МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ И СОКРЫТИЯ ИНФОРМАЦИИ

УДК 004.056.5

І.Ф. АУЛОВ, канд. техн. наук, К.Е. ЛИСИЦЬКИЙ

ЗАСОБИ МОДЕЛЮВАННЯ ТА АНАЛІЗУ РИЗИКІВ В СЕРЕДОВИЩІ ХМАРНИХ ОБЧИСЛЕНЬ

Вступ

Хмарні рішення представляють собою складні системи з дуже розгалуженою архітектурою, яка складається з великої кількості компонентів та зв'язків між ними, що в залежності від питомих вимог замовника можуть мати різні конфігурації. При побудові таких систем особливу увагу необхідно приділяти моделюванню та аналізу ризиків. Як показує практика, найбільшу ефективність від моделювання та аналізу загроз в системах, в тому числі системах хмарних обчислень, можливо досягти лише при застосуванні методів з моделювання та аналізу загроз на всіх етапах створення та життєвого циклу системи, починаючи з проектування архітектури майбутньої системи. Такий підхід дозволяє реалізувати забезпечення глибокого та послідовного захисту в системі. Для моделювання та аналізу ризиків може бути використане програмне забезпечення як з відкритим похідним кодом, так і з закритим, а також безкоштовне та те, що потребує придбання ліцензії.

1. Засоби моделювання та аналізу ризиків з відкритим кодом

Для аналізу можливості застосування в задачах моделювання загроз та оцінки ризиків в середовищі хмарних обчислень було обрано наступні програмні продукти з відкритим кодом:

- OWASP Threat Dragon;
- CAIRIS;
- Mozilla Seasponge.

1.1. OWASP Threat Dragon

OWASP Threat Dragon – це програма для моделювання загроз у веб-середовищі, що дозволяє створювати графічні моделі систем, та на їх основі виконувати автоматичну генерацію та аналіз загроз і їх наслідків. Розробники програми ставили перед собою мету з реалізації простого та зручного інтерфейсу користувача для створення моделей систем та потужного автоматизованого алгоритму з генерації та аналізу загроз за набором правил для використання програми на різних етапах розробки системи [1].

Програма розробляється в рамках проекту Open Web Application Security Project (OWASP) та поширюється як вільний продукт за ліцензією Apache 2.0. Поточною версією є версія 0.1.26, опублікована 17 травня 2017 року [2]. Проект OWASP з'явився 1 грудня 2001 року і був створений в якості неприбуткової благодійної організації в Сполучених Штатах 21 квітня 2004 року з метою забезпечення безпеки веб-застосунків в мережі Інтернет. До складу спільноти OWASP входять корпорації, освітні організації, а також приватні особи зі всього світу. Спільнота працює над створенням наукових статей, навчальних підручників, документації інструментів та технологій, присвячених безпеці веб-застосунків в мережі Інтернет, що публікуються відкрито [3].

Програма поставляється у вигляді електронного додатка для встановлення на ПК для OS X та Windows або веб-додатку для роботи через браузер. Як метод визначення та аналізу загроз використовується метод STRIDE.

Основними перевагами інструмента є:

- простий та зручний інтерфейс користувача;
- потужний автоматизований алгоритм з обробки та оцінці загроз за правилами, який

дозволяє залучати звичайних користувачів, що не є експертами до роботи;

– інтеграція з іншими інструментами життєвого циклу розробки;
– використання підходу STRIDE для класифікації загроз;
– відкритість вихідного коду;
– безкоштовність.

Головним недоліком проекту є те, що він знаходиться на етапі розробки, та деякий функціонал ще не реалізовано. Також проект може застосовуватися для моделювання загроз в хмарному середовищі, але не є спеціально розробленим для цього.

1.2. CAIRIS

CAIRIS представляє собою платформу для виявлення, визначення та перевірки безпеки систем на основі аналізу ризиків. CAIRIS був розроблений в рамках докторських досліджень Shamal Faily з реалізації програмних засобів для моделювання та аналізу безпеки програмного забезпечення на етапі розробки [4]. Утиліта знайшла своє широке застосування в різних сферах з аналізу безпеки та ризиків, в тому числі і критичних системах. Інтерфейс програми та закладений підхід також дозволяє використовувати її і для систем хмарних обчислень. Утиліта CAIRIS має відкритий вихідний код [5] та поширюється під ліцензією Apache Software.

CAIRIS є клієнт-серверним рішенням. Використання на сервері в якості мови програмування Python дозволяє підтримувати ОС на базі Linux, Windows, macOS. [5]. Доступ до клієнта надається через браузер. Останньою версією CAIRIS є версія 1.5.3 випущена 11 лютого 2018 року.

