УДК004.415.056:658.115

А. О. Азарова
А. А. Софина

Розроблення захищеного хмарного сервісу

Вінницький національних технічний університет

Анотація
У даному дослідженні розглянуто відповідні криптографічні засоби для забезпечення цілісності інформації. Проаналізовано переваги та недоліки існуючих хмарних сховищ, що уможливило формування інформаційно-орієнтованого підходу створення безпеки даних у хмарному середовищі.

Ключові слова: хмарне середовище, технології, алгоритм.

Abstract
This article discusses the appropriate cryptographic tools to ensure the integrity of information. The advantages and disadvantages of existing cloud storage are analyzed.
Keywords: *cloud environment, technologies, algorithm*

Хмарне середовище – це програми та платформи, які знаходяться та працюють на серверах хмарних провайдерів, які дозволяють інформаційними засобами віртуального середовища розширити програмно-технічні ресурси комп’ютерного пристрою користувача. Поява хмарних сховищ стала можливою у процесі розвитку технологій хмарних обчислень (англ. Cloud Computing), які реалізуються за умов динамічного масштабного доступу до розподілених зовнішніх мережевих ресурсів.

Вибір зазначеної технології зумовлений не тільки орієнтацією на соціальні і державні замовлення, наявні та передбачувані потреби суспільства, а й можливістю технологічно розробляти і реалізовувати відповідні хмарні додатки згідно з потребами регіональних соціальних партнерів та економіки в цілому.

Застосування «хмарних» технологій дає можливість використовувати сучасну і більш зручну комп'ютерну інфраструктуру, програмні засоби, електронні ресурси і сервіси, знижує витрати на створення локальних інформаційних інфраструктур шляхом більш раціонального використання обчислювальних ресурсів, що знаходяться в «хмарі» і виділяються користувачам за запитами.

Хмарні сховища мають цілу низку переваг:

– користувач може задіяти віртуальний комп’ютер практично будь-якої конфігурації для виконання ресурсоємних завдань;

– користувач може працювати в будь-якому місці за умов використання комп’ютерного пристрою, що має підключення до мережі Інтернет;

– користувач застрахований від збоїв у роботі пристрою і може за потреби ділитися результатами роботи з іншими користувачами;

– на відміну від установлення платних програм на окремому ПК, хмарні сховища у більшості безкоштовні або розрахунки проводять у вигляді абонентської плати.

Робота з хмарними технологіями дозволяє оперативно реагувати на появу нових бізнес завдань, знижує витрати і підвищує ефективність роботи підприємств та їх підрозділів. Такий підхід до роботи з інформацією може бути рекомендований як індивідуальним підприємцям і малому бізнесу, так і середньому і великому бізнесу: для будь-якого розміру суб’єкта господарювання може бути розроблена оптимальна бізнес-модель. Невеликі компанії в першу чергу цікавляться сервісами бухгалтерії і пошти, додатками для обміну інформацією, відновлення і архівації файлів. Найбільш великим організаціям цікаві віртуальні сервери і послуги зв'язку, а також складний комплекс різних сервісів.

Для захисту віртуальних середовищ доцільно застосовувати криптографічні алгоритми, яких існує доволі багато. Базовими критеріями класифікаційного поділу всіх алгоритмів є тайнопис і криптографія з ключем. Використовуючи тайнопис, відправник і одержувач роблять над повідом-

ленням перетворення, відомі лише їм двом. Стороннім особам невідомий сам алгоритм шифрування. Деякі фахівці вважають, що тайнопис не є криптографією взагалі.

Інший алгоритм впливу на дані, що передаються, відомий усім стороннім особам, але він залежить від деякого параметра – «ключа», яким володіють лише відправник і одержувач.

У свою чергу, даний метод містить у собі ще два напрямки, а саме симетричні та асиметричні криптоалгоритми. У симетричних криптоалгоритмах для шифрування і дешифрування повідомлення використовується один і той самий блок інформації (ключ). Асиметричний криптоалгоритм – це алгоритм, в якому для шифрування повідомлення використовується один («відкритий») ключ, відомий усім бажаючим, а для дешифрування – інший («закритий»), який існує тільки в одержувача.

