

УДК 37.091.33:004.031.42(045)

DOI: 10.31891/2219-9365-2019-63-1-68-73

МУЛЯР І. В.,

СІВАК А. С.

Хмельницький національний університет

МЕТОД НАДАННЯ ДОСТУПУ ДО СЕРВІСІВ ОДНОРАНГОВОЇ РОЗПОДІЛЕНОЇ ХМАРНОЇ СИСТЕМИ

У статті розкрито актуальність проблеми надання доступу до сервісів розподіленої хмарної системи, зокрема, охарактеризовано однорангову розподілену хмарну систему. Надано процес взаємодії основних компонентів для отримання доступу до веб-ресурсу з доменним ім'ям. Досліджено, що розподіл ресурсів між вузлами однорангової розподіленої хмарної системи з подальшим наданням сервісів за запитом реалізується за допомогою протоколу Kademlia в локальній мережі або мережі Інтернет і містить процеси публікації ресурсу на початковій стадії його власником, реплікації і безпосередньо надання доступу до ресурсів. Обґрунтовано метод надання доступу до сервісів розподіленої хмарної системи. Визначено, що для пошуку вузла реплікації, який має репліку запитуваного ресурсу або його частину, застосовується інфраструктура розподілених хеш-таблиць (Distributed Hash Table, DHT). У дослідженні визначено етапи валідації ідентифікатора вузла. Описано процеси додавання нового вузла, валідації автентичності, публікації ресурсу й отримання доступу до ресурсу надано у вигляді поетапної послідовності дій у межах методу надання доступу до сервісів розподіленої хмарної системи за допомогою графічного опису інформаційних потоків, взаємодії процесів оброблення інформації та об'єктів.

Ключові слова: метод, хмарна система, хеш-таблиці.

MULYAR I.,

SIVAK A.

Khmelnytskyi National University

METHOD OF PROVIDING ACCESS TO SERVICES, PEER TO PEER DISTRIBUTED CLOUD SYSTEM

In the article the urgency of the problem of granting access to services of distributed cloud system is disclosed, in particular, the peer distributed cloud system is characterized. The process of interaction of the main components is provided to access the domain name web resource. It is researched that the distribution of resources between nodes of a peer distributed cloud system with the subsequent provision of services on request is implemented using the Kademlia protocol on a local network or Internet and contains processes for publishing the resource at the initial stage of its owner, replication and directly providing access to resources. The method of granting access to the services of the distributed cloud system is substantiated. It is determined that the Distributed Hash Table (DHT) infrastructure is used to find a replication node that has a replica of the requested resource or part of it. The study identified the stages of identification of the node's validation. The process of adding a new node, validating authenticity, publishing a resource, and accessing a resource is described in the form of a step-by-step sequence of actions within the framework of the method of granting access to services of a distributed cloud system by graphical description of information flows, interaction of processes of information and objects processing.

Keywords: method, cloud system, hash tables.

Вступ. На сучасному етапі розвитку та реформування галузей суспільного буття досить актуальною є проблема надання доступу до сервісів розподіленої хмарної системи. Так, починаючи з 80-х років минулого століття з'являються кластерні системи [1], а на початку 90-х – Grid-комп'ютинг. Саме в цей час в наукових колах висловлюється думка щодо переваги використання розподілених архітектур для багатьох обчислювальних задач. Аналіз науково-технічної літератури дозволяє зазначити, що наступним кроком у розвитку комп'ютерних систем є впровадження хмарних технологій, завдяки яким розширилися можливості надання мережних, апаратних та програмних ресурсів на веб-серверах [2].

Поява хмарних технологій сприяла відмові від застосування децентралізованої архітектури як єдиної, а тому викликала значну кількість проблем: «велика вартість розгортання, високе енергоспоживання, значні прості й неефективне використання обладнання, зменшення продуктивності ресурсів зі збільшенням кількості користувачів, негативний вплив на навколишнє середовище».