Переваги CAIRIS на відміну від інших утиліт:

– простий та доступний інтерфейс, що дозволяє визначити вимоги до системи та її архітектуру, і на базі цього виконати моделювання та аналіз;
– проведення моделювання та аналізу ризиків з врахуванням особливості та впливу середовища моделювання на систему, компонентів та зв’язків між ними, а також значення ризиків;
– підтримка автоматичного масштабування в процесі роботи над моделлю та її доопрацювання на основі аналізу попередньо створених зв’язків та елементів системи;
– візуалізація результатів у вигляді звітів та діаграм;
– підтримка інтеграції з іншими інструментами за рахунок надання стандартного інтерфейсу для взаємодії та форматів даних;
– підтримка розширення функціоналу;
– простота встановлення, підтримка різних ОС, наявність прикладів;
– безкоштовність.

Недоліки програми полягають у відсутності шаблонів та наборів елементів, загроз для моделювання в системах хмарних обчислень.

1.3. Mozilla Seasponge

Mozilla Seasponge – це безкоштовний онлайн інструмент для моделювання загроз, який створений фондом Firefox за підтримки наукового товариства в рамках ініціативи Mozilla Winter of Security у 2014 році для допомоги системним адміністраторам визначити та оцінити ризики, з якими стикаються їх мережі. Інструмент базується на основі сучасних веб-технологій та є проектом з відкритим кодом, останнє оновлення якого було 7 січня 2016 року. Використання сучасних веб-технологій дозволяє працювати з інструментом за допомогою веб-браузера в різних операційних системах. Метою створення розробники SeaSponge вважають те, що моделювання загроз часто ігнорується в життєвому циклі розробки програмного забезпечення, незважаючи на те, що це дуже важливий аспект архітектури безпеки системи, тому необхідне рішення, що відповідає вимогам відкритості, безкоштовності та доступності всім розробникам, наприклад на відміну від закритого рішення, як інстру-

мент моделювання загроз від компанії Microsoft [6].

SeaSponge дозволяє моделювати систему, за допомогою якої можна визначити потенційні загрози та ризики, та підтримує кілька видів діаграм для моделювання логічних розділів вашої системи в окремих місцях. Кожна діаграма містить потоки даних, апаратні та логічні компоненти.

Переваги утиліти SeaSponge:

– відкритість вихідного коду;
– створення моделей систем за допомогою графічного інтерфейсу;
– можливість роботи на різних платформах за допомогою веб-браузера;
– безкоштовність.

До недоліків утиліти SeaSponge можна віднести:

– відсутність визначених шаблонів загроз та необхідність їх самостійної реалізації;
– відсутність стандартних компонентів для моделювання загроз в хмарі;
– розробка знаходиться на ранньому етапі, відсутня реалізація багатьох заявлених функцій.

2. Засоби моделювання та аналізу ризиків з закритим кодом

В якості засобів для вирішення задач моделювання загроз та оцінки ризиків в середовищі хмарних обчислень було розглянуто наступні програмні продукти закритим кодом:

– Microsoft Threat Modeling Tool;
– RiskWatch;
– vsRisk.

2.1. Microsoft Threat Modeling Tool

Програма Threat Modeling Tool розроблена компанією Microsoft для моделювання та аналізу загроз на етапі розробки та узгодження архітектури програмного забезпечення та представляє собою основний елемент в концепції життєвого циклу безпечної розробки програмного забезпечення (SDL) Microsoft [7]. Головним призначенням програми є мінімізація витрат на етапі проектування архітектури, впровадження та використання системи за рахунок використання адекватних мір з захисту, що відповідають загрозам.

Перша версія цього програмного забезпечення з’явилася в 2011 році під назвою Threat Analysis & Modeling Tool. На той час програмне забезпечення дозволяло експертам, не пов'язаним з безпекою, створювати та аналізувати моделі загроз для різних систем. В 2016 році вийшла оновлена версія програмного забезпечення, яка змінила назву на Microsoft Threat Modeling Tool та отримала розширену функціональність з моделювання та аналізу загроз в хмарному середовищі на основі технології Azure. Для вирішення цієї задачі програмне забезпечення в своєму складі має готовий набір стандартних компонентів хмари Azure та набір з загроз, які можуть бути реалізовані для компонентів та зв’язків між ними. Поточна версія поширюється вільно та доступна для завантаження на офіційному сайті Microsoft; працює в середовищі операційних систем Windows 7 та вище [8].

Визначення загроз та вразливостей системи в програмі базується на методах STRIDE та DREAD [8].

Основними перевагами програмного забезпечення є:

– моделювання, аналіз загроз та вразливостей безпеки на етапі проектування архітектури системи;
– автоматизація процесу моделювання та аналізу загроз, наявність зворотного зв’язку при моделюванні;
– візуалізація моделей та можливість отримання формалізованих звітів з аналізу моделі;
– наявність набору стандартних компонентів та загроз для моделювання та аналізу в середовищі хмарних обчислень;
– можливість додавати нові та редагувати чинні компоненти та загрози;

– використання методів STRIDE для класифікації загроз за типом та методу DREAD за наслідками;

– безкоштовність.

