ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.891

Байдюк М.М. (ХмНУ)
к.т.н., с.н.с. **Краснік А.В.** (ПАТ «Завод Маяк»)
к.т.н., доц. **Огнєвий О.В.** (ХмНУ)

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

У статті наведено найбільш критичні загрози для середовища хмарних обчислень. Для аналізу надійності визначено характеристики середовищ та їх класифікацію. Також відмічено загрози, які можуть бути здійснені з інформаційних ресурсів, що функціонують в хмарі, та методи боротьби з ними.

Розкрито поняття, віртуалізованої обчислювальної системи, що представляє собою сукупність потужних обчислювальних платформ і в яких функціонують віртуальні обчислювальні ресурси, звані віртуальними машинами. Показана класична схема розмежування доступу, яка працює у вигляді брандмауера для моніторингу безпеки середовища хмарних обчислень.

Особливу увагу приділено методу захисту інформації, розмежуванню доступу як сервісу безпеки, що тісно пов'язаний з політикою доступу та правилам фільтрації, що безпосередньо забезпечує конфіденційність інформації, а також знижує ймовірність реалізації загроз цілісності і правомірної доступності.

Визначено, що правила розмежування доступу для між мережевих екранів виражаються у вигляді правил фільтрації які містять ознаки у вигляді полів протоколів, або вмісту пакетів, за якими мережеве з'єднання класифікується як дозволене, заборонене або невизначене

Ключові слова: хмарні обчислення, розмежування доступу, політика даних, віртуальна машина, інформаційна взаємодія, гіпервізор, між мережевий екран.

Вступ. Процес розвитку інформаційних технологій відчуває потребу у використанні інноваційних рішень в області створення систем захисту корпоративних даних. Це пов'язано з тим, що з одного боку інтеграційні процеси дозволяють істотно полегшити і прискорити доступ до різних видів даних, але при цьому потрібно використання відкритої архітектури систем зберігання і обробки, що істотно знижує ступінь захищеності інформації від несанкціонованого доступу і підвищує ризики неавторизованого використання. Постійне ускладнення мережевої інфраструктури, що збільшуються швидкість процесів обміну даними і широке використання технологій розподілених сервісів висувають високі вимоги до ефективності функціонування систем розмежування доступу до інформаційних ресурсів.

Розвиток мережевих технологій в напрямку створення середовищ хмарних обчислень висуває нові вимоги до засобів розмежування доступу інформаційних сервісів - одному з основних компонент сучасних систем інформаційної безпеки. Ці вимоги випливають з необхідності врахування динамічного характеру процесів виділення обчислювальних і мережних ресурсів при конфігурації віртуальних машин і структури адресного простору, використовуваного для доступу до інформаційних сервісів.

Важливість вирішення завдань такого класу відзначається у таких вчених як Н.А. Гайдамакин, П.Д. Зегждой, В.Ю. Скибою, М. Сріватса, Т. Вангом і ін.

У сучасній літературі підхід до створення складних технічних систем, зв'язаність яких забезпечується за рахунок організації процесів обміну інформацією по мережі, отримав назву мережево-центричний. Цей підхід стосовно до задачі розмежування доступу вимагає забезпечення ситуаційної обізнаності та локальності дій кожного з між мережевих екранів(ММЕ), що входять в угруповання віртуальних машин, використовуваних в середовищі хмарних обчислень для реалізації політики даних.

Постановка задачі. При використанні середовища хмарних обчислень для розміщення інформаційних сервісів особливу актуальність набуває складна науково-технічна задача

розвитку технологій захисту інформації, що забезпечує виконання вимог політики даних в мережевому середовищі з динамічно змінними характеристиками.

Інформаційна безпека в широкому розумінні являє собою такий стан об'єкта захисту, яке виключає можливість нанесення шкоди властивостями об'єкта, обумовлена його взаємодією з інформаційної сферою

Актуальним завданням розмежування доступу є формалізація вимог розмежування доступу до інформаційних сервісів в середовищі хмарних обчислень, яке може бути представлене з використанням динамічно формованого набору правил фільтрації, що забезпечує виконання вимог політики даних.

