КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.668
УДК 004.8

Толкачова Анастасія Юріївна
аспірант, асистент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8196-7963
anastasiia.y.tolkachova@lpnu.ua

Піскозуб Андріян Збігнєвич
кандидат технічних наук, доцент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-3582-2835
andriian.z.piskozub@lpnu.ua

МЕТОДИ ДЛЯ ТЕСТУВАННЯ БЕЗПЕКИ ВЕБ-ЗАСТОСУНКІВ

Анотація. Тестування на проникнення є ключовим методом динамічної оцінки захищеності комп'ютерних мереж, інфраструктури, веб- та мобільних додатків, спрямованим на виявлення й експлуатацію вразливостей шляхом імітації ймовірних атак з боку зловмисників. Традиційно цей процес проводиться вручну, що вимагає високої кваліфікації фахівців з кібербезпеки та значного часу для підготовки, реалізації атак, аналізу результатів і формування звітів. Однак, із зростанням складності та кількості кіберзагроз виникла необхідність в автоматизованих інструментах, здатних пришвидшити процес тестування, підвищуючи при цьому його ефективність і точність. У статті здійснено огляд сучасних інструментів для тестування на проникнення, зокрема тих, що використовують методи штучного інтелекту (ШІ) для покращення виявлення вразливостей та оптимізації роботи пентестерів. Проаналізовано ряд популярних комерційних рішень, включаючи RidgeBot, vPenTest, Metasploit Pro, BreachLock PTaaS, Edgescan, Burp Suite Professional, AppCheck, NetSPI, Astra та Pentest-Tools.com. Для кожного інструменту розглянуто його основні можливості, платформи, на яких він здійснює тестування, основні типи вразливостей, які він здатний виявляти (такі як SQL-ін'єкції, XSS, CSRF, RCE та інші), а також специфічні технічні деталі реалізації. Також досліджено питання цінової політики для комерційних платформ, що дозволяє оцінити доцільність їх застосування залежно від потреб і специфіки підприємства. У статті підкреслюється важливість розвитку національних рішень для тестування на проникнення, зокрема в Україні, де інструмент такого рівня може відіграти важливу роль в забезпеченні інформаційної безпеки та зниженні ризиків витоку даних. Створення українських рішень також сприятиме збереженню коштів усередині країни, підтримуючи національну економіку і створюючи нові робочі місця для спеціалістів. З огляду на підвищений рівень кіберзагроз, розвиток таких інструментів є актуальним завданням для посилення кібербезпеки як приватного сектору, так і державних установ.

Ключові слова: безпека; тестування; вразливості; штучний інтелект; OWASP; BurpSuite; API; моделювання загроз.

ВСТУП

Тестування на проникнення — це підхід до динамічної оцінки захищеності комп'ютерної мережі, інфраструктури, веб-застосунку або мобільного застосунку шляхом підготовки та виконання кожної ймовірної атаки з метою виявлення та використання наявних вразливостей. Традиційно тестування проводиться вручну, де спеціалісти спочатку повинні дослідити цільову систему, а потім використати знайдені вразливості різними методами для проникнення в систему і компрометації мережевих ресурсів [1]. Цей процес вимагає відповідної підготовки людей, а також відповідного

проміжку часу для проведення оцінки, написання звіту тощо. Тому останнім часом автоматизовані моделі для тестування розробляються з використанням методів штучного інтелекту (ШІ). Ця стаття зосереджена на стислому огляді сучасних інструментів для проведення тестування на проникнення. Огляд зроблено для того, щоб дослідити значення методів штучного інтелекту для покращення тестування та виявлення вразливостей системи. Розглянуто існуючі методи, визначено їх важливість та інші характеристики.

Постановка проблеми. За останні роки штучний інтелект дав поштовх для створення нових інструментів тестування із використанням машинного навчання. Однак, веб-застосунки залишаються вразливими до різноманітних атак. Необхідно дослідити сучасні підходи тестування безпеки, щоб забезпечити ефективний захист і вчасне виявлення загроз.

Аналіз останніх досліджень і публікацій. У цій статті розглядаємо різноманітні інструменти для тестування, а також їхні методології.

