УДК 004.891

к.т.н., доц. **Огнєвий О.В.** (ХмНУ)
к.т.н., с.н.с. **Краснік А.В.** (ВІКНУ)
Байдюк М.М. (ХмНУ)

МОДЕЛЬ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ ДЛЯ ОПИСУ ПРОЦЕСІВ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СЕРВІСІВ

У статті проведено аналіз системи розмежування доступу в мережевому середовищі із динамічно змінними параметрами, до яких відноситься, зокрема, середовище хмарних обчислень. Модель опису процесів інформаційної взаємодії, пропонується використовувати для створення системи розмежування доступу до інформаційних ресурсів, заснованих на використанні алгоритмів оперативного синтезу правил фільтрації і динамічної конфігурації міжмережевих екранів. Оглянуто формальну специфікацію рольової моделі. Наведено опис інформаційного обміну та стану середовища хмарних обчислень. А саме три його розділи: інформаційний обмін в мережі віртуальних машин, інформаційний обмін у мережі управління та інформаційний обмін у захисті (security plane).

Особливу увагу приділено методу динамічного формування правил фільтрації для міжмережевих екранів у відповідності з мінливими параметрами інформаційної взаємодії, представлених у формі віртуальних з'єднань. Метод дозволяє оперативно реагувати на зміну складу віртуальних машин у середовищі хмарних обчислень та зміну мережевих, фізичних і логічних адрес ресурсів, у рамках яких функціонують інформаційні сервіси.

Розглянуто два підходи формування правил фільтрації для середовища хмарних обчислень, складових системи розмежування доступу. Перший підхід використовує формування правил фільтрації по подіям, другий ґрунтується на формуванні правил фільтрації для встановлених віртуальних з'єднань.

Ключові слова: Міжмережевий екран, розмежування доступу, середовище хмарних обчислень, віртуальні машини, гіпервізор, правила фільтрації, політика доступу.

Вступ. Для опису інформаційної взаємодії в середовищі хмарних обчислень, здійснюваного мережею, в роботі приведено модель інформаційної взаємодії, що описує

процеси розмежування доступу до інформаційних сервісів з урахуванням динамічних характеристик середовища хмарних обчислень.

В роботі запропоновано розвиток підходів до вирішення завдання розмежування доступу за допомогою міжмережевих екранів в середовищі хмарних обчислень.

Для формування політики даних в середовищі хмарних обчислень використана рольова модель розмежування доступу.

Постановка задачі. Створення моделі обумовлено необхідністю опису процесів інформаційного обміну між суб'єктом і об'єктом у мережевому середовищі з мінливими параметрами взаємодії. Мережеву взаємодію представлено у вигляді сукупності віртуальних з'єднань між суб'єктом та об'єктом, які реалізуються з допомогою протоколів транспортного рівня в мережах TCP/IP. У моделі політики доступу використовується поняття інформаційно-віртуального з'єднання, що дозволяє описати інформаційні сервіси, що функціонують у віртуальних машинах середовища хмарних обчислень, і правила доступу до них з використанням відомих понять, таких як веб-сервер, сервіс доступу ssh, віддалений робочий стіл, та інші. Опис інформаційно-віртуального з'єднання перетворюється в множина правил фільтрації, які дозволяють здійснити контроль мережевих з'єднань з допомогою міжмережевого екрана.

Виклад основного матеріалу. Розглянемо інформаційну взаємодію в середовищі хмарних обчислень. Згідно [1] для опису процесів розмежування доступу будемо використовувати поняття суб'єкта s і об'єкта o. Суб'єкт є активною сутністю, ініціатором взаємодії і за допомогою об'єкта, здійснює дію стосовно об'єкта o_2, при цьому здійснюється обмін інформацією комп'ютерною мережею.

