Гриб'юк О. О.
Інститут інформаційних технологій і засобів навчання НАПНУ

ПРОЦЕС РОЗГОРТАННЯ ХМАРНОГО СЕРЕДОВИЩА НАВЧАЛЬНОГО ЗАКЛАДУ В КОНТЕКСТІ ПІДТРИМКИ БЕЗПЕКИ МЕРЕЖІ

Ґрунтовна відмінність між традиційними центрами опрацювання даних і хмарним середовищем полягає у фізичному розташуванні навчальних матеріалів на серверах, що належать не користувачеві (наприклад, навчальному закладу), а сторонній організації. Очевидно, що використання послуг аутсорсингу та послуг провайдера MCP частково подолають проблеми, що виникають між власне фізичною інфраструктурою інформаційно-комунікаційних технологій і хмарним середовищем [1]. З використанням хмарних сервісів у користувача виникають емоційні проблеми, що полягають у неможливості візуального сприйняття сервера, де розміщені дані користувача.

Проблему впровадження комп'ютерної інфраструктури Cloud Computing досліджують Brain McConnell, Beyond Contact, Ronald L Krutz, Russel Dean Vienes, James Ransome , John Rittinghouse, John Rhoton та ін., виокремлюючи важливий принцип – питання безпеки в Cloud-системах. Гіпотетично рекомендується використовувати додаткові рівні безпеки в системах аудентифікації, шифрування, безпечного передавання даних, обмеження доступу до даних різних користувачів та інші механізми. Важливим є розуміння, що вимоги до безпеки не змінюються залежно від проведення обчислень в «хмарі», або поза «хмарою».

З формальної точки зору існує набір специфікацій щодо забезпечення безпеки. Особливу увагу в разі розгортання хмарного середовища навчального закладу слід приділяти безпеці зберігання і використання даних і прикладних програм, тому що завдання різних користувачів виконуються з використанням спільного обладнання та, не виключено, що тих самих інформаційних ресурсів, зокрема прикладних програм. Відповідно в процесі роботи неполадки на такому рівні повинні бути виключені, інакше все це сприятиме порушенню ідеології хмарних обчислень. Таким чином в Cloud Computing має бути подолана проблема безпеки використання програмного забезпечення.

Важливою проблемою є обмеження доступу до навчальних матеріалів (даних), наприклад, неспроможність обраного хмарного провайдера захистити компоненти своєї інфраструктури. Необхідними заходами є шифрування даних та виконання віддаленого резервного копіювання (в тому числі шифрування резервних копій та мережевих комунікацій на іншому хмарному сервісі, шифрування мережевого трафіка разом з web-трафіком). Рекомендується долучити додаткового хмарного провайдера для виконання автоматизованих процедур резервного копіювання, забезпечуючи гарантоване відновлення усіх даних та їх історію, навіть за умови фізичного знищення основного хмарного провайдера. Окрім того, необхідне налаштування рівня контролю щодо використання власних даних в хмарному середовищі та центрі опрацювання даних. Під час формування наборів даних для резервного копіювання рекомендується шифрування з використанням криптостійкого алгоритму, наприклад, Pretty Good Privacy, після чого можливе зберігання повідомлень (даних) навіть в незахищеному мережевому середовищі. Шифрування даних доцільно виконувати на окремому сервері резервного копіювання, що сприятиме створенню єдиної захищеної системи із збереженням облікових записів (усіх даних) для доступу до хмарного сховища.

У процесі вибору хмарного провайдера доцільно враховувати усі варіанти забезпеченням ним фізичного захисту даних та способів здійснення захисту мережі, в

тому числі окремих хостів. Неможливо визначити точне місцезнаходження хмарного провайдера, тобто фізичного розташування віртуального зберігання відповідних даних. Крім того, засобами хмарного провайдера забезпечуються задекларовані стандарти безпеки та процедури зберігання даних.