До недоліків можна віднести:

– закритість вихідного коду, що не дозволяє за необхідності розширити функціонал та перевірити коректність реалізації методів аналізу;

– підтримка ОС Windows;

– наявність компонентів та набору загроз тільки для моделювання та аналізу в середовищі хмари на базі технології Azure.

2.2. RiskWatch

З 1993 року компанія RiskWatch є світовим лідером у наданні рішення щодо оцінки ризиків. Підхід RiskWatch базується на тому, що ефективність керування ризиками безпеки та відповідності залежить від їх кількісної оцінки [9]. Утиліта була розроблена у 1988 році за участі Національного Інституту Стандартів та Технологій США, Міністерства Оборони США та Міністерства Оборони Канади. RiskWatch є комерційним та не надає відкритий код проекту.

RiskWatch працює на усіх пристроях, які мають доступ до інтернету, а також в офлайн режимі. Мінімальні системні вимоги, встановлені виробником: Windows Server 2008, JRE1.6, ApacheTomcat7.0, MySQL, MySQLDriver3.5, IE8Version 8.0.7600.16385, Firefox, Chrome [10].

RiskWatch підхід забезпечує попередню оцінку ризику та захисту від динамічних загроз, що можуть змінюватися.

RiskWatch зосереджений на забезпеченні:

– комплексного підходу, що ґрунтується на доказах та відповідає моделям ризику стандартів ISO 32001, Sandia Lab і FEMA;

– системи, яку клієнт може легко налаштувати для виконання будь-якого типу оцінок ризику, яка має відношення до своєї галузі;

– моделі підприємства, яке надає клієнтам єдиний вид ризиків у розподіленому підприємстві;

– захисту на основі оцінки ризику в режимі реального часу для зосередження зусиль та максимізації результатів;

– технологічного агностичного рішення, призначеного для підтримки різних екосистем;

– оновлення інформації про загрози та засобів протидії їм;

– актуального набору американських та міжнародних правил, найкращих практик і тематичних досліджень [9].

До переваг RiskWatch окрім відносної простоти використання можна віднести:

– глибоко відпрацьована та добре зарекомендована методологія аналізу ризиків;

– поєднання кількісної та якісної оцінки ризиків;

– велика база загроз, вразливостей та контрзаходів – база знань;

– можливість редагування та удосконалення бази знань;

– формування звітів.

Головним недоліком утиліти є закритість вихідного коду та необхідність купувати ліцензію для її використання.

2.3. vsRisk

Інструмент аналізу ризиків vsRisk був розроблений британською компанією IT Governance разом з Vigilant Software, це сучасний продукт аналізу ризиків, який базується на міжнародному стандарті ISO 27001. vsRisk є комерційним та не надає відкритий код проекту. vsRisk підтримує ОС Windows 7 та вище [11].

Цей програмний продукт надає простий та зрозумілий інтерфейс та має такі переваги:

– дозволяє оцінювати ризики порушення конфіденційності, цілісності та доступності

інформації для бізнесу, а також, з точки зору законодавства та контрактних обов'язків, перебуває в чіткій відповідності до стандарту ISO 27001;

– підтримує наступні стандарти (ISO/IEC 27002, BS7799-3:2006, ISO/IEC TR 13335-8:1998, NIST SP 800-30);

– містить інтегровану базу знань (загроз та вразливостей), яка регулярно оновлюється.

Окрім закритості вихідного коду та необхідності придбання ліцензії до недоліків vsRisk відноситься те, що він не надає кількісну оцінку ризиків, обмежуючись тільки якісною оцінкою ризиків.

Крім зазначеного недоліку, на поточний момент в базі знань vsRisk відсутні загрози та вразливості для моделювання систем хмарних обчислень.

3. Порівняння програмного забезпечення

Для порівняння програмного забезпечення для моделювання та аналізу загроз пропонується використовувати вимоги, що визначені в табл. 1.

Таблиця 1

Порівняння засобів моделювання та аналізу ризиків

ВИМОГИ	Microsoft Threat odeling Tool	OWASP Threat Dragon	CAIRIS	Mozilla Seasponge	RiskWatch	vsRisk
Підтримка моделювання та аналізу загроз в хмарному середовищі	+/-	+/-	+/-	-	+/-	-
Можливість застосування на різних етапах розробки системи	+	+	+	-	+	-
Автоматизований аналіз та формування звітів	+	+	+	-	+	-
Отримання якісної оцінки ризиків	+	+	+	+	+	+
Отримання кількісної оцінки ризиків	+	-	+	-	+	-
Простота застосування (можливість працювати без залучення експерту)	+	+	+	+	+/-	+
Інтеграція з іншими засобами	+/-	+	+	+	-	-
Можливість розширення функціональності	-	+	+	+	-	-
Кросплатформеність	-	+/-	+/-	+	+	-
Безкоштовність	+	+	+	+	-	-
Відкритість вихідного коду	-	+	+	+	-	-
Функціональність продукту, відповідає заявленому (розробка завершена)	+	-	+	-	+	+