Потужні трансформаторні підстанції, дизельні генератори, системи охолодження й резервні джерела живлення, які використовуються для підтримки працездатності хмарного центру обробки даних [4, 5] та мають істотний негативний вплив на навколишнє середовище. Крім того, підвищення популярності, затребуваності й кількості інформаційних інтернет-сервісів, а також збільшення кількості пристроїв і користувачів, для яких потрібно забезпечити доступність і гарантований час відгуку таких сервісів [3], призводить до того, що провайдери хмарних послуг змушені збільшувати потужності й кількість дата-центрів.

Варто зазначити, що для хмарних інфраструктур необхідно виконувати достовірне оцінювання, а також забезпечувати необхідний рівень доступності сервісів, одночасно з підвищенням енергоефективності [6], зменшенням споживання енергії й негативного впливу на навколишнє середовище [7].

Існуючі методи оцінювання й забезпечення готовності та доступності хмарних архітектур [8, 9, 10] дозволяють зробити висновок, що вони не надають можливості визначити фактичну доступність і продуктивність хмарних сервісів з використанням об'єктивних кількісних показників.

Ефективною, на нашу думку, буде модернізація інфраструктури хмарної системи шляхом усунення або розвантаження хмарних ЦОД, які є причиною споживання великої кількості енергії та виділення тепла і, як наслідок, негативного впливу на навколишнє середовище. Прикладом такої модернізації є перетворення хмарної архітектури на розподілений децентралізований тип, тобто коли кожен вузол надає виділену частину власних апаратних ресурсів у загальне користування.

Дослідження методу надання доступу до сервісів розподіленої хмарної системи. Доцільним буде розкрити сутність методу надання доступу до ресурсів розподіленої хмарної системи з необхідним рівнем якості обслуговування.

Ідея однорангової розподіленої хмарної системи (рис. 1) полягає в об'єднанні двох базових технологій: Grid-системи та Cloud (централізована клієнт-серверна система з підтримкою технології віртуалізації) за допомогою пірінгових мереж [11].

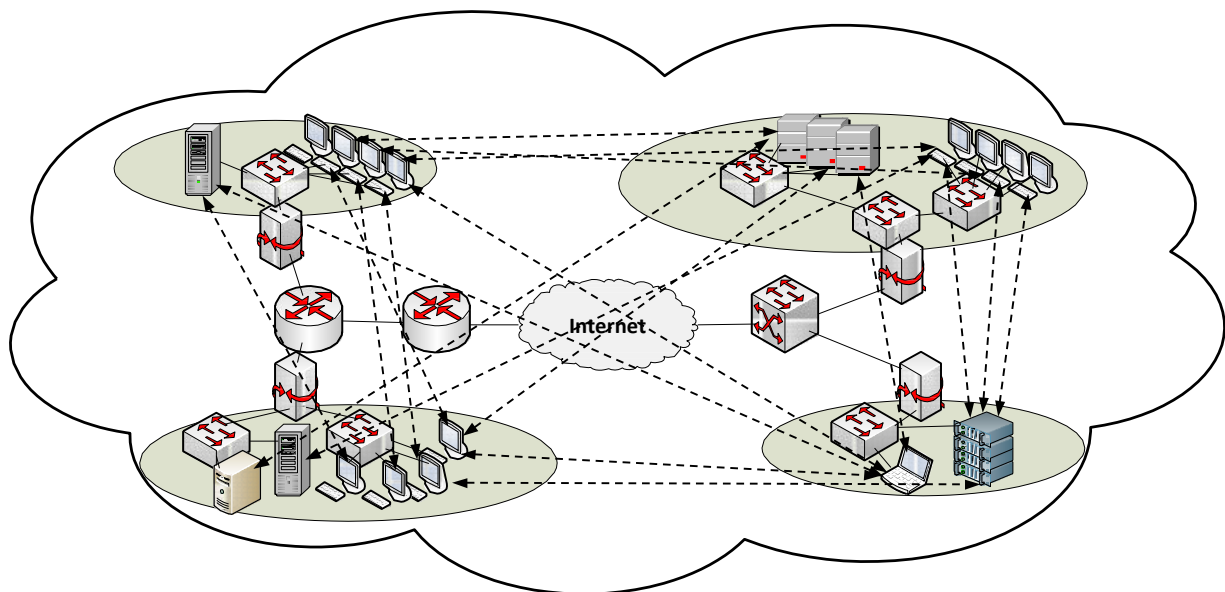


Рис. 1. Взаємодія користувачів однорангової розподіленої хмарної системи через глобальну мережу