Метою роботи є аналіз можливих загроз в середовищі хмарних обчислень та огляд існуючих методів захисту. Аналіз методу розмежування доступу до інформаційних сервісів з використанням між мережевих екранів та принцип його дії.

Аналіз відомих досліджень і публікацій. У документах Національного Інституту Стандартів і Технологій США NIST[1] питання захисту інформації відзначається як відкритий для обговорення. Для розробки стандартів і рішень в сфері хмарних обчислень в 2009 році був створений спеціальний саміт Cloud Standards Summit. Ініціатором об'єднання зусиль по стандартизації хмарних обчислень і зберігання даних виступила робоча група Object Management Group (OMG), що займається розробкою і просуванням об'єктно-орієнтованих технологій і стандартів. Метою є розвиток інформаційних технологій і узгодження стандартів з проблем середовищ хмарних обчислень в державному секторі[2].

За висвітленість питань інформаційної безпеки в середовищі ХО найбільший інтерес представляє організація CSA - некомерційна організація, створена з метою просування передового досвіду в галузі забезпечення безпеки хмарних обчислень, а також для підвищення рівня обізнаності з даної тематики всіх зацікавлених сторін. CSA виділяє для себе цілий ряд завдань для хмарних середовищ, серед яких підтримка взаємовідносин споживачів і постачальників послуг в частині вимог безпеки і контролю якості, незалежні дослідження в області захисту інформації, виявлення і запобігання мережевих атак на хмарні обчислення, розробка посібників та методичних рекомендацій щодо забезпечення безпеки. Зокрема, документ «Top Threats to Cloud Computing» [3] висвітлює можливі загрози, які виникають в середовищі хмарних обчислень. Найбільш значущі загрози в середовищі хмарних обчислень:

1. Неправомірне використання хмарних сервісів. Провайдери середовища хмарних обчислень надають клієнтам ілюзію необмежених обчислювальних, мережевих ресурсів і засобів зберігання даних. Доступ до публічного хмарного середовища може отримати практично кожен. Найчастіше для доступу достатньо наявності кредитної карти і адреси електронної пошти. Завдяки цьому, обчислювальні ресурси хмарних систем типу IaaS і PaaS активно використовуються для розсилки спаму, розподілених DDOS атак, розміщення шкідливого коду, злому паролів і інших злочинних дій.

2. Незахищені програмні інтерфейси. Хмарні провайдери надають своїм клієнтам програмні інтерфейси для управління сервісами і обчислювальними ресурсами. Як правило, інтерфейси доступу функціонують поверх протоколу HTTP з використанням SOAP повідомлень, або REST. Від безпеки і доступності програмних інтерфейсів залежить функціонування всієї середовища хмарних обчислень, тому керуючі сервіси повинні бути захищені криптографічними методами захисту. Крім того, повинна бути забезпечена авторизація та аутентифікація користувачів хмари і моніторинг компонентів СХО. Погіршує ситуацію, те що організації і треті особи можуть створювати «надбудови» над наданим провайдером сервісами для розширення їх функціональності, але в той же час, ці надбудови можуть містити потенційно вразливі місця і бути схильні до випадковим або зловмисному впливу.

3. Зловмисники інсайдери. Користувачі хмари, перебуваючи всередині середовища хмарних обчислень, можуть зробити злочинні дії, спрямовані на порушення політики інформаційної безпеки провайдера хмари, або інших його користувачів. Зловмисник може

здійснити атаку на обчислювальні ресурси інших користувачів, або на сервіси хмари, перебуваючи при цьому всередині периметра безпеки.

4. Спільні ресурси. СХО надає сервіси роздільної розподіленої інфраструктури. Користувачі поділяють єдині апаратні ресурси, а значить, потенційно схильні до дії з боку сусідів. Наприклад, зловмисник може здійснити перевантаження мережі, підсистеми введення виведення, або процесорних ресурсів, викликавши, таким чином, недоступність сервісів для інших користувачів. Широко використовуються апаратні складові, такі як кеші процесора, графічні обчислювачі, або ОЗУ не забезпечують необхідного рівня ізоляції віртуалізованних ресурсів і не спроектовані для багаторівневої архітектури. Для вирішення даної проблеми використовується програмна абстракція гіпервізора, який може містити уразливості в програмному коді.