Дані користувача хмарного сервісу знаходяться всередині певної гостьової операційної системи, що встановлена на віртуальній машині. Необхідні механізми контролю за доступом до даних у користувачів доступні з можливостями налаштування публічного доступу до них. Необхідний для обміну віртуальними «пакетами» мережевий трафік завжди невидимий для інших віртуальних хостів.

Важливою під час розгортання хмарного середовища є можливість створення ефемерних пристроїв зберігання даних в разі використання віртуального сервера, хоча, наприклад, в середовищі EC2 відсутність шифрування ефемерних пристроїв становить загрозу у зв'язку із затиранням ефемерних пристроїв нулями після завершення роботи з системою. Обережність під час шифрування файлової системи сприятиме уникненню конфліктів щодо вимог до рівня продуктивності окремих додатків та захисту даних.

Безпечність підходу щодо використання даних в хмарному середовищі полягає у монтуванні пристроїв блочного зберігання та ефемерних пристроїв з використанням зашифрованої файлової системи (encrypted filesystem). Управління запуском хмарного сервера з використанням зашифрованих файлових систем в хмарному середовищі спрощується і потребує підвищеного рівня захисту. Доцільніше зберігати паролі захисту системи в незашифрованій кореневій файловій системі, а не в хмарному середовищі. Таке зберігання паролів не проблематичне, оскільки метою шифрування файлової системи є захист від фізичного доступу до образу диска. Процес запуску віртуального сервера з використанням паролів доступу проілюстровано на рис.1. Більшість проблем щодо невідповідності використання нормативних актів і існуючих стандартів пов'язані зі створенням законодавчих документів до моменту повсюдного використання розгорнутих додатків в хмарній інфраструктурі. Безперечно, специфікація розгортання системи в хмарному середовищі можлива за рахунок реалізації змішаної архітектури, що складається з фізичних елементів та деяких віртуальних елементів. Хмарна інфраструктура, що спеціалізується на гібридних рішеннях, є одним з найбільш доцільних варіантів. В хмарній інфраструктурі змішаного середовища не зберігаються конфіденційні дані, оскільки їх опрацювання виконується на серверах підконтрольного користувачеві фізичного центру опрацювання даних.

