DOI: https://doi.org/10.36910/6775-2524-0560-2021-44-19
УДК 004.056
Піткевич Павло Ігорович, бакалавр технічних наук
https://orcid.org/0000-0002-1760-9395
Білоруський державний університет інформатики та радіоелектроніки

ПРИНЦИПИ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО РЕСУРСІВ СИСТЕМИ ХМАРНИХ ОБЧИСЛЕНЬ

Піткевич П. І. Принципи захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень. У статті розкрито принципи захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень. Наголошено, що продуктивність є важливим фактором для розгляду системи хмарних обчислень. Доступ до загальнодоступних хмар здійснюється через Інтернет і стикається з обмеженнями смуги пропускання, наданими їх відповідними постачальниками інтернет-послуг. Підкреслено, що масштабування до більшої пропускної здатності Інтернету може значно збільшити загальну вартість володіння хмарними рішеннями. Розглянута архітектура модулю контролю доступу, щодо забезпечення захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень, а також запропонована концептуальна схема реалізації процесів автентифікації та авторизації за допомогою модулю контролю доступу, яка відрізняється від існуючих комплексним підходом до класифікації облікових даних користувача і засобів, методів захисту, і може бути застосована до всіх інформаційних систем. Визначено основні архітектурні рішення побудови архітектури модулю контролю доступу, виявлено її переваги та недоліки з точки зору інформаційної безпеки, визначено основні моделі обслуговування хмарних обчислень, описана еталонна архітектура хмарних обчислень з точки зору захисту даних і моделі безпеки. Підкреслено, що архітектура контролю доступу має три основні частини, які працюють разом для обробки запитів доступу: модуль контролю доступу, який приймає/відхиляє/перенаправляє запити на доступ, віртуальна розподілена мережа, яка розгортає та контролює ресурси та послуги, а також централізована глобальна система управління ресурсами, яка обробляє переміщення запитів до інших хмар для віддаленого використання послуг/ресурсів. Наголошено, що глобальна система управління ресурсами діє як бар'єр між різними хмарними службами на одному рівні або різних шарах, а використання однієї централізованої глобальної системи управління ресурсами у запропонованій архітектурі ґрунтується на тому, щоб уникнути використання угоди про рівень послуг для кожного рівня обслуговування.

Ключові слова: несанкціонований доступ, модель безпеки, захист, ресурс, хмарні обчислення, управління, архітектура.

Питкевич П. И. Принципы защиты от несанкционированного доступа к ресурсам системы облачных вычислений. В статье раскрыты принципы защиты от несанкционированного доступа к ресурсам системы облачных вычислений. Отмечается, что производительность является важным фактором для рассмотрения системы облачных вычислений. Доступ к общедоступным облакам осуществляется через Интернет и сталкивается с ограничениями полосы пропускания, предоставленными их соответствующими поставщиками интернет-услуг. Подчеркнуто, что масштабирование до большей пропускной способности Интернета может значительно увеличить общую стоимость владения облачными решениями. Рассмотрена архитектура модуля контроля доступа, по обеспечению защиты от несанкционированного доступа к ресурсам системы облачных вычислений, а также предложена концептуальная схема реализации процессов аутентификации и авторизации с помощью модуля контроля доступа, которая отличается от существующих комплексным подходом к классификации учетных данных пользователя и средств, методов защиты, и может быть применена ко всем информационным системам. Определены основные архитектурные решения построения архитектуры модуля контроля доступа, выявлены ее преимущества и недостатки с точки зрения информационной безопасности, определены основные модели обслуживания облачных вычислений, описана эталонная архитектура облачных вычислений с точки зрения защиты данных и модели безопасности. Подчеркнуто, что архитектура контроля доступа имеет три основные части, которые работают вместе для обработки запросов доступа: модуль контроля доступа, который принимает/отклоняет/перенаправляет запросы на доступ, виртуальная распределенная сеть, которая разворачивает и контролирует ресурсы и услуги, а также централизованная глобальная система управления ресурсами, которая обрабатывает перемещения запросов к других облаков для удаленного использования услуг/ресурсов. Отмечено, что глобальная система управления ресурсами действует как барьер между различными облачными службами на одном уровне или разных слоях, а использование одной централизованной глобальной системы управления ресурсами в предложенной архитектуре основывается на том, чтобы избежать использования соглашения об уровне услуг для каждого уровня обслуживания.

