УДК 004.56

Л. М. Куперштейн, канд. техн. наук, доц.; А. В. Притула;
В. І. Маліновський, канд. техн. наук, доц.

АНАЛІЗ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ WEB-ДОДАТКІВ

У статті проаналізовано технології тестування на проникнення, які використовуються для виявлення вразливостей у веб-додатках. Розглянуто методи white box, grey box та black box, кожен з яких має свої унікальні підходи та переваги у виявленні вразливостей. Детально розглянуто стандарти OSSTMM, NIST, OWASP, PTES та ISAAF, кожен з яких надає свої методології та рекомендації для проведення тестування на проникнення. OSSTMM, наприклад, є міжнародною методологією, яка пропонує розділення на три основні класи безпеки та детально описує процедури підготовки до тестування. NIST фокусується на плануванні, виконанні та пост-експлуатації, підкреслюючи важливість збору інформації на етапі планування. OWASP наголошує на необхідності тестування захищеності на кожному етапі розробки програмного забезпечення, а PTES надає практичні рекомендації щодо кожного з семи етапів тестування на проникнення. ISAAF пропонує трифазний підхід, включаючи планування, проведення тестування та формування звіту. Крім того, у статті досліджено фреймворки Mitre ATT&CK, CIS Controls та Cyber Kill Chain, які допомагають організаціям зрозуміти та протидіяти кібератакам. Mitre ATT&CK відомий своїм широким охопленням атак та глибоким аналізом тактик і методів атак. CIS Controls зосереджуються на конкретних контролях безпеки, які можна безпосередньо застосувати для захисту систем, а Cyber Kill Chain надає структурований підхід до аналізу та запобігання кібератакам. У статті також надано рекомендації щодо впровадження та використання сучасних технік тестування на проникнення для підвищення рівня безпеки інформаційних систем. Результати дослідження можуть бути корисними для спеціалістів з кібербезпеки та розробників веб-додатків, допомагаючи їм краще розуміти та впроваджувати ефективні методи захисту від кібератак.

Ключові слова: *веб-додаток, тестування на проникнення, стандарти тестування на проникнення, фреймворки тестування на проникнення.*

Вступ

Тестування на проникнення, або пентестинг, є процесом імітації кібератак на інформаційні системи з метою виявлення вразливостей, які можуть бути використані зловмисниками [1]. Це важлива складова забезпечення безпеки веб-додатків, які стають дедалі більш поширеними у всіх сферах життя та бізнесу. Веб-додатки використовуються для виконання різних функцій, включаючи обробку конфіденційної інформації, здійснення фінансових транзакцій та надання онлайн-послуг. Тестування на проникнення дозволяє ідентифікувати та виправити вразливості, забезпечуючи захист даних і зниження ризику кібератак.

Сучасні веб-додатки можуть містити багато компонентів, які потребують тестування на безпеку. Це можуть бути самі додатки, їхні веб-інтерфейси (веб-API), віртуальні контейнери, репозиторії коду та інші складові. Кожен з цих компонентів може мати свої вразливості, які необхідно виявити та виправити для забезпечення комплексного захисту системи.

Дослідження щодо тестування на проникнення web-орієнтованих інформаційних систем, останнім часом стають надзвичайно актуальними через поширеність таких систем і зростання ролі web-технологій у всіх сферах життя. Сьогодні існує багато ризиків, пов'язаних з можливим порушенням конфіденційності, цілісності та доступності даних [2]. Висновки після проведення тестів на проникнення, а також подальші заходи забезпечення безпеки,

допомагають запобігти нанесенню економічної, фінансової і іншого виду шкоди. Під час такого тестування виявляються і перевіряються слабкі місця системи, спричинені програмними або технічними помилками, некоректними налаштуваннями та іншими дефектами. Крім того, тестування на проникнення дозволяє чітко продемонструвати актуальність виявлених вразливостей і значимість потенційних збитків.

У сучасному суспільстві та бізнесі роль web-додатків надзвичайно важлива. При їхній розробці використовуються різноманітні технології, які постійно розвиваються та удосконалюються. Однак використання web-додатків пов'язане з ризиками, що можуть призвести до порушення безпеки інформації [3]. Це пояснюється тим, що методи, що використовуються зловмисниками, неперервно еволюціонують. Причиною цього є вразливості компонентів web-додатків, які можуть бути присутніми в них від самого початку їх розробки або з'явитися на інших етапах процесу створення та експлуатації [4]. Це веде до недостатнього рівня захисту web-додатків від наявних загроз.

Метою цієї роботи є аналіз технологій тестування на проникнення web-додатків, узагальнення отриманих даних та розробка відповідних рекомендацій до використання.

