cryptographic algorithms (RSA, ECC) by Shor's algorithm is substantiated. The purpose of the study is to develop approaches to the system design of Challenge-Response authentication protocols based on structural specifications of code cryptosystems. Crypto-code constructions whose stability is based on the NP-complete problem of decoding a random linear code are considered. The use of algebro-geometric codes over GF(q) is proposed, which provides improved combinatorial properties and error correction capability. The mathematical apparatus for forming an information sequence and an error vector for authentication protocols is presented. An analysis of pseudorandom number generators (PRNGs) is carried out and the feasibility of using shift registers with nonlinear transformations (S-blocks) for forming Galois field elements is substantiated. It is shown that this approach allows to ensure high speed and cryptoresistance of the authentication process. The proposed method allows to determine the minimum number of processing modules and to set performance specifications, which significantly reduces the development time of protection systems. The results have practical significance for creating survivable information networks resistant to quantum threats.

Keywords: information protection, post-quantum cryptography, authentication, McAlice crypto-code system, Niederreiter crypto-system, algebrogeometric codes, pseudorandom number generators.

Надійшла до редакції (Received): 10.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

УДК 004.056.5:004.77:004.415 DOI: 10.31673/2409-7292.2026.032815

Сторчак Антон Сергійович
кандидат технічних наук, доцент, доцент кафедри кіберзахисту та безпеки спеціального зв'язку
Інститут спеціального зв'язку та захисту інформації, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: 0000-0002-5267-3122
E-mail: storchakanton@gmail.com

Печенюк Дмитро Ігорович
магістр Інституту спеціального зв'язку та захисту інформації
Інститут спеціального зв'язку та захисту інформації, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: 0009-0001-1980-1583
E-mail: dimkawork001@gmail.com

Конотопець Микола Миколайович
кандидат технічних наук, доцент, доцент кафедри кіберзахисту та безпеки спеціального зв'язку
Інститут спеціального зв'язку та захисту інформації, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: 0000-0002-6963-1877
E-mail: nikolyalux@gmail.com

Туровський Олександр Леонідович
доктор технічних наук, професор, завідувач кафедри технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0002-4961-0876
E-mail: s19641011@ukr.net

МЕТОДИКА ОЦІНКИ ВРАЗЛИВОСТЕЙ ВЕБ-СЕРВІСІВ ІЗ ВИКОРИСТАННЯМ АВТОМАТИЗОВАНИХ СКАНЕРІВ

У статті запропоновано методику комплексної оцінки вразливостей веб-сервісів, що поєднує автоматизоване сканування з ручною експертною верифікацією. Методика охоплює вісім послідовних етапів: планування, пасивну розвідку, активне мапування і фаззинг, аналіз інфраструктури та конфігурацій, динамічне тестування і перевірку бізнес-логіки, спеціалізоване тестування, фільтрацію результатів та формування рекомендацій. Розглянуто можливості SAST-, DAST-, IAST- і SCA-підходів, а також інструментів Burp Suite,

Nessus, Nuclei та спеціалізованих фаззерів. Експериментальне порівняння зі стандартним застосуванням комерційного DAST-сканера показало зростання точності виявлення з 0,26 до 0,80, збільшення кількості ідентифікованих точок входу з 18 до 64 та підтверджених критичних вразливостей з 2 до 6. Запропонований підхід зменшує частку хибнопозитивних спрацювань, підвищує повноту охоплення поверхні атаки й забезпечує обґрунтовану пріоритизацію ризиків за метриками CVSS.

Ключові слова: кібербезпека, веб-сервіси, оцінка вразливостей, автоматизовані сканери, тестування на проникнення, DAST, CVSS.

Вступ та формулювання проблеми

Стрімке зростання кількості веб-сервісів, що забезпечують надання електронних послуг, обробку персональних даних та підтримку критично важливих бізнес-процесів, суттєво підвищує вимоги до рівня їх інформаційної безпеки. Водночас сучасні веб-додатки характеризуються складною архітектурою, використанням численних фреймворків, API-інтеграцій і сторонніх компонентів, що збільшує площину атаки та ускладнює процес своєчасного виявлення вразливостей. Згідно з класифікацією найбільш поширених загроз, наведеною в матеріалах проєкту OWASP, та переліку критичних помилок безпеки OWASP Top 10, значна частина успішних атак на веб-ресурси пов’язана не зі складними експлойтами, а з типовими вразливостями: некоректним контролем доступу (Broken Access Control), криптографічними збоями та ін’єкційними вадами (зокрема, вразливістю до SQL-ін'єкцій) та міжсайтовим скриптингом (XSS) [1].Сучасні дослідження підтверджують, що імплементація рекомендацій OWASP є критично важливою для розробки безпечного програмного забезпечення та зниження ризиків експлуатації цих недоліків [2]. Це свідчить про те, що навіть за наявності світових стандартів, організації стикаються з проблемою відсутності системного підходу до регулярної та всебічної оцінки стану безпеки. Для виявлення вразливостей веб-сервісів широко застосовуються автоматизовані сканери вразливостей, зокрема OWASP ZAP, Burp Suite Professional, Acunetix (Invicti), Nessus та інші інструменти. Однак їх використання здебільшого має фрагментарний характер: результати сканування часто інтерпретуються без урахування контексту функціонування веб-сервісу, відсутні чіткі критерії пріоритизації знайдених вразливостей, а також не визначено послідовність застосування різних типів перевірок у межах єдиного процесу оцінювання.