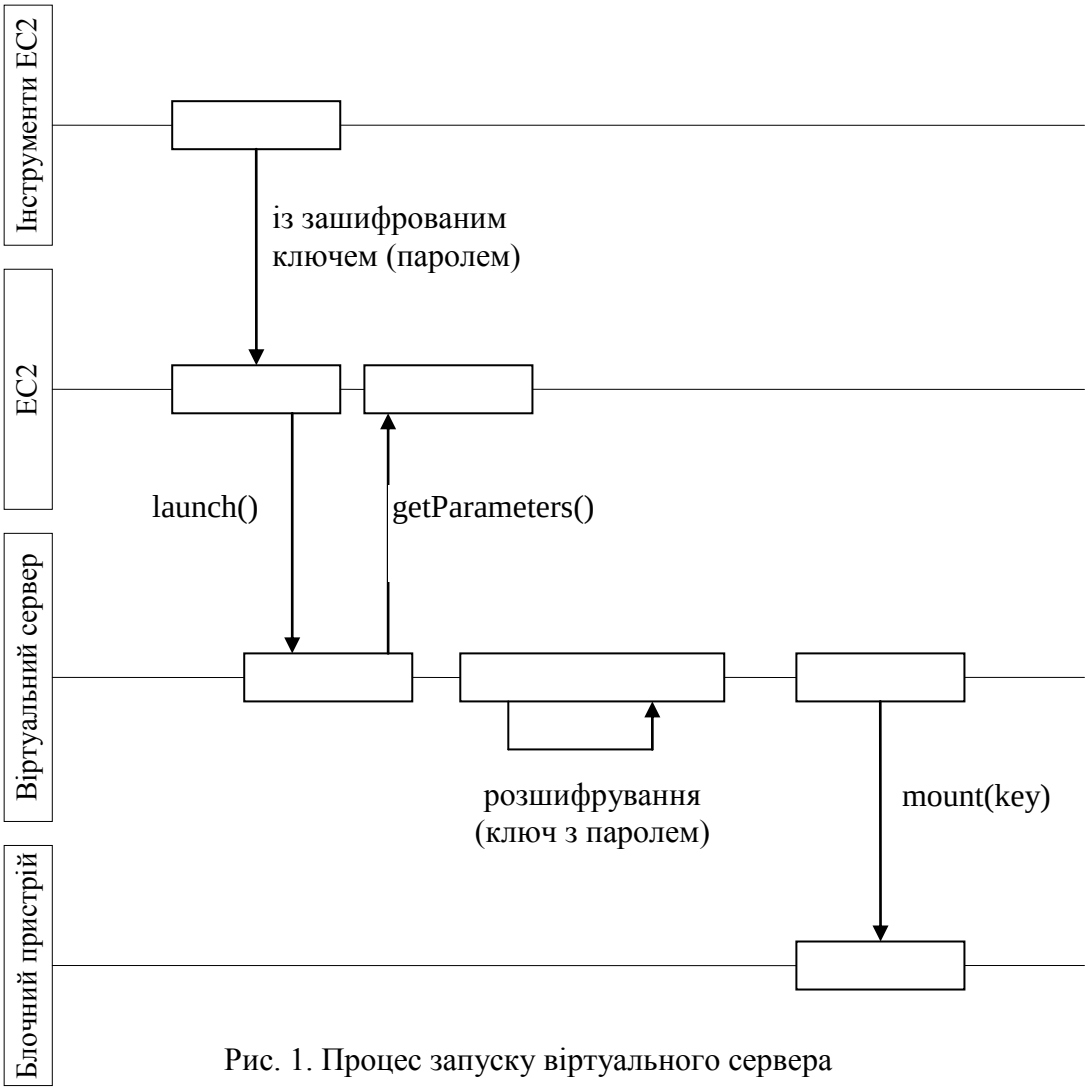

Рис. 1. Процес запуску віртуального сервера

Захист периметра одного чи кількох сегментів мережі здійснюється з використанням брандмауера (firewall) (рис.2). За допомогою брандмауера захищається зовнішній периметр мережі, пропускаються тільки трафіки http, https, ftp. Між захищеним сегментом мережі і зовнішнім периметром знаходяться проміжні системи – балансувальники навантаження, за допомогою яких спрямовується трафік в спеціальні місця, де знаходяться сервери додатків. Через них направляються запити до бази даних через інший брандмауер у внутрішню захищену мережу з внутрішніми базами конфіденційних даних. Пропонована структура (рис.2) використовується для отримання доступу до даних із збільшенням рівня секретності, причому організовується кілька рівнів (периметрів) захисту мережі за допомогою брандмауерів. В разі компрометації будь-якого внутрішнього сервера в межах конкретного сегмента автоматично надається повний доступ до інших серверів в цьому ж сегменті, що є недоліком такої інфраструктури.