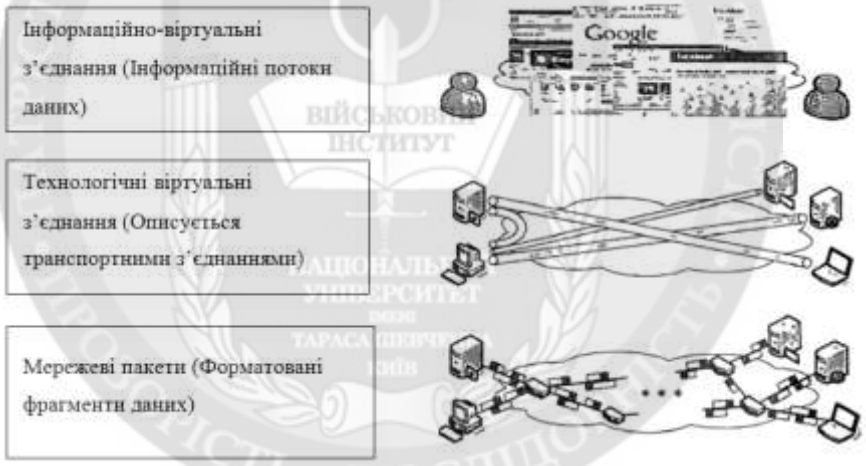

Рис. 1. Опис інформаційної взаємодії в формі віртуального з'єднання

Під міжмережевим екраном розуміється сервіс інформаційної безпеки, який забезпечує контроль мережевої взаємодії між віртуальними машинами в середовищі хмарних обчислень. Міжмережевий екран є монітором безпеки, активною компонентою інформаційного обміну, що здійснює контроль взаємодії, при цьому залишається невидимою для учасників інформаційного обміну. В роботі розглядаються міжмережеві екрани типу «стелі», які здійснюють контроль інформаційної взаємодії в невидимому режимі і не можуть бути ідентифіковані учасниками інформаційного обміну [2].

Основою рольових моделей є введення в суб'єктно-об'єктну модель комп'ютерної системи додаткової категорії активних сутностей – ролей. Можна дати наступне формальне визначення ролі[3]: роллю називається активно дієва в комп'ютерній системі абстрактна сутність, яка логічно взаємопов'язана з набором повноважень, необхідних для виконання певних функціональних обов'язків користувачами системи.

Формальна специфікація рольової моделі представляється наступним чином[4]:

1. Комп’ютерні системи представляється сукупністю наступних множин

– користувачів U;

– ролей R;

– повноважень P;

– сеансів C роботи користувачів з системою.

2. Рольові відносини встановлюються такими відображеннями множин сутностей системи:

– $F_{PR}: PxR$– відображення множини повноважень на множина ролей;

– $F_{UR}: UxR$– відображення множини користувачів на множина ролей.

3. Управління доступом в системі здійснюється на основі введення наступних функцій:

– $f_{user}: C \to U$ –значенням функції $u = f_{user}(c)$ є користувач $u \in U$, який здійснює даний сеанс в системі;

– $f_{roles}: C \to R$ – значенням функції $R_c = f_{roles}(c)$ є набір ролей $R_c \in R$ з доступних користувачеві, за яким користувач здійснює доступ в даному сеансі $c \in C$;

– $f_{permissions}: C \to P$ - значенням функції $P_c = f_{permissions}(c)$ є набір повноважень $P_c \in P$, доступних за всіма ролями, задіяними користувачем в даному сеансі $c \in P$.

4. Основне правило (критерій безпеки) рольового доступу визначається наступним чином: система функціонує безпечно, якщо і тільки якщо будь-який користувач $u \in U$, що працює в сеансі $c \in C$, може здійснювати дії (операції, процедури) у рамках повноважень р $p \in P$, за умови, що $p \in f_{permissions}(c)$.

