УДК 004.056

НЕЧІТКА МОДЕЛЬ ОЦІНКИ РИЗИКІВ WEB-ДОДАТКА

Тимчук О. С.

Донецький національний університет (м. Вінниця)

Запропоновано нову модель оцінки ризиків web-додатка. Проблеми невизначеності, що виникають при оцінці ризиків, вирішуються за допомогою методів теорії нечітких множин та систем другого типу.

Постановка проблеми. Підвищення складності web-додатків різко ускладнює процес їх захисту. Побудова додатків на базі нових сервісів і технологій з вузькими місцями збільшує кількість вразливостей, використання яких є ключовим об'єктом інтересу зловмисників. Базовим етапом при побудові системи безпеки web-додатка є оцінка ризиків [1]. При оцінці ризиків використовуються, як правило, моделі, побудовані на якісній оцінці факторів ризику. Кількісна оцінка вимагає великих витрат часу і додаткових знань, які не завжди доступні розробникам.

Аналіз останніх досліджень і публікацій. Основними моделями оцінки ризиків, які асоціюються з web-додатками, є: OWASP Risk Rating Methodology, Common Vulnerability Scoring System (CVSS), OCTAVE, AS / NZS МЕК 62198: 2015. Дослідниками в галузі інформаційної безпеки запропоновано ряд моделей оцінки ризиків, побудованих на базі нейронних мереж, еволюційних алгоритмів і теорії нечітких множин і систем першого типу [2]. При аналізі основних моделей і опублікованих результатів досліджень було встановлено, що фактори ризику web-додатка є невизначеними. Основні причини невизначеності:

- серед фахівців відсутня однозначна інтерпретація факторів ризику;
- фактори ризику представлені словесним описом, що носить інтуїтивний характер;
- тимчасові ряди факторів ризику мають нелінійну структуру;
- експлуатація вразливостей зловмисниками носить непостійний характер протягом певних періодів часу.

Традиційні методи теорії нечітких множин та систем першого типу не дозволяють в повному обсязі враховувати невизначеність такого роду. Тому перспективним є розвиток підходів теорії дискретних інтервальних нечітких множин та систем другого типу (DIT2FSs і DIT2FLSs) [3] для інтерпретації існуючих моделей оцінки ризиків web-додатків.

Мета статті. Розробити систему оцінки ризиків web-додатка. Система повинна бути побудована на базі OWASP Risk Rating Methodology. Для обліку невизначеності факторів ризику використовувати DIT2FLSs.

Основні матеріали дослідження. Оцінка ризику складається з 3 етапів [4]:

1. Ідентифікація ризику (risk identification). Ідентифікація ризиків web-додатка – складний і тривалий процес. Велика кількість існуючих типів вразливостей web-додатка (більше 150) унеможливлює розробку абсолютно безпечного додатка. Для спрощення процесу ідентифікації розроблено систему класифікації ризиків [1], а також пропонуються різні звіти про найбільш серйозні ризики, які притаманні практично всім web-додаткам.

2. Аналіз ризику (risk analysis). Згідно з OWASP Risk Rating Methodology, аналіз ризику складається з наступних етапів [1]:

- аналіз чинників уразливості (vulnerability factors);
- аналіз факторів загроз (threat agent factors);
- аналіз факторів технічного і бізнес збитків в результаті успішної експлуатації уразливості (technical and business impact factors).

Результатом кожного етапу аналізу є експертна оцінка фактору ризика, приведена до нормованого інтервалу [0; 10].

3. Визначення ступеня ризику (risk evaluation). Так як експертні оцінки факторів ризику володіють значною невизначеністю, в даній роботі для оцінки ступеня ризику пропонується використовувати засоби теорії DIT2FSs і DIT2FLSs.

Представимо модель оцінки ризиків web-додатка

$$R(t) = \left\{ \left\langle risk_i(t), CM_i(t) \right\rangle \right\}, i = \overline{1, I},$$

де $risk_i(t)$ – ступінь i-го ризику, ідентифікованого в момент часу t,

$CM_i(t)$ – контрзаходи для i-го ризику, що приймаються в момент часу t,

I – кількість ідентифікованих ризиків в момент часу t.

