ОСОБЛИВОСТІ КРИПТО-КОДОВИХ ЗАСОБІВ ЗАХИСТУ ДАНИХ ДЛЯ ХМАРНОГО СЕРЕДОВИЩА РОЗРОБКИ

Сафаров О.О., к.т.н.; Мінькова Я.В., магістрантка
Національний технічний університет "Дніпровська політехніка", Дніпро, Україна

В сучасних умовах наявний високий попит на хмарні сервіси. Застосування хмарних інтегрованих середовищ розробки суттєво міняє усталений за роки процес розробки програмного забезпечення. Розробнику більше не потрібна велика кількість програм між якими потрібно налагоджувати зв'язок, які необхідно оновлювати і з якими доводиться виконувати інші рутинні дії, все це тепер є зоною відповідальності провайдера даного сервісу. Проте безпечність подібних рішень на сьогоднішній день під великим питанням [1].

Для забезпечення інформаційної безпеки як окремих підприємств, так і держави в цілому важливим є питання оцінки ризиків, які виникають в процесі діяльності підприємств та застосування ними хмарних сервісів. Аналіз ризиків інформаційної безпеки є інструментом виявлення вразливостей і загроз, оцінки можливого їх впливу, що дозволяє вибирати адекватні захисні заходи для тих систем і процесів, у яких вони необхідні. Методики аналізу інформаційних ризиків дають змогу забезпечити ефективний і актуальний захист інформаційного простору підприємств і можливість вчасно реагувати на загрози інформаційній безпеці.

Тому постає задача вибору моделі подання знань в автоматизованій системі вибору засобів захисту даних в хмарних сервісах, що використовуються для розробки програмного забезпечення, на основі аналізу їх захищеності.

Найефективнішими за стійкістю до алгоритмів криптоаналізу є крипто-кодові засоби захисту інформації з недвійковими лінійними блоковими кодами, які виникають на алгебраїчних кривих – алгебро-геометричними кодами. Разом з тим практичне використання крипто-кодових засобів захисту інформації з недвійковими алгебраїчними блоковими кодами передбачає застосування методів і обчислювальних алгоритмів недвійкового рівновагового кодування [2].

На сьогоднішній день існуючий науково-методичний апарат, застосовувані методи і обчислювальні алгоритми не дозволяють реалізувати недвійкове рівновагове кодування, в тому числі і в крипто-кодових засобах захисту інформації. Отже, актуальним науково-технічним завданням, що має важливе прикладне значення в області побудови обчислювально ефективних криптографічних засобів захисту інформації, є розроблення методів і алгоритмів недвійкового комплексного забезпечення безпеки і достовір-

ності передавання даних у системі захисту інформації.

Так як хмарний сервіс і його уповноважений користувач природно можуть розглядатися в якості приймальної та передавальної сторін системи передачі інформації, то математична модель крипто-кодових засобів захисту інформації згідно з [3] може бути реалізована наступним чином.

Алгебраїчний блоковий *(n, k ,d)* код *C* (*n* – довжина кодового слова, k – довжина фрагменту, d – відстань Геммінга, подані в бітах) з швидким алгоритмом декодування маскується під випадковий *(n, k, d)* код *C** безпосередньо перемноженням перевірочної матриці *H* коду *C* на матриці маскування які зберігаються в таємниці X^u, P^u и D^u :

$$H_X^u = X^u \cdot H \cdot P^u \cdot D^u, \ u \in \{1,2, \dots s\}, \quad (1)$$

На прийомній стороні уповноважений користувач, який знає правило маскування (в даному випадку це не просто ключ, а повноцінний набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$) формує кодову послідовність $C_{X_i}^*$ як одне, будь-яке, з можливих рішень рівняння

$$S_{X_i} = C_{X_i}^* \cdot H_{X_i}^T, \quad (2)$$

тобто находить такий вектор $C_{X_i}^*$, який розкладається на суму у наступному вигляді:

$$C_{X_i}^* = C_{X_i} + M_i, \quad (3)$$

У даному рівнянні C_{X_i} – одне, також будь-яке, із можливих слів замаскованого *(n, k, d)* коду.