Дія d, що здійснюється суб'єктом стосовно об'єкта в мережевому середовищі, що реалізується у вигляді обміну пакетним трафіком комп'ютерною мережею. Для опису дії використовується абстракція віртуального з'єднання[5]. Для опису політики розмежування доступу віртуального з’єднання класифікуються на технологічні віртуальні з'єднання та інформаційні віртуальні з'єднання[6]. На рис. 1 представлені рівні опису інформаційних потоків в комп'ютерній мережі. На нижньому рівні знаходяться мережеві пакети, які можна описати як форматовані фрагменти даних. Технологічні віртуальні з'єднання представлені транспортними протоколами, такими як TCP і UDP, а характеристики сполук представлені значеннями полів протоколів і їх статичними параметрами. Інформаційні віртуальні з'єднання описують дію, скоєну суб'єктом стосовно об'єкта. Інформаційні віртуальні з’єднання можуть складатися з декількох технологічних віртуальних з’єднань. Прикладом інформаційних віртуальних з’єднань може бути сесія користувача у веб браузері, отримання файлу по протоколу FTP або сеанс чату в офісному засобі обміну повідомленнями. Необхідно зазначити, що можлива ситуація[7], коли в рамках одного технологічно-віртуального з’єднання може бути виконано кілька інформаційно-віртуальних з’єднань. Прикладом може служити виконання декількох запитів з HTTP зверненням за різними URL в рамках одного TCP з'єднання. В специфікації протоколу HTTP RFC 2616 зазначено, що обмін повідомленнями може здійснюватися в рамках однієї TCP сесії (механізм persistent connections), але дії можуть бути різними.

Наведемо опис інформаційного обміну та стану середовища хмарних обчислень[8]. Інформаційний обмін можна розділити на три рівні: інформаційний обмін в мережі віртуальних машин, інформаційний обмін у мережі управління та інформаційний обмін у захисту (security plane). Середовище хмарних обчислень складається з об'єктів, що належать трьом класам:

1. Керуючі компоненти;

2. Інформаційні ресурси середовища хмарних обчислень;

3. Система розмежування в середовищі хмарних обчислень.

До першого класу відносяться гіпервізори, в рамках яких здійснюється запуск віртуальних машин, сервера для зберігання даних, керуючі сервера та системи авторизації та аутентифікації. Інформаційний обмін між перерахованими компонентами необхідний для

функціонування середовища. До другого класу відносяться інформаційні сервіси, які функціонують у віртуальній машині середовища. Третій клас - компоненти системи розмежування доступу в середовищі хмари, яка складається з міжмережевих екранів і сервісу управління. Всі перераховані компоненти ідентифікуються мережевими адресами, які належать трьом підмережам: N_{man} – мережа керуючих компонент, N_{vm} – мережа віртуальних машин середовища, N_{sec} – мережа системи розмежування доступу.

Мережева взаємодія в хмарі контролюється за допомогою міжмережевих екранів[9], одиницею контролю є технологічні віртуальні з'єднання, через які здійснюється інформаційний обмін між суб'єктом та об'єктом. Розглянемо ініціалізацію з'єднання транспортного рівня на прикладі TCP. Міжмережевий екран здійснює перехоплення пакету, який не належить наявним технологічним віртуальним з'єднанням. На цьому етапі міжмережевий екран ідентифікує ресурс об'єкта-джерела і сам об'єкт джерело, а також ресурс суб'єкта. Наприклад, ресурс суб'єкта 10.0.0.100, ресурс джерела 10.0.0.200. TCP порт з яким здійснюється з'єднання, наприклад, має номер 8080, ідентифікує джерело в даному ресурсі. При подальшому інформаційному обміні стає відомий порт суб'єкта, наприклад 55609, інформація про технологічне віртуальне з'єднання поміщається в таблицю віртуальних з'єднань міжмережевого екрана. Таким чином, для кожного вступного пакета міжмережевий екран може ідентифікувати ресурси учасників взаємодії.

Важливою особливість IaaS системи є те, що віртуальні машини середовища запускаються авторизованим і аутентифікованим користувачем[10]. Тому будемо вважати, що кожен ресурс середовища хмарних обчислень діє від імені користувача, який здійснив запуск віртуальної машини. Таким чином, забезпечується вирішення важливого завдання - ідентифікація інформаційного ресурсу середовища. Однак, при наявності технологічних віртуальних з'єднань із зовнішніми ресурсами, можливі ситуації, коли суб'єкта або об'єкта інформаційної взаємодії ідентифікувати неможливо. Як було відзначено вище, політика розмежування доступу задається у вигляді правил фільтрації, які задають правила для інформаційних віртуальних з'єднань і технологічних віртуальних з'єднань. При цьому, якщо в класичних інформаційних системах правила міжмережевого екрана для технологічних віртуальних з'єднань формуються у вигляді відповідності заданих значень полів заголовків, у тому числі і IP адрес, то стосовно середовища хмарних обчислень, де адреси призначаються і звільняються динамічно, адреси з внутрішньої під мережі N_{vm} повинні бути замінені на користувачів середовища.