В роботі [2] наведено результати досліджень, присвячених процесу тестування на проникнення та застосовуваним інструментам. Показано, що належна організація тестування на проникнення сприяє покращенню інформаційної безпеки організацій. Це дозволяє виявити та усунути вразливості, що можуть стати потенційними точками для атак. Але залишилися невирішеними питання, пов’язані з обмеженими ресурсами та високими вимогами до кваліфікації фахівців, які ускладнюють регулярне проведення такого тестування. Причиною цього можуть бути об’єктивні труднощі, пов’язані з витратами на інструменти, а також постійна необхідність оновлювати методики відповідно до нових загроз. Це робить регулярне тестування складним завданням. Варіантом подолання відповідних труднощів може бути автоматизація деяких етапів тестування на основі сучасних технологій.

В роботі [3] наведено результати досліджень, присвячених автономному аналізу безпеки та тестуванню на проникнення. Показано, що використання методів підкріплювального навчання, зокрема Deep-Q Network (DQN), для побудови графів атак дозволяє значно підвищити ефективність виявлення вразливостей у хмарних мережах та системах Інтернету речей (IoT). Але залишилися невирішеними питання, пов’язані з обчислювальною складністю та ресурсними обмеженнями, що виникають при аналізі великих і динамічних мереж. Причиною цього можуть бути високі вимоги до обчислювальної потужності та складність налаштування моделі для роботи в умовах реального часу, що робить впровадження таких рішень обмеженим. Варіантом подолання відповідних труднощів може бути оптимізація алгоритмів або застосування гібридних моделей, що поєднують переваги автоматизованого аналізу та гнучкість ручного налаштування.

В роботі [4] наведено результати всебічного огляду літератури, присвяченого тестуванню на проникнення та його застосуванню у сфері безпеки мереж. Показано, що тестування на проникнення є важливим інструментом для захисту від атак на мережу, таких як атаки типу відмова в обслуговуванні (DoS) та вторгнення в мережу, особливо на платформах Microsoft Windows і Linux. Але залишилися невирішеними питання, пов’язані з обмеженнями сучасних інструментів для виявлення складних і багатоступеневих атак. Причиною цього можуть бути труднощі з масштабуванням тестів на великі корпоративні мережі та обмежена сумісність між платформами. Варіантом подолання відповідних труднощів може бути створення гнучких багатофункціональних платформ для тестування, що підтримують інтеграцію з різними операційними системами.

Мета статті полягає в тому, щоб проаналізувати та порівняти сучасні підходи до тестування безпеки веб-додатків. Стаття спрямована на огляд сучасних інструментів і методів, таких як ручне та автоматизоване тестування, а також розглядає новітні технології, включаючи машинне навчання та AI для виявлення вразливостей.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Інструменти тестування на проникнення допомагають виявити та усунути проблеми з безпекою. Було відібрано 10 найпопулярніших комерційних рішень за статистикою веб-сайту Gartner [5]. Необхідно зауважити, що інструменти не розкривають всіх своїх переваг публічно. Тому було використано наявну інформацію на їхніх сайтах візитках.

RidgeBot включає автоматизоване тестування на проникнення, менеджмент вразливостей, управління інфраструктурою. RidgeBot дозволяє мінімізувати ризики шляхом перевірки засобів контролю та процесів. Також забезпечує управління вразливостями шляхом автоматичного тестування. Цей інструмент використовує методи машинного навчання. Був створений у США [6].

vPenTest підтримує тестування веб-додатків та мережевої інфраструктури. Забезпечує швидке тестування через попередньо налаштовані шаблони й автоматизовані сценарії. Однак, платформа обмежена для більш гнучких і складних налаштувань, які можуть бути потрібні для великих або багатокомпонентних середовищ. Був створений у США [7].

Metasploit Pro дозволяє автоматизувати сканування, експлуатацію вразливостей та звітування, що значно скорочує час на тестування безпеки. Він підтримує додаткові функції, як-от соціальна інженерія та фішинг-кампанії, для комплексного тестування безпеки. Інструмент інтегрується в DevSecOps-процеси, полегшуючи постійний моніторинг і захист корпоративних середовищ. Був створений у США [7].