Далі, уповноважений користувач, використовуючи набір матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$ формує вектор

$$C^{-*} = C_X^* \cdot (D^u)^{-1} \cdot (P^u)^{-1}, \quad (4)$$

за допомогою якого він і здійснює демаскування кодової послідовності $C_{X_i}^*$.

Таким чином, здійснивши підстановку з рівняння (3), уповноважений користувач може використовувати результуюче рівняння, яке має наступний вигляд:

$$C^{-*} = C_X^* \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \left(C_{X_i} + M_i\right) \cdot (D^u)^{-1} \cdot (P^u)^{-1} = \\ = C_{X_i} \cdot (D^u)^{-1} \cdot (P^u)^{-1} + M_i \cdot (D^u)^{-1} \cdot (P^u)^{-1} \quad (5)$$

Зловмисник, не знаючи правил маскування, яке задається секретним ключем, тобто за допомогою набора матриць $\{X,P,D\}_u = \{X^u, P^u, D^u\}$, для дешифрування повідомлення змушений використовувати складний алгоритм декодування випадкового коду. Подібний алгоритм, в загальному випадку, відноситься до алгоритмів експоненціальної складності, тобто задача демаскування є доволі нетривіальною для зловмисника з точки зору необхідних для її вирішення ресурсів.

Таким чином, запропоновані механізми крипто-кодового захисту ін-

формації дозволяють реалізувати обмін конфіденційними повідомленнями з використанням відкритих ключових даних і інтегровано забезпечити потрібні показники безпеки і достовірності передачі даних у широкому спектрі відповідних систем, зокрема і в досліджуваному хмарному середовищі розробки Codeanywhere. А потрібна криптографічна стійкість забезпечується зведенням задачі встановлення інформаційних даних без знання секретного ключа до рішення теоретико-складної задачі декодування випадкового коду.

Перелік посилань

1. Fylaktopoulos, G. An overview of platforms for cloud based development **[Електронний ресурс]** // G. Fylaktopoulos, G. Goumas, M. Skolarikis, A. Sotiropoulos, and I. Maglogiannis. – SpringerPlus 5, 38, 2016. – Режим доступу до ресурсу: https://springerplus.springeropen.com/articles/10.1186/s40064-016-1688-5 .

2. Томашевський Б. П. Метод побудови крипто-кодових засобів захисту інформації на недвійкових рівновагових кодах : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.21 "Системи захисту інформації" / Томашевський Богдан Паїсійович ; Національний університет “Львівська політехніка”.– Львів, 2011. – 21 с.

3. Дудикевич В. Б. Крипто-кодовий захист інформації з недвійковим рівноваговим кодуванням / Дудикевич В. Б., Кузнєцов О. О., Томашевський Б. П. – Науково-технічний журнал «Сучасний захист інформації», №2, 2010. – С. 10.

Анотація

В роботі досліджено можливості здійснення захисту інформації при веденні процесу розробки в хмарному сервісі Codeanywhere за допомогою крипто-кодових засобів захисту інформації з недвійковими лінійними блоковими кодами. Наведено загальні засади та принципи математичного апарату, використання якого пропонується для забезпечення високого рівня криптографічної стійкості досліджуваної системи.

Ключові слова: хмарне середовище інтегрованої розробки, крипто-кодові системи захисту інформації, блоковий код, віддалена веб-розробка.

Abstract

The paper explores the possibilities of information protection during the Codeanywhere cloud service development process with the help of crypto-code means of information protection with non-binary linear block codes. The general essentials and principles of the used mathematical apparatus are offered for providing a high level of cryptographic stability of the investigated system are presented.

Keywords: cloud IDE, crypto-code information security systems, block code, remote web development.