УДК 37.091.33:004.031.42(045)

к.т.н., доц. **Кльоц Ю.П.** (ХмНУ)
к.т.н., доц. **Муляр І.В.** (ХмНУ)
к.т.н., доц. **Чешун В.М.** (ХмНУ)
Бурдюг О.В. (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2020/67-09

ВИКОРИСТАННЯ РОЗПОДІЛЕНИХ ХЕШ-ТАБЛИЦЬ НАДАННЯ ДОСТУПУ ДО ХМАРНИХ СЕРВІСІВ

У статті розкрито актуальність проблеми надання доступу до сервісів розподіленої хмарної системи, зокрема, охарактеризовано однорангову розподілену хмарну систему. Подано 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.

Застосування сучасних технологій адаптивних систем захисту інформації не дозволяє здійснювати повний контроль за інформаційними потоками середовища хмарних обчислень, оскільки вони функціонують на верхніх рівнях ієрархії. Тому для створення ефективних механізмів захисту ПЗ в середовищі хмарних обчислень потрібна розробка нових моделей загроз і створення методів відображення комп'ютерних атак, які дозволяють оперативно ідентифікувати приховані і потенційно небезпечні процеси інформаційної взаємодії.

Правила розмежування доступу, складають основу політики безпеки, включають і обмеження на механізми ініціалізації процесів доступу. В рамках розробленої моделі операцій формалізований опис прихованих загроз зводиться до появи контекстно-залежних переходів в мультиграфі транзакцій

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 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.

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

Вступ. Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації, сервіс-орієнтованої архітектури привели до величезного зростання хмарних обчислень. Хмарні обчислення – це модель забезпечення зручного доступу на вимогу через мережу до обчислювальних ресурсів, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера.

Середовище хмарних обчислень - це сукупність обчислювальних ресурсів у вигляді віртуальних машин, що надаються користувачеві за допомогою загальних сервісів доступу. Фізичний рівень хмарної системи складається з апаратних ресурсів, які необхідні для забезпечення сервісів, що надаються, і, як правило, включає сервери, системи зберігання і мережеві компоненти. Застосування технологій хмарних обчислень визначає необхідність розгляду можливих способів дестабілізуючих дій, що приводять до порушення функціонування компонентів інформаційного середовища.

Характерною особливістю сучасного середовища хмарних обчислень є активний характер суб'єктів і об'єктів інформаційної взаємодії. Це дозволяє розглядати цільову функцію системи безпеки як збереження конфіденційності, цілісності і доступності програмних і інфраструктурних сервісів, що надаються в режимі видаленого доступу в умовах динамічної

зміни стану обчислювальних ресурсів. Побудова перспективних механізмів забезпечення безпеки в середовищі хмарних обчислень зв'язується не із захистом від виявлених вразливостей, а полягає в можливості запобігання новим невідомим методам проведення атак, в розробці нових моделей загроз і методів запобігання або віддзеркалення комп'ютерних атак на інформаційні ресурси, які використовують можливості предикативної ідентифікації прихованих каналів і потенційно небезпечних процесів інформаційної взаємодії [1]

Важливим напрямом вдосконалення технологій захисту і систем інформаційної безпеки є протидія білатеральним загрозам, в яких суб'єкт і об'єкт процесів інформаційної взаємодії є потенційним носієм небезпечних дій. У таких випадках необхідно використовувати моделі загроз, які ідентифікують потенційні вразливості як на рівні процесів контролю доступу до ресурсів гостьових операційних систем (ОС) або додатків, так і на рівні системних викликів гіпервізора [2], який сам може стати джерелом руйнуючих дій що реалізовуються шляхом порушення функціонування планувальника завдань або диспетчера устаткування. Загрози, що виникають при цьому, необхідно не тільки оперативно виявляти, але і блокувати використовувані неавторизовані канали інформаційних дій, які в середовищі хмарних обчислень зазвичай реалізуються в прихованому для гостьових ОС режимах. Тому важливим чинником підвищення ефективності систем захисту від прихованих загроз є облік напряму передачі, синтаксису і контексту потоків даних, які передаються [2, 3].

Аналіз останніх досліджень і публікацій.