BreachLock PTaaS (Penetration Testing as a Service) — це хмарна платформа для автоматизованого тестування на проникнення, яка надає послуги як для веб-додатків, так і для API, хмарних сервісів і DevSecOps-середовищ. Вона забезпечує постійний моніторинг і оновлення в реальному часі. Був створений у США [8].

Edgescan платформа для управління вразливостями, яка поєднує автоматизоване сканування з ручною валідацією результатів. Вона підтримує тестування веб-додатків, мереж, API, хмарних середовищ і контейнерів. Платформа пропонує постійний моніторинг з оновленнями в реальному часі та інтеграцією в DevSecOps. Був створений в Ірландії [9].

Burp Suite Professional — це потужний інструмент для тестування безпеки веб-додатків, що надає можливості як для ручного, так і для автоматизованого сканування вразливостей. Він виявляє широкий спектр вразливостей. Burp Suite Professional включає інструменти, як-от Intruder для автоматизованого фаззингу, Repeater для детального тестування запитів, та Scanner для динамічного аналізу безпеки. Був створений у Англії [10].

AppCheck — це автоматизована платформа для сканування вразливостей веб-додатків, серверів і локальних мереж. AppCheck також пропонує регулярне сканування та інтеграцію з CI/CD для постійного моніторингу, що робить її ефективною для забезпечення безпеки веб-додатків і мереж. Був створений у Великій Британії [11].

NetSPI Penetration Testing Services — це комплексні послуги з тестування на проникнення, орієнтовані на корпоративні середовища, включаючи веб-додатки, мережеві пристрої, хмарні сервіси та складні багатофакторні середовища. NetSPI

пропонує індивідуальні звіти, що включають аналіз загроз, виявлення вразливостей та рекомендації з усунення. Платформа інтегрується з корпоративними системами для підтримки безпеки в реальному часі й може виконувати регулярне тестування завдяки хмарному доступу. Був створений у США [12].

Astra — це зручна платформа для тестування веб-додатків, API та CMS (наприклад, WordPress), орієнтована на забезпечення регулярного моніторингу безпеки. Вона виявляє стандартні вразливості, такі як SQL-ін'єкції, XSS, ін'єкції у файли, а також перевіряє права доступу та використання вразливих бібліотек. Astra інтегрується в CI/CD, дозволяючи проводити постійне сканування та отримувати звіти в реальному часі, що робить її придатною для малого та середнього бізнесу, який прагне постійного захисту своїх веб-ресурсів. Був створений в Індії [13].

Pentest-Tools.com платформа для тестування безпеки веб-додатків, внутрішніх мереж, серверів, хмарних сервісів і API. Вона пропонує широкий набір інструментів для різних типів тестування. Був створений в Румунії [14].

На табл. 1 наведено порівняння можливостей цих інструментів. Треба зауважити, що тут не було порівняно їхніх недоліків. Оскільки це лідери ринку і вони виконують свої задачі під кожний бізнес. Деякі з них мають загальні характеристики для всіх можливих видів тестування. Інші, такі як Burp Suite Professional спеціалізуються виключно на тестуванні веб застосунків та перевіряють усі можливі вразливості пов'язані з OWASP методологією. Також, треба підсумувати, що у всьому списку лідерів нема жодного інструменту, який був би створений в Україні. Це є важливим питанням, оскільки такий інструмент могла б використовувати наша держава у боротьбі з противником на фронті. Створення подібного інструменту дозволило б залишити гроші в середині нашої країни, а також створити робочі місця для спеціалістів. Окрім того, це б зменшило ризики витоку інформації, оскільки всі дані були б у руках спеціалістів з України.