5. Втрата або витік даних. Управління даними в хмарних системах здійснюється шляхом викликів сервісів і, наприклад, ненавмисний виклик сервісу видалення об'єкта призведе до того, що дані відновити буде неможливо, так як провайдер повинен забезпечити сумлінне видалення інформації і не несе відповідальності за помилки в коді або діях користувача хмари. Також конфіденційність інформації може бути скомпрометована в разі втрати або злому облікового запису користувача, або передачі даних по ненадійних каналах зв'язку.

6. Втрата або отримання даних облікового запису третіми особами. Так як управління ресурсами в хмарі здійснюється віддалено, шляхом взаємодії з мережі, то в разі отримання ідентифікаційних ключів, пароля, або будь-яких інших даних облікового запису користувача зловмисник отримує повний контроль над хмарними ресурсами і може, як роздобути дані користувача, так і видалити їх , або модифікувати.

7. Відсутність контролю над сервісами користувача. Дана загроза в першу чергу стосується IaaS і PaaS системи, в меншій мірі зачіпаючи SaaS сервіси. У IaaS системах користувач має повний контроль над програмним забезпеченням своїх ресурсів, при цьому хмарний провайдер не може забезпечити відсутність вразливостей в ПО користувача і зобов'язати його своєчасно встановлювати оновлення використовуваного програмного забезпечення.

Виклад основного матеріалу. Хмарні обчислення - це доступні через мережу обчислювальні ресурси. Хмарна система і її користувачі реалізують модель «клієнт-сервер», таким чином, клієнти відправляють повідомлення по комп'ютерній мережі до серверів, які виконують запит користувача, відправляючи результат в повідомленні-відповіді. У роботі під середовищем хмарних обчислень буде використовуватися наступне визначення що, більш повно відображає властивості даної системи:

Хмарні обчислення - це мережево-центрична модель, надання сервісу доступу на вимогу до роздільної сукупності реконфігурованих інформаційних і обчислювальних ресурсів, таких як мережі, сервери, засоби зберігання даних і інформаційні програми.

У систем хмарних обчислень можна виділити наступні ключові характеристики:

1. Самообслуговування. Споживач повинен мати можливість самостійно забезпечити себе обчислювальним ресурсом, наприклад, таким як сервер або мережеве сховище, без людської участі з боку провайдера. Всі операції по виділенню ресурсу повинні бути автоматизовані.

2. Відритий мережевий доступ. Сервіс надається по стандартній мережі передачі даних і доступний за стандартними інтерфейсами доступу, взаємодія з якими може бути здійснена за допомогою різних клієнтських платформ - мобільних пристроїв, лаптопів, робочих станцій. Під стандартною мережею розуміються IP мережі передачі даних.

3. Спільні ресурси. Обчислювальні ресурси хмарної системи розділяються на обслуговування для багатьох споживачів за допомогою моделі оренди різних фізичних і віртуалізованних ресурсів призначуваних і перепризначуваних відповідно до запитів клієнтів. Користувач послуги не володіє інформацією і не може контролювати точне місцезнаходження ресурсу, наприклад, таке як конкретний сервер, але може вказати більш високорівневу вимогу, наприклад, країну, регіон.

4. Масштабованість. Ресурси хмари повинні мати можливість масштабування, яке зазвичай автоматизовано для споживача сервісу серед хмарних обчислень виглядає як невичерпне джерело ресурсів, які можна запросити коли завгодно і в якій завгодно кількості.

5. Збалансованість. Середовище хмарних обчислень повинне контролювати і оптимізувати витрати ресурсів. Прикладом балансування навантаження може служити міграція віртуальних машин між обчислювальними вузлами, або видача потоків даних відразу з декількох серверів розподіленого сховища.

Класифікація середовищ хмарних обчислень, за рівнем сервісу, що надається[4].