За результатами порівняння можна зробити наступні висновки:

– жодна з програм в повній мірі не відповідає висунутим вимогам;

– програми OWASP Threat Dragon, Mozilla Seasponge – знаходяться на етапі розробки, та не можуть на поточний момент застосовуватися без суттєвої доробки;

– внаслідок відкритості коду та умов ліцензування програмне забезпечення OWASP Threat Dragon, CAIRIS та Mozilla Seasponge може бути доопрацьоване під потреби середовища хмарних обчислень;

– для застосування програмного забезпечення Microsoft Threat Modeling Tool необхідним є створення бази об'єктів, загроз та вразливостей для хмарного середовища, що побудоване не тільки на технологіях Windows Azure.

Висновки

Моделювання та аналіз ризиків для інформаційних систем є складною задачею та вимагає високого рівня кваліфікації від співробітника, який її проводить. Хоча моделювання ризиків в хмарному середовищі використовує аналогічні підходи тим, що застосовуються в інформаційно-телекомунікаційних системах внаслідок суттєвих відмінностей, пов`язаних з властивостями обробки інформації в хмарі та особливістю побудови хмари, вони мають суттєві відмінності, які необхідно враховувати. Для спрощення цього процесу та зменшення кількості помилок впроваджуються програмні продукти, які автоматизують дії та дозволяють перевіряти коректність розроблених моделей. В результаті дослідження були розглянуті програмні продукти моделювання та оцінки ризиків з відкритим та закритим вихідним кодом, а також комерційні продукти.

За результатами порівняння зроблені такі висновки: висунутим вимогам для моделювання та оцінки ризиків безпеки в хмарному середовищі повністю не відповідає жодний продукт; програмні продукти OWASP Threat Dragon, CAIRIS, Mozilla Seasponge не можуть бути застосовані та потребують доробок, але завдяки відкритості коду та умовам ліцензування це програмне забезпечення може бути доопрацьоване під потреби середовища хмарних обчислень та може бути розширені їх функціональні можливості. Застосування комерційних продуктів RiskWatch та vsRisk можливе лише при реалізації необхідного функціоналу їх розробниками. Закритість вихідних кодів продуктів та відсутність можливості розширення функціоналу сторонніми розробниками призводить до ризику неможливості їх застосування в майбутньому.

На сьогодні за сукупністю вимог та реалізованим функціональним можливостям найбільш перспективним є використання утиліти Microsoft Threat Modeling Tool. При цьому актуальними залишаються питання створення та підтримки бази загроз, елементів та зв’язків між ними в актуальному стані. Використання методологій STRIDE та DREAD, які використовуються в програмному продукті Microsoft Threat Modeling Tool дозволяє отримати попередні результати з аналізу ризиків системи на різних етапах її життєвого циклу, які надалі можуть бути основою більш детальних досліджень.

Список літератури:

1. OWASP Threat Dragon [Електронний ресурс]. Режим доступу: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.

2. OWASP Threat Dragon on Github [Електронний ресурс]. Режим доступу: https://github.com/mike-goodwin/owasp-threat-dragon-desktop.

3. The Open Web Application Security Project (OWASP) Електронний ресурс]. Режим доступу: https://www.owasp.org.

4. CAIRIS [Електронний ресурс]. Режим доступу: https://cairis.org/.

5. CAIRIS [Електронний ресурс]. https://github.com/failys/cairis.

6. Mozilla launches free, online threat modelling tool [Електронний ресурс]. Режим доступу: https://siliconangle.com/blog/2015/04/01/mozilla-launches-free-online-threat-modelling-tool/.

7. Microsoft Threat Modeling Tool [Електронний ресурс]. Режим доступу: https://docs.microsoft.com/en-us/azure/security/azure-security-threat-modeling-tool.

8. Threat Modeling [Електронний ресурс]. Режим доступу: https://msdn.microsoft.com/en-us/library/ff648644.aspx.

9. RiskWatch technical specifications [Електронний ресурс]. Режим доступу: http://www.riskwatch.com/wp-content/uploads/2014/05/SWDataSheet.pdf.

10. RiskWatch [Електронний ресурс]. Режим доступу: http://www.riskwatch.com/.

11. vsRisk [Електронний ресурс]. Режим доступу: https://www.vigilantsoftware.co.uk/product/vsrisk-standalone.

Акціонерне товариство
«Інститут інформаційних технологій», Харків;
Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 05.10.2018