В.Е. Байрамов, магістрант
Н.М. Лобанчикова, к.т.н., доц.
В.В. Мельниченко, магістрант
Житомирський державний технологічний університет

АНАЛІЗ ВРАЗЛИВОСТЕЙ ХМАРНИХ ТЕХНОЛОГІЙ

Хмарні технології з кожним роком все більше використовуються для задоволення різних потреб населення. І, якщо раніше, хмарні технології використовувалися вузьким колом IT-спеціалістів, то сьогодні дана технологія є доступною для кожного користувача. Використання безкоштовного поштового сервісу gmail компанії Google, Hotmail компанії Microsoft, використання віртуальних дискових просторів, додатків для спільної роботи віддалених користувачів та інші сервіси, що стали звичними для людства. Широке використання хмарних технологій призвело до появи специфічних для кіберпростору технологій загроз безпеки інформації. Тому досить актуальним є розробка нових інформаційних технологій захисту інформації в кіберпросторі та безпеки хмарних обчислень.

Хмарні обчислення (cloud computing) – це технологія розподіленої обробки даних в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс, тобто робочий майданчик на віддаленому сервері. Сучасні програмні продукти характеризуються збільшенням вимог до технічних характеристик комп'ютерів, навіть операційні системи все більше вимагаються ресурсів. Тому багато підприємств задаються питанням щодо доцільності закупки нового обладнання та розглядають як альтернативний варіант закупки лише тонких клієнтів, а в ролі термінального сервера використовувати сервер «хмари». Проведемо аналіз сервісів хмарних технологій. Все, що стосується Cloud computing (далі CC), зазвичай прийнято називати aaS – «as a Service», тобто «як сервіс», або «у вигляді сервісу». На даний час концепція передбачає надання наступних типів послуг своїм користувачам:

– Storage-as-a-Service («зберігання як сервіс»). Найпростіший з CC-сервісів, що представляє собою дисковий простір на вимогу користувача та дає можливість зберігати дані в зовнішньому сховищі, в «хмарі», у вигляді додаткового логічного диску або папці. Даний сервіс є базовим для інших, оскільки входить до складу практично кожного з них.

– Database-as-a-Service («база даних як сервіс»). Послуга надає можливість працювати з базами даних, подібно до СУБД, що встановлено на локальному ресурсі.

– Information-as-a-Service («інформація як сервіс»). Даний сервіс надає можливість віддалено використовувати будь-які види інформації, яка динамічно може змінюватися.

– Process-as-a-Service («управління процесом як сервіс»). Віддалений ресурс, який може зв'язати воєдино кілька ресурсів для створення єдиного бізнес-процесу.

– Application-as-a-Service («додаток як сервіс»). Також називається, Software-as-a-Service («ПЗ як сервіс»). Позиціонується як «програмне забезпечення на вимогу», яке розгорнуто на віддалених серверах і кожен користувач може отримувати до нього доступ за допомогою Інтернету, причому всі питання оновлення та ліцензій на дане забезпечення регулюється постачальником даної послуги.

– Platform-as-a-Service («платформа як сервіс»). Користувачеві надається комп'ютерна платформа з встановленою операційною системою і певним програмним забезпеченням.

– Integration-as-a-Service («інтеграція як сервіс»). Це можливість отримувати з «хмари» повний інтеграційний пакет, включаючи програмні інтерфейси між додатками і управління їх алгоритмами.

– Security-as-a-Service («безпека як сервіс»). Даний вид послуги надає можливість користувачам швидко розгортати продукти, що вимагають безпечного використання веб-технологій, електронного листування, локальної мережі. Користувачі даного сервісу мають змогу економити на розгортанні та підтримці своєї власної системи безпеки.

– Management / Governace-as-a-Service («адміністрування та управління як сервіс»). Дає можливість керувати і задавати параметри роботи одного або багатьох «хмарних» сервісів. Це в основному такі параметри, як топологія, використання ресурсів, віртуалізація.

– Infrastructure-as-a-Service («інфраструктура як сервіс»). Користувачеві надається комп'ютерна інфраструктура, зазвичай віртуальні платформи (комп'ютери), пов'язані в мережу, які він самостійно налаштовує під власні цілі.