1. Програмне забезпечення як сервіс (Software as a Service, SaaS).

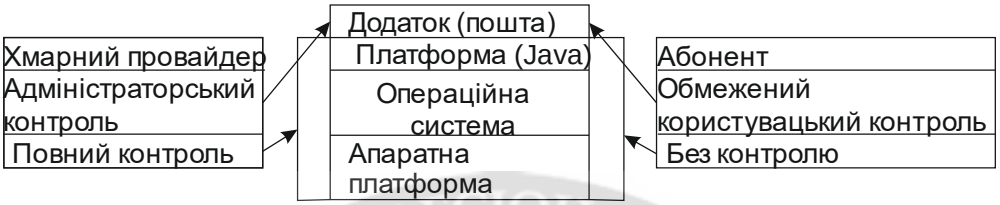

Рис. 1. Контроль SaaS додатка користувачем і провайдером середовища ХО

Споживачеві надається сервіс у вигляді додатків, запущених в хмарній інфраструктурі. Програма є доступною користувачеві з різних клієнтських пристроїв і додатків, наприклад, через веб браузер.

Споживач сервісу не контролює нижні рівні, включаючи мережі, сервери, операційні системи, але може поставити обмежений ряд налаштувань програми.

2. Платформа як сервіс (Cloud Platform as a Service, PaaS).

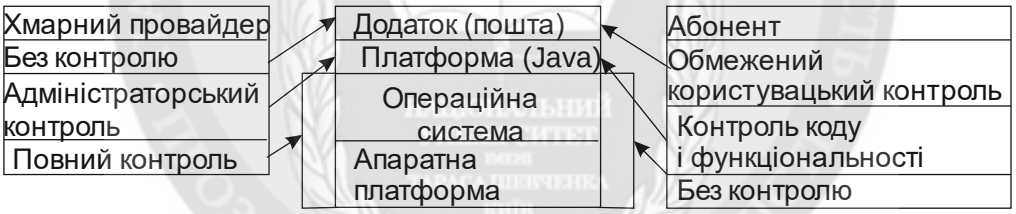

Рис. 2. Контроль PaaS додатка користувачем і провайдером середовища ХО

У даному випадку сервісом є обчислювальне середовище, в якій споживач може помістити власний додаток, який повинен підтримувати мови програмування, інтерфейси і технології, що надаються хмарним провайдером. Споживач не контролює нижні рівні, такі як сервера і операційні системи, але має доступ до конфігурації програми і задає функціональність розміщуваного сервісу.

3. Інфраструктура як сервіс (Infrastructure as a service, IaaS).

Рис. 3. Контроль IaaS додатка користувачем і провайдером середовища ХО

Споживачеві надається можливість управління обчислювальними ресурсами, сховищами і мережами. На обчислювальні ресурси споживач може самостійно встановити необхідне системне і прикладне програмне забезпечення.

В усіх СХО використовується віртуалізація. Віртуалізацією називається структура або методологія поділу ресурсів одного фізичного сервера на кілька середовищ виконання, шляхом застосування однієї або декількох концепцій або технологій, таких як апаратний і програмний поділ, поділ за часом, часткова або повна машинна симуляція і емуляція.

Віртуальну обчислювальну машину в неактивному стані можна визначити як сукупність образів жорсткого диска і метаданих, що описують конфігурацію віртуальної машини. Метадані містять інформацію про обсяг пам'яті віртуальної машини, кількості обчислювальних ядер або процесорів, фізичних мережевих інтерфейсів та інших периферійних пристроїв введення виведення. При цьому запущена віртуальна машина володіє також атрибутами використовуваного гіпервізора, унікальним ідентифікатором і налаштуваннями мережевих інтерфейсів. Взаємодія віртуальних машин, код яких виконується в ізольованих доменах, здійснюється по мережі. У зв'язку з цим, контроль мережевої взаємодії в середовищі хмарних обчислень встає на перше місце. Для функціонування мережевої підсистеми гіпервізор надає для віртуальних машин функціональність програмного мережевого моста, званого віртуальним комутатором, який представляє собою програмний компонент ОС гіпервізора. При цьому якщо необхідно забезпечити зв'язок віртуальних машин із зовнішнім світом, до програмного мосту підключається також фізичний інтерфейс гіпервізора, що знаходиться під управлінням ОС гіпервізора. Таким чином, взаємодія віртуальних машин в рамках одного гіпервізора здійснюється без використання фізичних ліній зв'язку та забезпечується програмним способом. Відповідно засіб контролю такого трафіку може бути теж або програмним комплексом, що функціонує в рамках гіпервізора, або апаратним засобом, інтегрованим з програмною реалізацією мережевого моста.