Ключевые слова: несанкционированный доступ, модель безопасности, защита, ресурс, облачные вычисления, управление, архитектура.

Pitkevich Pavel Igorevich. Principles of protection against unauthorized access to resources of the cloud computing system. The article reveals the principles of protection against unauthorized access to the resources of the cloud computing system. It is emphasized that productivity is an important factor for considering the cloud computing system. Public clouds are accessed over the Internet and face bandwidth restrictions provided by their respective ISPs. It is emphasized that scaling to higher Internet bandwidth can significantly increase the total cost of owning cloud solutions. The architecture of the access control module for protection against unauthorized access to cloud computing system resources is considered, as well as the conceptual scheme of implementation of authentication and authorization processes using the access control module is proposed. , and can be applied to all information systems. The main architectural solutions of the architecture of the access control module are identified, its advantages and disadvantages from the point of view of information security are revealed, the basic models of cloud computing service are defined, the reference architecture of cloud computing from the point of view of data protection and security model is described. It is emphasized that the access control architecture has three main parts that work together to handle access requests: an access control module that receives / rejects / redirects access requests, a virtual distributed network that deploys and controls resources and services, and a centralized global system resource

management, which handles the movement of requests to other clouds for remote use of services / resources. It is emphasized that the global resource management system acts as a barrier between different cloud services at the same level or different layers, and the use of one centralized global resource management system in the proposed architecture is based on avoiding the use of service level agreement for each service level.

Key words: unauthorized access, security model, protection, resource, cloud computing, management, architecture.

Постановка проблеми. В умовах сьогодення, хмарні обчислення є однією з найперспективніших сучасних технологій завдяки своєму масштабованому, гнучкому та економічному доступу до обчислювальних ресурсів. Тим не менш, враховуючи масштабність даної технології, зросла концентрація бізнес-даних та рівня обчислювальної потужності, що становить ризики безпеки. Окреслений факт вимагає особливих міркувань від постачальників послуг, оскільки кібератаки розгортаються для націлювання на інфраструктуру хмарних обчислень. Подолання кібератак у середовищі хмарних обчислень є складним завданням як через масштаб проблеми, так і через зростаючу складність атак. Одна з останніх проблем безпеки пов'язана з відсутністю надійної архітектури контролю доступу, яка б могла захистити хмарні служби та ресурси від несанкціонованого доступу та зловживання даними.

Аналіз останніх досліджень і публікацій. Наразі, однією з головних тем багатьох дискусій є хмарні обчислення, і ключовим моментом в них виступає безпека хмарних обчислень. Загалом наукові здобутки приналежні до переваг та недоліків стандартів безпеки залишаючи осторонь принципи формування механізмів захисту. Так, низка науковців [1] підійшли до розгляду питання актуальності хмарних обчислень. Авторами розглянуто основні технології хмарних обчислень, проаналізовано розвиток хмарних технологій від започаткування до сьогодення Перераховано обов'язкові характеристики хмарних обчислень, які встановлені Національним інститутом стандартів.

Р.О. Баглай [2] провів аналіз загроз безпеки інформаційних технологій при впровадженні хмарних обчислень для забезпечення безперебійної та ефективної діяльності банківських установ і запропонував заходи щодо мінімізації цих загроз.

Принципи інформаційної безпеки технологій хмарних обчислень розкрила Т. І. Червякова [3]. У роботі проведено аналіз теоретичних і практичних аспектів інформаційної безпеки технології хмарних обчислень, здійснено визначення їх принципів і перспектив. В. П. Ткаченко, І. В. Огірко та О. І. Огірко [4] запропонували модель ГРІД технології.

