УДК 004.738.5

Т.Г. Білова, В.О. Ярута

Харківська державна академія культури, Харків

ПРОБЛЕМИ ШИФРУВАННЯ ДАНИХ В ХМАРНИХ ОБЧИСЛЕННЯХ

Проаналізовано основні загрози інформації в хмарних обчисленнях. Визначено підходи до організації безпеки в залежності від моделі обслуговування. Розглянуто проблеми та перспективи шифрування даних в хмарах, сформульовано основні принципи шифрування інформації в поєднанні с іншими методами захисту.

***Ключові слова**: хмарні технології, модель обслуговування, безпека даних, шифрування даних.*

Вступ

Постановка задачі та аналіз досліджень. Постійно зростаючі витрати на створення і експлуатацію інформаційних систем, істотне зростання збитку від інформаційних ризиків змушують підприємства та організації шукати нові шляхи підвищення ефективності інформаційної сфери.

Хмарні технології – зручна та ефективна модель доступу до конфігурованих обчислювальних ресурсів, що можуть бути оперативно представлені з мінімальними експлуаційними витратами [1, 2]. Розвиток хмарних обчислень потребує вирішення задач безпеки даних в новому середовищі. Основні загрози інформації в хмарі подібні до тих, що існують в будь-який інформаційній системі [3, 4], і для яких розроблено надійні засоби захисту. Але постає питання про адаптацію загально відомих методів захисту до особливостей хмарних моделей.

Актуальним є аналіз існуючих рішень та розробка основних принципів забезпечення безпеки хмарних обчислень, зокрема підходів до шифрування даних в хмарі.

Мета та завдання дослідження. *Метою* даного дослідження є аналіз існуючих ризиків при обробці інформації в хмарі та розробка рекомендацій щодо використання методів шифрування для підвищення надійності захисту даних.

У відповідності з поставленою метою слід вирішити наступні *завдання*: проаналізувати основні загрози безпеки в хмарах в залежності від моделі надання послуг; визначити переваги та недоліки використання типових методів захисту інформації в хмарі; сформулювати основні принципи шифрування даних в хмарі.

Основна частина

Існують три моделі розташування прикладань:

– в інфраструктурі замовника (повний контроль за інфраструктурою, апаратним і програмним забезпеченням при високих капітальних витратах);

– у компанії-хостера (менший контроль за інфраструктурою, апаратним і програмним забезпеченням, базується на оплаті фіксованого числа ресурсів, що зазвичай передбачає затрати навіть у тих випадках, коли орендовані ресурси не використовуються);

– в хмарі (відсутній контроль за інфраструктурою, апаратним забезпеченням).

Постачальники хмарних рішень вкладають величезні матеріальні та інтелектуальні ресурси в забезпечення інформаційної безпеки даних у хмарі. Рівень безпеки в більшості випадків набагато вище того, який користувачі можуть забезпечити своїми засобами. Але традиційні методи захисту даних дуже часто зосереджені на побудові централізованої мережі і периметра безпеки за допомогою таких інструментів, як міжмережеві екрани і системи виявлення вторгнень [5]. Такий підхід не забезпечує достатній захист від атак типу APT (advanced persistent threat), які характеризуються тим, що хакер (або група) маскує свою діяльність під повсякденні операції, у зв'язку з чим їх важко виявити.

Багато компаній також впроваджують аудит баз даних, контроль доступу до каталогу і системи для аналізу вхідної інформації від сторонніх систем (SIEM - Security Information and Event Management) для збору інформації про виконувані операції і процеси, але моніторинг та кореляція подій самі по собі не забезпечують безпеку даних.

На основі аналізу моделей обслуговування хмарних обчислень можна виділити наступні загрози, що притаманні кожній з них [6]:

1. IaaS – інфраструктура як послуга. Вразливість даної моделі полягає в ізоляції різних замовників в хмарі, яку забезпечує технологія віртуалізації. В даному випадку віртуалізація повинна забезпечувати правильну сегментацію віртуальних машин клієнтів, що знаходяться на одній фізичній сутності, а також необхідно забезпечити захист від підміни IP і MAC адресів клієнта, щоб у клієнта не було можливості скористатися чужим аккаунтом.

2. SaaS – програмне забезпечення як послуга. Для цієї моделі обслуговування характерні класичні загрози: XSS-вразливості та вразливості, пов'язані з аутентифікацією (витік паролів і т.п.). Тут повинна дотримуватися сувора політика в галузі управління ідентифікацією та контролю доступу до додатків.

3. PaaS – платформа як послуга. Основною проблемою для даної моделі, як і для IaaS, є забезпечення ізоляції замовників, а також загрози, пов'язані з ненадійним шифруванням при передачі даних. Виходом є сувора аутентифікація для користувачів, постійний аудит та дотримання конфіденційності.