Ще однією особливістю віртуалізованої системи є можливість атаки на гіпервізор з віртуальної машини. Методом такої атаки є використання вразливостей в паровіртуалізованних драйверах віртуальної машини і в коді гіпервізора, через які можна отримати доступ до ресурсів, що знаходяться поза віртуальною машиною, в тому числі і до привілейованого домену гіпервізора. Як приклад такої вразливості можна привести CVE-2011-1751 в гіпервізорі KVM, яка дозволяє виконати довільний код у керуючій операційній системі гіпервізора.

Керуючі сервера середовища хмарних обчислень є критично важливими компонентами, від функціонування яких залежить працездатність всієї середовища ХО[4]. Перераховані компоненти схильні до загрозам, які можуть бути здійснені з віртуальних машин або із захоплених гіпервізорів. Можуть бути здійснені атаки типу «відмова в обслуговуванні», мережевий доступ до ОС сервера, відправлення некоректних повідомлень до керуючих сервісів хмари.

Необхідно, також, відзначити загрози і об'єкти атаки в середовищі ХО, які можуть бути здійснені з інформаційних ресурсів, що функціонують в хмарі:

1. Загроза захоплення керуванням хмарою;
2. Загроза отримання контролю над гіпервізором;
3. Загроза перехоплення і модифікації складу віртуальної машини;
4. Загроза прослуховування трафіку;
5. Загроза порушення кордонів ізоляції віртуальної машини.

Для протидії вищеозначених загрозам в наведені механізми, які можуть бути застосовані для захисту хмарних систем:

1. Використання стійких механізмів аутентифікації і авторизації.
2. Підключення засобів моніторингу гіпервізора і керуючих компонентів хмари.
3. Використанням системи виявлення атак.
4. Розміщення керуючої мережі хмари і мережі віртуальних машин в окремих фізичних каналах зв'язку.

5. Використання коштів розмежування, контролю та керування доступом.

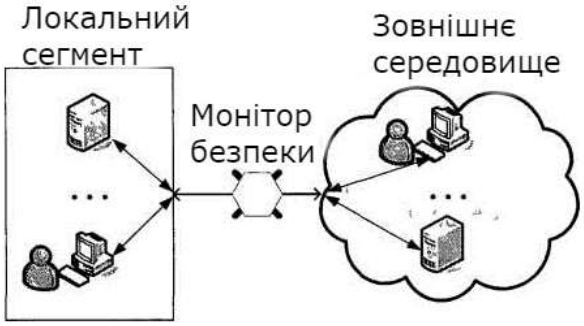

Рис. 4. Класична схема розмежування доступу

Перші два пункти відносяться безпосередньо до хмарної платформи і можуть контролюватися в заданих межах в залежності від використовуваної технології. Третій і четвертий пункти повинні бути забезпечені при розгортанні хмарної системи. Окремої уваги необхідно приділити п'ятому пункту - засобам контролю і розмежування доступу.