Розглянемо метод конфігурації міжмережевих екранів, що призначений для забезпечення виконання політики доступу до інформаційних сервісів, що функціонують у віртуальних машинах середовища хмарних обчислень. Для конфігурування міжмережевих екранів системи захисту необхідно сформувати множину правил фільтрації. Політика доступу може бути задана в одній з наявних моделей доступу, наприклад, у рольовій.

Метод заснований на перетворенні привілеїв ролей в правила фільтрації для міжмережевих екранів за допомогою трансляції ідентифікаторів користувачів у мережеві адреси, що належать їм віртуальним машинам[11]. Привілеєм ролі є множина правил доступу до інформаційних сервісів, які задані для користувачів середовища хмарних обчислень. Формування множини правил фільтрації здійснюється при зміні стану середовища хмарних обчислень, яке виражено у вигляді множини адрес IP з мітками користувачів, що здійснили запуск віртуальної машини із заданою адресою. Метод застосовується до хмарних систем класу «інфраструктура як сервіс»[12], в яких привілеї представлені у вигляді правил доступу до інформаційних сервісів користувачів хмарного середовища, сформульованих у термінах мережевих протоколів, що робить можливим трансляцію привілеїв в правила фільтрації між мережевого екрана. Інформація про ролі, правила фільтрації і користувачів хмари знаходиться на сервісі управління міжмережевими екранами.

Процес формування правил фільтрації Rul_{vm} у відповідності зі станом середовища хмарних обчислень. Метод динамічної конфігурації правил фільтрації для міжмережевих екранів в системі розмежування даних в середовищі хмарних обчислень ґрунтується на інтеграції програмного сервісу керування системою розмежування даних із сервісами середовища хмарних обчислень і одержанні необхідної інформації про зміну складу віртуальної машини, що функціонують у середовищі (рис. 2).

Рис. 2. Схема методу конфігурації правил фільтрації

Стан середовища задамо множиною IP адрес віртуальних машин з мітками користувачів:

$$State = \{vm_{ui}\}, i = \overline{1..n}, State \subset VMxU$$

При зміні множини State необхідно здійснювати генерацію правил фільтрації і конфігурацію міжмережевих екранів. Для цього розроблено метод динамічної конфігурації правил фільтрації для міжмережевих екранів в системі розмежування даних в середовищі хмарних обчислень. При отриманні команди про зупинення або запуску віртуальної машини сервіс управління системою розмежування даних здійснює генерацію правил фільтрації та їх розподіл за міжмережевим екраном[13].

Операція генерації правил фільтрації для привілеїв P, що реалізується шляхом підставлення IP адрес суб'єкта (адреси віртуальної машини користувача, що володіє привілеєм) і об'єкта a_0 (адреса віртуальної машини користувача, що представляє інформаційну систему) в кожне правило rul привілеї $p \in P$ позначена $gen(a_s, a_0, p)$:

$$(p = < u_s, \{rul_i\} >) \xrightarrow{gen} \{a_s, a_0, rul_i >\}, i = \overline{1..n}.$$

При запуску віртуальної машини у середовищі хмарних обчислень виконується алгоритм, представлений у вигляді псевдокоду. При зупинці віртуальної машини у середовищі хмарних обчислень виконується алгоритм видалення з Rul_{vm} усіх правил фільтрації, які містять адресу завершальній віртуальної машини.

Виконання політики забезпечується тим, що розроблений метод здійснює генерацію правил фільтрації для кожної віртуальної машини середовища хмарних обчислень, що належить користувачам, яким дозволений доступ до сервісів користувача запущеної віртуальної машини, а також правил фільтрації для дозволеного доступу із запущеної

віртуальної машини до сервісів у віртуальні машини інших користувачів. Інша мережева взаємодія заборонена. Запропонований метод забезпечує ситуаційну обізнаність міжмережевих екранів, здійснюється розмежування доступу до інформаційних ресурсів, які функціонують у віртуальних машинах, запущених у гіпервізорах середовища хмарних обчислень.