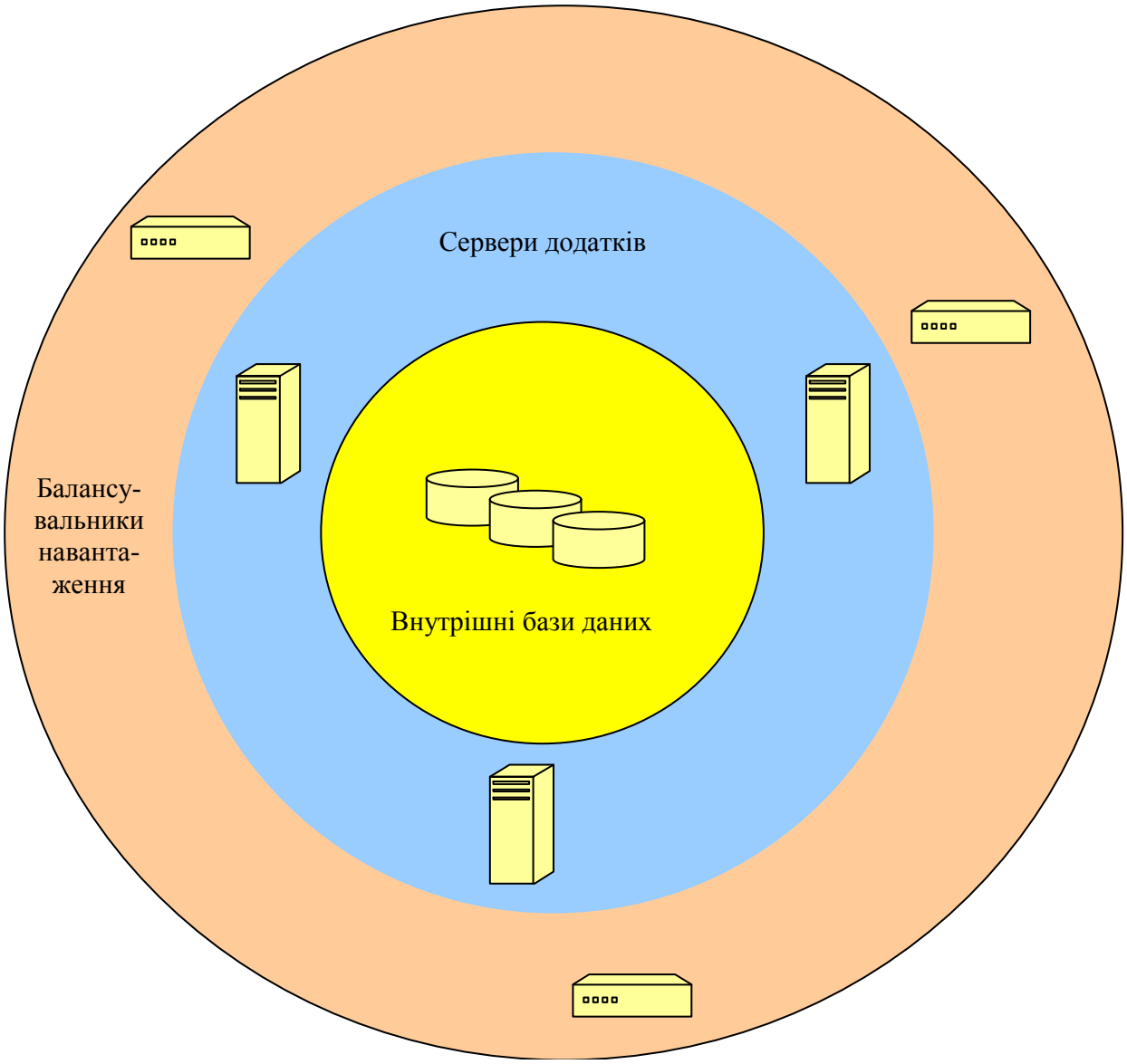

Рис. 2. Захист периметра мережі засобами брандмауера

В хмарному середовищі не існує периметрів і сегментів мережі. Всі віртуальні сервери знаходяться в мережі на одному рівні, а управління трафіком здійснюється з використанням засобів груп безпеки (security) (рис.3). Окремий сервер може відноситись до різних груп безпеки і в правилах для конкретного сервера можуть об’єднувати правила для всіх груп, куди віднесено даний сервер.

Ефективність організації системи безпеки мережі в хмарному середовищі залежить від багатьох факторів. Наприклад, на кожному віртуальному сервері доцільно запускати тільки один мережевий сервіс та сервіси, призначені для адміністрування. Зосередження на одному сервері кількох сервісів може призвести до виникнення векторів вірусних атак, що зумовлює отримання доступу до даних на сервері, або використання сервера як буферної зони для отримання прав доступу до мережі.

