УДК 681.321

Ю.Л. Поночовний, І.О. Черницька, І.В. Замковець

Полтавський національний технічний університет імені Юрія Кондратюка, Полтава

АНАЛІЗ ЗАГРОЗ І ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ З ПОСЛУГОЮ PaaS

В статті розглянуто основні хмарні послуги та виділено переваги і характеристики безпеки моделі PaaS. Проаналізовано особливості архітектури відомих хмар Google App Engine та Amazon Elastic Beanstalk з послугою PaaS. Обидва провайдери хмарних послуг підтримують набір різних API та мов програмування. Проведено аналіз розподілу загроз інформаційній безпеці у хмарних PaaS – середовищах між споживачами та постачальниками хмарних послуг. Проаналізовані співвідношення між загрозами та заходами забезпечення безпеки з метою визначення повноти перекриття груп заходів і загроз.

Ключові слова: *хмарні обчислення, PaaS, cloud security, стандарти з безпеки, вразливості, споживачі хмарних послуг, провайдери хмарних послуг.*

Вступ

Сучасний технологічний розвиток вплинув на збільшення попиту використання хмарних технологій, які можна розглядати як комп'ютерну парадигму з відповідними можливостями: більшою гнучкістю і доступністю при відносно невисокій вартості.

Зручне і безпечне користування хмарними сервісами базується на принципах довіри між провайдерами послуг та користувачами, але також довіра не можлива без підтримки та забезпечення пунктів домовленості (Service Level Agreement, SLA). Ще одним фактором гарантії такої довіри є всебічне забезпечення регламентуючими стандартами на міжнародному та національному рівнями.

Враховуючи відносно молодий вік галузі хмарних обчислень та розтягнуті строки прийняття міжнародних стандартів, на сьогодні стан розвитку останніх у сфері інформаційної безпеки хмарних послуг наступний:

– з одного боку прийняті міжнародні стандарти ISO/IEC [1,2] та ITU [3 – 5], що регламентують визначення і архітектуру хмарних обчислень;

– з іншого боку впроваджено стандарти з сертифікації систем за рівнями інформаційної безпеки, з менеджменту безпеки [6 – 8].

Але в галузі інформаційної безпеки хмарних систем в даних час переважно домінують національні стандарти та рекомендації міжнародних форумів та альянсів [9, 10].

Так як розроблені на даних час регламентуючі документи мають загальний характер, актуалізуються питання конкретизації заходів з безпеки та загроз відносно конкретних видів хмарних послуг [11, 12].

Метою даної статті є проведення аналізу архітектури систем з послугою PaaS та визначення залежностей між загрозами та заходами з забезпечення інформаційної безпеки в таких системах для подальшого покращення захисту.

Виклад основного матеріалу

Огляд характеристик хмарних обчислень з послугою PaaS

Попит на користування хмарними обчисленнями збільшується з кожним роком завдяки їх основним характеристикам, що були найбільш комплексно і фундаментально охарактеризовані Національним інститутом стандартів і технологій (National Institute of Standards and Technology, NIST) [13 – 15]:

– самообслуговування на вимогу (On-demand self-service), у споживача є можливість отримати доступ до обчислювальних ресурсів в односторонньому порядку в міру потреби;

– широкий мережевий доступ (Broad network access), надані обчислювальні ресурси доступні по мережі через стандартні механізми для різних платформ, тонких і товстих клієнтів;

– об'єднання ресурсів в пули (Resorce pooling), обчислювальні ресурси провайдера об'єднуються в пули, що включають в себе різні фізичні та віртуальні ресурси які можуть бути динамічно призначені і перепризначені відповідно до запитів користувачів;

– миттєва еластичність (Rapid elasticity), ресурси можуть бути еластично виділені і звільнені для швидкого масштабування пропорційно до попиту;

– вимірюваний сервіс (Measured service), хмарні системи автоматично керують і оптимізують ресурси за допомогою засобів вимірювання, реалізованих на рівні абстракції для різних сервісів, також використані ресурси можна відстежувати і контролювати.

Хмарні сервіси [1, 14] відносно своєї архітектури розподіляються на 3 головні моделі (рис. 1).

Модель «платформа як сервіс» (PaaS) надає можливість споживачеві самостійного розгортання в хмарній інфраструктурі додатків, реалізованих за допомогою мов програмування, бібліотек, служб і засобів, що підтримуються провайдером послуг. Споживач при цьому не керує базовою інфраструктурою хмари, але має контроль над розгорнутими

додатками і, можливо, деякими параметрами конфігурації середовища хостингу.