Розмежування доступу як сервіс безпеки невідривно пов'язаний з політикою доступу, визначає повноваження суб'єктів при зверненні до об'єктів, і механізму, що реалізує цю політику. Політика інформаційної безпеки може бути задана з використанням однієї з поширених мандатних, дискреційних і рольових моделей[6]. Кінцевим засобом, що здійснює розмежування доступу, є монітор безпеки, який в роботі позначений у вигляді брандмауера. Однак якщо класичним методом застосування між мережевих екранів в комп'ютерних мережах є розмежування доступу між сегментами мереж, то СХО має особливості, які вимагають окремого розгляду. У середовищі ХО відсутній в явному вигляді периметр безпеки, який можна виділити в класичних комп'ютерних мережах. Так як інформаційні ресурси в хмарі запускаються різними користувачами, але при цьому функціонують в одному обчислювальному середовищі і можуть бути запущені в одному гіпервізорі і підключені до одного програмного комутатора, то виділити вищезазначені межі сегментів в комп'ютерній мережі хмари не можна. Це призводить до того, що між мережевий екран повинен мати інформацію про приналежність інформаційного ресурсу хмари тій чи іншій групі або користувачеві, щоб здійснювати виконання політики безпеки в області розмежування доступу. Правила розмежування доступу для між мережевих екранів виражаються у вигляді правил фільтрації для яких сформульована алгебра. Правила фільтрації містять ознаки у вигляді полів протоколів, або вмісту пакетів, за якими мережеве з'єднання класифікується як дозволене, заборонене або невизначене [5]. Важливим параметром при фільтрації трафіку є мережева адреса інформаційного сервісу. У середовищі хмарних обчислень адреси інформаційних ресурсів змінюються динамічно, можуть бути призначені або звільнені користувачем хмарної системи. Тому, необхідно забезпечити механізм відповідності між користувачами хмарної системи і адресами інформаційних ресурсів. Також необхідно відзначити можливість міграції інформаційних ресурсів між гіпервізорами. В процесі функціонування віртуальна машина може бути переміщена на інший вузол віртуалізації з метою розподілу навантаження в хмарній системі або для проведення сервісних робіт на звільненому вузлі. Система розмежування доступу повинна враховувати можливість міграції віртуальних машин.

Висновки. На основі опису загроз на стан захищеності ресурсів середовищ хмарних обчислень та методів боротьби з ними виявляється, що використання стандартних підходів не дозволяє вирішити проблему підвищення рівня захищеності середовища хмарних обчислень. Тому для створення інформаційної безпеки в середовищі хмарних обчислень, потрібна розробка нових методів, алгоритмів, програмних продуктів, що дозволять попередити вторгнення різних загроз чи швидко виявляти їх та знешкоджувати.

ЛІТЕРАТУРА:

1. NIST Cloud Computing Synopsis and Recommendations, SP 800-146 [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST SP800146.pdf,

2. Емельянова Ю. Г. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления / Ю. Г. Емельянова, В. П. Фраленко // Программные системы: теория и приложения: электрон, научн. журн. 2011. No 4(8), с. 17-31. [Електронний ресурс]. Режим доступа: http://psta.psiras.ru/readypsta2011 4 17-31 .pdf.

3. Cloud Security Alliance, Top Threats to Cloud Computing, Март 2010. [Електронний ресурс]. Режим доступу: http://www.cloudsecurityalliance.Org/topthreats/csathreats.v 1.0

4. Клементьев И. П. Введение в Облачные вычисления. / И. П. Клементьев, В. А. Устинов // – Издательство УГУ, 2009. 233 с.

5. Заборовский В.С. Многоядерная вычислительная платформа для высокопроизводительных межсетевых экранов. Высокопроизводительные вычислительные системы / В.С.Заборовский, А.А. Лукашин, С.В. Купреенко // Материалы VII Международной научной молодежной школы. –Таганрог : Изд-во ТТИЮФУ, 2010. 336 с.

6. Девянин П.Н., Модели безопасности компьютерных систем: учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин. - М.: Издательский центр «Академия», 2005. 144 с.

REFERENCES:

1. NIST Cloud Computing Synopsis and Recommendations, SP 800-146 [Elektronniy resurs]. Rezhim dostupu: http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST SP800146.pdf,

2. Emelyanova Y.G. Analiz problem i perspektivy sozdaniya intellektualnoy sistemy obnaruzheniya i predotvrashcheniya setevyh atak na oblachnye vychisleniya / Y. G. Emelyanova, V. P. Fralenko // Programmnye sistemy: teoriya i prilozheniya: elektron, nauchn. zhurn. 2011. No 4(8), s. 17-31. [Elektronniy resurs]. Rezhim dostupa: http://psta.psiras.ru/readypsta2011 4 17-31 .pdf.

