СОВЕРШЕНСТВОВАНИЕ И РАЗВИТИЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

УДК 004.75

І.Ф. АУЛОВ, І.Д. ГОРБЕНКО, д-р техн. наук

АНАЛІЗ ФОРМАЛЬНОЇ МОДЕЛІ БЕЗПЕКИ ХМАРИ NIST

Вступ

Сьогодні все більше в світі корпорацій, підприємств та організацій розглядають можливості з переходу та використання хмарних технологій для роботи. Також можливість використання хмарних сервісів та технологій в якості заміни та модернізації існуючої інфраструктури розглядається США, державами Європейського союзу та іншими провідними державами світу [1, 2].

Такі переваги використання хмарних технологій, як швидкість розгортання та масштабування, відсутність капіталовкладень в побудову інфраструктури та зменшення витрат на підтримку, можливість використовувати застаріле обладнання в якості терміналу доступу до обчислювальних ресурсів хмари, висока надійність та стійкість до відмов сприяють їх швидкому поширенню в світі.

При всій сукупності переваг, є ряд суттєвих недоліків в існуючих моделях хмар, які гальмують розповсюдження технологій хмарних обчислень. До головних можна віднести відсутність єдиного міжнародного правового регулювання в сфері хмарних обчислень, недовіра до постачальника послуг з боку користувачів, проблема зміни постачальника послуг або проблема стандартизації хмарних рішень, питання загальної безпеки хмари. Детально переваги та недоліки хмарних обчислень розглянуті в статті [3].

Для вирішення питань загальної безпеки в хмарі та довіри до постачальника послуг необхідною умовою є розробка моделі хмари та моделі безпеки в хмарі.

Мета статті – аналіз запропонованої моделі хмари та моделі безпеки NIST, яка на сьогодні перебуває в процесі розгляду та доступна у вигляді чернетки [4, 5].

1. Модель хмари

Першочерговою задачею при аналізі будь-якої системи є побудова моделі цієї системи з завданим рівнем деталізації. Модель хмари, запропонована NIST, включає в себе п’ять основних ролей: користувач хмари, провайдер хмарних послуг, провайдер доступу до хмарних послуг, аудитор хмари, хмарний брокер (рис. 1).

Рис.1. Модель хмари

Розглянемо окремо кожну з ролей та функції, що вона виконує.

1) *Користувач хмари* – особа або організація, яка підтримує ділові відносини з постачальниками хмарних послуг і використовує їх сервіси.

Взаємодія користувача з постачальником хмарних послуг відбувається через брокера, використовуючи постачальника доступу до хмарних послуг. В залежності від потреб користувач використовує різні рівні сервісів, що пропонуються постачальником, у зв'язку з чим має доступ до програмних додатків в хмарі (SaaS), операційної системи та розробки програмних додатків (PaaS), віртуальних комп'ютерів та компонентів мережі (IaaS). Спожиті користувачем ресурси можуть бути виміряні як час роботи додатків чи операційної системи, використана загальна процесорна потужність тощо.

2) *Провайдер хмарних послуг* – особа або організація відповідальна за створення та управляння хмарою та її службами. Провайдер також займається підтримкою інфраструктури та програмного забезпечення, яке забезпечує роботу хмари.

В залежності від рівня надання послуг провайдер може займатися розгортанням хмарних послуг, конфігурувати, підтримувати і оновлювати роботу програмних додатків хмарної інфраструктури (SaaS), управляти обчислювальною інфраструктурою для платформи та контролювати програмне забезпечення компонентів хмари: стеку програмного забезпечення, баз даних та іншого службове забезпечення (PaaS), контролювати програмне забезпечення, яке необхідне для доступу користувачів до хмарних послуг: хостові ОС і гіпервізор віртуалізації, а також фізичні сервери, мережеве обладнання, пристрої зберігання даних (IaaS).