Дана архітектура базується на принципі рівноправної взаємодії вузлів системи, які зв'язані між собою за допомогою мережі Інтернет або локальної мережі. Вузлами реплікації є робочі станції користувачів-учасників «хмари», які надають частину своїх ресурсів у загальне користування. Відповідь на запит користувача кешується на дисковому просторі його робочої станції, який потім на вимогу можна надати іншим учасникам однорангової розподіленої хмарної системи. Таким чином, з ростом популярності ресурсу буде збільшуватися продуктивність системи в цілому.

Принцип рівноправності покладено в основу взаємодії учасників однорангової розподіленої хмарної системи. Кожен вузол може виступати в ролі клієнта (якщо він запитує ресурс) і в ролі сервера (якщо він надає ресурс або його частину). Аналіз наукової літератури дозволяє виділити ще одну роль – власник ресурсу, який має повні права на нього.

Доменне ім'я використовується як глобальний ідентифікатор ресурсу для інтеграції з існуючими Інтернет сервісами, яке пов'язує з собою ряд ресурсних записів. Ресурсний запис (A) використовується для зберігання адрес власника ресурсу і вузлів, які мають повну репліку ресурсу. Додаткові ресурсні записи (TXT) застосовується для зберігання унікального ідентифікатора ресурсу в одноранговій мережі. Унікальним ідентифікатором ресурсу в одноранговій мережі є хеш-сума його вмісту. На рис. 2 зображено процес отримання запитуваного ресурсу за доменним ім'ям `http://domain-name.com/resource-name`, що складається з N частин (складових).

Вузол, який знаходиться за NAT, застосовує механізми для з'єднання з приватною мережею [12]. Для пошуку вузла реплікації, який має репліку запитуваного ресурсу або його частину, застосовується інфраструктура розподілених хеш-таблиць (Distributed Hash Table, DHT). Велика кількість пірінгових сервісів була реалізована на базі інфраструктури DHT [13], серед яких можна виділити I2P, BitTorrent та ін. Багато з них побудовано на базі протоколу Kademlia [14], який забезпечує координацію взаємодіючих один з одним вузлів розподіленої однорангової архітектури без участі додаткових трекер-серверів.

З метою підвищення оперативності відповіді на запит за основу взято принцип розподілу ресурсів між вузлами хмарної системи з децентралізованою структурою. Розподіл ресурсів між вузлами однорангової розподіленої хмарної системи з подальшим наданням сервісів за запитом реалізується за допомогою протоколу Kademlia [14] в локальній мережі або мережі Інтернет і містить процеси публікації ресурсу на початковій стадії його власником, реплікації і безпосередньо надання доступу до ресурсів.