Із зарубіжних авторів варто відзначити такі роботи як: Rizov V. [5], Sultan N. [6], Cacciatore K., Czarkowski P., Dake S., Garbutt J., Hemphill B., Jainschigg J., Moruga A., Otto A., Peters C., Whitaker B.E. [7], Kar J., Mishra M. R. [8], Reshetova E., Karhunen J., Nyman T., Asokan N. [9], White J.S., Pilbeam A.W. [10], Monov L., Karev M. [11], Xavier M.G., Neves M.V., Rossi F.D., Ferreto T.C., Lange T. [12], Morabito R. [13], Patel A., Taghavi M., Bakhtiyari K., Junior J.C. [14] та інші.

Проте, враховуючи описані наукові набутки, за темою, питання розкриття принципів захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень залишається відкритим та потребує детального опрацювання.

Постановка завдання. Розкрити принципи захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень.

Викладення основного матеріалу дослідження. Хмарні обчислення – це сукупність технологій віртуалізації та розподілених обчислень націлених на розподілену обробку даних, при якій ресурси обчислювальних систем, програмне забезпечення та інформація надаються користувачеві за запитом через віртуальну мережу. Контроль доступу до ресурсів системи хмарних обчислень є однією з найважливіших проблем безпеки, оскільки хмара «ділиться» фізичними ресурсами та програмами з різними організаціями та користувачами. Виходом є відключення доступу, проте це призведе до втрати спільного службового призначення. Таким чином, гнучкість є необхідністю при розробці механізму контролю доступу, оскільки вона повинна мати можливість враховувати різні типи політик та доменів. Методи контролю доступу діляться на: дискреційний контроль доступу; обов'язковий контроль доступу; рольовий контроль доступу; контроль доступу на основі атрибутів. Перший метод – дискреційний контроль доступу – це політика доступу, де власник має повний контроль і визначає авторизацію та дозволи інших користувачів. Крім того, як тільки один користувач володіє об'єктом, дозволи можуть бути надані іншим необхідним користувачам. Дискреційний контроль доступу зазвичай використовується зі списком контролю доступу. Таким чином, дискреційний контроль доступу дає можливість власнику легко і зручно налаштувати права користувача. Такий підхід дозволяє користувачеві легко отримати доступ до бази даних авторизації, яка містить індекс авторизованих користувачів, коли потрібно внести зміни. Однак дискреційний контроль доступу не може забезпечити

потік інформації для тих, хто запитує, і обмежити використання інформації для тих, хто не має дозволу. Ця проблема може стати потенційною вразливістю, яку можна використати, оскільки зловмисник може загрожувати цілісності даних [15]. Другий метод – обов'язковий контроль доступу – це політика доступу, де адміністратор відповідає за створення політики. З іншого боку, обов'язковий контроль доступу визначається власником. Оскільки обов'язковий контроль доступу є більш обмежувальним, ніж дискреційний контроль, обов'язковий контроль доступу використовується організаціями, які містять важливі дані або секретну інформацію. Користувачі або власники об'єкта не можуть надавати ключі авторизації чи дозволи входу іншим особам. Адміністратор – єдина особа, яка має можливість змінювати статус безпеки іншого користувача. Обов'язковий контроль доступу використовується для захисту мереж, файлових систем та забезпечення авторизації користувачів, запобігаючи доступу неавторизованих користувачів до приватної інформації. Мітка обов'язковий контроль доступу може бути застосована до користувача, що обмежить кількість рішень, доступних для останнього [16]. Крім того, коли рівень безпеки окремої особи або суб'єкта потребує зміни, змінити рівень безпеки буде неможливо. Це одне з основних обмежень методу обов'язкового контролю доступу. Третім методом виступає рольовий контроль доступу – це політика доступу, яка формулюється на основі ідеї, що роль повинна надавати дозволи авторизованій особі. Рольовий контроль доступу оптимізовано для підприємств та масштабних програм, а також цей метод доступу підтримується комерційною системою управління базами даних (СУБД) [16]. Крім того, рольовий контроль доступу заохочують організації, які хочуть зручно керувати авторизацією користувачів і застосовувати засоби контролю доступу до своїх політик. Для того, щоб зрозуміти процес рольового контролю доступу, важливо вивчити та визначити три основні правила, які використовуються цим методом. Перше правило – це призначення ролей, згідно з яким роль повинна бути призначена, перш ніж особа може отримати будь-який дозвіл. Друге правило – це авторизація ролей, яка вимагає, щоб особа отримала дозвіл на призначену роль. Третє правило – це авторизація дозволів, яка не дозволяє особі виконувати несанкціоновані дозволи, призначаючи кожній ролі власні дозволи.