Провайдер, що надає послуги на рівні SaaS виконує більшість обов'язків з управління та контролю додатків та інфраструктури, в той час як споживачі мають обмежений адміністративний контроль додатків. На рівні PaaS користувачу надається доступ до середовища розробки додатків для хмарних сервісів (IDE) та набору компонентів програмного забезпечення для розробки (SDK), при цьому користувач має доступ до налаштувань програмного забезпечення та деяких налаштувань хмарного середовища, можливий також доступ до деяких налаштувань нижнього рівня: операційної системи, мережі, файлового сховища. Рівень сервісу IaaS представлений віртуалізацією фізичних компонентів до яких має доступ користувач: сервери, комп'ютерні мережі, мережне обладнання та інше підтримуюче обладнання.

3) *Аудитор хмари* – особа або організація, яка може виконувати незалежну експертизу хмарного сервісу на основі перевірки відповідності побудованої хмари стандартам, оцінці послуг, що надаються провайдером хмари з точки зору контролю безпеки, недоторканності приватного життя, продуктивності і т.д.

Аудит безпеки також включає перевірку дотримання політики безпеки, регулюючих документів та відповідності до чинних законів про конфіденційність, цілісність та доступність інформації на всіх етапах розробки та експлуатації хмари.

4) *Хмарний брокер* – особа або організація, яка керує використанням, продуктивністю і доставкою хмарних послуг, а також веде переговори між провайдерами хмари і споживачами.

Основною задачею брокера – є полегшення взаємодії користувачів з провайдерами хмарних послуг за рахунок поліпшення управління доступом до хмарних сервісів, ідентифікацією користувачів, отримання результатів звітності, підвищення рівня безпеки. Також брокер може виконувати функції агрегації послуг: поєднувати в собі та інтегрувати кілька служб в одну або кілька нових послуг, забезпечувати інтеграцію даних та їх безпечне переміщення між споживачем хмари і провайдером хмарних послуг. Функція арбітражу брокера схожа на функцію агрегації послуг, однак послуги, що агрегуються, не є фіксованими та є можливість обирати та об'єднувати послуги від декількох провайдерів.

5) *Провайдер доступу до хмарних послуг* – посередник, який забезпечує підключення і транспортування хмарних послуг від хмари до споживачів.

Зазвичай, постачальниками доступу до хмарних послуг виступають провайдери телекомунікаційних мереж, що фізично з'єднують та забезпечують передачу інформації між про-

вайдерами хмарних послуг та їх користувачами. Головними вимогами, що висуваються до провайдерів є надання безперервного, надійного та безпечного каналу доступу до провайдера хмарних послуг.

2. Аналіз складу та функцій компонентів моделі безпеки хмари

На основі моделі хмари (рис. 1) NIST було запропоновано формальну модель безпеки хмари, яка визначає компоненти безпеки для кожної з ролей в хмарі. Компоненти безпеки було розмішено відповідно функції та областей діяльності ролі в хмарі. У випадку, коли ролі (або компоненти формальної моделі хмари) виконують ідентичні функції безпеки або виконують їх разом, компонент безпеки охоплює декілька ролей (компонентів формальної моделі хмари) [5].