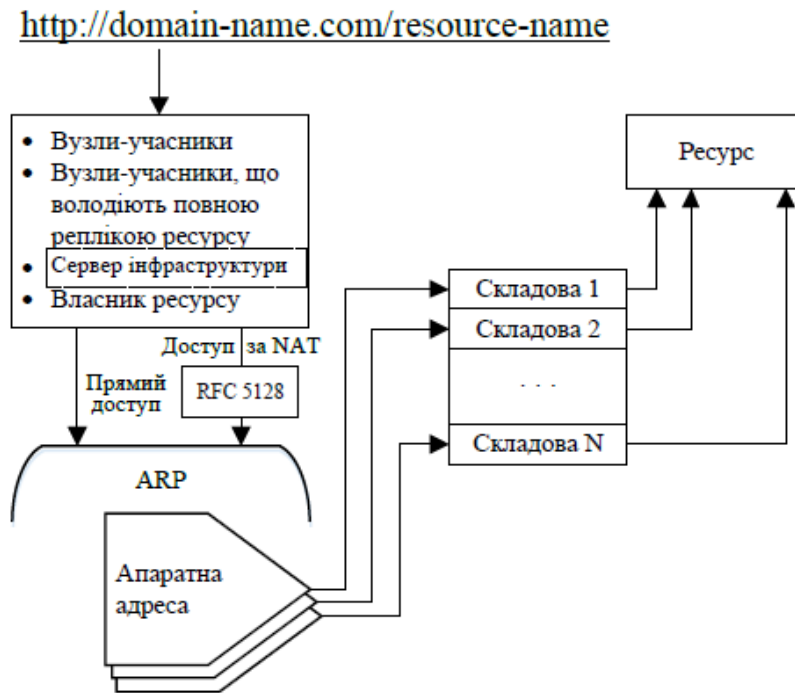


Рис. 2. Схема процесу отримання ресурсу за доменним ім'ям

Інформація у вигляді відповіді на запит вузла-учасника однорангової розподіленої хмарної системи зберігається на дисковому просторі його робочій станції, а потім надається в спільне користування іншим вузлам-учасникам. Процес розподілу ресурсів координується за допомогою DNS-сервера шляхом модифікації ресурсних записів.

Організація взаємодії вузлів здійснюється за допомогою спеціалізованого програмного забезпечення, встановленого на робочих станціях всіх вузлів-учасників однорангової розподіленої хмарної системи. Доступ до ресурсів для вузлів, які не є учасниками однорангової розподіленої хмарної системи, виконується завдяки стандартній взаємодії з сервером власника ресурсу або вузлами, що володіють повною реплікою ресурсу, за допомогою їх мережних адрес з урахуванням завантаженості каналів зв'язку і робочій станції власника ресурсу або вузлів, які мають повну репліку ресурсу.

На рис. 3 надано процес взаємодії основних компонентів для отримання доступу до веб-ресурсу <http://domain-name.com/resource-name>.

Взаємодія відбувається таким чином. На першому етапі вузол-учасник виконує стандартний запит до ресурсу <http://domain-name.com/resource-name> через веб-браузер на своїй робочій станції. На другому етапі вузол-учасник за допомогою прикладного програмного забезпечення виконує запит до додаткового ресурсного запису DNS-сервера ідентифікатора ресурсу ID_res з доменним ім'ям <http://domain-name.com/resource-name>, а також ідентифікаторів базових вузлів реплікації. Ця інформація необхідна для запуску на третьому етапі стандартного процесу пошуку DHT-lookup «FIND_NODE» найближчого за XOR-метрикою вузла реплікації ресурсу з ідентифікатором ID_res. На наступному етапі виконується запит типу «FIND_VALUE» на надання доступу до ресурсу до вузла з відповідним ідентифікатором. На завершальному етапі відбувається завантаження контенту для запитувача вузла через веб-браузер і збереження відповіді на запит на дисковому просторі цього вузла.

Процес публікації ресурсу полягає у відкритті доступу до інформації, що публікується (наприклад, веб-ресурсу), додаванні DNS-запису відповідності адреси власника ресурсу і доменного імені. Коли інший вузол-учасник на надання ресурсу, він звертається до DNS-сервера і отримує адресу власника ресурсу. Після отримання доступу безпосередньо до ресурсу або його частини інформація у вигляді відповіді на запит зберігається на дисковому просторі вузла-учасника, і такий вузол може надати цей ресурс (або його складову) за запитом іншим вузлам мережі за допомогою протоколу Kademlia, тобто виступити в ролі