Поява хмарних технологій сприяла відмові від застосування децентралізованої архітектури як єдиної, а тому викликала значну кількість проблем: «велика вартість розгортання, високе енергоспоживання, значні простої 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 - 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 сервісі, 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.

Використання технології між мережного екранування з урахуванням специфіки захищеності середовища. Для цього необхідна формалізація вимог розмежування доступу до інформаційних сервісів [9]. Така формалізація може бути представлена з використанням динамічно формованого набору правил фільтрації, що забезпечує виконання вимог політики доступу. При цьому зростаюча складність алгоритмів фільтрації пред'являє високі вимоги до продуктивності між мережевих екранів, що робить необхідним використання методів

паралельної обробки віртуальних з'єднань за допомогою віотуальних машин. У сучасній літературі підхід до створення складних технічних систем, зв'язаність яких забезпечується за рахунок організації процесів обміну інформацією з мережі, отримав назву мережево-центричний. Цей підхід стосовно задачі розмежування доступу вимагає забезпечення ситуаційної обізнаності та локальності дій кожного з між мережевих екранів, що входять до складу віртуальних машин.

Тому існує низка взаємозв'язаних завдань: для хмарних інфраструктур необхідно виконувати достовірне оцінювання, а також забезпечувати необхідний рівень доступності сервісів, одночасно з підвищенням енергоефективності [8], зменшенням споживання енергії й негативного впливу на навколишнє середовище [4]. Аналіз існуючих моделей і методів оцінювання й забезпечення готовності та доступності хмарних архітектур [8, 10] дає змогу зробити висновок, що вони не надають можливості визначити фактичну доступність і продуктивність хмарних сервісів з використанням об'єктивних кількісних показників.

Постановка задачі. Використання традиційних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень з урахуванням гнучкості, масштабованості (підтримка апаратних платформ різного класу) пропонованих програмно-технічних рішень і мінімізації витрат. Запропоновані методи зниження продуктивності ресурсів зі збільшенням кількості користувачів [6] не враховують повною мірою особливостей впровадження хмарних архітектур. Таким чином, актуальним науково-прикладним завданням є розробка методу надання доступу до ресурсів розподіленої хмарної системи з необхідним рівнем якості обслуговування.

Дослідження методу надання доступу до сервісів розподіленої хмарної системи

Для того, щоб проаналізувати доступності сервісів хмарної системи з клієнт-серверною архітектурою було досліджено функціональні й надійнісні характеристики інфраструктури хмарного ЦОД і його окремих компонентів, на базі яких функціонують сервіси. Доцільним буде розкрити сутність методу надання доступу до ресурсів розподіленої хмарної системи з необхідним рівнем якості обслуговування.

Standards and Technology - NIST) у документі «Cloud Computing Reference Architecture» [12] подав огляд еталонної архітектури хмарних обчислень, який ідентифікує основних суб'єктів, їх діяльність і функції у хмарних обчисленнях (рис1)