Висновки. Розроблена формалізована модель процесів розмежування доступу до інформаційних сервісів, що враховує динамічний характер виділених ресурсів і структуру протоколів мережевої взаємодії. Модель ґрунтується на використанні поняття інформаційно-віртуального з'єднання, як способу опису мережевої взаємодії в середовищі хмарних обчислень. Для опису привілеїв суб'єктів використовується рольова модель, в якій привілеї ролей виражені у формі правил фільтрації інформаційних сервісів для користувачів середовища хмарних обчислень. Адекватність моделі підтверджується тим, що будь-яку мережеву взаємодію в мережах TCP/IP можна представити у вигляді віртуального з'єднання, і модель містить в собі необхідні параметри для того щоб здійснити контроль мережевих з'єднань на відповідність політиці доступу.

ЛІТЕРАТУРА:

1. Гайдамакин Н. А. Розмежування доступу до інформації в комп'ютерних системах. Єкатеринбург: Видавництво Уральського Університету, 2003. – 328 с.
2. Заборовский, В.С. Средства защиты информации на основе скрытной многоуровневой фильтрации / В.С. Заборовский, А.В. Силиненко // II Всероссийская научно-практическая конференция «Методы и средства технической защиты конфиденциальной информации» : докл. конф., Обнинск, 7-9 июня 2005 г. - Обнинск, 2005. – С. 78-80.
3. RFC2616. HypertextTransferProtocol – HTTP/1.1 [Электронный ресурс] / R.Fielding, T. Bemers-Lee. - Электрон, дан. - ISI, June, 1999. - Режим доступа: http://www.ietf.org/rfc/rfc2616.txt, свободный. - Загл. с экрана (дата обращения 01.09.2012).
4. Заборовский, В.С. Средства защиты информации на основе скрытной многоуровневой фильтрации / В.С. Заборовский, А.В. Силиненко // II Всероссийская научно-практическая конференция «Методы и средства технической защиты конфиденциальной информации» :докл. конф., Обнинск, 7-9 июня 2005 г. - Обнинск, 2005. – С. 78-80.
5. Силиненко А.В. Разграничение доступа в IP-сетях на основе моделей состояния виртуальных соединений: диссертация на соискание ученой степени кандидата технических наук: 05.13.19 : защищена 04.03.10 / Силиненко Александр Витальевич. - СПб, 2010. 145 с.
6. Мулюха В.А. Разграничение доступа в компьютерных сетях на основе классификации и приоритетной обработки пакетного трафика: диссертация на соискание ценой степени кандидата технических наук: 05.13.19 : защищена 23.12.2010 / Мулюха Владимир Александрович. - СПб, 2010. 150 с.
7. В.С. Заборовский, А.А. Лукашин. Система контроля доступа в среде облачных вычислений. // Научно-технические ведомости СПбГПУ. Информатика, Телекоммуникации, Управление. №4 (152) 2012. - СПб.: Изд-во Политехи. Ун-та, 2012. 142 с.
8. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем,- М.: Горячая линия - Телеком, 2000. – 452 с.
9. Клементьев И. П. Устинов В. А. Введение в Облачные вычисления. / Издательство УГУ, 2009. – 233 с.
10. СилиненкоА.В. Разграничение доступа в IP-сетях на основе моделей состояния виртуальных соединений: диссертация на соискание ученой степени кандидата технических наук: 05.13.19 : защищена 04.03.10 / Силиненко Александр Витальевич. - СПб, 2010. 145 с.
11. В.С. Заборовский, А.А. Лукашин. Система контроля доступа в среде облачных вычислений. // Научно-технические ведомости СПбГПУ. Информатика, Телекоммуникации, Управление. №4 (152) 2012. - СПб.: Изд-во Политехи. Ун-та,2012. 142 с.
12. Заборовский, В.С. Средства защиты информации на основе скрытной многоуровневой фильтрации / В.С. Заборовский, А.В. Силиненко // II Всероссийская научно-практическая конференция «Методы и средства технической защиты конфиденциальной информации» :докл. конф., Обнинск, 7-9 июня 2005 г. - Обнинск, 2005. – С. 78-80.