сервера. Для цього його ідентифікатор додається в глобальну розподілену хеш-таблицю (DHT) ідентифікаторів ресурсів [14]. У разі, якщо інший вузол-учасник однорангової розподіленої хмарної системи запитує той самий ресурс, він отримує доступ до нього за ідентифікатором найближчого за XOR-метрикою [14] вузла реплікації, що володіє ресурсом частково або повністю, або за однією з адрес, що містяться в ресурсних записах DNS для даного ресурсу. Якщо вузол-учасник запитує всі частини ресурсу, на дисковому просторі його робочої станції буде закешовано весь ресурс повністю. У такому випадку цей вузол буде мати повну репліку ресурсу, а його адреса буде додана до основного ресурсного запису (A-запису) DNS-сервера. Таким чином, зі збільшенням популярності ресурсу більша кількість вузлів-учасників однорангової розподіленої хмарної системи може ним поділитися. Для виконання серверних функцій кожен вузол-учасник має надати в спільне користування частину власних апаратних ресурсів – дискового простору й потужності центрального процесора. Якщо вузли не є учасниками однорангової розподіленої хмарної системи, вони можуть отримати доступ до ресурсу завдяки стандартному способу взаємодії з сервером (робочою станцією) власника ресурсу або вузлами, що володіють повною реплікою ресурсу, за їхніми адресами з урахуванням завантаженості каналів зв'язку і станції власника ресурсу або вузлів, які володіють повною реплікою ресурсу шляхом відправлення стандартного запиту до основного ресурсного запису DNS-сервера й отримання адреси власника ресурсу та (або) вузлів, які мають повну репліку ресурсу.

Перевірка цілісності ресурсу та ідентичність реплік проводиться шляхом обчислення хеш-функції отриманого ресурсу і зіставлення зі значенням ідентифікатора цього ресурсу. Крім того, на проміжному етапі перед завантаженням контенту виробляється процес валідації вузла, що надає ресурс.



Рис. 3. Схема процесу надання доступу до ресурсів

Вузол, що надає ресурс, для підтвердження свого ідентифікатора відправляє повідомлення такого формату

ID_node	
Kpub1	SigKpriv2(Kpub1)
Kpub2	SigKpriv2(Kpub2)

На першому етапі валідації ідентифікатора вузла виконується перевірка автентичності переданих відкритих ключів Kpub1 і Kpub2 за рахунок механізму цифрового підпису. Якщо перевірка пройшла успішно, перевіряється істинність співвідношення

$$ID_{node} = Hash(K_{pub1} + Sig_{Kpriv2}(K_{pub1})),$$

де ID_{node} – ідентифікатор вузла, переданий в повідомленні;

K_{pub1} – відкритий ключ 1;

$Hash(Data)$ – оператор обчислення хеш-функції даних $Data$;

$Sig_{K_{priv2}}(K_{pub1})$ – цифровий підпис даних K_{pub1} , отриманий за допомогою ключа K_{priv2} .

Якщо рівність виконується, то валідація пройшла успішно і вузол-відправник вважається успішно ідентифікованим і підтвердженим. Незалежно від ролі будь-який вузол-учасник однорангової розподіленої хмарної системи отримує високошвидкісний доступ до всіх ресурсів системи завдяки можливості отримати ресурс від найближчого вузла-учасника, який має копію цього ресурсу.

Описані процеси додавання нового вузла, валідації автентичності, публікації ресурсу й отримання доступу до ресурсу подано у вигляді поетапної послідовності дій у межах методу надання доступу до сервісів розподіленої хмарної системи за допомогою графічного опису інформаційних потоків, взаємодії процесів оброблення інформації та об'єктів, які є частиною цих процесів, IDEF3 на рис. 4.



Рис. 4. Метод надання доступу до сервісів розподіленої хмарної системи

Висновки. Отже, запропонований метод надання доступу до сервісів реалізує новий підхід, у межах якого виконується розподіл ресурсів у хмарній мережі з децентралізованою структурою, об'єднуючи переваги технологій GRID, хмарних обчислень і пірингових мереж. Особливістю запропонованого методу є самоорганізація процесу реплікації ресурсів засобами робочих станцій вузлів-учасників системи: цей процес не вимагає втручання адміністратора або сторонніх механізмів.