Крім того, існує розрив між теоретичними рекомендаціями щодо тестування безпеки та практичними процедурами, які застосовуються фахівцями під час аудиту веб-ресурсів. Автоматизоване сканування нерідко розглядається як самодостатній етап перевірки, тоді як його результати потребують методично обґрунтованої обробки, верифікації та узагальнення.

Актуальною науково-прикладною проблемою є відсутність цілісної методики оцінки вразливостей веб-сервісів, що поєднувала б можливості автоматизованих сканерів із логічно впорядкованою послідовністю етапів перевірки, правилами інтерпретації результатів і підходами до визначення пріоритетності усунення виявлених недоліків безпеки. Рішення цієї проблеми дозволить підвищити ефективність процесу аудиту безпеки веб-сервісів, зменшити ймовірність пропуску критичних вразливостей та забезпечити системність у застосуванні інструментів автоматизованого аналізу. Незважаючи на високу швидкість автоматизованих засобів, вони мають обмеження у виявленні вразливостей логіки бізнес-процесів та схильні до генерації хибних результатів. Це зумовлює необхідність створення методики, яка б поєднувала автоматизовані методи з експертним аналізом для досягнення необхідного рівня валідності результатів.

Мета статті

Мета статті полягає в розробці методики комплексної оцінки вразливостей веб-сервісів, що базується на інтеграції відкритих і комерційних автоматизованих засобів сканування та методів ручного експертного аналізу для визначення послідовності етапів перевірки, інтерпретації й пріоритизації результатів, досягнення максимальної повноти виявлення вразливостей і недоліків безпеки та верифікації отриманих результатів.

Об’єктом дослідження є процес оцінювання безпеки веб-сервісів.

Предметом дослідження є методика комплексної оцінки вразливостей веб-сервісів, що базується на поєднанні можливостей автоматизованих засобів сканування та методів верифікації результатів для підвищення достовірності виявлення загроз.

Для досягнення поставленої мети необхідно виконати такі завдання:

1. Визначити місце SAST-, DAST-, IAST- і SCA-підходів у комплексному оцінюванні веб-сервісів;

2. Сформувати послідовність етапів аудиту від розвідки до ручної верифікації та звітування;

3. Визначити показники результативності методики та експериментально порівняти її зі стандартним автоматизованим скануванням.

Аналіз останніх досліджень і публікацій

Аналіз наукових праць свідчить, що теоретичне підґрунтя для оцінки захищеності веб-орієнтованих систем закладено в роботах таких закордонних та вітчизняних дослідників, як Б. Антал, М. Фелдман, О. Кузнецов, В. Саваев. Значна частина їхніх публікацій присвячена порівняльному аналізу ефективності алгоритмів виявлення вразливостей, що реалізовані у відомих DAST-системах (наприклад, Burp Suite та OWASP ZAP). Зокрема, у дослідженнях Д. Відалса акцентується увага на математичних моделях оцінки ймовірності виявлення дефектів коду за допомогою автоматизованих засобів.

Методологічні аспекти проведення аудитів безпеки та класифікації загроз детально висвітлені в стандартах та інструкціях міжнародних консорціумів OWASP (Open Web Application Security Project) та NIST (National Institute of Standards and Technology). Їхні напрацювання формують базу для розуміння векторів атак, проте вони пропонують загальні рекомендації, які часто важко адаптувати до специфічних бізнес-процесів без розробки внутрішніх корпоративних методик. Окремий напрям досліджень, представлений у працях С. Кавуна та Х. Шера, стосується інтеграції засобів аналізу безпеки в цикли швидкої розробки програмного забезпечення (DevSecOps). Автори наголошують на необхідності автоматизації, проте вказують на проблему надмірної кількості непідтверджених даних, які генеруються сканерами. Окрім класичних підходів, сучасні наукові дослідження все частіше фокусуються на порівняльному аналізі ефективності відкритих та комерційних засобів динамічного (DAST) і статичного (SAST) тестування безпеки [3]. Окремим перспективним напрямом, що активно розвивається в останні роки, є застосування методів машинного навчання для автоматизації тестування на проникнення та вибору відповідного інструментарію [4].

