МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ
І ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ШАМРАЙ ЕДУАРД ВАСИЛЬОВИЧ

УДК 004.056

МЕТОДИ І ЗАСОБИ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ WEB-СЕРВЕРІВ

123 «Комп'ютерна інженерія»

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль 2018

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж **Тиш Євгенія Володимирівна,** Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: кандидат технічних наук, доцент кафедри інформатики і математичного моделювання **Гащин Надія Богданівна,** Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 28 грудня 2018 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №34 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд. 603

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Сучасний розвиток інформаційних технологій характеризується вдосконаленням існуючих та створенням нових технологій, методів і засобів, а також методологій у галузях комп'ютерної інженерії, інженерії програмного забезпечення, штучного інтелекту та машинного навчання. При цьому спостерігається тренд міграції та накопичення як програмних (програмно-апаратних) засобів, так і самих даних в мережі Internet.

У контексті розвитку комп'ютерної інженерії спостерігається тенденція щодо взаємодії вбудованих систем з різноманітними хмарними сховищами, набувають широкого застосування технології «розумних будинків», «розумних міст» і т.п. Інженерія програмного забезпечення характеризується створенням високорівневих технологій побудови та керування Big Data, вдосконаленням існуючих алгоритмів, методів і засобів розробки та управління програмними проектами, що дають змогу знизити поріг входу у дану галузь. Штучний інтелект та машинне навчання забезпечують «інтелект» програмних та програмно-апаратних систем, що зумовлено наявністю великої кількості даних та стрімким розвитком алгоритмів даної сфери.

Однак, враховуючи тренд розвитку інформаційних технологій в сторону використання мережі Internet, крім забезпечення функціональності та зручності використання інформаційних систем, необхідно забезпечити їх надійність, зокрема, захищеність. Це стосується web-серверів, оскільки вони є основою для функціонування програмного забезпечення в мережі Internet та зберігання даних.

Для забезпечення та підвищення надійності інформаційних систем розроблено ряд вітчизняних та закордонних стандартів (стандарти серії ГОСТ 34.ххх, ISO/IEC 15288, EIA 632, EIA 731, DOD 2167A, DEF Stan 00-55 та ін.). Однак їх застосування обмежується недосконалістю формального представлення критеріїв, відсутністю стандартизованих процедур проведення процесу оцінювання надійності та їх формального опису.

Дослідженню надійності ІС, зокрема її програмної складової, присвячено ряд наукових та науково-прикладних публікацій, як українських науковців (В.С. Харченко, О.М. Тарасюк, А.А. Орехова, Є.В. Бебешко, К.М. Лавріщева, Г.В. Коваль, В.В. Скляр), так і закордонних (S. Gnesi, S. Russo, R. Bloomfield, G. Mayers, M. Holsted). У цих роботах досліджується надійність як ІС, так і програмних систем, пропонується ряд методів та моделей, що дають змогу підвищити адекватність відображення потреб замовника на реалізацію властивостей стійкості та надійності ІС, врахувати та забезпечити ряд додаткових характеристик. Однак комплексного підходу щодо оцінювання надійності, зокрема, захищеності web-серверів, який би давав змогу уніфікувати та кількісно виражати показники, а також формально описував процедуру оцінювання захищеності, у цих роботах не наведено.

Тому актуальною задачею у сфері інформаційних технологій є вдосконалення методів та засобів оцінювання захищеності web-серверів, які б дали змогу більш повно, адекватно та однозначно виражати ступінь захищеності програмних продуктів та виявляти їх потенційні вразливості.

Метою роботи є дослідження існуючих методів і засобів оцінювання захищеності web-серверів, вдосконалення та адаптація Safety Case методології для підвищення точності та повноти результатів оцінювання захищеності web-серверів.

Для досягнення вказаної мети в роботі поставлено наступні **задачі**:

– аналіз наукових публікацій та стандартів з надійності програмного забезпечення для визначення сучасного стану та шляхів удосконалення процесів оцінювання захищеності web-серверів;

– дослідження та обґрунтування технологій забезпечення та оцінювання захищеності програмного забезпечення комп'ютерних систем;

– обґрунтування та удосконалення методології Safety Case для підвищення ефективності оцінювання захищеності web-серверів;

– побудова та формалізація моделі оцінювання захищеності web-серверів на основі Safety Case ядер;

– обґрунтування і вдосконалення методу оцінювання захищеності web-серверів;

– аналіз засобів підтримки процесу оцінювання захищеності web-серверів та розробка архітектури засобу підтримки запропонованого методу;

– апробація запропонованих моделі і методу для оцінювання захищеності web-серверів.