3. Cloud Security Alliance, Top Threats to Cloud Computing, Mart 2010. [Elektronniy resurs]. Rezhim dostupu: http://www.cloudsecurityalliance.Org/topthreats/csathreats.v 1.0

4. Klementev I. P. Vvedenie v Oblachnye vychisleniya. / I. P. Klementev, V. A. Ustinov // – Izdatelstvo UGU, 2009. 233 s.

5. Zaborovskiy V.S. Mnogoyadernaya vychislitelnaya platforma dlya vysokoproizvoditelnyh mezhsetevyh ekranov. Vysokoproizvoditelnye vychislitelnye sistemy / V.S.Zaborovskiy, A. A. Lukashin, S. V. Kupreenko // Materialy Sedmoy Mezhdunarodnoy nauchnoy molodezhnoy shkoly. –Taganrog : Izd-vo TTIYuFU, 2010. 336 s.

6. Devyanin P.N., Modeli bezopasnosti kompyuternyh sistem: ucheb. posobie dlya stud. vyssh. ucheb. zavedeniy / P. N. Devyanin. - M.: Izdatelskiy tsentr «Akademiya», 2005. 144 s.

Рецензент: д.т.н., с.н.с. Селюков О.В., заступник директора ТОВ «Укрспецконсалтинг».

Байдюк Н.Н., к.т.н., с.н.с. Красник А.В., к.т.н., доц. Огневой А.В.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СРЕДЕ ОБЛАЧНЫХ ВИЧИСЛЕНИЙ

В статье приведены наиболее критические угрозы для среды облачных вычислений. Для анализа надежности определены характеристики сред и их классификацию. Также отмечено угрозы, которые могут быть осуществлены с информационных ресурсов, функционирующих в облаке, и методы борьбы с ними.

Раскрыто понятие, виртуализированной вычислительной системы, представляющей собой совокупность мощных вычислительных платформ и в которых функционируют виртуальные вычислительные ресурсы, называемые виртуальными машинами. Показана классическая схема разграничения доступа, которая работает в виде брандмауэра для мониторинга безопасности среды облачных вычислений.

Особое внимание уделено методу защиты информации, разграничению доступа как сервиса безопасности, тесно связан с политикой доступа и правилам фильтрации, что непосредственно обеспечивает конфиденциальность информации, а также снижает вероятность реализации угроз целостности и правомерной доступности.

Определено, что правила разграничения доступа для между сетевых экранов выражаются в виде правил фильтрации, которые содержат признаки в виде полей протоколов, или содержимого пакетов, за которыми сетевое соединение классифицируется как разрешенное, запрещенное или неопределенное

Ключевые слова: облачные вычисления, разграничение доступа, политика данных, виртуальная машина, информационное взаимодействие, гипервизор, межсетевой экран.

Baydyuk N.N., Ph.D. Krasnik A.V., Ph.D. Ognjevyj A.V.

PROVIDING INFORMATION SECURITY IN CLOUD COMPUTING ENVIRONMENTS

The article presents the most critical threats for the cloud computing environment. Reliability analysis defined the characteristics of the environments and their classification. Also the threats which can be implemented with information resources, functioning in the cloud, and methods of dealing with them.

The concept of virtualized computing system, which is a combination of powerful computing platforms in which operate the virtual compute resources called virtual machines. Shows the classic scheme of access control, which works as a firewall for security monitoring in cloud computing.

Special attention is paid to the technique of information protection, access control as a service security is closely linked to the access policy and filtering rules that directly provides the confidentiality of the information and reduces the likelihood of realization of threats to the integrity and legitimate availability.

Determined that the rules of differentiation of access between the network screens are expressed in the form of filtering rules that contain signs field protocols, or content packages, for which the network connection is classified as permitted, prohibited or undefined

Keywords: cloud computing, access control, data policy, virtual machine, communication, hypervisor, firewal.