Попри наявність ґрунтовних праць із порівняння інструментів та опису типів вразливостей, залишається недостатньо опрацьованим питання процедурної інтеграції результатів різних засобів аналізу. Більшість публікацій фокусуються або на суто ручному тестуванні, або на автоматизованому скануванні як окремих процесах. Питання створення єдиного алгоритму, який би регламентував перехід від автоматизованого виявлення до ручної верифікації та фінальної пріоритезації ризиків, наразі висвітлено лише фрагментарно.

Саме відсутність формалізованої послідовності дій, яка б поєднувала ці підходи в межах однієї методики, визначає необхідність проведення цього дослідження.

Виклад основного матеріалу дослідження

Забезпечення захищеності сучасних веб-сервісів потребує застосування багаторівневого підходу, оскільки кожна архітектурна складова містить специфічні вектори загроз. Системний аналіз засобів оцінки безпеки дозволяє класифікувати їх за методологією аналізу та принципами взаємодії з об’єктом дослідження.

У сучасній практиці аудиту безпеки виділяють чотири ключові методологічні підходи, які охоплюють різні етапи життєвого циклу веб-сервісів:

1. SAST (Static Application Security Testing): передбачає аналіз вихідного коду або бінарних файлів без виконання програми. Метод дозволяє виявити вразливості на ранніх

етапах розробки, точно вказуючи на місце виникнення дефекту [5]. Основними обмеженнями є значна кількість хибнопозитивних спрацювань та неможливість виявлення помилок конфігурації середовища виконання;

2. DAST (Dynamic Application Security Testing): тестування працюючого застосунку шляхом імітації зовнішніх атак. Підхід ідентифікує вразливості в реальному середовищі експлуатації, перевіряє стійкість до ін'єкцій та помилок автентифікації. Ефективність методу залежить від повноти мапування веб-ресурсу;

3. IAST (Interactive Application Security Testing): гібридний підхід, що використовує програмні агенти всередині середовища виконання для моніторингу активності під час проведення динамічних тестів. Це забезпечує високу точність виявлення загроз шляхом поєднання даних про вхідні параметри з аналізом виконання коду;

4. SCA (Software Composition Analysis): метод аналізу сторонніх бібліотек і залежностей. Цей підхід є критично важливим, оскільки значну частину коду сучасних веб-сервісів складають компоненти з відкритим вихідним кодом. Метод фокусується на ідентифікації відомих вразливостей у запозичених модулях.

Ринок засобів сканування вразливостей поділяється на комерційні платформи та інструменти з відкритим вихідним кодом. Комерційні рішення характеризуються високим рівнем автоматизації, наявністю технічної підтримки та розвиненими модулями звітності. Вони пропонують власні закриті бази сигнатур та алгоритми аналізу бізнес-логіки. Використання виключно комерційних сканерів має певні недоліки, що обумовлює необхідність їх доповнення відкритими інструментами з таких причин:

- спеціалізація: відкриті інструменти часто є вузькоспеціалізованими, що дозволяє проводити глибшу перевірку окремих платформ або конкретних типів вразливостей.
- актуальність баз: шаблони для відкритих сканерів часто отримують оновлення щодо нових критичних вразливостей швидше, ніж комерційні системи.
- прозорість перевірок: відкриті засоби дозволяють аудитору повністю контролювати механіку кожного запиту, що запобігає порушенню працездатності сервісу під час тестування.

Інтеграція обох типів рішень у межах єдиної методики забезпечує синергію, де комерційні системи гарантують широке охоплення, а відкриті інструменти – глибину аналізу.

Ефективність автоматизованого сканування безпосередньо залежить від якості попереднього збору даних про об'єкт дослідження. Пропуск вразливостей часто стається через неповне визначення поверхні дослідження веб-сервісу. Пасивна розвідка дозволяє визначити межі об'єкта без прямого впливу на сервер. Використання засобів збору інформації з відкритих джерел допомагає виявити забуті піддомени, тестові середовища та технічні параметри інфраструктури. Активне мапування та фаззинг є критичними для виявлення логічної архітектури. Застосування фаззингу дозволяє ідентифікувати:

- приховані директорії та файли конфігурації;
- незадокументовані точки входу та параметри запитів;
- адміністративні інтерфейси, які не індексуються стандартними засобами навігації.

Необхідність цих попередніх етапів обґрунтована трансформацією процесу оцінки з випадкового пошуку на цілеспрямований аналіз. Завдяки попередньому збору даних сканери вразливостей отримують конкретні вектори для перевірки, що мінімізує кількість хибнопозитивних спрацювань та забезпечує повноту виявлення недоліків безпеки.

Для реалізації комплексної оцінки захищеності веб-сервісів необхідно використовувати сукупність інструментів, що спеціалізуються на різних рівнях взаємодії із цільовою системою. Сучасний інструментарій доцільно розділити на кілька функціональних груп.

До засобів пасивної розвідки належать рішення для збору інформації без прямої взаємодії з ресурсом (Shodan, BBOT, Subfinder, WhatWeb, Amass). Їх застосування дозволяє ідентифікувати технологічний стек та поверхню атаки, не залишаючи слідів у системних журналах об'єкта.