Рольовий контроль доступу надає доступ до користувача на основі ієрархії ролей, яка визначається кількістю програм. Для запобігання зловживанню інформацією існує розділення ролей, яке стосується окремої ролі, призначеної кожному користувачеві. Рольовий контроль доступу дотримується певного масиву адміністративних політик для ефективної роботи, які класифікуються як: централізовані, ієрархічні, кооперативні, право власності та децентралізовані. Деякі дослідники вважають, що рольовий контроль доступу слід використовувати як політику доступу до хмарних обчислень. Однак іноді буває важко визначити, які привілеї належать до формату різних користувачів, а які користувачі отримують різні види та рівні ролей. Привілей на зміну ролі дозволяє змінювати дозволи, призначені для кожної з ролей. При спробі змінити роль користувача це може викликати плутанину, оскільки кожна роль вакансії має свій власний набір дозволів. Більше того, оскільки хмара є відносно новою парадигмою, існує ще кілька питань, які необхідно вирішити, щоб рольовий контроль доступу повністю розкрив свій потенціал та забезпечив більш ефективний контроль доступу.

Четвертий метод – контроль доступу на основі атрибутів. В останні роки метод контролю доступу на основі атрибутів стає все більш значущим через зростання популярності великих розподілених систем. Цей метод надає ефективне рішення контролю, оскільки атрибути користувачів – це критерії, які використовуються для визначення авторизації користувача. Ця політика доступу покращує рольовий контроль доступу у таких областях як:

– делегування повноважень атрибутів;
– децентралізація атрибутів;
– втручання атрибутів.

Для захисту конфіденційності облікових даних метод контролю доступу на основі атрибутів містить кілька політик щодо збереження конфіденційності користувачів та цілісності даних. Окреслений метод дуже гнучкий і здатний підтримувати широкий спектр політик і доменів. Крім того, метод контролю доступу на основі атрибутів має можливість забезпечити автоматизовані переговори щодо довіри, що дозволяє проводити аудит у разі необхідності.

Після того, як відповідні вимоги авторизації будуть виконані, можна розробити архітектуру безпеки розподіленої хмари з кінцевою метою безпечного та надійного контролю доступу. Ця архітектура може бути побудована за допомогою трьох основних компонентів, які працюють разом: глобальна система управління ресурсами, менеджер віртуальних ресурсів та модуль контролю доступу. У якості бази застосуємо метод рольового контролю доступу завдяки його прямому адмініструванню та його здатності з легкістю масштабувати вгору та вниз. Однак конструкція розподіленої архітектури

безпеки є достатньо гнучкою та загальною для роботи з іншими типами політики контролю доступу, такими як дискреційний контроль доступу. Доступ до інфраструктури хмарних обчислень починається з простого запиту користувача. Перш ніж з'явиться можливість подивитися на три компоненти, які складають архітектуру розподіленого контролю доступу, необхідно глибше подивитися на потік запитів користувачів хмари, які система буде обробляти.

Виходячи з політики методу рольового контролю доступу, запит користувача хмарної системи може бути представлений за допомогою чотирьох кордонів таким чином: облікові дані користувача, привілеї, запитуваний ресурс/послуга та файл журналу активності. Кожен запит починається з першої автентифікації користувача через модуль контролю доступу. Після перевірки облікових даних користувача права користувача визначаються та призначаються клієнту на основі ролей користувача. Права користувача будуть видимими та обробленими усіма модулями контролю доступу, які отримують запити, щоб переконатися, що користувачі не заходять у несанкціоновані зони хмарної інфраструктури. Розділ запитуваного ресурсу буде діяти як тіло запиту для віртуальної мережі на читання та надання доступних ресурсів запитуваним користувачам. Файл журналу активності відстежуватиме всю активність доступу, яка відбувається за обліковими даними користувача та призначеними привілеями. Потім ця інформація надсилатиметься до бази даних файлів журналу, пов'язаної з базою даних облікових даних користувачів у задній частині інфраструктури хмарних обчислень. Це буде важливо при розслідуванні шкідливих інцидентів та дій, що відбуваються в системі хмарних обчислень. Процеси автентифікації та авторизації за допомогою модулю контролю доступу показані на рис.1.