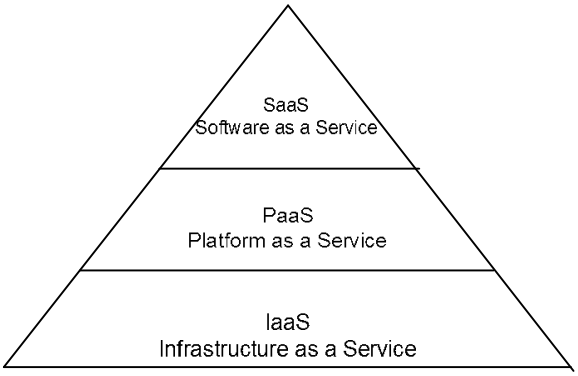

Рис. 1. Базові моделі хмарних послуг

Переваги моделі PaaS:

1) допомагає покращити ефективність ключових IT-процесів при створенні додатків і сервісів з суттєвим зниженням витрат;

2) дозволяє значно скоротити час на розгортання проектів;

3) дає можливість компаніям більш швидко адаптувати свої додатки та IT-послуги відносно організаційних потреб.

Аналіз архітектурних рішень хмарних обчислень з послугою PaaS

Прикладом відомих хмар з PaaS є Google App Engine [16], Windows Azure [17], Amazon Elastic Beanstalk [18, 19].

Google App Engine (GAE) (рис. 2) є PaaS-платформою з повністю віддаленою інфраструктурою від користувачів. Фізично, GAE представлена на веб-сервері або сервері додатків, в залежності від того, що використовує розробник (Python або Java). Google App Engine повністю підтримує мови програмування Python, Java і Go. GAE працює в так званій «пісочниці», яка ізолює і захищає процеси операційної системи (ОС). Google не забезпечує доступ до ресурсів ОС нижнього рівня. Замість цього служба пропонує багатий набір API для ресурсів більш високого рівня, щоб охопити більшість типових потреб. API-інтерфейси забезпечують програмований доступ до широкого набору послуг (SQL, NoSQL, Mail, MapReduce і Log послуги) [20].

Amazon Elastic Beanstalk (AEB) (рис. 3) є платформою PaaS, що побудована на вершині інфраструктури Amazon. AEB запускає програми в межах створених віртуальних машин хмари EC2 і забезпечує повний доступ до операційної системи і інших компонентів інфраструктури на більш низькому рівні.

AEB підтримує мови програмування Java, .NET, PHP і Python. Щоб використовувати AEB, треба просто завантажити файл розгортання додатків в хмарі Amazon за допомогою консолі Amazon Web Services або з репозиторія Git, а потім визначити, яку версію додатку потрібно розгорнути і в якому середовищі (ОС, сервер додатків, БД і т.д.) Проте, якщо клієнти бажають налаштувати конфігурацію інфраструктури, вони повинні мати повний доступ до всіх компонентів системи [19, 20].

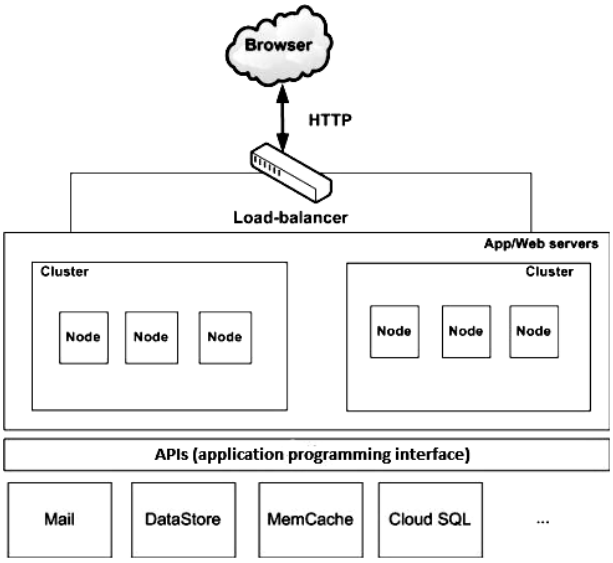

Рис. 2. Архітектура PaaS-платформи Google App Engine [20].