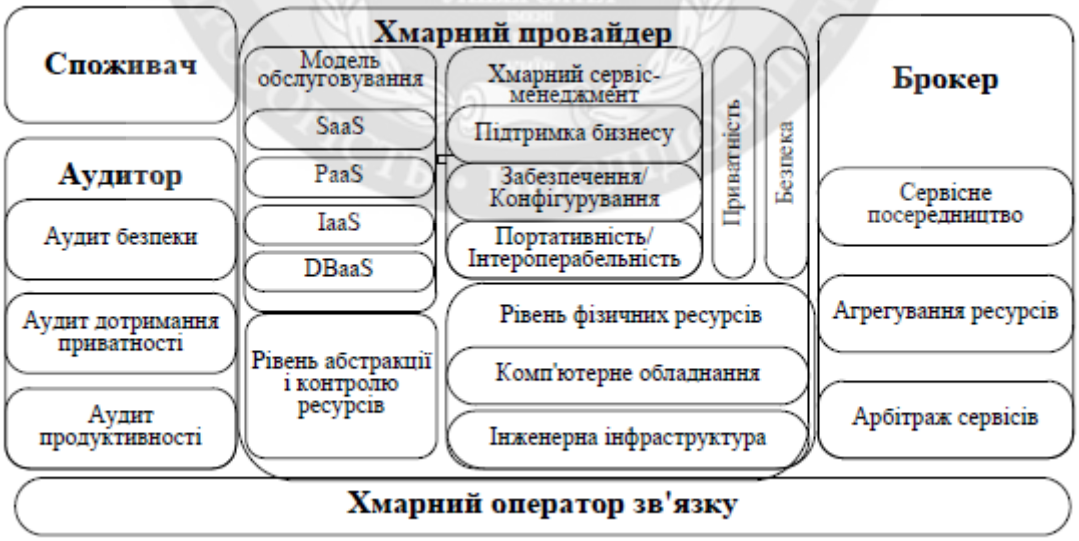

Рисунок 1 – Еталонна архітектура хмарних обчислень NIST

Ідея однорангової розподіленої хмарної системи (рис. 2) полягає в об'єднанні двох базових технологій: Grid-системи та Cloud (централізована клієнт-серверна система з підтримкою технології віртуалізації) за допомогою пірингових мереж [13].

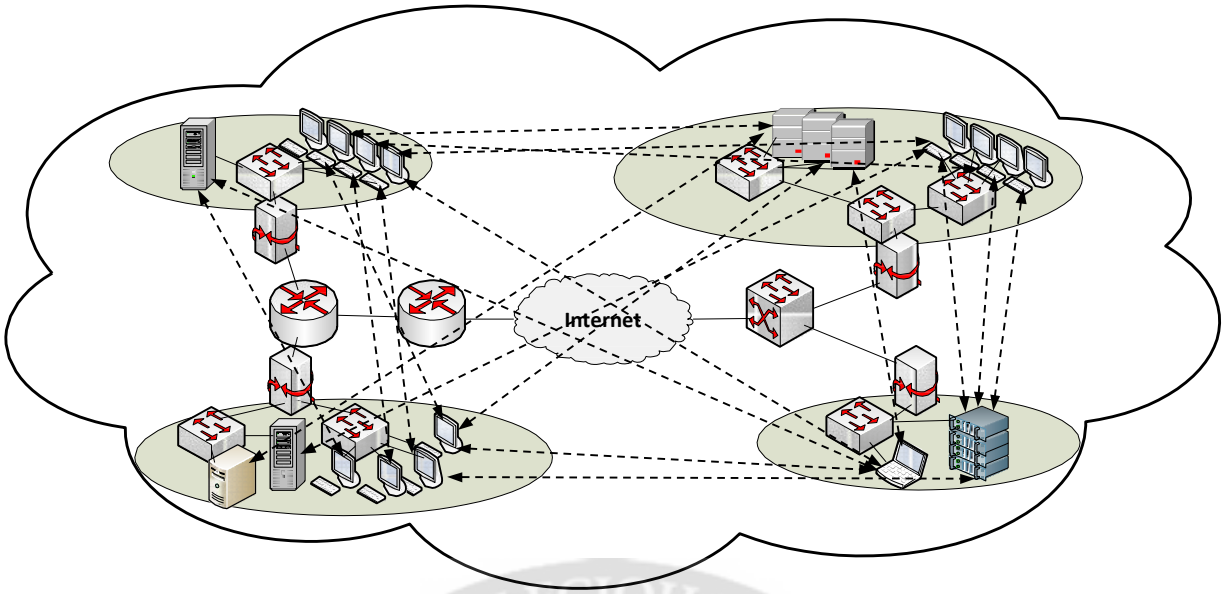

Рисунок 2 - Взаємодія користувачів однорангової розподіленої хмарної системи через глобальну мережу

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 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.