13. Лукашин А. А. Разработка и исследование моделей информационного взаимодействия для модульных подсистем обработки сетевого трафика в межсетевых экранах: Магистр, дис. 230100 / А. А. Лукашин. – СПб., 2009. 204 с.

REFERENCES:

1. Gaydamakin N. A. Rozmezhuvannya dostupu do InformatsIYi v komp'yuternih sistemah. Ekaterinburg: Vidavnitstvo Uralskogo UnIversitetu. 2003. 328 s.

2. Заborovskiy, B.C. Sredstva zaschityi informatsii na osnove skryitnoy mnogourovnevoy filtratsii / B.C. Zaborovskiy, A.V. Silinenko // II Vserossiyskaya nauchno-prakticheskaya konferentsiya «Metodyi i sredstva tehnicheskoy zaschityi konfidentsialnoy informatsii» : dokl. konf., Obninsk, 7-9 iyunya 2005 g. - Obninsk, 2005. – S. 78-80.

3. RFC2616. HypertextTransferProtocol – HTTP/1.1 [Elektronnyiy resurs] / R.Fielding, T. Bemers-Lee. - Elektron, dan. - ISI, June, 1999. - Rezhim dostupa:http://www.ietf.org/rfc/rfc2616.txt, svobodnyiy. - Zagl. s ekrana (data obrascheniya 01.09.2012).

4. Заborovskiy, B.C. Sredstva zaschityi informatsii na osnove skryitnoy mnogourovnevoy filtratsii / B.C. Zaborovskiy, A.V. Silinenko // II Vserossiyskaya nauchno-prakticheskaya konferentsiya «Metodyi i sredstva tehnicheskoy zaschityi konfidentsialnoy informatsii» :dokl. konf., Obninsk, 7-9 iyunya 2005 g. - Obninsk, 2005. – S. 78-80.

5. Silinenko A.B. Razgranichenie dostupa v IP-setyah na osnove modeley sostoyaniya virtualnyih soedineniy: dissertatsiya na soiskanie uchenoy stepeni kandidata tehnicheskih nauk: 05.13.19 : zaschischena 04.03.10 / Silinenko Aleksandr Vitalevich. - SPb, 2010. 145 s.

6. Mulyuha V.A. Razgranichenie dostupa v kompyuternyih setyah na osnove klassifikatsii i prioritetnoy obrabotki paketnogo trafika: dissertatsiya na soiskanie tsenoy stepeni kandidata tehnicheskih nauk: 05.13.19 : zaschischena 23.12.2010 / Mulyuha Vladimir Aleksandrovich. - SPb, 2010. 150 s.

7. V.S. Zaborovskiy, A.A. Lukashin. Sistema kontrolya dostupa v srede oblachnyih vyichisleniy. // Nauchno-tehnicheskie vedomosti SPbGPU. Informatika, Telekommunikatsii, Upravlenie. #4 (152) 2012. - SPb.: Izd-vo Politehi. Un-ta, 2012. 142 s.

8. Зegzhda D.P., Ivashko A.M. Osnovyi bezopasnosti informatsionnyih sistem,- M.: Goryachaya liniya - Telekom, 2000. 452 s.

9. Klementev I.P. Ustinov V.A. Vvedenie v Oblachnyie vyichisleniya. / Izdatelstvo UGU, 2009. 233 s.

10. SilinenkoA.B. Razgranichenie dostupa v IP-setyah na osnove modeley sostoyaniya virtualnyih soedineniy: dissertatsiya na soiskanie uchenoy stepeni kandidata tehnicheskih nauk: 05.13.19 : zaschischena 04.03.10 / Silinenko Aleksandr Vitalevich. - SPb, 2010. 145 s.

