УДК 004.7

АНАЛІЗ ПРОЦЕСУ ВПРОВАДЖЕННЯ ХМАРНИХ ТЕХНОЛОГІЙ У СВІТІ

Рабченюк С.І., Прус Р.Б.
Київський національний університет імені Тараса Шевченка, м. Київ
E-mail: komawka_875@mail.ru

Analysis of cloud technology implementation in the world

Analysis of cloud technology development in different states of the world is conducted. The main ways of novel information and communication technology development are defined. The model of cloud protection, which contains specific recommendations related to various security functions and combines best practices of asset protection while using cloud services, is proposed. The governmental measures of particular countries conducted to improve the quality of service and improve security are described.

Актуальність. В ході швидкого розвитку інформаційних технологій певні сектори державних та приватних організації переходять на хмарні обчислення. У сучасному житті додатки великих постачальників послуг передаються у хмарні сховища і працюють в декількох великих центрах обробки даних. Громадські дані по поглинанню хмарних обчислень показують, що протягом декількох наступних років близько 80% організацій залежатимуть від хмарних обчислень. Подальшому розвитку і шляхам побудови нової інфраструктури різних країн, новим технологічним рішенням реалізації ІТ систем, присвячуються сучасні науково-практичні конференції, ведуться дослідження та публікуються огляди. Хмарні технології дозволяють створити потужну інформаційно-телекомунікаційну систему з новою архітектурою та можливостями.

Мета доповіді – проведення аналізу рівня впровадження хмарних технологій, систем та сервісів інформаційної безпеки у різних країнах світу; пропозиція розробки і застосування деяких рекомендацій щодо роботи над стратегією розвитку захищених хмарних мереж.

Міжнародне товариство провадить активні реформи в законодавчій базі на основі розробки та впровадження стандартів, технічних вимог, правових актів, тим самим сприяючи розвитку новітніх технологій у сфері інформатизації міжнародного суспільства.

Державні органи можуть бути ключовими гравцями в області хмарних обчислень, адже вони пропонують масштабованість, еластичність, високу продуктивність, стійкість до відмов і безпеку, а в той же час вона може включити й спростити взаємодію громадян з урядом за рахунок зниження часу обробки інформації, зниження вартості державних послуг та підвищення безпеки даних громадян.

У ході аналізу нормативно-правової діяльності країн, які становлять 80% світового ринку впровадження інформаційно-комунікаційних технологій, було з’ясовано, що значна частина діяльності міжнародних організацій стрімко рухається у напрямку створення законодавчого поля сприятливого для

використання хмарних технологій. Серед таких держав високу позицію посідає Японія, у на дванадцяту виходить Польща, на чотирнадцятому місці — Росія. Дослідження проводилося за сімома критеріями, що характеризують направленість законодавства на продуктивний розвиток хмарних технологій. До таких критеріїв належать: наявність положень щодо конфіденційність даних, кіберзлочинність, безпека, підтримка впроваджених бізнес-стандартів і створення й функціонування законодавства на світовому рівні.

У законодавстві України визначення хмарних обчислень узагалі відсутнє, однак у затвердженій розпорядженням Кабінету Міністрів Україна від 15 травня 2013 р. «Стратегії розвитку інформаційного суспільства в Україні» використовується поняття хмарних технологій, а саме в пункті, що передбачає формування сучасної інформаційної інфраструктури.

На підставі попереднього аналізу стану імплементації та розширення використання хмарних технологій у країнах Європи, модель Plan-Do-Check-Act (PDCA) була ідентифікована як підходяща для безперервного процесу моделювання системи менеджменту інформаційної безпеки при використанні хмарних технологій. Використання циклу PDCA підводить до визначення основи для створення захищених хмарних мереж. Ця модель застосовується у сфері інформаційної безпеки, оскільки чітко ідентифікує окремі етапи процесу і включає в себе поняття про оцінку (Check) і налаштування/оновлення (Act), що дуже важливо з точки зору усіх мережевих та інформаційних аспектів безпеки.