Традиційно організаційно-технічними методами забезпечення безпеки в будь-якій інформаційній системі є наступні:

– створення і вдосконалення системи забезпечення інформаційної безпеки;

– розробка, використання і вдосконалення засобів захисту інформації;

– створення систем і засобів запобігання несанкціонованого доступу до оброблюваної інформації;

– виявлення технічних пристроїв і програм, що представляють небезпеку для нормального функціонування інформаційних систем.

Але в хмарі цього недостатньо. Поступово відбувається зміна концепції інформаційної безпеки від ідеї захищеного периметра до хмарної моделі захисту додатків, даних і сервісів. Комплексний захист повинен базуватися на наступному:

1) системи раннього попередження про початок атаки, відображення підозрілих вхідних запитів, докладну безперервну аналітику даних і т.п.;

2) шифрування даних, особливу увагу слід приділити слабким місцям: ключам шифрування, контролю доступу, моніторингу і доступу до даних. Якщо ключі шифрування недостатньо захищені, то вони уразливі для крадіжки, якщо ж ключі захищені добре, але контроль доступу не досить надійний, то є можливість отримати доступ до конфіденційних даних під виглядом авторизованого користувача.

Основним недоліком хмарних технологій є погана захищеність і недостатнє забезпечення конфіденційності інформації в хмарі. Слід розглянути наступні аспекти [6]:

– конфіденційність зберігання даних користувача – дані не можуть бути переглянуті або змінені іншими людьми, включаючи операторів;

– конфіденційність інформації під час перегляду або виконання інших операцій – дані не можуть бути показані або змінені іншими людьми під час їх виконання (завантаження в системну пам'ять);

– конфіденційність під час передачі даних.

Для доступу користувачів до своїх даних необхідна процедура однозначної ідентифікації. Користувачі можуть отримати доступ до своєї інформації самі та/або дозволити авторизацію інших користувачів для доступу до своїх даних.

На практиці при міграції в хмари потрібно знайти баланс між централізованими заходами забезпечення інформаційної безпеки, відповідальність за які несе постачальник інфраструктурних послуг, і локальними, забезпечуваними клієнтом. Насамперед необхідно визначити, хто і які ресурси хмари контролює. Це обумовлено самою організацією хмар.

Так, надаючи IaaS-послуги, провайдер не може контролювати дії клієнта, пов'язані з установкою додаткових програмних компонентів і їх налаштуванням з урахуванням вимог безпеки. Провайдер PaaS-послуг не може гарантувати, що клієнти належним чином розроблятимуть своє програмне забезпечення на хмарній платформі. Провайдер SaaS-послуг не може контролювати коректність організації доступу на клієнтській стороні. Завдання провайдера – створення базового захищеного середовища, в якому дані різних клієнтів будуть ізольовані один від одного, а також у забезпеченні контролю дій своїх системних адміністраторів.

Таким чином, ефективне рішення щодо забезпечення інформаційної безпеки хмарної інфраструктури повинно включати:

1) закритий доступ до даних – необхідно забезпечити надійне управління ключами шифрування;

2) політики доступу – тільки авторизовані користувачі повинні мати доступ до конфіденційної інформації;

3) інтелектуальна система, яка повинна збирати інформацію для аналізу поведінки користувачів і оповіщати у разі виявлення підозрілої активності.

Забезпечення інформаційної безпеки в хмарі – не тривіальна задача, однак, при відповідному підході можливий ідеальний баланс всіх переваг хмарної моделі і високого рівня захисту, безпеки та доступності даних та інформаційних систем.

З боку користувача найбільш надійною гарантією контролю за даними є шифрування [8]. В випадку передачі в систему ключа дешифрування є впевненість, що сторонні користувачі того ж сервісу не отримають доступу до важливих даних. Сам процес передачі ключа шифрування і взаємної аутентифікації користувача і серверів хмари також повинен бути побудований на основі криптографії з відкритим ключем. Однак відсутність закінчених та ефективних рішень, які гарантували би криптографічний захист даних при обробці їх в хмарі, пов’язана з наступними проблемами:

– шифрування, вбудоване в хмарну інфраструктуру, сильно гальмує роботу хмарних додатків;

– дешифрування віртуальної машини перед її запуском може сильно уповільнити як запуск програми, так і її роботу;

– для перенесення віртуального середовища з одного вузла кластера на другий також потрібно виконати цикл шифрування – дешифрування. Затримки, що виникають при цьому, можуть істотно сповільнити роботу хмарного додатку;

– процедура взаємної аутентифікації користувача і хмари також має певні проблеми, як за швидкістю (асиметрична криптографія досить ресурсомістка), так і за логікою (який саме сервер аутентифікувати, якщо їх може бути декілька, і вони передають дані з одного вузла на інший).