Розглянуто метод надання доступу до сервісів розподіленої хмарної системи, який на відміну від існуючих базується на використанні розподілених хеш-таблиць і пасивної реплікації даних по вузлах користувачів, що дозволяє підвищити оперативність відповіді на запит при зростанні кількості користувачів.

Література

1. Технологии Web, Grid, Cloud для гарантоспособных ИТ-инфраструктур : монография / В. С. Харченко и др. ; Харьков. нац. аэрокосм. ун-т им. Н. Е. Жуковского. – «ХАИ», 2013. – 868 с.
2. Струбицький Р. П. Аналіз загроз хмарковим сховищам даних та методів їх захисту / Р. П. Струбицький, П. Р. Струбицький, Н. Б. Шаховська // Наукові праці. Комп'ютерні технології. – 2013. – № 217. – С. 35–38.
3. Рыжкова О. В. Сравнительный анализ эффективности использования алгоритмов изменения размера окна перегрузок в сетях Cloud Computing / О. В. Рыжкова // Радиоэлектронні і комп'ютерні системи. – 2012. – № 7(59). – С. 73–78.
4. Рыжкова О. В. Оценка критичности отказов коммутаторов уровня доступа кластера центра обработки данных / О. В. Рыжкова // Радиоэлектронні і комп'ютерні системи. – 2013. – № 5(64). – С. 337–341.
5. Яновская О. В. Модели надежности компонентов облачного дата-центра / О. В. Яновская, В. С. Харченко // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка "Проблеми енергозабезпечення та енергозбереження в АПК України". – 2014. – Вып. 154. – С. 86–88.
6. Яновская О. В. Модели доступности сервисов распределенных облачных систем / О. В. Яновская // Наука і техніка Повітряних Сил Збройних Сил України. – 2016. – № 1(22). – С. 124–130.
7. Зеленая ИТ-инженерия : в 2 т. : монография / В. С. Харченко, А. Г. Бажанов, А. Г. Бажанов и др. / Под ред. В. С. Харченко. – Харьков : Нац. аэрокосм. ун-т им. Н. Е. Жуковского "ХАИ", 2014. – Т. 2 : Системы, индустрия, социум. – 688 с.
8. Технологии высокой готовности для программно-технических комплексов космических систем / В. С. Харченко, О. Н. Одарушенко, Ю. Л. Поночовный и др. – Харьков : Нац. аэрокосм. ун-т им. Н. Е. Жуковского "ХАИ", Гос. центр регулирования

качества поставок и услуг, 2010. – 372 с.

9. Dong, S. K. Availability Modeling and Analysis of a Virtualized System / S. K. Dong, F. Machida, K. S. Trivedi // 15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC '09, 2009. – P. 365–371.
10. Ghosh, R. Modeling and performance analysis of large scale IaaS Clouds / R. Ghosh, F. Longo, V. K. Naik, K. S. Trivedi // Future Generation Computer Systems, 2013. – Vol. 29 (5). – P. 1216–1234.
11. Peer-to-peer network [Electronic resource]. – Access mode: <http://www.infosec.gov.hk/english/technical/files/peer.pdf>. – 10.04.2016.
12. Srisuresh, P. RFC 5128. State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs) / P. Srisuresh, B. Ford, D. Kegel // The Internet Engineering Task Force (IETF), 2008. – 32 p.
13. Designing a DHT for low latency and high throughput / F. Dabek, J. Li, E. Sit, et al. // Conference on Symposium on Networked Systems Design and Implementation (NSDI). USENIX Association Berkeley. – San Francisco, 2004. – Vol. 1. – P. 85–98.
14. Zhou, Y. Kad-D: An Improved Model Based on Kademia / Y. Zhou, S. Liu, and G. Huang // Multimedia Information Networking and Security (MINES). – 2011. – P. 123–127.