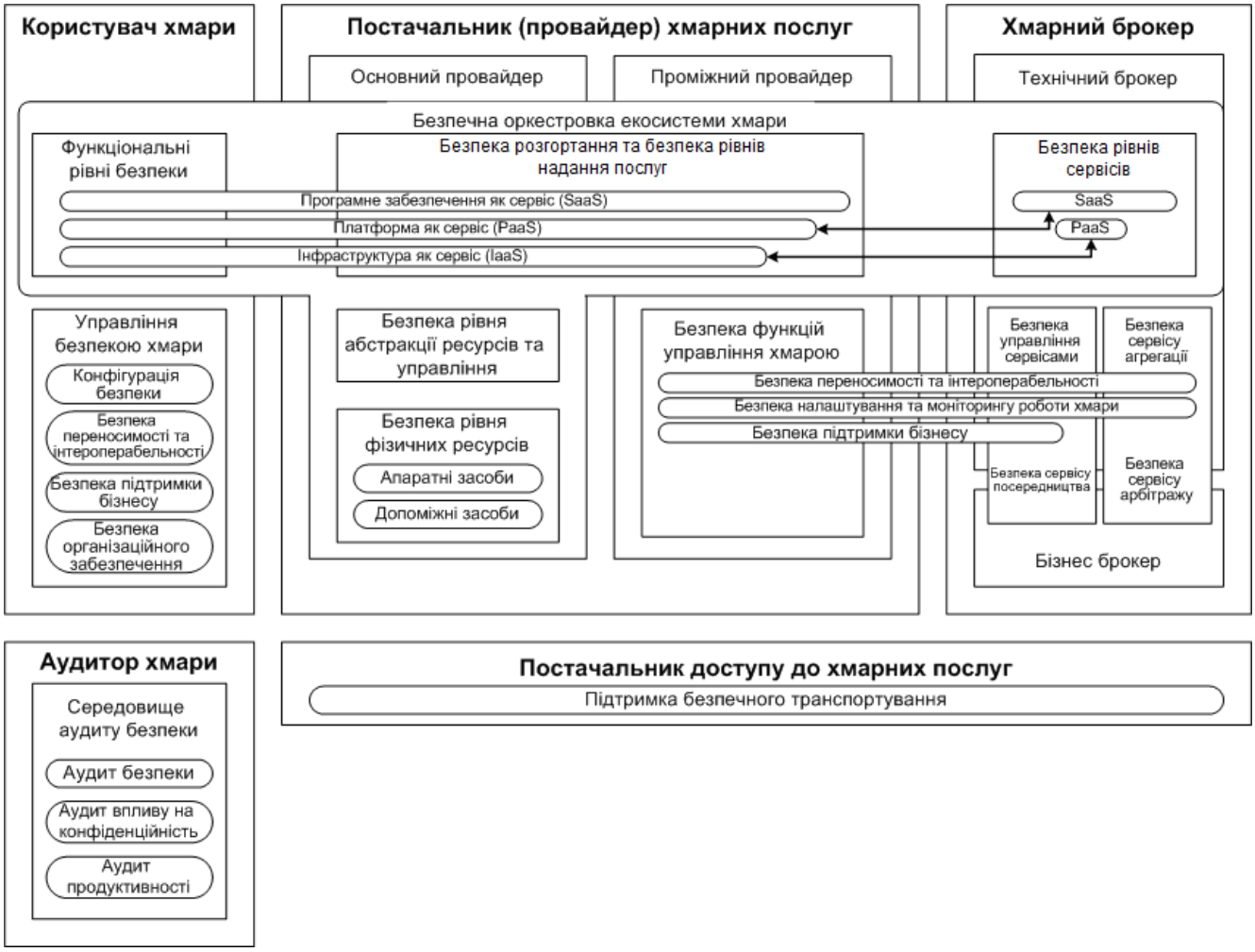

Рис.2. Формальна модель безпеки в хмарі

Розглянемо більш детально компоненти архітектури безпеки та їх основні функції [4, 5].

До складу ролі «Користувач хмари» входять наступні компоненти безпеки:

1) *Управління безпекою хмари* – компонент безпеки, що включає в себе всі функції, які необхідні для управління та роботи сервісу, який використовує користувач хмарних послуг. Він поділяється на наступні субкомпоненти:

– конфігурація безпеки, що включає інструменти та політики, використання яких забезпечує налаштування безпеки хмарних ресурсів з дотриманням стандартів безпеки, технічних умов та правил, в тому числі угод з надання відповідного рівня сервісу. В рамках цього компонента повинні бути розглянуті питання безпеки оперативного розгортання хмарних систем, зміни та оновлення в конфігурації розгорнутої системи, моніторингу, звітності, вимірювання та обліку спожитих ресурсів, забезпечення рівня обслуговування;

– безпека переносимості та інтероперабельності гарантує переміщення та розгортання між різними провайдерами хмарних послуг або брокерами даних, додатків, сервісів користувача з дотриманням конфіденційності, цілісності та надійності;

– безпека підтримки бізнесу включає питання безпеки з ведення ділових відносин з іншими ролями в хмарі. Наприклад: управління контрактами (підписання, розірвання, виконання), закупівля послуг, керування обліковими записами користувачів та інше;

– безпека організаційного забезпечення, що охоплює політику, процедури і процеси, що надаються організацією для підтримки безпечного управління споживанням хмарних послуг.