Симетричні криптоалгоритми виконують перетворення невеликого (1 біт або 32-128 біт) блоку даних в залежності від ключа таким чином, що прочитати оригінал повідомлення можна тільки, знаючи цей секретний ключ.

Авторами обґрунтовано доцільність застосування саме криптографічного алгоритму шифрування даних – RC5 для розроблення оптимального алгоритму захисту хмарного додатку.

Було створено програмний продукт, який реалізовано мовою C#. Ця мова має досить потужну бібліотеку .NET Framework, яка підтримує зручність побудови різних типів додатків мовою C, дозволяючи легко будувати Інтернет-служби та інші види компонентів, досить просто зберігати й отримувати інформацію з бази даних та інших сховищ даних. Середовищем розроблення авторами було обрано Visual Studio 2019. За допомогою даного середовища було також розроблено інтерфейсну частину проекту. Розроблений програмний продукт було протестовано і перевірено на працездатність. Було розглянуто два режими програми, а саме: шифрування та дешифрування. Кожен із режимів працює так, як закладено в алгоритмі. Даний додаток шифрує і дешифрує задані файли, також завантажує в хмару і дозволяє завантажити з неї.

Отже, захищений хмарний сервіс є досить актуальним, оскільки він надає користувачеві зручне і безпечне віртуальне середовище для зберігання і оброблення інформації, що об'єднує в собі апаратні засоби, програмне забезпечення, канали зв'язку, а також службу технічної підтримки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Биков В. Ю. Хмарні технології, ІКТ-аутсорсинг і нові функції ІКТ підрозділів освітніх і наукових установ. Інформаційні технології в освіті. №10. 2011. С. 8–23.
2. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. К. : Видавнича група BHV, 2013. 608 с.
3. Азарова А. О., Шиян А. А., Нікіфорова Л. О. Розроблення захищеного консолідованого інформаційного ресурсу аналізу діяльності морських портів України. Інформаційні технології та комп'ютерна інженерія. 2020. С. 27-36.
4. Азарова А. О., Ляхович Л. М. Розроблення захищеного консолідованого інформаційного ресурсу засобів електронного врядування. Вісник ХНУ. Технічні науки. 2020. № 3. С. 81-87.
5. Azarova A., Azarova L., Rosol N., Bystritskiy O. Models and methods of electronic digital signature. Theoretical and scientific foundations of engineering: collective monograph / International Science Group. Boston : Primedia eLaunch, 2020. 180 p. P. 24 – 33. Available at :DOI:10.46299/isg.2020. MONO.TECH.II.
6. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Захищений засобами двофакторної авторизації месенджер для організації комінікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір №97856. Дата реєстрації 05.06.2020 р. Заявка № 99244 від 02.06.2020 р.
7. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Процедура реєстрації у захищеному месенджері для організації комунікаційних процесів на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97857. Дата реєстрації 05.06.2020 р. Заявка №99245 від 02.06.2020 р.
8. Азарова А. О., Азарова Л. Є., Білий Р. О., Міронова Ю. В. Комп'ютерна програма «Отримання та надсилання повідомлень користувачами у створеному месенджері для реалізації комунікаційного процесу на підприємстві». Свідоцтво про реєстрацію авторського права на твір № 97858. Дата реєстрації 05.06.2020 р. Заявка № 99246 від 02.06.2020 р.

Азарова Анжеліка Олексіївна − к.т.н., професор каф. МБІС, заст. декана ФМІБ з наукової роботи та міжнародного співробітництва.

Софина Андрій Анатолійович – ст. гр. УБ-16б, Факультет менеджменту на інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: wintervinnitsa@gmail.com.

Azarova Anzhelika A. – PhD in technique, professor, deputy Dean of the Faculty of management and information security by scientific work and international cooperation.

Sofyna Andrii A. – student of group UB-16b, Faculty of management and information security, Vinnytsia National Technical University, Vinnytsia, e-mail: wintervinnitsa@gmail.com.