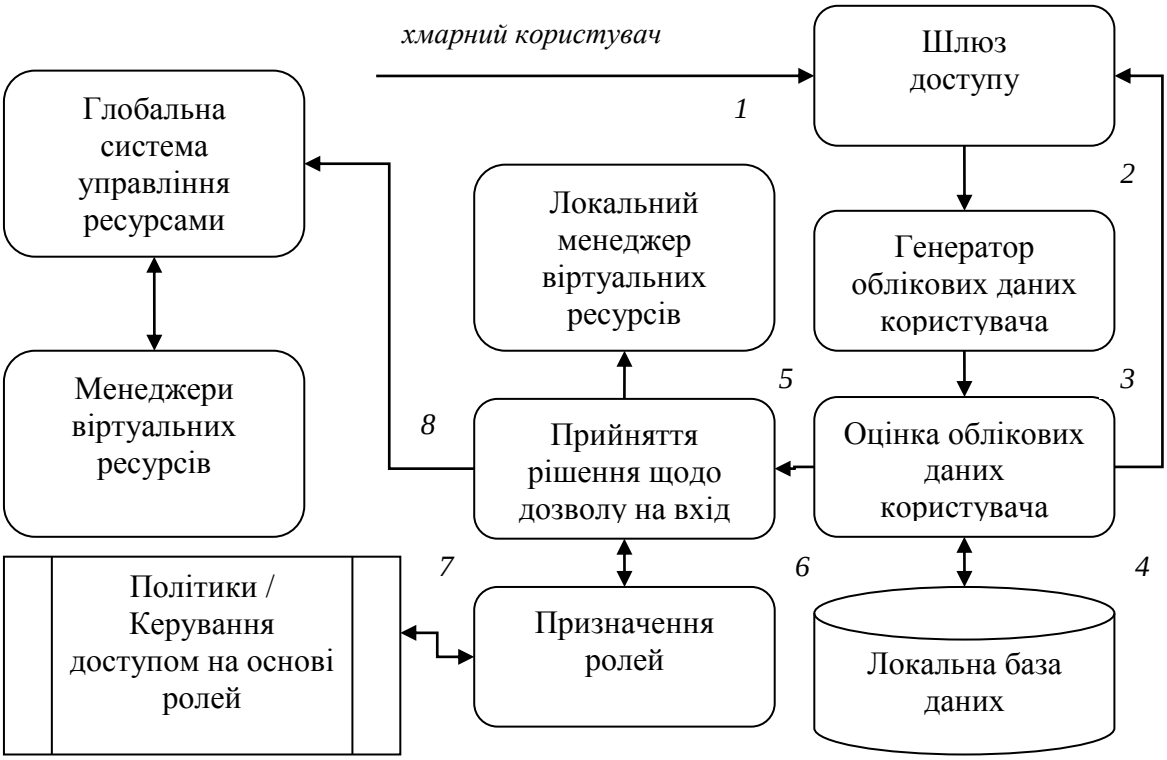

Рис. 1. Схема реалізації процесів автентифікації та авторизації за допомогою модулю контролю доступу

Запропонована схема реалізації процесів автентифікації та авторизації за допомогою модулю контролю доступу володіє наступними параметрами:

Нижче наведено деякі зі значень запропонованої нами архітектури.