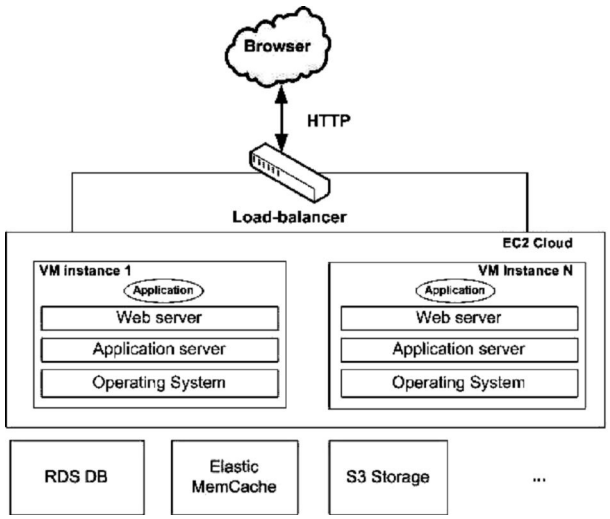

Рис. 3. Архітектура PaaS-платформи Amazon Elastic Beanstalk [20].

Загрози і заходи забезпечення безпеки користувачів і провайдерів послуги PaaS

Відповідно до міжнародних стандартів [1, 2], будь-яке хмарне обчислення включає в себе щонайменше 2 типи учасників, що несуть відповідальність за безпеку хмарної послуги (Cloud Security – CS):

– Cloud Service Customer (CSC) – споживач хмарної послуги;

– Cloud Service Provider (CSP) – постачальник хмарної послуги.

Розглянувши рекомендації, що викладені в проекті стандарту [21], можна виокремити головні вразливості та заходи із забезпечення безпеки в хмарних обчисленнях з послугою PaaS.

Вразливості для споживачів характеризуються:

CSC-1 – невизначеністю відповідальності,

CSC-2 – втратою управління,

CSC-3 – втратою довіри,

CSC-4 – тісним зв'язком з провайдером хмарних послуг,

CSC-5 – незахищеністю від несанкціонованого доступу з боку споживачів хмарних послуг,

CSC-6 – недоліком управління інформацією / хмарними ресурсами.

Вразливості для постачальників характеризуються:

CSP-1 – невизначеністю при розподілі відповідальності;

CSP-2 – неузгодженістю політик безпеки;

CSP-3 – безперервною модернізацією;

CSP-4 – припиненням надання послуг внаслідок технічних збоїв;

CSP-5 – неможливістю міграції образів віртуальних машин через несумісність апаратного і програмного забезпечення;

CSP-6 – ліцензійними політиками;

CSP-7 – конфліктом юрисдикцій різних країн;

CSP-8 – здійсненням незахищеного адміністрування хмарних послуг;

CSP-9 – загальнодоступністю інфраструктури;

CSP-10 – використанням технологій віртуалізації;

CSP-11 – порушенням доступності хмарного сервера;

CSP-12 – недобросовісністю постачальників хмарних послуг;

CSP-13 – зловживаннями з боку постачальників хмарних послуг;

CSP-14 – зловживаннями з боку споживачів хмарних послуг.

Відповідно до [21], для хмарних обчислень з послугою PaaS визначено такі заходи із забезпечення інформаційної безпеки:

MCS-1 – з ідентифікації і автентифікації суб'єктів доступу і об'єктів доступу;

MCS-2 – з управління доступом суб'єктів доступу до об'єктів доступу;

MCS-3 – щодо обмеження програмного середовища;

MCS-4 – щодо захисту машинних носіїв інформації;

MCS-5 – із видалення залишкової інформації;

MCS-6 – із реєстрації подій безпеки;

MCS-7 – із криптографічного захисту інформації, що зберігається і передається;

MCS-8 – з антивірусного захисту;

MCS-9 – із виявлення і запобігання вторгнень;

MCS-10 – із контролю (аналізу) захищеності інформації;

MCS-11 – щодо забезпечення цілісності інформації та програмних засобів;

MCS-12 – щодо забезпечення доступності інформації;

MCS-13 – щодо захисту хмарного сервера, його засобів і систем зв'язку та передачі даних;

MCS-14 – із міжмережевого екранування;

MCS-15 – із централізованого управління.

Аналіз впливу перерахованих типів заходів як протидії загрозам безпеці користувачів і провайдерів послуги PaaS представлено у вигляді таблиці співвідношень (табл. 1). Проведений аналіз показав, що найбільшу кількість заходів із забезпечення безпеки (15 заходів) необхідно виконати для протидії загрозам типу CSP-14 (зловживання з боку споживачів хмарних послуг). Навпаки, найменшої кількості заходів з безпеки (3 заходи) необхідно провести для протидії загрозам типу CSC-4 (викликаним тісним зв'язком із провайдером хмарних послуг).