Таблиця 1

Порівняння можливостей платформ для автоматизованого тестування

Інструмент	Платформи, що тестуються	Вразливості, що перевіряються	Технічні деталі
RidgeBot	Веб-сервери, додатки, мережеві пристрої, бази даних	SQL-ін'єкції, XSS, слабкі паролі, неправильні конфігурації серверів, вразливі API	Автоматизоване сканування на основі ботів, тестування Active Directory
vPenTest	Веб-додатки, внутрішні мережеві інфраструктури	Поширені веб-вразливості (OWASP Top 10), конфігурації серверів, відкриті порти	Вбудовані сканери, попередньо налаштовані шаблони для швидкого тестування
Metasploit Pro	Локальні/віддалені сервери, веб-додатки, хмарні середовища, мережеві пристрої	SQL-ін'єкції, віддалене виконання коду, перебір паролів, XSS, CSRF, DoS	2000+ готових експлойтів, розробка експлойтів на замовлення, інтеграція з Nmap
BreachLock PTaaS	Веб-додатки, API, хмарні сервіси, платформи DevSecOps	OWASP Top 10, конфігурації доступу, політики безпеки (наприклад, ACL), хмарні конфігурації	Хмарна платформа, доступ до звітів у режимі реального часу, автоматизоване тестування
Edgescan	Веб-додатки, мережева інфраструктура, хмара, контейнери, API	RCE, SQL-ін'єкції, проблеми з контролем доступу, неправильні конфігурації	Автоматизоване сканування з ручною перевіркою, API та порталом моніторингу

Burp Suite Professional	Веб-додатки, API	SQL-ін’єкції, XSS, CSRF, проблеми з автентифікацією, конфігурації серверів	Вбудовані модулі для ручного та автоматизованого тестування (Intruder, Repeater)
AppCheck	Веб-додатки, сервери, локальні мережі	XSS, SQL-ін’єкції, RCE, проблеми з правами доступу до файлів	Автоматизоване сканування, інтеграція CI/CD для регулярного моніторингу
NetSPI Penetration Testing Services	Веб-додатки, мережеві пристрої, хмарні сервіси, складні середовища	Стандартні вразливості, багатоетапні атаки, незахищені API, недоліки бізнес-логіки	Звіти, ручне тестування під керівництвом експертів, корпоративна інтеграція
Astra	Веб-додатки, API, CMS-системи (наприклад, WordPress)	OWASP Топ 10, XSS, SQL ін’єкції, файлові ін'єкції, вразливі бібліотеки	Проста у використанні платформа, регулярне сканування вразливостей, інтеграція CI/CD
Pentest-Tools.com	Веб-додатки, внутрішні мережі, сервери, хмарні сервіси, API	SQL-ін’єкції, XSS, проблеми з автентифікацією, неправильні конфігурації серверів, незахищені протоколи	Інтуїтивно зрозумілий інтерфейс, готові шаблони, детальна звітність

Наступним важливим пунктом для розгляду є фінанси. Всі ці інструменти є комерційними лідерами. У табл. 2 наведена уся доступна інформація про ціноутворення цих інструментів на 2024 рік з прив’язкою до долара по курсу приблизно 42 грн.

Таблиця 2

Цінова політика комерційних інструментів на 2024 рік

Назва інструменту	Ціна
RidgeBot	Індивідуальне ціноутворення (типово для підприємств)
vPenTest	Близько 199 доларів на місяць для базових тарифних планів
Metasploit	$2,000+ на рік
BreachLock PTaaS	Від $200/місяць
Edgescan	Індивідуальне ціноутворення, залежно від обсягу
Burp Suite Professional	$449/рік за користувача
AppCheck	Близько 2 100 доларів на рік
NetSPI Penetration Testing Services	Індивідуальне ціноутворення (проектне, корпоративне)
Astra	$199/міс
Pentest-Tools.com	$66/місяць для базових тарифних планів