Засоби активного мапування та фаззингу (Nmap, FFUF, Gobuster, Dirsearch, httpx, Dirb) забезпечують детермінацію логічної архітектури, виявлення відкритих портів та прихованих директорій. Використання високопродуктивних фаззерів на цьому етапі є критичним для реконструкції повної файлової структури сервера.

Комплексні системи динамічного аналізу (DAST) та інфраструктурні сканери (Burp Suite Professional, Acunetix (Invicti), OWASP ZAP, Nessus, OpenVAS, Nuclei) становлять ядро автоматизованого тестування. Вони дозволяють виявляти типові вразливості прикладного та системного рівнів, включаючи помилки конфігурації та вразливі компоненти.

Для верифікації специфічних векторів атак використовуються вузькоспеціалізовані сканери (Nikto, WPScan, Wapiti, SQLMap, XSStrike) та платформи аналізу API (Postman). Це дозволяє провести глибоку перевірку окремих компонентів, таких як бази даних або системи управління контентом.

Запропонована методика базується на ітераційному підході, що передбачає синергію вищезазначених класів інструментів. Процес оцінки реалізується через вісім послідовних етапів, логічний взаємозв'язок між якими та циклічність процесу верифікації представлено на рис. 1.

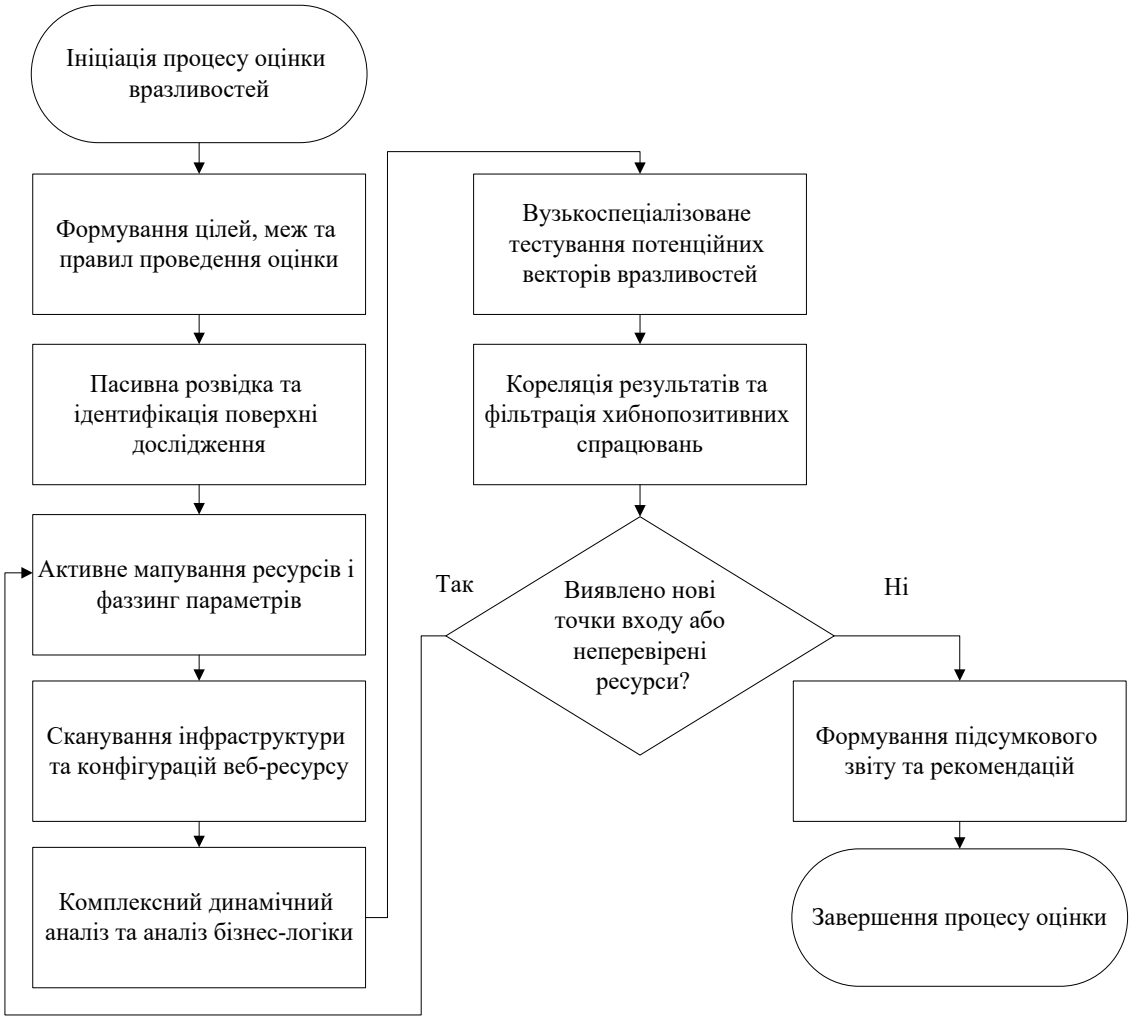

Рис. 1. Структурно-логічна схема методики комплексної оцінки вразливостей веб-сервісів