2) *Безпечна оркестровка екосистеми хмари* – компонент безпеки, що представляє сукупність елементів системи, які підтримують надання хмарних послуг в організації, координацію і управління обчислювальними ресурсами хмарних сервісів з метою надання безпечних послуг користувачам. Цей компонент вимагає різних рівнів участі від ролей в хмарі в залежності від типу хмарного сервісу та моделі його розгортання. Субкомпонентом цього компонента для користувача хмари є функціональні рівні безпеки, що реалізуються користувачем для забезпечення необхідної функціональності, та нерозривно корелює з наборами компонентів безпеки, що реалізовані іншими хмарними суб'єктами. В якості верхнього шару використовується інтерфейс наданий провайдером послуг чи брокером.

Компоненти безпеки ролі «Провайдер хмарних послуг» розміщені на всіх рівнях хмари, що контролюються провайдером та визначаються в залежності від сервісів, що їм реалізуються та надаються, а саме сервіс впровадження, сервіс оркестровки, сервіс управління хмарою, сервіс безпеки та конфіденційності. Існує два типи провайдерів: основний та провайдер-посередник. Основний провайдер надає послуги клієнтам за допомогою технічного брокеру або провайдера-посередника. Аналогічно свої послуги клієнтам надає провайдер-посередник, крім цього він може співпрацювати з декількома основними провайдерами. В зв’язку з чим провайдер-посередник не тільки включає всі компоненти безпеки основного провайдера, але додатково включає компонент безпеки для роботи з декількома провайдерами.

Відповідно до складу провайдера хмарних послуг в моделі хмари (рис. 1) модель безпеки визначає такі компоненти:

1)*Безпечна оркестровка екосистеми хмари* – компонент безпеки, що складається з трьох основних субкомпонентів:

– безпека розгортання та безпека рівнів надання послуг – компонент безпеки склад якого залежить від моделі розгортання хмари та рівня надання послуг. Змінюється в залежності від свого складу для інших ролей в хмарі.

– безпека рівня абстракції ресурсів та управління – компонент безпеки, необхідний для забезпечення та управління доступом до фізичних обчислювальних ресурсів і використовуючий в якості рівня абстракції програмне забезпечення, що повинно гарантувати ефективне, безпечне та надійне використання фізичних ресурсів.

– безпека рівня фізичних ресурсів – компонент безпеки, що включає в себе компоненти безпеки, які необхідні для безпечного функціонування як основних компонентів системи (обчислювального та мережного обладнання, засобів накопичення та зберігання інформації) так і допоміжних (системи кліматичного контролю та кондиціонування, протипожежної безпеки, мережі живлення тощо).

2)*Безпека функцій управління хмарою* – архітектурний компонент, який включає в себе компоненти, пов’язані з функціями обслуговування, управління, конфігурації та моніторингу роботи хмари, що надаються користувачу провайдером послуг. Складається з трьох субкомпонентів:

– безпека переносимості та інтероперабельності – компонент безпеки, що гарантує надійне та безпечне переміщення даних та сервісів користувача, провайдером хмари з дотриманням чинного законодавства, нормативних актів, політики безпеки, договору з користувачем;

– безпека налаштування та моніторингу роботи хмари – компонент безпеки, що включає інструменти та політики, використання яких забезпечує безпечне налаштування та забезпечення ресурсами хмари. Увага приділяється дотриманню стандартів безпеки, технічних умов та інструкцій, в тому числі угоди сервісного обслуговування користувача провайдером. В рамках компонента безпеки розглядаються питання безпеки функцій провайдера: забезпечення ресурсами на вимогу, швидке розгортання хмари, зміна обсягу, моніторинг та вимірювання ресурсів, що споживаються та інше.