Такі інструменти, як RidgeBot, Edgescan і NetSPI, надають індивідуальні ціни, які часто підходять для великих або дуже специфічних корпоративних додатків. Astra, vPenTest і Pentest-Tools.com пропонують варіанти підписки, що робить їх більш гнучкими для невеликих компаній або команд. Burp Suite Professional і Metasploit Pro мають річні ліцензії, що робить їх кращим вибором для постійного внутрішнього тестування. Отже, популярні платні інструменти для автоматизації пентесту мають різні специфіки та різні політики ціноутворення. З відомої нам інформації лише один з них використовує штучний інтелект для автоматизації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Тестування на проникнення залишається критично важливим елементом у забезпеченні кібербезпеки сучасних інформаційних систем, оскільки дозволяє ідентифікувати та усувати вразливості до того, як ними можуть скористатися зловмисники. Огляд інструментів для автоматизованого тестування на проникнення, проведений у цій статті, показав, що сучасні комерційні рішення здатні значно спростити та пришвидшити процес виявлення ризиків, а також забезпечують високу ефективність завдяки впровадженню штучного інтелекту і машинного навчання. Проте залишається ряд викликів, таких як висока вартість програмного забезпечення, необхідність його регулярного оновлення та забезпечення сумісності з різноманітними платформами та середовищами. Подальші дослідження у цій сфері можуть бути спрямовані на розробку національних рішень для тестування на проникнення, які відповідатимуть специфічним потребам українських підприємств та державних установ. Важливо також приділити увагу питанням зниження вартості таких інструментів, можливостям їхньої інтеграції з різними системами безпеки та адаптації до новітніх загроз. Окрім того, перспективним напрямом є вдосконалення технологій автоматизованого виявлення складних і багатоступеневих атак, а також розвиток методів для інтеграції цих інструментів у процеси DevSecOps, що дозволить посилити інформаційну безпеку та оперативно реагувати на нові загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Піскозуб, А., Журавчак, Д., & Толкачова, А. (2023). Дослідження вразливостей у чатботах з використанням великих мовних моделей. *Ukrainian Scientific Journal of Information Security, 29(3),* 111–117. https://doi.org/10.18372/2225-5036.29.18069
2. Shebli, H. M. Z. A., & Beheshti, B. D. (2018). A study on penetration testing process and tools. У *2018 IEEE long island systems, applications and technology conference (LISAT). IEEE.* https://doi.org/10.1109/lisat.2018.8378035
3. Chowdhary, A., Huang, D., Mahendran, J. S., Romo, D., Deng, Y., & Sabur, A. (2020). Autonomous security analysis and penetration testing. У *2020 16th international conference on mobility, sensing and networking (MSN). IEEE.* https://doi.org/10.1109/msn50589.2020.00086
4. Vats, P., Mandot, M., & Gosain, A. (2020). A comprehensive literature review of penetration testing & its applications. У *2020 8th international conference on reliability, infocom technologies and optimization (trends and future directions) (ICRITO). IEEE.* https://doi.org/10.1109/icrito48877.2020.9197961
5. *Products in penetration testing tools category.* (б. д.). https://www.gartner.com/reviews/market/penetration-testing-tools
6. *Automated penetration testing tool | ridgebot | ridge security.* (б. д.). Ridge Security. https://ridgesecurity.ai/products/
7. *Network penetration testing platform | vpentest.* (б. д.). Vonahi Security: Automated Penetration Testing & Cyber Security Services. https://www.vonahi.io/services/network-penetration-testing
8. *Metasploit | penetration testing software, pen testing security | metasploit.* (б. д.). Metasploit. https://www.metasploit.com/
9. *PTaaS - BreachLock.* (б. д.). BreachLock. https://www.breachlock.com/products/ptaas/
10. *Home.* (б. д.). Edgescan. https://www.edgescan.com/
11. *Burp suite professional.* (б. д.). Web Application Security, Testing, & Scanning - PortSwigger. https://portswigger.net/burp/pro
12. *AppCheck | A complete enterprise security testing solution.* (б. д.) https://appcheck-ng.com/
13. *NetSPI penetration testing as a service (ptaas).* (б. д.). https://www.netspi.com/netspi-ptaas/
14. *Astra Pentest.* (б. д.). https://www.getastra.com/pentest
15. *Penetration testing toolkit, ready to use.* (б. д.). Pentest-Tools.com. https://pentest-tools.com/
16. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Anastasiia Tolkachova
Academic degree, Academic title, Position
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8196-7963
anastasiia.y.tolkachova@lpnu.ua

Andriian Piskozub
Academic degree, Academic title, Position
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-3582-2835
andriian.z.piskozub@lpnu.ua