Для побудови методики було проведено формалізацію веб-сервісу як об’єкта обстеження. Веб-сервіс було представлено у вигляді множини компонентів W:

$$W = \{E, P, T, D\},$$

де $E = \{e_1, e_2, \dots, e_n\}$ – множина ідентифікованих точок входу; $P = \{p_1, p_2, \dots, p_m\}$ – множина параметрів запитів та вхідних даних; $T = \{t_1, t_2, \dots, t_k\}$ – множина технологічних компонентів стека; $D = \{d_1, d_2, \dots, d_l\}$ – множина асоційованих активів.

Процес оцінювання вразливостей було визначено як функцію M, що перетворює стан об'єкта W у множину верифікованих недоліків безпеки V:

$$M : W \xrightarrow{8\ stages} V,\ \ V = \{v_1, v_2, \dots, v_n\},$$

де M – сукупність алгоритмів та процедур методики; W – вихідна множина компонентів веб-сервісу; V – фінальна множина ідентифікованих та підтверджених вразливостей; n – загальна кількість виявлених вразливостей.

Етап 1. Планування та підготовка. Даний етап визначає вихідні параметри та обмеження процесу оцінювання. Під час його реалізації визначаються цілі, межі дозволеного сканування (scope) та правила взаємодії між сторонами. Зокрема, узгоджується перелік систем, що підлягають перевірці, збирається необхідна документація, аналізуються політики безпеки та формується детальний план тестування для мінімізації впливу на працездатність сервісів.

Етап 2. Пасивна розвідка та збір інформації. Метою етапу є агрегація даних про зовнішній периметр об'єкта без прямої активної взаємодії з його ресурсами. Використовуючи можливості інструментів Shodan та BBOT, здійснюється збір інформації про відкриті порти, банери сервісів та асоційовані мережеві активи. Ключовим завданням є пошук корпоративних адрес електронної пошти та ідентифікаторів користувачів для оцінки ризиків атак на рівні автентифікації. За допомогою Subfinder проводиться розширення поверхні атаки через виявлення піддоменів, включаючи приховані технічні ресурси. Інструмент WhatWeb застосовується для ідентифікації технологічного профілю (CMS, версії бібліотек, серверне програмне забезпечення), що дозволяє співвіднести отримані дані з відомими базами вразливостей (CVE).

Етап 3. Активне мапування та фаззинг. На цьому етапі здійснюється перехід до активного вивчення логічної архітектури веб-сервісу [7]. Використовуючи Amass, httpx та Nmap (який зарекомендував себе як комплексне рішення для всебічного дослідження мережевої інфраструктури) [5], проводиться верифікація доступності знайдених активів та мапування відкритих мережевих служб [8]. Пріоритетним завданням є ідентифікація адміністративних інтерфейсів та пошук відкритих директорій. За допомогою інтенсивного фаззингу інструментами FFUF, Gobuster, Dirsearch та Dirb реалізується пошук прихованих каталогів, конфігураційних файлів (.env, .conf), резервних копій баз даних та незадокументованих точок входу. Це дозволяє реконструювати повну файлову структуру та виявити критичні витоки інформації на рівні серверної ієрархії. Ефективність розширення поверхні дослідження (S) на етапах розвідки та мапування визначалася як сукупність ідентифікованих точок входу:

$$S = \sum_{i=1}^{n} E_i + \sum_{j=1}^{m} P_j + \sum_{k=1}^{l} D_k\ ,$$

де $E_i -$ кількість виявлених ендпоінтів та сервісів; P_j – кількість унікальних параметрів запитів та точок вводу даних; D_k – кількість ідентифікованих прихованих директорій та об'єктів.

Етап 4. Сканування інфраструктури та конфігурацій. Етап спрямований на детермінацію вразливостей системного рівня та помилок адміністрування серверного оточення. Професійні системи Nessus та OpenVAS (Greenbone) проводять аналіз на наявність критичних недоліків у налаштуваннях операційних систем, веб-серверів та супутніх служб. За допомогою Nuclei здійснюється цілеспрямований пошук специфічних помилок конфігурування за допомогою актуальних шаблонів, що дозволяє виявити слабкі місця в налаштуваннях SSL/TLS, небезпечні HTTP-методи та вразливі JavaScript-бібліотеки.