– автономність модулю контролю доступу у застосуванні політики контролю доступу (тобто модуль контролю доступу служить першим шаром захисту);

– універсальність, співпраця як усередині, так і між хмарним зв'язком досягти;

– мінімізація часу відгуку, спосіб підключення глобальної системи управління ресурсами до кожного модуля контролю доступу дозволяє мінімізувати час запиту-відповіді на віддалені запити;

– розширення захисту – другий рівень захисту, створення додаткового файлу, який можна використовувати для подачі системи виявлення та запобігання вторгненням;

– широкий спектр використання, файл журналу також може бути використаний глобальною системою управління ресурсами для забезпечення «відповідності» кожного постачальника хмарних послуг у наданні послуг клієнтам.

У запропонованій архітектурі модулю контролю доступу (рис. 1) розглядається шлюз доступу, який існує на кожному рівні обслуговування хмари для захисту ресурсів від будь-якого прямого несанкціонованого доступу. Він працює, зосереджуючись на обробці та схваленні запитів на автентифікацію та авторизацію, які надходять і виходять із хмари, перш ніж потрапити до віртуальної мережі для розгортання служб. Крім того, кожен модуль контролю доступу безпосередньо аналізується за допомогою глобальної системи управління ресурсами для задоволення запитів віддаленого обслуговування. Крім того, він надає файл журналу активності кожного автентифікованого користувача до глобальної системи управління ресурсами, щоб можна було підтримувати та контролювати поточну зайнятість ресурсів та використання послуг кожного рівня хмари. Глобальна система управління ресурсами також може використовувати цю інформацію для виявлення будь-якої шкідливої діяльності на глобальному віртуальному рівні. Таким чином, глобальна система управління ресурсами має найбільш точну інформацію про всі наявні ресурси, якими керує віртуальна розподілена мережа. Це дозволяє запропонованій архітектурі гарантувати, що запити віддаленого обслуговування не будуть пересилатися більш ніж на два переходи, що зменшує загальний час запиту-відповіді.

Крім того, модуль контролю доступу можна розглядати як обробний центр, який складається з таких частин: шлюз контролю доступу, екстрактор/оцінювач облікових даних, пункт прийняття рішення про авторизацію, призначення ролей та банк політик. Коли надходить запит, він надходить на шлюз контролю доступу. На цей момент запит містить інформацію про клієнта, облікові дані доступу, потрібну службу з рівня хмари та бажаний рівень привілеїв та дозволів цієї служби.

Коли користувач надсилає запит до модулю контролю доступу, він містить бажаний рівень авторизації та конкретні облікові дані для автентифікації, які будуть використовуватися протягом усього процесу запиту. Ці облікові дані виймаються шлюзом контролю доступу та надсилаються оцінювачу облікових даних для цілей автентифікації (крок 2). Оцінювач облікових даних перевіряє облікові дані користувача у локальній базі даних і формує рішення про доступ (крок 4). Якщо запит буде відхилено через неправильні облікові дані, клієнт буде повідомлений через шлюз контролю доступу. Однак, якщо доступ надано, запит буде перенаправлено до модулю прийняття рішення щодо доступу (крок 5). Модуль прийняття рішення щодо доступу пересилає запит до модулю призначення ролі, який оцінює бажані привілеї (наприклад, дозвіл на читання або запис) для запитуваної послуги/ресурсу на основі ролі користувача запитуваного клієнта (крок 6). У нашому випадку ця оцінка ролі буде оцінена та визначена на основі збереженої політики керування доступом на основі ролей у банку політик (крок 7). Як тільки рівні авторизації визначаються через банк політик, затверджений запит із рівнем авторизації буде надіслано до відповідної локальної віртуальної розподіленої мережі (крок 8). Обмеження можуть бути застосовані на основі запиту, призначеного роллю, щодо його оцінки запитуваної послуги та відповідних запитуваних привілеїв, знайдених у запиті користувача. Це гарантуватиме, що користувачі зможуть використовувати послуги та ресурси лише в контексті свого запиту.

Після того, як модуль контролю доступу схвалить запит клієнта, облікові дані слід зберігати в локальному кеші модулю контролю доступу, щоб гарантувати, що майбутні запити від того самого клієнта не повинні проходити через усі звичайні процедури контролю доступу. Це прискорить процес автентифікації за рахунок відносно невеликого використання сховища. Однак рівень авторизації повинен визначатись і призначатись модулем контролю доступу кожного разу, виходячи з того, які послуги чи ресурси запитував клієнт. Це забезпечить суворе дотримання політики контролю доступу до всіх послуг та ресурсів, які провайдер хмарних послуг пропонує своїм клієнтам.