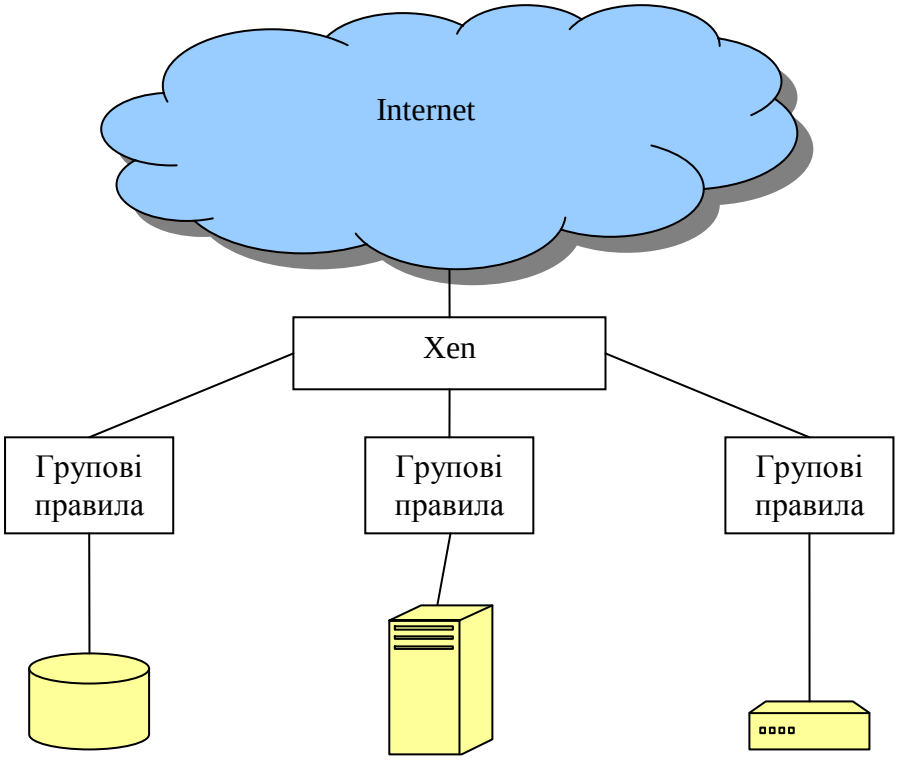

Рис.3. Візуалізація концепції правил брандмауерів в хмарному середовищі

Недоцільно надавати доступ користувачам до даних з високим рівнем захищеності, а іншим користувачам для несанкціонованого отримання даних доведеться подолати три різних вектори вірусних атак. Очевидно, захист кожного сервера потребує використання конкретного порту для підтримки конкретного сервісу. підсилення з одночасною роботою на ньому конкретного сервісу. Доцільно обмежувати доступ до сервісів сторонніх користувачів, окрім персоніфікованих користувачів. Навіть за умов обмеження використання балансувальника навантаження рекомендується використання зворотного проксі-сервера (reverse proxy). За допомогою зворотного проксі-сервера (reverse proxy) ретранслюються запити користувача із зовнішнього середовища на один або кілька серверів, що логічно розташовані у внутрішній мережі. Зазвичай reverse proxy розташовуються перед web-серверами і використовуються в ролі брандмауера на прикладному рівні для балансування навантаження в мережі між кількома web-серверами та підвищення їх безпеки.

Для автоматичного усунення проблем безпеки в мережі рекомендується продумане використання динамізації хмарного середовища. Мережеві системи виявлення вторгнень призначені для попередження про можливість атак до їх початку та для відображення атак, що розпочалися і тривають. Виявлення вторгнення в мережу здійснюється шляхом маршрутизації усього трафіка через систему, що використовується для його аналізу, або відповідно шляхом пасивного моніторингу трафіка з одного комп’ютера відповідної локальної мережі. В хмарному середовищі додаткова система виявлення вірусних атак ефективна завдяки можливостям швидкого виявлення та знешкодження шкідливого вмісту мережевих пакетів.

Оригінальним підходом для запуску та використання віддаленого сервера NIDS на балансувальнику навантажень є його встановлення на сервер перед мережею (рис.4), завдяки чому здійснюється моніторинг усього трафіка в мережі.