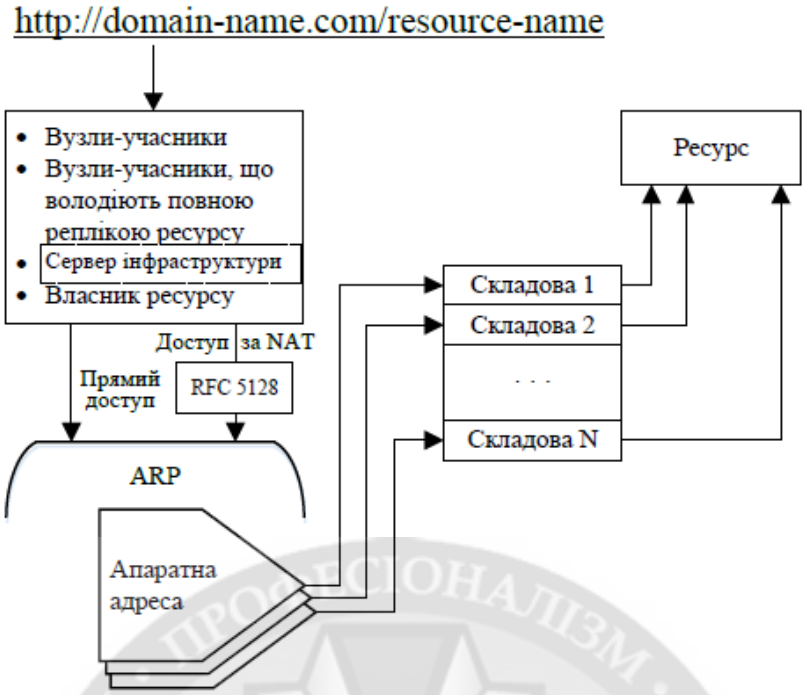

Рисунок 3 – Схема процесу отримання ресурсу за доменним ім’ям

Інформація у вигляді відповіді на запит вузла-учасника однорангової розподіленої хмарної системи зберігається на дисковому просторі його робочої 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 робочої станції власника ресурсу або вузлів, які мають повну репліку ресурсу.

На рис. 3 подано 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.

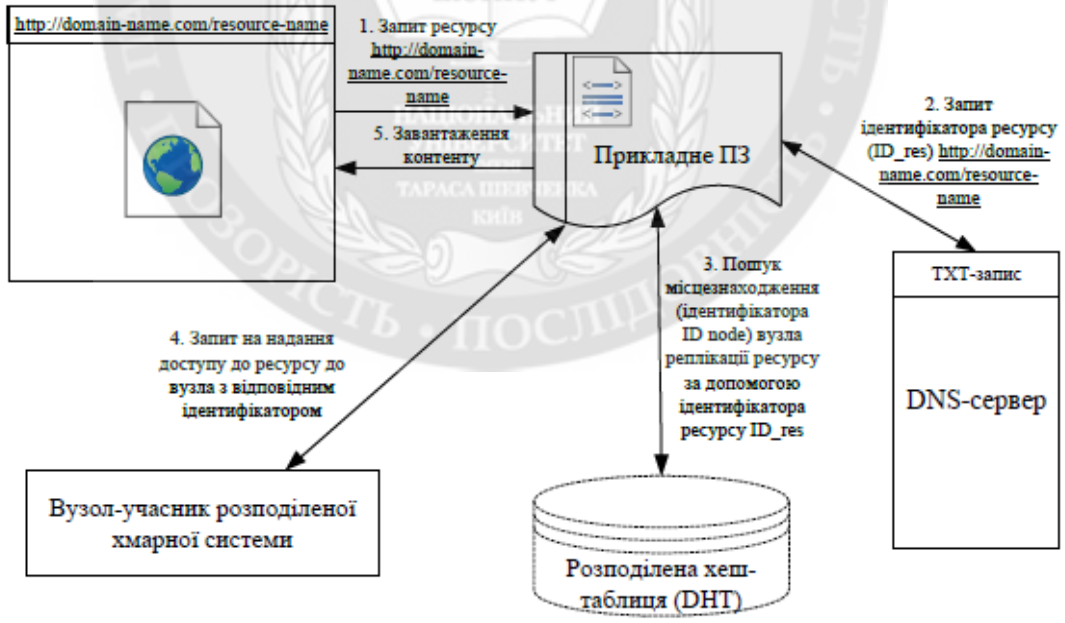

Рисунок 4 - Схема процесу надання доступу до ресурсів

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

$$ID_{node} = Hash\left(K_{pub}1 + Sig_{K_{priv}2}(K_{pub}1)\right),$$

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

$K_{pub}1$ – відкритий ключ 1;

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

$Sig_{K_{priv}2}(K_{pub}1)$ – цифровий підпис даних $K_{pub}1$, отриманий за допомогою ключа $K_{priv}2$.