Об'єкт дослідження: процес оцінювання захищеності програмного забезпечення.

Предмет дослідження: моделі, методи і засоби оцінювання захищеності web-серверів.

Методи дослідження. Для вирішення поставлених задач використано наступні методи: аналіз та узагальнення – при проведенні аналізу існуючих методів і засобів оцінювання захищеності web-серверів; теорії надійності, теорії ймовірності і математичної статистики,теорії множин – для формалізації та побудови моделі і методу оцінювання захищеності web-серверів; проектування та програмування – при побудові архітектури та бази даних програмного засобу автоматизації процесу оцінювання захищеності web-серверів; експеримент та вимірювання – для апробації запропонованого методу і моделі.

Наукова новизна одержаних результатів:

– уперше обґрунтовано та доповнено модель оцінювання захищеності web-серверів на основі Safety Case ядер, що дало змогу структурувати та автоматизувати обчислення критеріїв захищеності web-серверів та підвищити достовірність і точність оцінок;

– набув подальшого розвитку метод оцінювання захищеності web-серверів на основі Safety Case ядер та COTS компонентів, що дало змогу забезпечити більшу повноту і достовірність оцінок, у порівнянні з відомими методами, а також проводити оцінку захищеності на основі приватних і загального профілю вимог.

– уперше спроектовано архітектуру засобу підтримки процесу оцінювання захищеності web-серверів із застосуванням шарів Фаулера, що дало змогу визначити програмні модулі та типи зв'язків між, а також забезпечити гнучкий механізм взаємодії розробленого засобу і зовнішніми джерелами загроз та вразливостей.

Практичне значення одержаних результатів. Впровадження запропонованої моделі і методу оцінювання захищеності web-серверів реалізовано та впроваджено у вигляді інструменту, який дає змогу автоматизувати процеси побудови Safety Case ядер, забезпечити централізоване управління ними та підтримувати рішення експерта.

Публікації. Результати дослідження апробовано на VII міжнародній науково - технічній конференції молодих учених і студентів «Актуальні задачі сучасних технологій» (28-29 листопада 2018 р.) Тернопільського національного технічного університету імені Івана Пулюя та на VI науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (12-13 грудня 2018 року) у вигляді тез конференцій:

Структура роботи. Робота складається з пояснювальної записки та графічної частини. Пояснювальна записка складається із вступу, шести розділів, висновків, переліку посилань та додатку. Обсяг роботи: пояснювальна записка – 136 арк. формату А4, графічна частина – 10 аркушів формату А1.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність дослідження методів і засобів оцінювання захищеності web-серверів, сформульовано мету, задачі і методи дослідження, наведено наукову новизну та практичне значення одержаних результатів.

У першому розділі «Аналіз функціональності та вразливостей сучасних web-серверів» досліджено функціональність, застосування та структуру сучасних web-серверів, проведено аналіз та класифікацію вразливостей і загроз, яким піддаються web-сервери, інструментальні засоби і бази даних для виявлення та зберігання інформації про загрози, визначено місце процесу забезпечення та оцінювання захищеності web-серверів при експлуатації web-додатків. Проаналізовано методи оцінювання загроз та вразливостей web-серверів, у результаті якого встановлено, що більшість методів передбачає експертне оцінювання загроз, а також застосування багатьох автоматизованих засобів їх виявлення.

У другому розділі «Ієрархічні моделі та методи для прогнозування прийняття рішень щодо пріоритетів характеристик комп'ютерних систем» визначено особливості процесу оцінювання захищеності web-серверів і встановлено доцільність застосування методології Safety Case, обґрунтовано можливості вдосконалення цієї методології. Обґрунтовано та доповнено модель оцінювання захищеності web-серверів на основі Safety Case ядер, що дало змогу структурувати та автоматизувати обчислення критеріїв захищеності web-серверів та підвищити достовірність і точність оцінок. Запропоновано метод оцінювання захищеності web-серверів на основі Safety Case ядер та COTS компонентів, що дало змогу забезпечити більшу повноту і достовірність оцінок, у порівнянні з відомими методами, а також проводити оцінку захищеності на основі приватних і загального профілю вимог.