Етап 5. Комплексний динамічний аналіз та аналіз бізнес-логіки. Даний етап передбачає глибоке поведінкове тестування застосунку в режимі реального часу за допомогою систем

© Сторчак А.С., Печенюк Д.І., Конотопець М.М., Туровський О.Л. Методика оцінки вразливостей веб-сервісів із використанням автоматизованих сканерів. Сучасний захист інформації, 3(67), 163–172. https://doi.org/10.31673/2409-7292.2026.032815

Burp Suite Professional, Acunetix (Invicti), OWASP ZAP [9]. Основна увага зосереджена на аналізі точок входу: від форм реєстрації до API-інтерфейсів. Проводиться автоматизоване тестування на вразливості класів Injection, Broken Access Control та сесійної безпеки. Досліджується стійкість бізнес-логіки до маніпуляцій, що дозволяє виявити дефекти, які неможливо ідентифікувати шляхом сигнатурного аналізу.

Етап 6. Вузькоспеціалізоване тестування та експлуатація вразливостей. Після ідентифікації потенційних векторів проводиться їхня верифікація за допомогою спеціалізованого інструментарію. SQLMap використовується для автоматизації виявлення та експлуатації ін'єкцій у бази даних, тоді як XSStrike забезпечує аналіз вразливостей типу Cross-Site Scripting (XSS). Для тестування безпеки програмних інтерфейсів використовується Postman, а для специфічних середовищ – WPScan. Інструмент Wapiti застосовується для аудиту форм та параметрів запитів, що забезпечує додатковий рівень перевірки результатів попередніх етапів.

Етап 7. Аналіз результатів та оцінка рівня критичності. Отримані дані було піддано ретельному аналізу для елімінації хибнопозитивних спрацювань (False Positives). Здійснювалася кореляція даних між різними класами сканерів для верифікації наявності вразливостей. Кожна виявлена вразливість оцінювалася за метриками CVSS v3.1, що дозволило об'єктивно визначити рівень ризику (Low, Medium, High, Critical) з урахуванням складності експлуатації та потенційного впливу на конфіденційність, цілісність і доступність даних. Для кількісного оцінювання загального стану захищеності веб-сервісу було введено інтегральний показник ризику (R_{score}), який розраховувався як зважена сума показників критичності всіх верифікованих вразливостей:

$$R_{score} = \sum_{i=1}^{V_{true}} (w_i \cdot CVSS_i) ,$$

де V_{true} – кількість верифікованих вразливостей; $CVSS_i$ – числовий показник критичності i-ї вразливості; w_i – ваговий коефіцієнт впливу на бізнес-логіку (приймався рівним 1.0 для загальних компонентів та 1.2 для критичних модулів).

На основі отриманого показника ризику визначалася цільова функція ефективності методики ($f(M)$). Даний показник відображає якість ідентифікації загроз відносно витрачених часових ресурсів та отриманої похибки:

$$f(M) = \frac{R_{score}}{T \cdot (V_{false}+1)} \rightarrow max ,$$

де T – сумарний час проведення оцінювання; $V_{false}-$ кількість ідентифікованих хибнопозитивних результатів.

Додавання одиниці у знаменнику використано як регуляризуючий коефіцієнт для запобігання діленню на нуль у випадку повної відсутності хибнопозитивних спрацювань

Етап 8. Формування звіту та розробка рекомендацій. На завершальному етапі всі виявлені технічні недоліки та результати тестування консолідуються в підсумковий звіт. Документ поєднує в собі оцінку бізнес-ризиків для керівництва компанії та містить детальні технічні рекомендації для розробників щодо ефективного усунення знайдених вразливостей. Системна реалізація всіх етапів методики забезпечує перехід від фрагментарного сканування до цілісного управління рівнем захищеності веб-сервісів.

З метою оцінювання ефективності запропонованої методики було проведено експериментальне дослідження на спеціалізованому тестовому веб-сервісі, що містить інтегровані вразливості різних класів. На першому етапі було виконано стандартне сканування комерційним сканером Acunetix (Invicti) без застосування методики. На другому етапі було застосовано запропоновану методику.

Як свідчать отримані результати, стандартне використання комерційних DAST-інструментів дозволяє оперативно провести первинне сканування, проте характеризується

низькою точністю (Precision 0,26) та обмеженою глибиною мапування об’єкта (18 точок входу).

Таблиця 1

Порівняльна характеристика результатів оцінювання захищеності веб-сервісу

Показник (Метрика)	**Стандартне сканування**	**За запропонованою методикою**	**Різниця/ефективність**
Загальна кількість виявлених вразливостей	35	51	+45,7%
Підтверджені вразливості (True Positives)	9	41	+356,6%
Хибнопозитивні спрацювання (False Positives)	26	10	-61,5%
Точність виявлення (Precision)	0,26	0,80	+207,7%
Виявлені точки входу (Endpoints/Parameters)	18	64	+255,6%
Підтверджені критичні вразливості (High/Critical)	2	6	+200%
Час аналізу (загальний), год	2,5	6,0	+140,0%
Ефективність виявлення $f(M)$ на одиницю часу	3,6 вразливостей/год	6,83 вразливостей/год	+89,7%

Застосування запропонованої методики дозволило досягти таких результатів:

1. Зростання достовірності – показник точності (Precision) зріс із 0,26 до 0,80 (+207,7%), що підтверджує ефективність процедур фільтрації та ручної верифікації;
2. Максимізація охоплення – завдяки етапам активного фаззингу та мапування, кількість ідентифікованих векторів атаки (точок входу) зросла в 3,5 раза (з 18 до 64);
3. Виявлення критичних загроз – кількість верифікованих критичних вразливостей збільшилася з 2 до 6, що свідчить про спроможність методики до аналізу складної бізнес-логіки;
4. Оптимізація часу на верифікацію — при зростанні загального часу аналізу на 140%, кількість підтверджених критичних загроз збільшилася на 200%, що забезпечило вищу ефективність виявлення вразливостей (True Positives) на одиницю часу роботи;
5. Підвищення якості ідентифікації прихованих активів – впровадження багаторівневого алгоритму дозволило виявити на 180% більше прихованих директорій та адміністративних інтерфейсів, які при стандартному скануванні залишалися недоступними для ідентифікації.

Результати проведеного дослідження свідчать, що використання комерційних DAST-інструментів без застосування цілісної методології призводить до фрагментарної оцінки рівня захищеності інформаційної системи. Значний відсоток хибнопозитивних результатів знижує ефективність процесу аудиту, вимагаючи від фахівців додаткових часових витрат на верифікацію неактуальних даних. Запропонований ітераційний підхід вирішує цю проблему шляхом інтеграції процедур фільтрації, що дозволяє зосередити ресурси на аналізі реальних векторів загроз. Реалізація процедур мапування та фаззингу посприяла виявленню прихованих компонентів архітектури веб-сервісу, що забезпечило виявлення вразливостей, які неможливо було б ідентифікувати за допомогою базового налаштування автоматизованих сканерів. Порівняльний аналіз підтверджує, що додаткові витрати часу на ручну верифікацію є виправданими, оскільки це забезпечує вищу достовірність результатів та дозволяє виявити дефекти бізнес-логіки, що мають найвищий рівень ризику для функціонування об’єкта дослідження.

Застосування цієї методики сприяє системному управлінню вразливостями та забезпечує основу для своєчасного впровадження превентивних заходів захисту, що є необхідною

© Сторчак А.С., Печенюк Д.І., Конотопець М.М., Туровський О.Л. Методика оцінки вразливостей веб-сервісів із використанням автоматизованих сканерів. Сучасний захист інформації, 3(67), 163–172. https://doi.org/10.31673/2409-7292.2026.032815

умовою для забезпечення сталого функціонування критично важливих веб-сервісів в умовах постійного зростання кіберзагроз.

Висновки

Запропоновано нову методику комплексної оцінки вразливостей веб-сервісів базується на ітераційному підході та синергії різних класів засобів автоматизованого аналізу та методів ручної перевірки. Методика включає в себе вісім взаємопов'язаних етапів, які відповідають логічній послідовності проведення повноцінного аудиту безпеки, а саме: планування та підготовка, пасивна розвідка та збір інформації, активне мапування та фаззинг, сканування інфраструктури та конфігурацій, комплексний динамічний аналіз та аналіз бізнес-логіки, вузькоспеціалізоване тестування та експлуатація вразливостей, аналіз результатів та фільтрація хибних спрацювань, а також формування звіту та розробка технічних рекомендацій щодо усунення виявлених недоліків.

На відміну від існуючих підходів, запропонована методика завдяки коректній постановці завдання на дослідження, використанню багаторівневої структури аналізу, ієрархії та деталізації процесів перевірки, здатна забезпечити максимальну повноту охоплення поверхні атак. Сутність методики полягає у модифікуванні стандартних процедур сканування шляхом інтеграції можливостей відкритих і комерційних автоматизованих засобів із методами ручного аналізу на етапах верифікації. Це дозволяє враховувати особливості архітектури сучасних веб-ресурсів, систематизувати процес виявлення дефектів безпеки та забезпечити перехід від фрагментарного використання інструментів до цілісного моніторингу стану захищеності. Застосування ітераційного підходу дозволяє не лише ідентифікувати технічні вразливості, а й оцінювати стійкість бізнес-логіки веб-сервісів до маніпуляцій, що суттєво підвищує точність прийняття рішень щодо рівня критичності ризиків.

Завдяки використанню процедур фільтрації даних та пріоритизації результатів за метриками CVSS, розроблена методика дозволяє мінімізувати кількість хибнопозитивних спрацювань, підвищити швидкість ідентифікації точок входу та забезпечити високу достовірність отриманих результатів. Це дозволяє формувати обґрунтовані рекомендації для розробників та адміністраторів систем, що сприяє оперативному усуненню критичних прогалин у захисті.