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. 5.

Рисунок 5 – Метод надання доступу до сервісів розподіленої хмарної системи

Висновки. У будь-якій обчислювальній системі існують інтерфейсні рівні взаємодії між різними модулями(компонентами), що дозволяють використовувати недокументовані можливості, з одного боку, для проведення атак зловмисником, з іншої – для реалізації механізмів моніторингу з боку систем контролю і захисту ПЗ середовища хмарних обчислень.

Для досягнення цілей інформаційного забезпечення запропоновано шляхи підвищення ефективності набуття знань, зокрема, за допомогою аналізу і синтезу структури інформаційного забезпечення та визначення послідовності інформаційних об'єктів предметної області. Також запропонований підхід визначення такої траєкторії освоєння матеріалу, яка безпосередньо сприяє досягненню мети інформаційного забезпечення на основі вже наявних знань.

Запропоновано спосіб формування інформаційного забезпечення, призначений для ієрархічного мережевого представлення предметної області, що дозволяє структурувати контент інформаційно-довідкових та інших систем, що відрізняється від відомих використанням взаємопов'язаних етапів відбору, кластеризації та впорядкування контенту.

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 піринговых мереж. Особливістю запропонованого методу є самоорганізація процесу реплікації ресурсів засобами робочих станцій вузлів-учасників системи: цей процес не вимагає втручання адміністратора або сторонніх механізмів.

Отримані результати можуть бути використані для підтримки прийняття рішень при придбанні та застосуванні знань, а саме: при створенні інформаційного забезпечення виробничих процесів, в частині розробки елементів методичного забезпечення інформаційних систем, в корпоративних системах навчання персоналу; при розробці програм окремих курсів підвищення кваліфікації, а так само комплексів програм з подальшим їх коригуванням; інформаційного забезпечення систем електронного навчання; при формуванні програм дистанційної освіти; при розробці та наступним коригуванням навчальних планів; формуванні навчальних, довідкових матеріалів, курсів лекцій для окремих дисциплін.

ЛІТЕРАТУРА:

1. Технологии Web, Grid, Cloud для гарантоспособных ИТ- инфраструктур [Текст] : монография/ В. С. Харченко и др; Харьков. нац. аэрокосм. ун-т им. Н. Е. Жуковского. – «ХАИ», 2013. – 868 с.

2. Муляр І.В. Аналіз проблем забезпечення функціональної безпеки інформаційних систем обробки даних / І.В. Муляр, А.В. Джулій, М.В. Костюк // Вимірювальна та обчислювальна техніка в технологічних процесах: Міжнародний науково-технічний журнал.-Хмельницький, 2013. – №1 -С. 133-138.

3. Рыжкова, О.В. Сравнительный анализ эффективности использования алгоритмов изменения размера окна перегрузок в сетях Cloud Computing [Текст] / О. В. Рыжкова // Радіоелектронні і комп'ютерні системи. – 2012. – № 7(59). – С. 73 – 78.

4. Муляр І.В. Метод предикативної ідентифікації процесів для захисту від прихованих загроз в середовищі хмарних обчислень / С.В. Лєнков , В.М. Джулій , О.В. Селюков, І.В. Муляр // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 55. – С. 145-154.

5. Яновская, О.В. Модели надежности компонентов облачного дата-центра [Текст] / 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 [Текст] / О. В. Яновская // Наука і техніка Повітряних Сил Збройних Сил України.– 2016. – № 1(22). – С. 124 – 130.

7. Ленков С.В. Динамічні показники оцінки рівня функціональної безпеки інформаційної системи / С.В. Лєнков, В.М. Джулій, І.В. Муляр // Сучасна спеціальна техніка. Науково практичний журнал. - ДНДІ МВС України, 2016. - Вип. №2(45). - С.59-67.