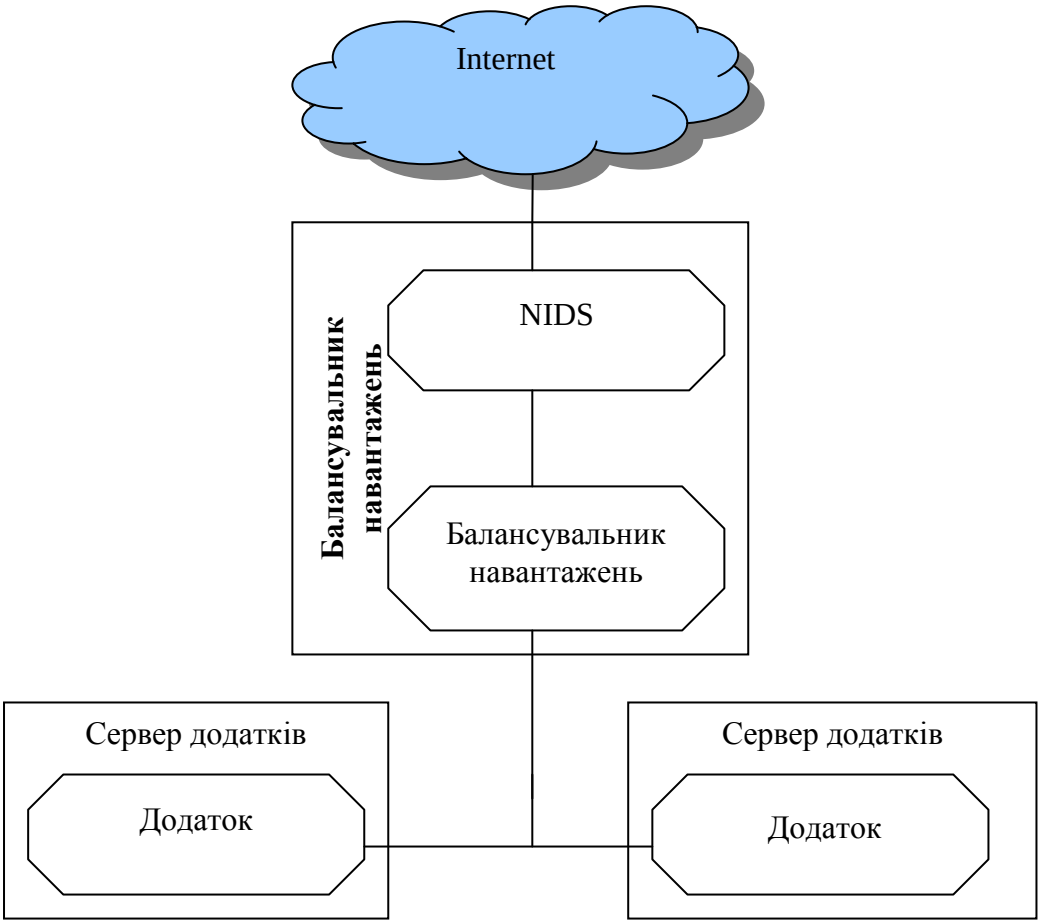

Рис 4. Мережева система для виявлення вторгнень і виконання моніторингу трафіка

Виявивши спосіб компрометації балансувальника навантажень, вірусний атакуючий не тільки захоплює контроль над балансувальником навантажень, але й отримує можливість призупинення процесу виявлення вторгнень. Альтернативний підхід полягає в реалізації системи виявлення вторгнень на сервері в позиції за балансувальником навантажень, що використовується як проміжна точка між балансувальником навантажень та іншими компонентами системи. В традиційному центрі опрацювання даних або в хмарних інфраструктурах встановлюються системи виявлення вторгнень згідно чітко продуманого алгоритму. На кожному хості у хмарному середовищі встановлюється мінімально необхідний набір програмного забезпечення. В хмарному середовищі розгортання окремих додатків з підтримкою системи безпеки передбачає встановлення поновлень безпеки на всі AMI, тестування результатів, перезавантаження усіх віртуальних серверів, за рахунок чого мінімізуються в хмарі набори різних операцій, унеможливлюючи виникнення помилки.

