud [Text] / R. Chandramouli // Fifth International Conference on Cloud Computing, GRIDs, and Virtualization, Venice, Italy, 2014. – P. 37–43.
6. Chandramouli, R. NIST Cryptographic Key Management Issues & Challenges in Cloud Services [Electronic resource] / R. Chandramoli, S. Chokhani, M. Iorga. – National Institute of Standards and Technology, 2013. – 31 p. doi: 10.6028/nist.ir.7956
7. Luna, J. Leveraging the Potential of Cloud Security Service-Level Agreements through Standards [Text] / J. Luna, N. Suri, M. Iorga and A. Karmel // IEEE Cloud Computing. – 2015. – Vol. 2, Issue 3. – P. 32–40. doi: 10.1109/mcc.2015.52
8. Choo, K. A Cloud Security Risk-Management Strategy [Text] / K. Choo // IEEE Cloud Computing. – 2014. – Vol. 1, Issue 2. – P. 52-56. doi: 0.1109/mcc.2014.27
9. Зикратов, И. А. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода [Текст] / И. А. Зикратов, С. В. Одегов // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 121–126.
10. Juliadotter, N. Cloud Attack and Risk Assessment Taxonomy [Text] / N. Juliadotter, K. Choo // IEEE Cloud Computing. – 2015. – Vol. 1, Issue 2. – P. 14-20. doi: 10.1109/mcc.2015.2
11. Аулов, І. Ф. Аналіз формальної модели безпеки хмари NIST [Текст]: Всеукр. межвед. науч.-техн. сб. / І. Ф. Аулов, І. Д. Горбенко // Радиотехника. – 2014. – Вып. 176. – С. 131–137.