У третьому розділі «Побудова моделі та розробка методу оцінювання захищеності web-серверів» на основі UML нотацій визначено ролі та функціональні вимоги до автоматизованої системи підтримки процесу побудови моделі та реалізації методу оцінювання захищеності web-серверів, що дало змогу врахувати особливості Safety Case методології спроектовано архітектуру засобу підтримки процесу оцінювання захищеності web-серверів із застосуванням шарів Фаулера, що дало змогу визначити програмні модулі та типи зв'язків між ними з подальшою реалізацією, а також реалізовано процедури кількісного оцінювання та проведено експериментальні дослідження щодо вразливості web-серверів Apache та IIS.

У четвертому розділі «Обґрунтування економічної ефективності» обґрунтовано економічну ефективність проведення досліджень дипломної роботи магістра шляхом проведення відповідних розрахунків, що дало змогу встановити термін окупності на рівні 1,74 року при ціні 41790,55 грн..

У п'ятому розділі «Охорона праці та безпека в надзвичайних ситуаціях» проаналізовано вимоги з охорони праці та безпеки в надзвичайних ситуаціях, що дало змогу визначити шляхи мінімізації негативного впливу комп'ютерної техніки на користувачів засобу автоматизації процесу оцінювання захищеності web-серверів.

У шостому розділі «Екологія» проаналізовано методи узагальнення екологічної інформації та досліджено джерела шуму і вібрацій, методи їх знешкодження.

У загальних висновках до дипломної роботи магістра наведено результати виконання розділів дипломної роботи магістра, їх наукове та практичне значення при дослідженні методів і засобів оцінювання захищеності web-серверів.

Додатки до пояснювальної записки містять матеріали конференцій у яких опубліковано основні результати дипломної роботи магістра.

У графічній частині до дипломної роботи магістра проілюстровано основні наукові та практичні результати щодо запропонованих методів і засобів оцінювання захищеності web-серверів.

ВИСНОВКИ

Основні наукові та практичні результати роботи полягають у наступному:

Проведено аналіз наукових публікацій та стандартів з надійності програмного забезпечення і визначено сучасний стан та шляхи удосконалення процесів оцінювання захищеності web-серверів. На сучасному етапі для оцінювання захищеності web-серверів використовуються в основному експертні технології, а для одержання кількісних оцінок використовуються автоматизовані засоби. Критерії і процедури проведення оцінювання захищеності є слабоформалізованими та неуніфікованими. Основними шляхами підвищення ефективності процесу оцінювання захищеності є формалізація та автоматизація процедур визначення оцінок загроз та вразливостей.

Досліджено технології оцінювання захищеності програмного забезпечення комп'ютерних систем та обґрунтовано застосування методології Safety Case ядер для забезпечення та оцінювання захищеності web-серверів. Перевагами такої методології є гнучкість застосування та масштабованість, поєднання комплексних

підходів, що включають відомі методи оцінювання надійності та експертні технології.

Встановлено та обґрунтовано доцільність модифікації Safety Case методології шляхом доповнення моделі оцінювання захищеності web-серверів, що дало змогу структурувати та автоматизувати обчислення критеріїв захищеності web-серверів та підвищити достовірність і точність оцінок.

Побудовано та формалізовано модель оцінювання захищеності web-серверів на основі теоретико-множинних нотацій, що дало змогу в подальшому автоматизувати кроки з побудови Safety Case ядер.

Формалізовано метод побудови приватного профілю вимог щодо захищеності web-серверів, що дозволило розвинути метод оцінювання захищеності web-серверів на основі Safety Case ядер та COTS компонентів і дало змогу забезпечити більшу повноту і достовірність оцінок, у порівнянні з відомими методами, а також проводити оцінку захищеності на основі приватних і загального профілю вимог.

Формалізовані модель і метод дали змогу виявляти потенційні загрози та вразливості у захищеності web-серверів і є базисом для подальшого розвитку методів прогнозування захищеності web-серверів та попередження загроз.

Проаналізовано засоби підтримки процесу оцінювання захищеності web-серверів та спроектовано архітектуру засобу підтримки запропонованого методу, що дало змогу визначити програмні модулі та типи зв’язків між ними з подальшою реалізацією і підвищити часову ефективність обчислення показників захищеності.

Апробовано запропоновані моделі і методу для оцінювання захищеності web-серверів на основі реалізації процедур кількісного оцінювання захищеності web-серверів Apache та IIS.

Обґрунтовано економічну ефективність проведення досліджень дипломної роботи магістра шляхом проведення відповідних розрахунків, що дало змогу встановити термін окупності на рівні 1,74 року при ціні 41790,55 грн.