В хмарному середовищі можливе експериментування з різними конфігураціями і перебудовою образів комп’ютера. Дібравши конфігурацію для конкретного сервісного профілю, можна попередньо підсилити захист системи перед розгортанням даного образа в хмарному середовищі. Але попередньо рекомендується вилучення облікових записів користувачів і паролей, що зберігаються в файлі конфігурації.

Зручність та логічність використання комп’ютерної інфраструктури Cloud Computing з часом сприятиме зростанню рівня довіри користувачів, особливо в навчальному процесі та адмініструванні навчальних закладів, та доцільному користуванню хмарними обчисленнями.

Перед розгортанням хмари важливо визначитися з вимогами щодо вибору антивірусного захисту програмного забезпечення. Оскільки кількість вірусів збільшується щоденно, розробники антивірусного програмного забезпечення не в змозі забезпечити захист від кожного з них, тому їх продукт забезпечує захист лише від вже описаних вірусів. За допомогою мережевих систем виявлення вторгнень здійснюється моніторинг мережевого трафіка, виявляючи аномальну активність. Відповідно, мережеві системи виявлення вторгнень на рівні хосту (HIDS) функціонують аналогічно до антивірусних систем та додатково на їх основі досліджується система на всі ознаки компрометації, формуються повідомлення про всі випадки зміни системних сервісів та файлів операційної системи. Без мережевих систем виявлення вторгнень на рівні хосту (HIDS) не рекомендується розгортати сервери в хмарному середовищі. В хмарній інфраструктурі доцільно обирати централізовану конфігурацію, щоб розробити профіль безпеки підвищеного рівня із високим ступенем захисту окремих сервісів за принципом «один сервер – один сервіс». Сегментація даних відповідно до різних рівнів конфіденційності є основним засобом мінімізації впливу будь-якої вірусної атаки на продуктивність системи в цілому. Рекомендується забезпечувати доступ до віртуальних серверів динамічним встановленням відкритих ключів (паролів) на цільовий сервер, передаючи ключі через адміністративний інтерфейс, а не за рахунок облікового запису користувача, вбудованого в образ комп'ютера. При зміні користувача рекомендується будувати інший образ комп'ютера із необхідними для нового користувача змінами.

Ґрунтовний підхід полягає у використанні існуючих засобів управління хмарною інфраструктурою, або у розробці необхідного інструментарію, завдяки чому зберігаються облікові дані користувачів за межами хмарної інфраструктури та з'являється можливість динамічно додавати (вилучати) облікові записи користувачів на хмарні сервери під час виконання. Такий підхід потребує створення і запуску адміністративного сервісу на кожному хості. В хмарному середовищі в разі компрометації доцільне копіювання кореневої файлової системи на один із томів, копіювання томів в разі зупинки сервера та його заміні.

Список використаних джерел

1. Гриб'юк О.О Перспективи впровадження хмарних технологій в освіті / Гриб'юк О.О.// Теорія та методика електронного навчання:. Збірник наукових праць. – Випуск IV. – Кривий Ріг: Видавничий відділ КМІ, 2013. – С. 45 – 58.
2. Гриб'юк О.О. Вплив інформаційно-комунікаційних технологій на психофізіологічний розвиток молодого покоління. "Science", the European Association of pedagogues and psychologists. International scientific-practical conference of teachers and psychologists "Science of future": materials of proceedings of the International Scientific and Practical Congress. Prague (Czech Republic), the 5th of March, 2014/ Publishing Centerof the European Association of pedagogues and psychologists "Science", Prague, 2014, Vol.1. 276 p. - S. 190-207.
3. Гриб'юк О.О., Жалдак М.І. Психолого-педагогічні вимоги до комп'ютерно-орієнтованих систем навчання математики. / Гриб'юк О.О., Жалдак М.І. // Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. Серія 2: комп'ютерно-орієнтовані системи навчання: Зб. наук. праць – К.: НПУ імені М.П. Драгоманова, 2013. – С. 3 – 19.