Зазначені проблеми аутентифікації можна вирішити за допомогою PKI-інфраструктури, протоколу SSL і сертифікатів. Водночас, подібну інфраструктуру потрібно адаптувати до умов хмари і реалізувати відповідні механізми.

Слід відмітити, що для захисту даних неефективно шифрувати віртуальне середовище цілком. Досить зашифрувати власне самі дані, обсяг яких значно менше [7].

Це позначиться на роботі системи зберігання, але проте забезпечить захист даних.

Крім апаратно-програмних засобів, безпека даних може бути досягнута також відповідними правилами поведінки і взаємодії об'єктів, високою професійною підготовкою персоналу, безвідмовністю роботи техніки, надійністю всіх видів забезпечення функціонування об'єктів.

Конфіденційність інформації полягає в тому, що аудитори зобов'язані забезпечувати збереження документів, отриманих або що складаються ними в ході аудиторської діяльності, і не мають права передавати ці документи або їх копії яким би то не було третім особам без згоди власника економічного суб'єкта.

Висновки

Шифрування даних в хмарі повинне реалізовуватися на базі надійних ключових рішень з управління доступом, щоб забезпечити гарантований захист ключів. Шифрування дає найкращій ефект лише спільно з іншими технологіями захисту даних і дозволяє отримати додаткову інформацію щодо забезпечення безпеки для побудови всебічного багаторівневого підходу до захисту та конфіденційності даних і зниження ризиків злому в хмарі і за її межами.

Подальші дослідження у даному напрямі повинні охоплювати питання вибору найбільш ефективних методів і алгоритмів шифрування в хмарі.

Список літератури

1. Білова, Т.Г. Перспективи використання хмарних технологій в системах електронного документообігу / Т.Г. Білова, В.О. Ярута [Текст] // Системи обробки інформації. – Х., 2014. – Вип. 4 (120). – С. 86–89.

2. Белова, Т.Г. Анализ проблем доверия в облачных технологиях [Текст] / Т.Г. Белова, И.А. Побеженко, В. В. Побеженко // Східно-Європейський журнал передових технологій. – Х., 2013. – № 2 (62). – С. 59–62.

3. Білова, Т.Г. Аналіз ризиків референтної структури хмарних обчислень / Т.Г. Білова, В.О. Ярута, І.О. Побіженко [Текст] // Наука і техніка Повітряних Сил Збройних Сил України. – Х., 2014. – Вип. 3 (16). – С. 144-147.

4. Побіженко, І.О. Перспективи використання хмарних технологій для організації навчального процесу у вищих навчальних закладах / І.О. Побіженко, Т.Г. Білова, В.О. Ярута [Текст] // Збірник наукових праць Харківського університету Повітряних Сил. – Х., 2014. – Вип. 4 (41). – С. 167-170.

5. Информационная безопасность в облаке [Электронный ресурс]. – Режим доступа к матеріалам : http://www.treolancloud.ru.

6. Котяшичев, И.А. Защита информации в «Облачных технологиях» как предмет национальной безопасности [Текст] / И.А. Котяшичев, Е.А. Бырылова // Молодой ученый. – 2015. – № 6.4. – С. 30-34.

7. Котяшичев, И.А. К вопросу о безопасности облачных технологий в информационной среде [Текст] / И.А. Котяшичев, С.В. Смоленцев // Молодой ученый. – 2014. – № 5.1. – С. 25-28.

8. Шнайдер, Удо. Безопасность при использовании облачных сервисов / Удо Шнайдер [Электронный ресурс] // Журнал сетевых решений/LAN». – 2013. – № 04. – Режим доступа: http://www.osp.ru/lan/2013/04/13035155.

Надійшла до редколегії 25.08.2015

Рецензент: д-р техн. наук, проф. Г.Г. Асєєв, Харківська державна академія культури, Харків.

ПРОБЛЕМЫ ШИФРОВАНИЯ ДАННЫХ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Т.Г. Белова, В.А. Ярута

Проведен анализ основных угроз информации в облачных вычислениях. Определены подходы к организации безопасности в зависимости от модели обслуживания. Рассмотрены проблемы и перспективы шифрования данных в облаках, сформулированы основные принципы шифрования информации в сочетании с другими методами защиты.

Ключевые слова: *облачные технологии, модель обслуживания, безопасность данных, шифрование данных.*

PROBLEMS OF DATA ENCRYPTION FOR CLOUD COMPUTING

T.G. Belova, V.O. Yaruta

The analysis of the main threats to the information in the cloud is carried out. Approaches to the organization of security, depending on the service model, are defined. The problems and prospects of encrypting data in the clouds are considered, the basic principles of encryption of information in combination with other methods of protection are formulated.

Keywords: *cloud computing, service model, data security, data encryption.*