11. V.S. Zaborovskiy, A.A. Lukashin. Sistema kontrolya dostupa v srede oblachnyih vyichisleniy. // Nauchno-tehnicheskie vedomosti SPbGPU. Informatika, Telekommunikatsii, Upravlenie. #4 (152) 2012. - SPb.: Izd-vo Politehi. Un-ta,2012. 142 s.

12. Заborovskiy, B.C. Sredstva zaschityi informatsii na osnove skryitnoy mnogourovnevoy filtratsii / B.C. Zaborovskiy, A.V. Silinenko // II Vserossiyskaya nauchno-prakticheskaya konferentsiya «Metodyi i sredstva tehnicheskoy zaschityi konfidentsialnoy informatsii» :dokl. konf., Obninsk, 7-9 iyunya 2005 g. - Obninsk, 2005. – S. 78-80.

13. Lukashin A. A. Razrabotka i issledovanie modeley informatsionnogo vzaimodeystviya dlya modulnyih podsistem obrabotki setevogo trafika v mezhsetevyih ekranah: Magistr, dis. 230100 / A. A. Lukashin. – SPb., 2009. 204 s.

Рецензент: д.т.н., проф. Лєнков С.В., головний науковий співробітник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

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

МОДЕЛЬ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ ДЛЯ ОПИСАНИЯ ПРОЦЕССОВ РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СЕРВИСАМ

В статье проведен анализ системы разграничения доступа в сетевой среде с динамически изменяемыми параметрами, к которым относится, в частности, среда облачных вычислений. Проанализирована модель описания процессов информационного взаимодействия. Предлагается её использовать для создания системы разграничения доступа к информационным ресурсам, основанных на использовании алгоритмов оперативного синтеза

правил фильтрации и динамической конфигурации межсетевых экранов. Осмотрено формальную спецификацию ролевой модели. Приведено описание информационного обмена и состояние среды облачных вычислений. А именно три его раздела: информационный обмен в сети виртуальных машин, информационный обмен в сети управления и информационный обмен в защите (security plane).

Особое внимание уделено методу динамического формирования правил фильтрации для межсетевых экранов в соответствии с меняющимися параметрами информационного взаимодействия, представленных в форме виртуальных соединений. Метод позволяет оперативно реагировать на изменение состава виртуальных машин в среде облачных вычислений и изменение сетевых, физических и логических адресов ресурсов, в рамках которых функционируют информационные сервисы.

Рассмотрены два подхода формирования правил фильтрации для среды облачных вычислений, составляющих системы разграничения доступа. Первый подход использует формирования правил фильтрации по событиям, второй основывается на формировании правил фильтрации для установленных виртуальных соединений.

Ключевые слова: Межсетевой экран, разграничение доступа, среда облачных вычислений, виртуальные машины, гипервизор, правила фильтрации, политика доступа.

Ph.D. Ognievyi O.V., Ph.D. Krasnik A.V., Baydyuk N.N.

MODEL OF INFORMATION INTERACTION FOR THE DESCRIPTION OF PROCESSES OF DIFFERENTIATION OF ACCESS TO INFORMATION SERVICES

In the article the analysis of the system of access delimitation in a network environment with a dynamically changeable parameters, which include, in particular, the cloud computing environment. The model of description of information interaction processes is analyzed. It is proposed to use to create system of delimiting access to in formation resources based on the use of operational algorithms for operative synthesis of filtering rules and dynamic configuration of firewalls. Examined the formal specification of a role model. The description of information exchange and the state of the cloud computing environment. Namely its three sections: information exchange in a network of virtual machines, information exchange in the network management and information protection (security plane).

Particular attention is paid to the method of dynamic generation of filter rules for firewalls in accordance with the changing parameters of information interaction, presented in the form of virtual connections. The method allows to respond quickly to changes in the composition of the virtual machines in the cloud computing environment and changing the network physical and logical addresses of resources in which information services operate.

Two approaches of forming the filtering rules for cloud computing environment, components of system of differentiation of access. The first approach uses the formation of filtering rules on events, the second is based on the formation of filtering rules for established virtual connections.

Keywords: Firewall, access differentiation, cloud computing, virtual machine, hypervisor, filtering rules access policy.