Як тільки затверджений запит надійде до віртуальної розподіленої мережі, він перевірить наявність потрібного ресурсу. Якщо запитуваний ресурс доступний, він буде локально розгорнутий до клієнта, а журнал активності буде ініційований модулем контролю доступу. Якщо запитуваний ресурс недоступний або він локально не існує на рівні хмари, запит користувача буде надіслано до глобальної системи управління ресурсами для подальшої допомоги. Після цього глобальна система знайде запитуваний ресурс і перенаправить запит користувача до відповідного модулю контролю доступу. Як наслідок, модуль контролю доступу залишатиметься автономною з точки зору застосування своєї локальної політики контролю доступу до запиту користувача, а не посередницької політики.

Хмарні обчислення – це метод доставки обчислювальних послуг з великого, високо віртуалізованого центру обробки даних до багатьох незалежних кінцевих користувачів, за допомогою спільних програм та об'єднаних ресурсів. Через неоднорідність та деталізацію віртуальних ресурсів

бажано мати віртуальну розподілену мережу на кожному рівні обслуговування хмари з єдиною метою управління віртуальними ресурсами, які викликаються до використання. Він несе відповідальність за розгортання служб. Коли запитуваний ресурс не існує або якщо ресурс недоступний локально, запит буде розглядатися як запит на віддалене обслуговування та передаватися до глобальної системи управління ресурсами. Остання буде використовувати свою глобальну базу даних для пересилання віддаленого запиту до відповідної віртуальної мережі через хмарний цільовий модуль контролю доступу. Цільовий модуль контролю доступу може застосовувати свою політику локального контролю доступу, щоб гарантувати, що для використання будуть застосовані лише авторизовані та запитувані послуги.

Глобальна система управління ресурсами діє як бар'єр між різними хмарними службами на одному рівні або різних шарах.

Використання однієї централізованої глобальної системи управління ресурсами у запропонованій архітектурі ґрунтується на тому, щоб уникнути використання угоди про рівень послуг для кожного рівня обслуговування (наприклад, SaaS, IaaS і PaaS). Якщо угоди про рівень послуг кожного рівня на різних хмарних платформах не тісно пов'язані між собою, запит віддаленого обслуговування може опинитися в тупиковій ситуації під час пошуку потрібної віртуальної розподіленої мережі. Він також не гарантує, скільки переходів має пройти запит віддаленого обслуговування, перш ніж він досягне потрібної віртуальної мережі. Тому використання централізованої глобальної системи управління ресурсами, аналізованої з кожним модулем контролю доступу, не тільки спрощує конструкцію контролю доступу, але і скорочує загальний час запиту-відповіді.

Щоб уникнути єдиних точок відмови централізованої глобальної системи управління ресурсами, можна запровадити надмірність. Хоча це не вимагається в запропонованій архітектурі, єдина угода про рівень послуг може перебувати в глобальній системі управління ресурсами, щоб не враховувати всі стандартні політики та процедури, щодо відповідності. Коли користувач запитує ресурси з локальної хмари, але вони не існують у зазначеному місці, запит може бути оброблений через централізовану глобальну систему управління ресурсам. Однак, якщо потрібний ресурс існує в тій самій хмарі, але на іншому рівні, запит можна надіслати безпосередньо в інший сектор або рівень хмарних послуг, щоб віддалено отримати необхідні послуги та ресурси.