– Testing-as-a-Service («тестування як сервіс»). Дає можливість тестування локальних або «хмарних» систем з використанням тестового програмного забезпечення з «хмари» (при цьому жодного устаткування або забезпечення на підприємстві, не потрібно).

Можливості хмарних обчислень: доступ до особистої інформації з будь-якого комп'ютера, що підключений до Інтернету; можливість працювати з інформацією з різних пристроїв (ПК, планшети, телефони і т.п.); незалежність від операційної системи комп'ютера користувача – веб-сервіси працюють в браузері будь-яких ОС; одну інформацію можна переглядати і редагувати одночасно з різних пристроїв; багато платних програм є безкоштовними веб-додатками; запобігання втрати інформації, вона зберігається в хмарних сховищах; завжди актуальна і оновлена інформація; використання останніх версій програм і оновлень; можливість об'єднання інформації з іншими користувачами; легко ділитися інформацією з людьми в будь-якій точці земної кулі.

До недоліків хмарних обчислень слід віднести: необхідність постійного з'єднання з Інтернет; програмне забезпечення та його «кастомізація» (є обмеження у використанні програмного забезпечення та іноді не має можливості налаштувати його під свої власні цілі); конфіденційність даних, що зберігаються в публічних «хмарах», в даний час, викликає багато суперечок, але в більшості випадків експерти сходяться в тому, що не рекомендується зберігати найбільш цінні для компанії документи на публічній «хмарі»; «хмара» сама по собі є достатньо надійною

системою, однак при проникненні в неї зловмисник отримує доступ до величезного сховища даних; використання систем віртуалізації в яких, як гіпервізор, використовуються ядро стандартних ОС (наприклад Windows), що дозволяє використовувати вразливості системи; для побудови власної хмари необхідно виділити значні матеріальні ресурси, що не вигідно щойно створеним і малим компаніям; подальша монетизація ресурсу.

В результаті проведених досліджень виділено наступні вразливості хмарних сервісів: надання послуг будь-якому користувачу, який має банківську картку, призвело до використання хмарних сервісів (PaaS, IaaS та ін.) та ресурсів хмари для генерування DDOS атак, запуску неправомірних кодів підбору та зламу паролів, розміщення шкідливого програмного забезпечення, створення ботнет мереж та ін; надаючи IaaS-сервіс, провайдер не в змозі контролювати дій користувача, що пов'язані з встановленням додаткових програмних компонентів та їх налаштування відповідно до вимог встановленої політики безпеки; провайдери PaaS-сервісу не можуть гарантувати, що клієнти будуть розробляти своє програмне забезпечення у відповідності до встановленої політики безпеки на наданій платформі; провайдери SaaS-сервісу не можуть контролювати коректність організації доступу на стороні клієнта; надаючи користувачам набір програмних інтерфейсів для керування ресурсами, віртуальними машинами чи сервісами повинні забезпечити захист цих інтерфейсів від різного роду атак зловмисників; враховуючи той факт, що в багатьох випадках користувач сервісів не знає точно місцезнаходження провайдера та сервісу, яким користується, а також йому невідома політика набору співробітників провайдером, то виникає велика загроза впровадження в персонал крякерів та представників злочинних структур, які цілenаправлено можуть діяти проти користувача; використання віртуалізації апаратних ресурсів призводить до ймовірності існування вразливостей гіпервізора в керуванні доступом до віртуальної машини та апаратних ресурсів, який може привести до збільшення привілеїв певного користувача або навіть до отримання несанкціонованого доступу до фізичного обладнання хмарного сервера.

У результаті проведеного аналізу досліджено сервіси хмарних технологій, визначено їх призначення та особливості використання, взаємозв'язок. Визначено, що зростання користувачів послуг та сервісів, призвело до розширення кола вразливостей та потребує розробки нових інформаційних технологій захисту. Представлено можливості використання хмарних технологій для користувачів та їх недоліки. Проведений аналіз дозволив виявити вразливості хмарних сервісів та визначити на їх базі напрямки розробки нових інформаційних технологій для удосконалення захисту хмарних сервісів.