Загалом, з огляду на запропоновану нову методику, можна зазначити, що мета статті, яка полягала в розробці методики комплексної оцінки вразливостей веб-сервісів на основі інтеграції відкритих і комерційних автоматизованих засобів сканування та методів ручного експертного аналізу для визначення послідовності етапів перевірки, інтерпретації й пріоритизації результатів, досягнення максимальної повноти виявлення вразливостей і недоліків безпеки та верифікації отриманих результатів, повністю досягнута.

Подальші дослідження будуть спрямовані на вдосконалення алгоритмів автоматизованої верифікації логічних вразливостей прикладного рівня, розвиток методів аналізу безпеки програмних інтерфейсів та розробку нових комплексних підходів до забезпечення безпеки веб-ресурсів у динамічних середовищах.

Перелік посилань

1. Андрусяк І., Севериненко Д. Методи та засоби моніторингу функціонування веб-сервісів. Herald of Khmelnytskyi National University. Technical sciences. 2025. № 347(1). С. 11-19.

2. Методи та моделі проєктування системи автоматизованого пошуку вразливостей у web-додатках / Івануса А. І. та ін. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 110–122.

3. Семенець О., Тецький А. Аналіз методів та засобів вибору та комплексування сканерів вразливостей для тестування на проникнення інтернет систем. Measuring and computing devices in technological processes. 2024. № 2. С. 336-347.

4. Максимович М. В. Використання методів штучного інтелекту для виявлення вразливостей нульового дня. Сучасний захист інформації. 2025. № 4. С. 123-132.

5. Alhamed M., Rahman M. H. A systematic literature review on penetration testing in networks: future research directions. Applied Sciences. 2023. Vol. 13, № 12. 6986.

6. Morhul D. M., Nariezhnii O. P., Hrinenko T. O. Модель порушника та модель загроз для веб-сервісу QRNG. Radiotekhnika. 2025. № 221. С. 31-38.

© Сторчак А.С., Печенюк Д.І., Конотопець М.М., Туровський О.Л. Методика оцінки вразливостей веб-сервісів із використанням автоматизованих сканерів. Сучасний захист інформації, 3(67), 163–172. https://doi.org/10.31673/2409-7292.2026.032815

7. Design and development of a large language model-based tool for vulnerability detection / Zhuravchak A. et al. Eastern-European Journal of Enterprise Technologies. 2025. Vol. 2, № 2 (134). С. 75-83.

8. Експрес-аудит як інструмент оцінки вразливостей в системах обробки даних: підходи, методики та рекомендації / Сиропятов О. А. та ін. Informatics & Mathematical Methods in Simulation. 2024. Vol. 14, № 4.

9. SQLI-ScanEval: A framework for design and evaluation of SQLI detection using vulnerability and penetration testing scanners / Bashir H. et al. Engineering Reports. 2026. Vol. 8, № 1.

Anton Storchak
Candidate of Technical Sciences, Associate Professor
Institute of Special Communications and Information Protection
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
ORCID: 0000-0002-5267-3122
E-mail: storchakanton@gmail.com

Dmytro Pecheniuk
Master’s student
Institute of Special Communications and Information Protection
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
ORCID: 0009-0001-1980-1583
E-mail: dimkawork001@gmail.com

Mykola Konotopets
Candidate of Technical Sciences, Associate Professor
Institute of Special Communications and Information Protection
National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
ORCID: 0000-0002-6963-1877
E-mail: nikolyalux@gmail.com

Oleksandr Turovsky
Doctor of Technical Sciences, Professor, Head of the Department of Technical Systems of Cyber Defense
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0002-4961-0876
E-mail: s19641011@ukr.net

METHODOLOGY FOR ASSESSING WEB-SERVICE VULNERABILITIES USING AUTOMATED SCANNERS

The article proposes a comprehensive methodology for assessing web-service vulnerabilities that combines automated scanning with manual expert verification. The methodology comprises eight consecutive stages: planning, passive reconnaissance, active mapping and fuzzing, infrastructure and configuration analysis, dynamic testing and business-logic assessment, specialized testing, result filtering, and reporting. The capabilities of SAST, DAST, IAST, and SCA approaches, as well as Burp Suite, Nessus, Nuclei, and specialized fuzzers, are considered. Experimental comparison with conventional use of a commercial DAST scanner demonstrated an increase in detection precision from 0.26 to 0.80, growth in identified entry points from 18 to 64, and an increase in confirmed critical vulnerabilities from 2 to 6. The proposed approach reduces false positives, broadens attack-surface coverage, and supports risk prioritization using CVSS metrics.

Keywords: cybersecurity, web services, vulnerability assessment, automated scanners, penetration testing, DAST, CVSS.

Надійшла до редакції (Received): 14.08.2026
Прийнята до друку (Accepted): 08.09.2026
Опубліковано онлайн (Available online): 15.09.2026

© Сторчак А.С., Печенюк Д.І., Конотопець М.М., Туровський О.Л. Методика оцінки вразливостей веб-сервісів із використанням автоматизованих сканерів. Сучасний захист інформації, 3(67), 163–172. https://doi.org/10.31673/2409-7292.2026.032815