Висновки і перспективи подальших досліджень. У роботі досліджено принципи захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень. Хмарні обчислення знаходяться в постійному розвитку, щоб забезпечити клієнтів різними рівнями послуг відповідно до запитів. Фундаментальний і багатосторонній аналіз принципів захисту від несанкціонованого доступу до ресурсів для інформаційної безпеки є невід'ємною передумовою розробки і супроводу успішних і ефективних заходів щодо захисту інформації в умовах хмарних обчислень. Запропонована архітектура безпеки розподіленого контролю доступу має вимоги до авторизації які є суттєвими перед розробкою архітектури розподіленого контролю доступу: децентралізована адміністрація, безпечна розподілена співпраця та класифікація облікових даних. Архітектура контролю доступу має три основні частини, які працюють разом для обробки запитів доступу: модуль контролю доступу, який приймає/відхиляє/перенаправляє запити на доступ, віртуальна розподілена мережа, яка розгортає та контролює ресурси та послуги, а також централізована глобальна система управління ресурсами, яка обробляє переміщення запитів до інших хмар для віддаленого використання послуг/ресурсів.

Перспективи подальших досліджень ґрунтуються на розробці моделі системи захисту від несанкціонованого доступу до ресурсів системи хмарних обчислень на основі центру обробки даних.

Список бібліографічного опису.

1. Орел. О., Дирда М. Дослідження актуальності хмарних обчислень / Modern engineering and innovative technologies, 2018. №05-01. С. 95-98.
2. Баглай Р. О. Загрози безпеки хмарних технологій для банків / Р. О. Баглай // Системи обробки інформації. 2018. Вип. 1. С. 127-135. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2018_1_20.
3. Червякова Т.І. Інформаційна безпека технології хмарних обчислень. / Т.І. Червякова // Вісник Національного транспортного університету. Серія «Технічні науки». Науково-технічний збірник. – К.: НТУ, 2020. – Вип. 1 (46). С. 427-436.
4. Ткаченко В. П. Інформаційна модель Грід технології / В. П. Ткаченко, І. В. Огірко, О. І. Огірко // Системи обробки інформації. 2017. Вип. 4. С. 88-91. – Режим доступу: http://nbuv.gov.ua/UJRN/soi_2017_4_20.

References.

1. Rizov V. Information Sharing for Cyber Threats // Information & Security: An International Journal. 2018. Vol. 39, Issue 1. P. 43–50. doi: http://doi.org/10.11610/isij.3904

2. Sultan N. Making use of cloud computing for healthcare provision: Opportunities and challenges. International Journal of Information Management. 2014. – V. 34. – P. 177–184.
3. Cacciatore K., Czarkowski P., Dake S., Garbutt J., Hemphill B., Jainschigg J., Moruga A., Otto A., Peters C., Whitaker B.E. Exploring Opportunities: Containers and OpenStack. OpenStack White Paper. 2015. – 19 p. URL: https://www.openstack.org/assets/pdf-downloads/Containers-and-OpenStack.pdf
4. Kar J., Mishra M. R. Mitigating Threats and Security Metrics in Cloud Computing // Journal of Information Processing Systems. 2016. Vol. 12, Issue 2. P. 226– 233. doi: http://doi.org/10.3745/jips.03.0049
5. Reshetova E., Karhunen J., Nyman T., Asokan N. Security of OS-level virtualization technologies. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1407.4245v1.pdf
6. White J.S., Pilbeam A.W. A survey of virtualization technologies with performance testing. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1010.3233.pdf
7. Monov L., Karev M. How to Counter Hybrid Threats? // Information & Security: An International Journal. 2018. Vol. 39, Issue 2. P. 113–126. doi: http://doi.org/10.11610/isij.3909
8. Xavier M.G., Neves M.V., Rossi F.D., Ferreto T.C., Lange T., De Rose C.A.F. Performance Evaluation of Container-Based Virtualization for High Performance Computing Environments. In: 21st Euro. Int. Conf. on Parallel, Distrib. & Network-based Processing. IEEE, 2013. – P. 233–240.
9. Morabito R. Power Consumption of Virtualization Technologies: an Empirical Investigation. arXiv.org: Cornell University Library. URL: http://arxiv.org/pdf/1511.01232v1.pdf
10. Patel A., Taghavi M., Bakhtiyari K., Junior J.C. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of Network and Computer Applications. 2013. V. 36. – P. 25–41.
11. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2018. – 316 с.
12. Моделі та методи контролю доступу: що вам підходить?, 2020. – Режим доступу. – https://worldvision.com.ua/ua/modeli-i-metody-kontrolya-dostupa-chto-vam-podkhodit/.