Відповідно до положень теорії DIT2FSs і DIT2FLSs представимо модель оцінки ступеня ризику

$$risk_i(t) = F(IN_i(t), LI, LO, R),$$
$$IN_i(t) = \left\langle in_n^i \right\rangle, n = \overline{1, N},$$
$$LI = \left\langle li_n \right\rangle,$$
$$R = \left\langle r_m \right\rangle, m = \overline{1, M},$$

де $IN_i(t)$ – набір чітких вхідних значень (експертні оцінки факторів i-го ризику),

N – кількість вхідних значень,

LI – набір вхідних лінгвістичних змінних другого типу, які описують фактори ризику web-додатка,

LO – результуюча лінгвістична змінна другого типу, що описує рівень ризику web-додатка,

R – набір нечітких правил, на основі яких визна-

чається рівень ризику web-додатка,

M – кількість нечітких правил,

F – операція нечіткого логічного висновку (алгоритм Mamdani).

У даній роботі ступінь ризику web-додатка визначається на базі чотирьох експертних оцінок

$$IN_i(t) = \left\langle in_1^i, in_2^i, in_3^i, in_4^i \right\rangle,$$

де in_1^i – оцінка i-ої уразливості; значення приводиться до нормованого інтервалу $[0;10]$,

in_2^i – оцінка джерел загроз для i-ої уразливості; значення приводиться до нормованого інтервалу $[0;10]$,

in_3^i – оцінка можливого технічного збитку в результаті експлуатації i-ої уразливості; значення приводиться до нормованого інтервалу $[0;10]$,

in_4^i – оцінка можливого бізнес збитку в результаті експлуатації i-ої уразливості; значення приводиться до нормованого інтервалу $[0;10]$.

Набір LI містить 4 лінгвістичних змінних

$$LI = \langle li_1, li_2, li_3, li_4 \rangle,$$

де li_1 – лінгвістична змінна, що описує рівні оцінки вразливостей; містить 3 терми: none to very little, a moderate amount, a maximum amount; визначена на універсальній множині $X_1 = [0;10]$ (рис. 1а),

li_2 – лінгвістична змінна, що описує рівні оцінки джерел загроз; містить 5 термів: none to very little, some, a moderate amount, a large amount, a maximum amount; визначена на універсальній множині $X_2 = [0;10]$ (рис. 1б),

li_3 – лінгвістична змінна, що описує рівні оцінки можливого технічного збитку в результаті експлуатації уразливості; містить 3 терми: negligible, moderate, critical; визначена на універсальній множині $X_3 = [0;10]$ (рис. 1в),

li_4 – лінгвістична змінна, що описує рівні оцінки можливого бізнес збитку в результаті експлуатації уразливості; містить 5 термів: negligible, minor, moderate, critical, catastrophic; визначена на універсальній множині $X_4 = [0;10]$ (рис. 1г).

Результуюча лінгвістична змінна описує ступені ризику web-додатка; містить 4 терми: low, medium, high, extreme; визначена на універсальній множині (рис. 1д).

У даній роботі вибір термів лінгвістичних змінних і форми функцій приналежності заснований на OWASP Risk Rating Methodology та моделі оперування словами Jerry M. Mendel [4].

Набір правил містить 225 нечітких правил типу *IF-THEN*. Для кожного правила експертом встановлено ступінь довіри до правила.

Приклад нечіткого правила з набору R:

r : *IF* $in_1 \in$ "a moderate amount" *AND*
$in_2 \in$ "a large amount" *AND*
$in_3 \in$ "critical" *AND*
$in_4 \in$ "catastrophic"
THEN "high"
WEIGHT IS 0.95

Ранжування ідентифікованих ризиків за отриманими оцінками дозволяє виконати управління найбільш значущими з них, виділяючи для цього необхідні ресурси. Вибір необхідних контрзаходів може бути побудований на базі існуючих довідників, які пропонують для кожного типу ризику web-додатка відповідні заходи протидії. Приклад контрзаходів, які радить OWASP Risk Rating Methodology для розробників web-додатків [1]:

Ризик – некоректна автентифікація та управління сеансами.