METHODS FOR TESTING THE SECURITY OF WEB APPLICATIONS

Abstract. Penetration testing is a key method of dynamic security assessment of computer networks, infrastructure, web and mobile applications aimed at identifying and exploiting vulnerabilities by simulating possible attacks by intruders. Traditionally, this process is carried out manually, requiring highly skilled cybersecurity professionals and considerable time to prepare, execute attacks, analyse the results and generate reports. However, with the growing complexity and number of cyber threats, there is a need for automated tools that can speed up the testing process while increasing its efficiency and accuracy. This article provides an overview of modern penetration testing tools, in particular those that use artificial intelligence (AI) methods to improve vulnerability detection and optimise pentesters' performance. A number of popular commercial solutions are analysed, including RidgeBot, vPenTest, Metasploit Pro, BreachLock PTaaS, Edgescan, Burp Suite Professional, AppCheck, NetSPI, Astra, and Pentest-Tools.com. For each tool, we consider its main capabilities, the platforms it tests on, the main types of vulnerabilities it can detect (such as SQL injection, XSS, CSRF, RCE, etc.), as well as specific technical details of implementation. The article also examines the pricing policy for commercial platforms, which allows assessing the feasibility of their use depending on the needs and specifics of the enterprise. The article emphasises the importance of developing national solutions for penetration testing, in particular in Ukraine, where a tool of this level can play an important role in ensuring information security and reducing the risk of data leakage. The creation of Ukrainian solutions will also help to keep money in the country, supporting the national economy and creating new jobs for specialists. Given the increased level of cyber threats, the development of such tools is an urgent task to strengthen cybersecurity in both the private sector and public institutions.

Keywords: security; testing; vulnerabilities; artificial intelligence; OWASP; BurpSuite; API; threat modelling.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Piskozub, A., Zhuravchak, D., & Tolkacheva, A. (2023). Research of vulnerabilities in chatbots using large language models. *Ukrainian Scientific Journal of Information Security, 29(3),* 111–117. https://doi.org/10.18372/2225-5036.29.18069
2. Shebli, H. M. Z. A., & Beheshti, B. D. (2018). A study on penetration testing process and tools. In *2018 IEEE long island systems, applications and technology conference (LISAT). IEEE.* https://doi.org/10.1109/lisat.2018.8378035
3. Chowdhary, A., Huang, D., Mahendran, J. S., Romo, D., Deng, Y., & Sabur, A. (2020). Autonomous security analysis and penetration testing. In *2020 16th international conference on mobility, sensing and networking (MSN). IEEE.* https://doi.org/10.1109/msn50589.2020.00086
4. Vats, P., Mandot, M., & Gosain, A. (2020). A comprehensive literature review of penetration testing & its applications. In *2020 8th international conference on reliability, infocom technologies and optimization (trends and future directions) (ICRITO). IEEE.* https://doi.org/10.1109/icrito48877.2020.9197961
5. *Products in penetration testing tools category.* (n. d.). https://www.gartner.com/reviews/market/penetration-testing-tools

6. *Automated penetration testing tool | ridgebot | ridge security.* (n. d.). Ridge Security. https://ridgesecurity.ai/products/
7. *Network penetration testing platform | vpentest.* (n. d.). Vonahi Security: Automated Penetration Testing & Cyber Security Services. https://www.vonahi.io/services/network-penetration-testing
8. *Metasploit | penetration testing software, pen testing security | metasploit.* (n. d.). Metasploit. https://www.metasploit.com/
9. *PTaaS - BreachLock.* (n. d.). BreachLock. https://www.breachlock.com/products/ptaas/
10. *Home.* (n. d.). Edgescan. https://www.edgescan.com/
11. *Burp suite professional.* (n. d.). Web Application Security, Testing, & Scanning - PortSwigger. https://portswigger.net/burp/pro
12. *AppCheck | A complete enterprise security testing solution.* (n. d.) https://appcheck-ng.com/
13. *NetSPI penetration testing as a service (ptaas).* (n. d.). https://www.netspi.com/netspi-ptaas/
14. *Astra Pentest.* (n. d.). https://www.getastra.com/pentest
15. *Penetration testing toolkit, ready to use.* (n. d.). Pentest-Tools.com. https://pentest-tools.com/
16. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.