Таблиця 1

Співвідношення між загрозами та заходами із забезпечення безпеки в системах Cloud PaaS

	Загрози безпеці в системах хмарних обчислень																			
		CSC-						CSP-												
Заходи із забезпечення інформаційної безпеки (MCS-)		1	2	3	4	5	6	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	1					+	+		+	+				+	+	+	+				+
	2	+	+	+		+	+	+	+	+				+	+	+				+	+
	3		+/-			+	+/-		+/-			+	+								+
	4		+/-	+	+/-	+				+	+		+			+		+	+	+	+
	5		+/-	+			+/-		+/-			+				+	+				+
	6	+		+		+/-	+	+	+						+	+	+	+			+
	7		+	+		+				+	+				+	+		+	+	+	+
	8		+	+/-	+/-	+	+/-		+						+	+			+	+	+
	9	+	+			+	+	+	+	+/-					+	+					+
	10	+	+			+	+	+	+		+				+	+		+			+
	11	+	+	+		+	+	+	+	+	+							+	+		+
	12		+	+						+	+	+	+	+				+			+/-
	13	+	+	+		+	+/-	+	+/-		+					+		+		+	+
	14		+				+/-									+			+	+	+
	15	+	+		+	+	+	+	+									+			+/-

Примітки: *«+» – захід забезпечує безпеку за даним типом загрози в повному обсязі; «+/-» – захід частково забезпечує безпеку за даним типом загрози.*

Найбільш ефективним заходом з точки зору максимального перекриття типів загроз є MCS-2 (управління доступом суб'єктів доступу до об'єктів доступу) – він перекриває 12 типів загроз. А заходи MCS-3 (щодо обмеження програмного середовища) та MCS-14 (міжмережеве екранування) перекривають найменшу кількість типів загроз – вони перекривають по 7 та 6 типів загроз відповідно.

Висновки

У роботі проаналізовано базові послуги хмарних обчислень, регламентовані міжнародними і національними стандартами. Акцентовано увагу на основних характеристиках та перевагах послуги PaaS. Розглянуто архітектуру PaaS-платформ провайдерів Google App Engine та Amazon Elastic Beanstalk.

Проведено аналіз основних загроз безпеки в хмарних середовищах та засобів із забезпечення безпеки користувачів та провайдерів послуги PaaS. На основі виділених співвідношень між загрозами та заходами із забезпечення безпеки визначено найбільш складний тип загроз CSP-14 (зловживання з боку споживачів хмарних послуг) та найбільш ефективний тип заходів безпеки MCS-2 (управління доступом суб'єктів доступу до об'єктів доступу).

В подальшому планується проведення аналізу співвідношень між загрозами та заходами із забезпечення інформаційної безпеки для хмарних послуг IaaS та SaaS.

Список літератури

1. ISO/IEC 17788:2014 Information technology - Cloud computing – Overview and vocabulary [Text]. – impl. 15.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 16 p.

2. ISO/IEC 17789:2014 Information technology - Cloud computing – Reference architecture [Text]. – impl. 10.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 53 p.

3. Recommendation ITU-T Y.3500. Information technology – Cloud computing – Overview and vocabulary [Text]. – impl. 13.08.2014 – Geneva: Inter-national Telecommunication Union, 2014. – 18 p.

4. Recommendation ITU-T Y.3501. Cloud com-puting framework and high-level requirements [Text]. – impl. 22.05.2013 – Geneva: International Telecommunication Union, 2013. – 26 p.

5. Recommendation ITU-T Y.3502. Information technology – Cloud computing – Reference architecture [Text]. – impl. 13.08.2014 – Geneva: International Telecommunication Union, 2014. – 62 p.

6. ISO/IEC 27000:2014. Информационные технологии. Методы обеспечения защиты. Системы управления защитой информации. Общий обзор и словарь [Текст]. – введ. 15.01.2014. – Женева: Международная организация по стандартизации, 2014. – 44 с.

7. ISO/IEC 15408-1:2009. Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model [Text]. – impl. 15.12.2009. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 64 p.

8. Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности [Текст]. – введ. 18.04.2008. – Женева: Международный союз электросвязи, 2008. – 64 с.

9. NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing. [Text]. – impl. 01.12.2011. – Gaithersburg: NIST, 2011. – 80 p.

10. D:A-5.1 Report on A4Cloud contribution to standards. Version 1.1. Deliverable Lead Organisation [Електронний ресурс] // Cloud Accountability Project (CSA) – Режим доступу: http://www.a4cloud.eu/sites/default/files/ D15.1 Report on A4Cloud contribution to standards.pdf.

11. Поночовный Ю.Л. Стандарты информационной безопасности для облачных технологий и тенденции их развития / Ю.Л. Поночовный, А.А. Фурманов, В.С. Харченко // Радіоелектронні і комп'ютерні системи. – 2015. – № 4. – С. 25-33.

12. Hibbard E. A. Latest in Cloud Computing Standards [Електронний ресурс] // Eric A. Hibbard – Режим доступу: http://www.slideshare.net/rnewton/sum-mary-cloudstandardseahv2130225 – 24.05.2016 р.

13. NIST SP 500-291, Cloud Computing Standards Roadmap. – impl. 01.07.2011. – Gaithersburg: NIST, 2011. – 76 p.

14. NIST Special Publication 800-145. The NIST Definition of Cloud Computing. – impl. 01.11.2011. – Gaithersburg: National Institute of Standards and Technology, 2011. – 7 p.

15. NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloud Computing. – impl. 01.12.2011. – Gaithersburg: National Institute of Standards and Technology, 2011. – 80 p.

16. Google Applications Overview [Електронний ресурс] – Режим доступу: https://appengine.google.com/ – 24.05.2016 р.

17. Microsoft Azure: Cloud Computing Platform & Services [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/en-us/ – 24.05.2016 р.

18. AWS Elastic Beanstalk [Электронный ресурс]– Режим доступа: http://aws.amazon.com/ru/elastic-beanstalk/ – 24.05.2016 г.

19. Amazon turns surprise Q3 profit as AWS cloud growth soars. [Електронний ресурс] – Режим доступу: http://www.computerweekly.com/news/4500256048/Amazon-turns-surprise-Q3-profit-as-AWS-cloud-growth-soars– 24.05.2016 р.

20. Gorelik Eugene. Cloud computing models. [Text] // Eugene Gorelik. – Cambridge: Massachusetts Institute of Technology, 2013. – 82 p.

21. Проект ГОСТ Р Требования по защите информации, обрабатываемой с использованием технологий «Облачных вичислений». Основные положения [Электронный ресурс] // Техэксперт: Машиностроение – Режим доступа: http://docs.cntd.ru/document/1200102839 – 24.05.2016 г.

Надійшла до редколегії 18.05.2016

Рецензент: д-р техн. наук, проф. В.С. Харченко, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків.

АНАЛИЗ УГРОЗ И МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ В СИСТЕМАХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ С УСЛУГОЙ PaaS

Ю.Л. Поночовный, И.А. Черницкая, И.В. Замковец

В статье рассмотрены основные облачные услуги и выделены преимущества и характеристики безопасности модели PaaS. Проанализированы особенности архитектуры известных облаков Google App Engine и Amazon Elastic Beanstalk с услугой PaaS. Оба провайдеры облачных услуг поддерживают набор различных API и языков программирования. Проведен анализ распределения угроз информационной безопасности в облачных PaaS – средах между потребителями и поставщиками облачных услуг. Проанализированы соотношения между угрозами и мерами обеспечения безопасности с целью определения полноты перекрытия групп мероприятий и угроз.

Ключевые слова: *обычные вычисления, PaaS, cloud security, стандарты по безопасности, уязвимости, потребители облачных услуг, провайдеры облачных услуг.*

ANALYSIS OF THREATS AND MEASRES OF SECURITY IN CLOUD COMPUTING (PaaS)

Y.L. Ponochovnyy, I.O. Chernytska, I.V. Zamkovets

In the article main cloud services were described and advantages and characteristics of the security model of PaaS were highlighted. The features of architecture of well-known clouds such as Google App Engine and Amazon Elastic Beanstalk with PaaS service were analyzed. Both providers of cloud services supports different API and programming languages. Distribution of information security threats in the PaaS cloud – environment between consumers and providers of cloud services was analyzed. The correlation between threats and security measures in order to determine the completeness of overlapping groups of measures and threats was analyzed.

Keywords: *cloud computing, PaaS, cloud security, security standards, cloud service customer, cloud service provider.*