References

1. Tehnologii Web, Grid, Cloud dlja garantyosposobnyh IT-infrastruktur : monografija / V. S. Harchenko i dr. ; Har'kov. nac. ajerokosm. un-t im. N. E. Zhukovskogo. – «HAI», 2013. – 868 s.
2. Strubytskyi R. P. Analiz zahroz khmarkovym skhovyshcham danykh ta metodiv yikh zakhystu / R. P. Strubytskyi, P. R. Strubytskyi, N. B. Shakhovska // Naukovi pratsi. Kompiuterni tekhnolohii. – 2013. – № 217. – S. 35–38.
3. Ryzhkova O. V. Sravnitel'nyj analiz jeffektivnosti ispol'zovaniya algoritmov izmeneniya razmera okna peregruzok v setjah Cloud Computing / O. V. Ryzhkova // Radioelektronni i komp'juterni sistemi. – 2012. – № 7(59). – S. 73–78.
4. Ryzhkova O. V. Ocenka kritichnosti otkazov kommutatorov urovnja dostupa klastera centra obrabotki dannyh / O. V. Ryzhkova // Radioelektronni i kompiuterni systemy. – 2013. – № 5(64). – S. 337–341.
5. Janovskaja O. V. Modeli nadezhnosti komponentov oblachnogo data-centra / O. V. Janovskaja, V. S. Harchenko // Visnyk Kharkivskoho natsionalnogo tekhnichnogo universytetu silskoho hospodarstva imeni Petra Vasylenka "Problemy enerhozabezpechennia ta enerhozberezhennia v APK Ukrainy". – 2014. – Vyp. 154. – S. 86–88.
6. Janovskaja O. V. Modeli dostupnosti servisov raspredelennyh oblachnyh sistem / O. V. Janovskaja // Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy. – 2016. – № 1(22). – S. 124–130.
7. Zelenaja IT-inzhenerija : v 2 t. : monografija / V. S. Harchenko, A. G. Bazhanov i dr. / Pod red. V. S. Harchenko. – Har'kov : Nac. ajerokosm. un-t im. N. E. Zhukovskogo "HAI", 2014. – T. 2 : Sistemy, industrija, socium. – 688 s.
8. Tehnologii vysokoj gotovnosti dlja programmno-tehnicheskikh kompleksov kosmicheskikh sistem / V. S. Harchenko, O. N. Odarushhenko, Ju. L. Ponochovnij i dr. – Har'kov : Nac. ajerokosm. un-t im. N. E. Zhukovskogo "HAI", Gos. centr regulirovaniya kachestva postavok i uslug, 2010. – 372 s.
9. Dong, S. K. Availability Modeling and Analysis of a Virtualized System / S. K. Dong, F. Machida, K. S. Trivedi // 15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC '09, 2009. – P. 365–371.
10. Ghosh, R. Modeling and performance analysis of large scale IaaS Clouds / R. Ghosh, F. Longo, V. K. Naik, K. S. Trivedi // Future Generation Computer Systems, 2013. – Vol. 29 (5). – P. 1216–1234.
11. Peer-to-peer network [Electronic resource]. – Access mode: <http://www.infosec.gov.hk/english/technical/files/peer.pdf>. – 10.04.2016.
12. Srisuresh, P. RFC 5128. State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs) / P. Srisuresh, B. Ford, D. Kegel // The Internet Engineering Task Force (IETF), 2008. – 32 p.
13. Designing a DHT for low latency and high throughput / F. Dabek, J. Li, E. Sit, et al. // Conference on Symposium on Networked Systems Design and Implementation (NSDI). USENIX Association Berkeley. – San Francisco, 2004. – Vol. 1. – P. 85–98.
14. Zhou, Y. Kad-D: An Improved Model Based on Kademia / Y. Zhou, S. Liu, and G. Huang // Multimedia Information Networking and Security (MINES). – 2011. – P. 123–127.

Рецензія/Peer review : 05.12.2018 Надрукована/Printed : 14.02.2019

Рецензент: д. т. н., проф. Говорущенко Т. О.