Контрзаходи – єдиний набір елементів сильного контролю за автентифікацією та управлінням сеансами:

- відповідати всім вимогам до автентифікації та управління сеансами, визначеним у стандарті підтвердження безпеки додатків (ASVS) OWASP V2 (автентифікація) та V3 (управління сеансами);
- мати простий інтерфейс для розробників (задля емуляції, використання або в якості основи гарним прикладом є автентифікатор та інтерфейс прикладного програмування користувача ESAPI);
- докладати всіх зусиль задля попередження атак XSS (міжсайтове виконання сценаріїв), що використовуються для крадіжки ІН сесій.

Для запропонованої моделі оцінки ризиків web-додатка розроблено багатоплатформний калькулятор ризиків "Fuzzy Risk Calculator" на базі пакету бібліотек підтримки DIT2FLS (DIT2FLS Toolbox and Package Library) [3].

Для проектування і розробки "Fuzzy Risk Calculator" використано Microsoft Visual Studio 2013, технологію .NET, мову програмування C#.

Вимоги для експлуатації "Fuzzy Risk Calculator":

1. Операційна система – починаючи з Windows XP з пакетом оновлень 3 (SP3) (тільки 32-розрядні);
2. Microsoft .NET Framework 4.0.

Висновки. Розроблено нову модель оцінки ризиків web-додатка. Оцінка ризиків побудована на базі аналізу факторів ризику. Для оцінки факторів в роботі пропонується використовувати методи теорії дискретних інтервальних нечітких множин та систем другого типу.

На базі запропонованої моделі, розроблено багатоплатформний калькулятор ризиків "Fuzzy Risk Calculator". При тестуванні "Fuzzy Risk Calculator" були отримані позитивні результати.