Модель PDCA включає наступні етапи:

1. **Plan**: Цей етап зосереджений на налаштуванні політик та їх узгодженні із стратегією реалізації управління для досягнення цілей безпеки. На етапі планування першочерговим завданням є аналіз ризиків – ідентифікація та оцінка активів, що планується розмістити у хмарі; визначення аспектів інформаційної безпеки актуальних для цих активів (захист конфіденційності, цілісності, доступності); оцінка рівня завданої шкоди у разі реалізації загроз та їх ймовірностей. Вибір архітектури (приватна, публічна, гібридна чи громадська) та моделі надання послуг (IaaS, PaaS, SaaS) також є необхідною частиною даного етапу, як і розробка вимог безпеки та конфіденційності. Наприклад, у урядом Греції розроблено мінімальні вимоги до провайдерів хмарних технологій на основі національного законодавства та вимог безпеки у галузі інформаційно-комунікаційних технологій (ІКТ), а у Об'єднаному Королівстві розроблено 14 принципів безпеки хмарних технологій, яким повинні слідувати постачальники.

2. **Do**: Цей етап включає в себе реалізацію рішень, прийнятих на попередньому етапі, причому головною метою є дотримання усіх визначених вимог безпеки. Підлягають розгляду питання передачі інформації за межі країни. Цей етап включає також акредитацію і сертифікацію та розробку угоди про надання послуг з метою контролю якості. У Іспанії, приміром, чітко визначені суб'єкти – клієнт і провайдер, що дозволяє розділити їх ролі; а самооцінка якості рішення використовується для прогнозування результатів їх впровадження.

3. **Check**: Ця фаза орієнтована на розгляд та оцінку роботи (ефективності

та результативності) системи на основі даних моніторингу (перевірка журналів, трафіку, веб-додатків, обладнання). Наприклад, у Іспанії проводять плановий аудит кожні два роки групи із внутрішніх та зовнішніх аудиторів, а також позапланові аудити для підтвердження акредитації та оцінки якості системи безпеки. У Об'єднаному Королівстві такі перевірки проводять щорічно офіційно уповноважені консультанти.

4. **Act**: Цей етап включає в себе виправлення недоліків або прогалин, виявлених на етапі перевірки – урегулювання конфлікту між клієнтом та провайдером у разі порушення угоди, оновлення системи шифрування, переакредитація, анулювання угоди із поверненням активів клієнту або їх знищенням.

Висновки. Державні органи можуть бути ключовим гравцем в області хмарних технологій, які пропонують масштабованість, еластичність, високу продуктивність, відмовостійкість і безпеку, а також ефективність витрат. У той же час вони можуть спростити громадянам взаємодію з урядом за рахунок зниження часу обробки інформації, знизити вартість послуг та підвищити безпеку даних громадян. Державним органам, у тому числі міністерствам, урядовим установам і державним адміністраціям хмарні технології пропонують великий потенціал для управління безпекою і стійкістю в традиційних середовищах ІКТ та зміцнення своєї національної стратегії розвитку хмарних технологій.

Запропоновані рішення для захисту хмарних технологій структуровані згідно широко використовуваної моделі Plan-Do-Check-Act. Представлена система розроблена на основі всебічного дослідження, яке включає вивчення сучасних практик та досвіду впровадження урядових хмарних технологій. Аналіз показав, що різні країни використовують різні практики реєстрації доказів, інструменти моніторингу, розв'язання випадків порушення угоди про надання послуг, процедури акредитації. Розроблено різні політики для управління інцидентами. У цілому, дана модель захисту хмарних технологій повинна стати одним із основних інструментів при плануванні міграції активів у хмару та при оцінці ефективності механізмів і процедур безпеки.

Література

1. 2013 BSAGlobal Cloud Computing Scorecard [Електронний ресурс]. — Режим доступу: http://cloudscorecard.bsa.org/2013/assets/PDFs/BSA_GlobalCloudScorecard2013.pdf.
2. Безопасность в облаке / Cisco [Електронний ресурс]. – Режим доступу: http://www.cisco.com/ web/UA/about/news/2011/11152011b.html.
3. Kroes Neelie. Towards a EuropeanCloudComputingStrategy / NeelieKroes [Electronicresource]. — Modeofaccess: http://europa.eu/rapid/pressReleasesAction.do?referen ce=SPEECH/11/50.
4. European Union Agency for Network and Information Security Science and Technology Park of Crete (ITE) Vassilika Vouton, 700 13, Heraklion, Greece.