8. Муляр І.В. Метод надання доступу до сервісів однорангової розподіленої хмарної системи / І.В. Муляр, А. С. Сівак // Вимірювальна та обчислювальна техніка в технологічних процесах.-2019.- № 1 (63).-С. 68-73

9. Dong, S.K. Availability Modeling and Analysis of a Virtualized System [Text] / S. K. Dong, F. Machida, K. S. Trivedi // 15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC '09, 2009. – P. 365 – 371.

10. Муляр І.В. Розробка математичної моделі та методу її вирішення для підвищення ефективності використання обчислювальних ресурсів на основі технології віртуалізації / І.В. Муляр , Г.В. Гусляков , Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016. – Вип. № 54. – С. 134-143.

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) [Text] / P. Srisuresh, B. Ford, D. Kegel // The Internet Engineering Task Force (IETF), 2008. – 32 p.

13. Муляр, І.В. Модель оцінки ймовірнісно-часових характеристик інформаційної взаємодії в мережі інтернет речей / І.В. Муляр, О.В. Сєлюков, В.М. Джулій, Б.М. Кізюн // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. № 63. – С.96-107.

14. Zhou, Y. Kad-D: An Improved Model Based on Kademlia [Text] / Y. Zhou, S. Liu, and G. Huang. // Multimedia Information Networking and Security (MINES). – 2011. – P. 123 – 127.

REFERENCES:

1. Tekhnolohyy Web, Grid, Cloud dlia harantosposobnыkh YT-ynfrastruktur [Tekst] : monohrafyia / V. S. Kharchenko y dr; Kharkov. nats. aэrokosm. un-t ym. N. E. Zhukovskoho. – «KhAY», 2013. – 868 s.

2. Muliar I.V. Analiz problem zabezpechennia funktsionalnoi bezpeky informatsiinykh system obrobky danykh / I.V. Muliar, A.V. Dzhulii, M.V. Kostiuk // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh: Mizhnarodnyi naukovo-tekhnichnyi zhurnal. -Khmelnytskyi, 2013.-№1 -S. 133-138.

3. Rizhkova, O. V. Sravnytelnыi analyz эffektyvnosty yspolzovanyia alhorytmov yzmenenyia razmera okna perehruzok v setiakh Cloud Computing [Tekst] / O. V. Rizhkova // Radioelektronni i kompiuterni systemy. – 2012. – № 7(59). – S. 73 – 78.

4. Muliar I.V. Metod predykatyvnoi identyfikatsii protsesiv dlia zakhystu vid prykhovanykh zahroz v seredovyshchi khmarnykh obchyslen / S.V. Lienkov, V.M. Dzhulii, O.V. Seliukov, I.V. Muliar // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2017. – Vyp. № 55. – C. 145-154.

5. Yanovskaia, O. V. Modely nadezhnosty komponentov oblachnoho data-tsentra [Tekst] / O. V. Yanovskaia, V. S. Kharchenko // Visnyk Kharkivskoho natsionalnoho tekhnichnoho universytetu silskoho hospodarstva imeni Petra Vasylenka "Problemy enerhozabezpechennia ta enerhozberezhennia v APK Ukrainy". – 2014. – Vыp. 154. – S. 86 – 88.

6. Yanovskaia, O. V. Modely dostupnosty servysov raspredelennыkh oblachnыkh system [Tekst] / O. V. Yanovskaia // Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy.– 2016. – № 1(22). – S. 124 – 130.

7. Lenkov S.V. Dynamichni pokaznyky otsinky rivnia funktsionalnoi bezpeky informatsiinoi systemy / S.V. Lienkov , V.M. Dzhulii , I.V. Muliar // Suchasna spetsialna tekhnika. Naukovo praktychnyi zhurnal. - DNDI MVS Ukrainy, 2016. - Vyp. №2(45). - C.59-67.

8. Muliar I.V. Metod nadannia dostupu do servisiv odnoranhovoi rozpodilenoi khmarnoi systemy / I.V. Muliar, A. S. Sivak // Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh.-2019.- № 1 (63).-S. 68-73

9. Dong, S. K. Availability Modeling and Analysis of a Virtualized System [Text] / S. K. Dong, F. Machida, K. S. Trivedi // 15th IEEE Pacific Rim International Symposium on Dependable Computing PRDC 09, 2009. – P. 365 – 371.