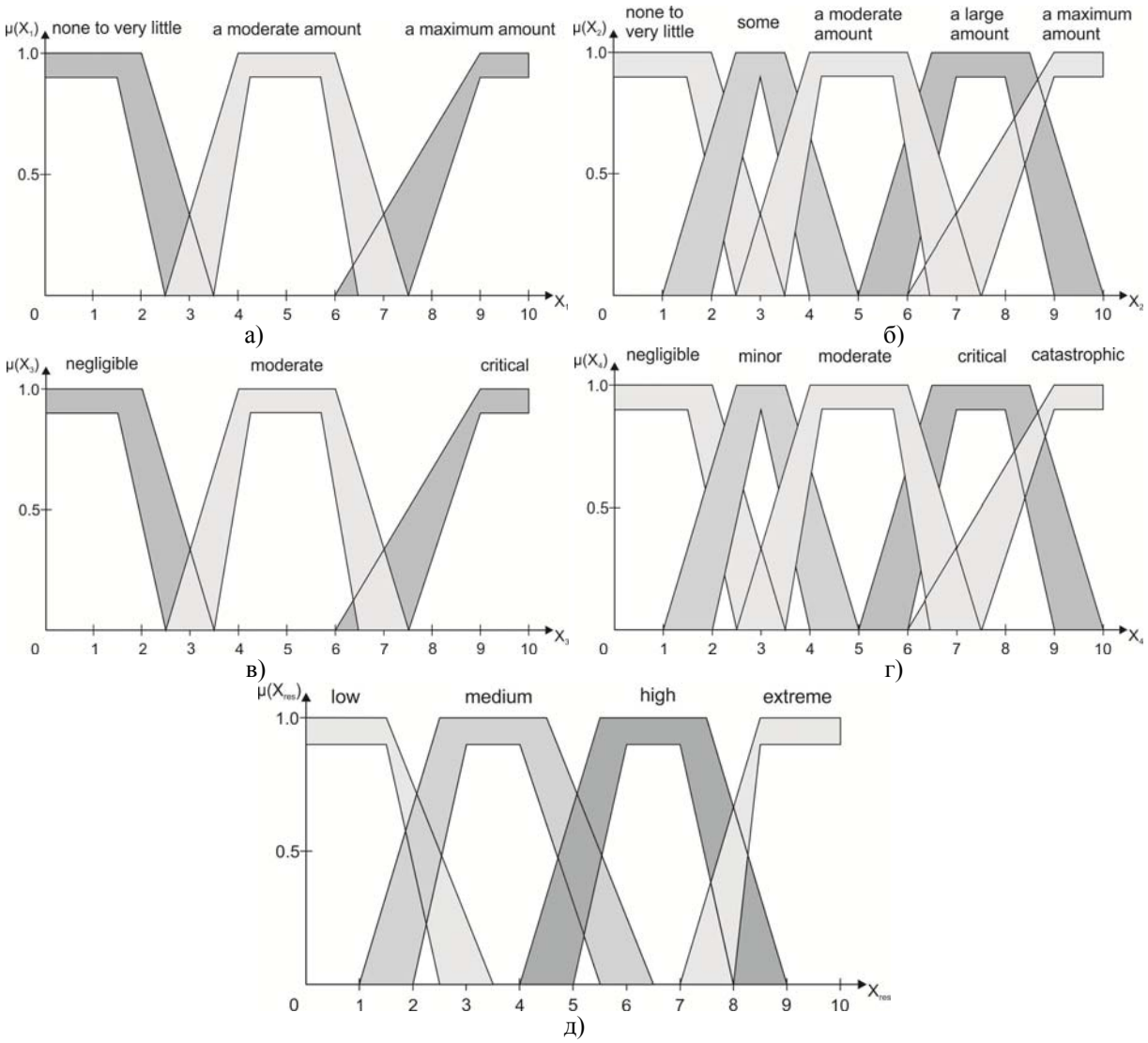

Рисунок 1 – Лінгвістичні змінні (вхідні і результуюча) моделі оцінки ризику.
(а), (б), (в), (г) – вхідні, (д) – результуюча.

Список використаних джерел.

1. OWASP Risk Rating Methodology. [Електронний ресурс]. Режим доступу: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology/ — Дата доступу: 01.10.2015.

2. Bartos J. Fuzzy tool for conducting information security risk analysis / J. Bartos, B. Walek, C. Klimes, R. Farana // Proceedings of the 15th International Carpathian Control Conference (ICCC), Velke Karlovice. – 28-30 May 2014. – P. 28-33.

3. Petrenko T. Package Library and Toolbox for Discrete Interval Type-2 Fuzzy Logic Systems / T. Petrenko, O. Tymchuk // Proceedings of the 18th International Conference on Soft Computing (MENDEL), Brno, Czech Republic. –27-29 June 2012. – P. 233-238.

4. ISO 31000:2009. Risk management - Principles and guidelines. [Електронний ресурс]. Режим доступу: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43170/ — Дата доступу: 01.10.2015.

5. Mendel J. Perceptual Computing: Aiding People in Making Subjective Judgments / J. Mendel, D. Wu // Wiley-IEEE Press; 1 edition . – 2010. – 336 p.

Аннотация

НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНКИ РИСКОВ WEB-ПРИЛОЖЕНИЯ

Тимчук О. С.

Предложена новая модель оценки рисков web-приложения. Проблемы неопределенности, возникающие при оценке рисков, решаются с помощью методов теории нечетких множеств и систем второго типа.

Abstract

FUZZY RISK ASSESSMENT MODEL FOR WEB-APPLICATION

O. Tymchuk

This paper presents the new risk assessment model for web-application. The problems of uncertainty occurring in risk assessment are solved by the methods of the theory of type-2 fuzzy sets and systems.