Проаналізовано вимоги з охорони праці та безпеки в надзвичайних ситуаціях, що дало змогу визначити шляхи мінімізації негативного впливу комп’ютерної техніки на користувачів засобу автоматизації процесу оцінювання захищеності web-серверів.

Проаналізовано методи узагальнення екологічної інформації та досліджено джерела шуму і вібрацій, методи їх знешкодження.

Проаналізовано використання альтернативних джерел енергії в Україні та проведено аналіз статистичних показників в екології.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Шамрай Е.В. Підхід Safety Case ядер для забезпечення захищеності web серверів / Е.В. Шамрай, Є.В. Тиш// Матеріали VII міжнародній науково - технічній конференції молодих учених і студентів «Актуальні задачі сучасних технологій» (28-29 листопада 2018 р.) Тернопільського національного технічного університету імені Івана Пулюя – Тернопіль, ТНТУ – 2018 – с. 195.

2. Шамрай Е.В. Рольова модель засобу автоматизації процесу оцінювання захищеності web-серверів / Е.В. Шамрай, Є.В. Тиш – Матеріали VI науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (12-13 грудня 2018 року) – Тернопіль, ТНТУ – 2018 – с. 86.

АНОТАЦІЯ

Шамрай Е.В. Методи і засоби оцінювання захищеності web-серверів

Дипломна робота на здобуття освітнього ступеня магістра 123 – Комп'ютерна інженерія. – Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль 2018.

У дипломній роботі магістра проведено аналіз функціональності та організації web-серверів у результаті якого виявлено можливі компоненти ураження та способи проникнення «зловмисників» для нанесення шкідливого впливу на безпеку та надійність функціонування серверів. Це дало змогу врахувати потенційно-слабкі місця web-серверів та визначити атрибути вразливостей, рівень їх критичності, які необхідно врахувати в процесі оцінювання захищеності web-серверів.

Проаналізовано та класифіковано відомі загрози та вразливості web-серверів, встановлено ступінь їх автоматизованого та ручного виявлення, що в подальшому повинні бути включеними у метод оцінювання безпеки та захищеності web-серверів.

Обґрунтовано та доповнено модель оцінювання захищеності web-серверів на основі Safety Case ядер, що дало змогу структурувати та автоматизувати обчислення критеріїв захищеності web-серверів та підвищити достовірність і точність оцінок. Спроектовано архітектуру засобу підтримки процесу оцінювання захищеності web-серверів із застосуванням шарів Фаулера, що дало змогу визначити програмні модулі та типи зв'язків між ними з подальшою реалізацією. Реалізовано процедури кількісного оцінювання захищеності web-серверів, проведено експериментальні дослідження щодо вразливості web-серверів Apache та IIS.

Формалізовано метод побудови приватного профілю вимог щодо захищеності web-серверів із застосуванням теоретико-множинних нотацій, що в подальшому дало змогу створювати Safety Case ядра автоматизованим шляхом.

Ключові слова: ЗАХИЩЕНІСТЬ, WEB-СЕРВЕР, ЗАГРОЗА, ВРАЗЛИВІСТЬ, МЕТОД, ЗАСІБ.

ANNOTATION

Shamrai E.V. Methods and tools of web-servers protection assessment

The diploma paper for obtaining the Master's degree 123 – Computer engineering – Ternopil Ivan Puluj National Technical University, Ternopil 2018.

The master's thesis analyzes the functionality and organization of web-servers, which resulted in identifying the possible components of the damage and methods of penetration of "intruders" to inflict harmful influence on the security and reliability of the functioning of the servers. This made it possible to take into account the potential weaknesses of web servers and to identify the attributes of vulnerabilities, their level of criticality, which need to be taken into account in the process of assessing the security of web-servers.

The well-known threats and vulnerabilities of web-servers are analyzed and classified, their degree of automated and manual detection is determined, which in future should be included in the method of security assessment and security of web-servers.

The safety case model of Web server security evaluation was substantiated and supplemented, which made it possible to structure and automate the calculation of web server security criteria and increase the reliability and accuracy of evaluations. The architecture of the means to support the process of evaluating the security of web servers using Fowler layers was designed, which allowed to determine the software modules and the types of links between them and subsequent implementation. Procedures for quantifying the security of web servers were implemented, pilot studies on the vulnerability of Apache and IIS web servers were conducted.

The method of constructing a private profile of requirements for the security of web-servers with the use of multiple theoretical notations was formalized, which subsequently enabled the creation of Safety Case kernels by automated means.

Keywords: SECURITY, WEB SERVER, THREAT, VULNERABILITY, METHOD, TOOL.