– безпека підтримки бізнесу – компонент безпеки, що забезпечує безпеку взаємодії провайдера хмарних послуг з клієнтами у ділових відносинах.

Роль «Хмарний брокер» поділяється на два типи: технічний брокер та бізнес брокер. Загалом в складі ролі «Хмарний брокер» можна виділити п'ять основних архітектурних компонентів безпеки:

1)*Безпека сервісу агрегації* – архітектурний компонент, що включає компоненти безпеки, які підтримують злиття і інтеграцію різних ізольованих послуг в одній або декількох нових послугах. Брокер забезпечує інтеграцію даних і забезпечує безпечне перенесення даних між споживачами та провайдерами хмарних послуг, що засновані на політиці безпеки споживача.

2)*Безпека сервісу арбітражу* – архітектурний компонент, аналогічний до попереднього, за винятком того, що послуги, які агрегуються, не є фіксованими.

3)Безпека сервісу посередництва – архітектурний компонент, що включає компоненти безпеки, які підвищують рівень безпеки надання послуги посередництва, при цьому використовується політика безпеки користувача.

4)*Безпека управління сервісами* – архітектурний компонент, включає компоненти безпеки, які підтримують управління всіма необхідними сервісними функціями для роботи брокера.

5)*Безпечна оркестровка екосистеми хмари* – архітектурний компонент, що включає всі компоненти безпеки, які повинен реалізувати технічний брокер, для забезпечення функціональних можливостей та реалізації додаткових послуг в залежності від типу хмарного сервісу та моделі розгортання.

Як було зазначено вище, аудитор хмари проводить незалежну оцінку хмарних сервісів, операцій в інформаційних системах, продуктивності, впливу хмарної архітектури на безпеку. Аудит хмари передбачає перевірку усіх її компонентів та суб’єктів, що в свою чергу вимагає наявності компонента безпеки – середовище аудиту безпеки. Компоненти безпеки і пов'язані з ними елементи управління, як правило, не залежать від типу моделі хмари. Обов’язковими механізмами, які повинні бути реалізовані в компонентах безпеки для проведення аудиту, є отримання інформації про наявні компоненти безпеки та компоненти управління безпекою; безпечне архівування результатів аудиту; безпечне зберігання колекцій даних; отримання інформації про розташування даних та законів, якими вони регулюються; отримання результатів вимірювання продуктивності, споживання ресурсів тощо; інформація про угоди між суб’єктами в хмарі; інформація про механізми захисту та забезпечення конфіденційності.

Постачальник доступу до хмарних послуг складається з єдиного компонента: підтримка безпечного транспортування, основною метою якого є забезпечення конфіденційності, цілісності та доступності сервісів, що надаються користувачу брокером або провайдером хмарних послуг.

Висновки

Формальна модель хмари, запропонована NIST, складається з п’яти основних ролей: користувача, провайдера, брокера, аудитора та постачальника доступу до хмари.

Необхідність використання ролі брокера в моделі зумовлена відсутністю стандартів в сфері надання хмарних послуг, що ускладнює перехід користувачів від одного провайдера до іншого та керування конфігурацією хмари користувачем. Також брокер виконує функції з

агрегації сервісів різних провайдерів, що дозволяє розширювати набір послуг одного провайдера за рахунок використання інших провайдерів. За відсутності стандартів в сфері надання хмарних послуг, які будуть встановлювати перелік та механізми надання послуг брокерами, ця роль буде дублювати роль провайдера послуг в частині роботи з клієнтами, вводити додатковий рівень абстракції, з відповідними наслідками у вигляді здороження послуги, та збільшення компонентів системи, що впливають на загальну безпеку в хмарі, тому вважаємо принциповою необхідністю розробки та прийняття стандартів, які будуть регулювати інтерфейс надання хмарних послуг.