10. Muliar I.V. Rozrobka matematychnoi modeli ta metodu yii vyrishennia dlia pidvyshchennia efektyvnosti vykorystannia obchysliuvalnykh resursiv na osnovi tekhnolohii virtualiz / I.V. Muliar , H.V. Husliakov , L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU, 2016. – Vyp. № 54. – C. 134-143.

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) [Text] / P. Srisuresh, B. Ford, D. Kegel // The Internet Engineering Task Force (IETF), 2008. – 32 p.

13. Mulyar I.V., Selyukov O.V., Dzhuliy V.M. and Kizyun B.M.(2019) “Model′ otsinky ymovirnisno-chasovykh kharakterystyk informatsiynoyi vzayemodiyi v merezhi internet rechey” [Model of estimation of probabilistic-temporal characteristics of information interaction in the Internet of things network], Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, №63, pp.96-107.

14. Zhou, Y. Kad-D: An Improved Model Based on Kademlia [Text] / Y. Zhou, S. Liu, and G. Huang. // Multimedia Information Networking and Security (MINES). – 2011. – P. 123 – 127.

Ph.D. Klots Yu.P., Ph.D. Muliar I.V., Ph.D. Cheshun V.M., Burdyug O.V.

USE OF DISTRIBUTED HASH TABLES TO PROVIDE ACCESS TO CLOUD SERVICES

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.

Application of modern technologies of adaptive information security systems does not allow full control over the information flows of the cloud computing environment, since they function at the upper levels of the hierarchy. Therefore, to create effective mechanisms for protecting software in a cloud computing environment, it is necessary to develop new threat models and to create methods for displaying computer attacks that allow operatively to identify hidden and potentially dangerous processes of information interaction.

Rules of access form the basis of security policy and include restrictions on the mechanisms of initialization processes access. Under the developed operations model, the formalized description of hidden threats is reduced to the emergence of context-dependent transitions in the multigraph transactions.

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.

к.т.н., доц. Кльоц Ю.П., к.т.н., доц. Муляр И.В., Чешун В.Н., Бурдюг О.В.

ИСПОЛЬЗОВАНИЕ РАСПРЕДЕЛЁННЫХ ХЕШ-ТАБЛИЦ ДЛЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ОБЛАЧНЫХ СЕРВИСОВ

В статье раскрыты актуальность проблемы предоставления доступа к сервисам распределенной облачной системы, в частности, охарактеризованы одноранговую распределенную облачную систему. Подано процесс взаимодействия основных компонентов для доступа к веб-ресурса с доменным именем. Доказано, что распределение ресурсов между узлами одноранговой распределенной облачной системы с последующим предоставлением сервисов по запросу реализуется с помощью протокола Kademlia в локальной сети или сети Интернет и содержит процессы публикации ресурса на начальной стадии его владельцем, репликации и непосредственно предоставления доступа к ресурсам.

Применение современных технологий адаптивных систем защиты информации не позволяет осуществлять полный контроль за информационными потоками среды облачных вычислений, поскольку они функционируют на верхних уровнях иерархии. Поэтому для создания эффективных механизмов защиты ПО в среде облачных вычислений требуется разработка новых моделей угроз и создания методов отображения компьютерных атак, которые позволяют оперативно идентифицировать скрытые и потенциально опасные процессы информационного взаимодействия.

Правила разграничения доступа, составляют основу политики безопасности, включают и ограничения на механизмы инициализации процессов доступа. В рамках разработанной модели операций формализованное описание скрытых угроз сводится к появлению контекстно-зависимых переходов в мультиграфом транзакций.

Обоснован метод предоставления доступа к сервисам распределенной облачной системы. Определено, что для поиска узла репликации, который имеет реплику запрашиваемого ресурса или его часть, применяется инфраструктура распределенных хеш таблиц. В исследовании определены этапы валидации идентификатора узла. Описаны процессы добавления нового узла, валидации подлинности, публикации ресурса и получения доступа к ресурсу представлен в виде поэтапной последовательности действий в рамках метода предоставления доступа к сервисам распределенной облачной системы с помощью графического описания информационных потоков, взаимодействия процессов обработки информации и объектов.

Ключевые слова: метод, облачная система, хеш-таблицы.