Проблему довіри до постачальника послуг в запропонованій моделі пропонується вирішувати за рахунок реалізації механізму аудиту хмари та ролі аудитору. Це дозволяє підвищити загальний рівень довіри до постачальника послуги, але остаточно не вирішує проблему. Наприклад, дані користувача зберігаються та обробляються на стороні провайдера, що може призвести до несанкціонованого витоку або блокування. Також слід зауважити, що за такої моделі аудитор хмари може бути однією з слабких ланок захисту. Зловмисник, отримавши доступ до інформації аудиту, автоматично отримує інформацію про найбільш вразливі місця в системі, які можуть бути використані для проведення атак. Тому вимоги до аудитору хмари повинні бути визначені в міжнародних стандартах, а їх робота контролюватися на рівні держав.

Що стосується питання відповідності законодавств різних держав в сфері обробки, зберігання, передавання інформації, то запропонована модель хмари не вирішує цієї проблеми. Одним з шляхів її вирішення є створення національного провайдера хмарних послуг, який надає послуги, використовуючи ресурси хмари, що знаходяться на території держави. При цьому такий провайдер міг би виконувати функції прозорого посередника між користувачами та провайдерів інших держав.

В хмарі повинні бути вирішені такі питання безпеки, як автентифікація, авторизація, доступність, конфіденційність, управління ідентифікацією, цілісність, аудит, моніторинг безпеки, реагування на інциденти та управління політикою безпеки.

Аналіз формальної моделі безпеки хмари показав, що безпека моделі хмари охоплює всі компоненти архітектури. Формальна модель безпеки хмари NIST подана у вигляді ієрархії, де основними архітектурними елементами виступають: компоненти безпеки, що включають в себе функції, механізми безпеки або субкомпоненти безпеки. По-перше, таке подання дозволяє спростити проведення аналізу за рахунок встановлення рівня деталізації з подальшим розглядом окремих компонентів на кожному з рівнів. По-друге, провести аналіз їх зв'язків та впливу на інші компоненти системи та на систему в цілому.

Суттєвою перевагою моделі безпеки хмари, що наводиться в [5], є наявність таблиць, які встановлюють відповідність між компонентами безпеки хмари та забезпеченням контролю згідно SP 800-53. В свою чергу, стандарт SP 800-53 має таблиці відповідності до стандартів УІБ ISO 27001 та критеріїв оцінки інформаційної безпеки ISO 15408.

Одним з недоліків запропонованої моделі безпеки є відсутність ролі порушника. Наявність цієї ролі зумовлена необхідністю при реальному впровадженні комплексної системи безпеки хмари, аналізувати можливості порушника, щодо реалізації потенційних загроз в системі та його впливу на компоненти архітектури. Без детального вивчення моделі загроз та моделі порушника заходи щодо забезпечення безпеки будуть неефективними та можуть призвести до суттєвих втрат провайдера хмарних послуг.

Також недоліком моделі безпеки хмари є нечіткий поділ функцій та рівнів безпеки для компонента оркестрування хмарою між ролями користувача, провайдера та брокера, який залежить від моделі розгортання хмари та рівня послуг, що надаються. В подальшому це може призвести до суттєвих проблем з безпекою в хмарі та сферами відповідальністю кожної з ролей.

Список літератури: 1. *Federal* Cloud Computing Strategy. – Режим доступу : http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf 2. *Unleashing* the Potential of Cloud Computing in Europe. European Commission / Brussels, 27.9.2012COM(2012) 529 final. – Режим доступу : http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf 3. *Хмарні* обчислення та аналіз питань інформаційної безпеки в хмарі / І.Ф. Аулов, І.Д. Горбенко // Прикладна радіоелектроніка: науч.-техн. журнал. – 2013. – Т. 12. – №2. – С. 194-201. 4. *NIST* SP 500-292, Natl. Inst. Stand. Technol. Spec. Publ. 500-292, 35 p, 2011. – Режим доступу : http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 5. *NIST* SP 500-299 Natl. Inst. Stand. Technol. Spec. Publ. 500-299, 201 p, 2013. – Режим доступу :http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity/NIST_Security_Reference_Architecture_2013.05.15_v1.0.pdf

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 14.02.2014