Основна частина

Згідно термінології НД ТЗІ 1.1-003-99, тестування на проникнення – це випробування, метою яких є здійснення спроби обминути або відключити механізми захисту [5]. Як правило, сценарій тестування на проникнення виглядає наступним чином:

- планування тесту на проникнення;
- збір інформації про цільові системи;
- пошук вразливостей;
- проникнення в систему;
- складання звітів;

очищення систем від наслідків тесту.

Враховуючи це, існує декілька підходів до проведення тестування на проникнення [6]:

- white box – імітація дій зловмисників по зламу системи, які мають доступ до системи та повну інформацію про її побудову;
- grey box – імітація дій зловмисників по зламу системи, які мають часткову інформацію про систему (діапазони IP-адрес, ідентифікатори бездротових мереж, доступ до системи з низьким рівнем привілеїв та ін.);
- black box – імітація дій зловмисників, у яких є тільки назва компанії та практично нульові відомості про систему.

Для проведення тестування на проникнення веб-додатків на сьогодні існують наступні найбільш розповсюджені методики:

- Open Source Security Testing Methodology Manual (OSSTMM);
- National Institute of Standards and Technology (NIST);
- Open Web Application Security Project (OWASP);
- Penetration Test Execution Standard (PTES);
- Information System Security Assessment Framework (ISSAF).

OSSTMM є міжнародною методологією для оцінки інформаційної безпеки, розробленою ISECOM (Institute for Security and Open Methodologies) [7]. Мета цієї методології полягає в наданні керівних принципів для оцінки безпеки, включаючи розділення на три основні класи безпеки: COMSEC (communication security channel – комунікаційний канал безпеки), PHYSSEC (physical security channel – фізичний канал безпеки) та SPECSES (spectrum security channel – спектральний канал безпеки). Ці класи поділяються на п'ять каналів взаємодії з активами організації, які повинні бути перевірені тестувальником, включаючи фізичну безпеку, бездротові та інформаційно-телекомунікаційні мережі, мережі передачі даних, а також людський фактор через використання методів соціальної інженерії. Основні переваги цієї

методології полягають у докладному описі процедур підготовки до тестування, методів та підходів до оцінки безпеки, а також у ретельному поясненні ключових термінів та понять у галузі інформаційної безпеки. Однак ця методологія не включає опису інструментів, що використовуються для виконання тестів, хоча надає набір правил та процедур, які допомагають зрозуміти ступінь захищеності веб-додатків від різних видів атак.

Методологія NIST Special Publication 800-115 розподіляє процес оцінювання інформаційної безпеки на три основні фази: планування, виконання та пост-експлуатація [8]. Фаза планування, за словами авторів методології є вирішальною для успішної оцінки безпеки, вона використовується для збору інформації, необхідної для виконання оцінки, наприклад про активи, що підлягають оцінці, загрози, що представляють інтерес щодо активів, і засоби контролю безпеки, які будуть використовуватися для пом'якшення цих загроз, а також для розробки підходу до оцінювання. Оцінку безпеки слід розглядати як будь-який інший проєкт із планом управління проєктом для вирішення цілей і завдань, обсягу, вимог, ролей і обов'язків команди, обмежень, факторів успіху, припущень, ресурсів, часових рамок і результатів. Основні цілі на етапі виконання полягають у виявленні вразливостей і їх перевірці, якщо це необхідно. Ця фаза має стосуватися діяльності, пов'язаної з запланованим методом і технікою оцінювання. Хоча конкретні дії для цього етапу відрізняються залежно від типу оцінювання, після завершення цього етапу оцінювачі виявлять вразливі місця системи, мережі та організаційного процесу. Остання включає фаза в себе аналіз отриманих даних, виявлення причин вразливостей, розробку рекомендацій щодо їх усунення та підготовку звіту. Цей документ містить загальний огляд технік перевірки безпеки комп'ютерних систем, включаючи веб-додатки, з коротким описом. Наприклад, перевірка мережі на предмет зловживання, аналіз журналів, перевірка конфігурацій системи, перевірка цілісності файлів, сканування вразливостей, а також бездротових мереж тощо. Більше того, в документі наводяться посилання на програмні продукти, необхідні для проведення тестування, а також на інші нормативні документи та методології. Проте слід зазначити, що цей документ був розроблений у 2008 році і на сьогоднішній день він не відповідає сучасному рівню розвитку інформаційних технологій та методам проникнення у веб-додатки.

Автори методики OWASP Testing Guide наголошують на тому, що необхідно впроваджувати тестування захищеності веб-додатків на кожному з етапів розробки програмного забезпечення [9]. Згідно методики OWASP Testing Guide, тестування проводиться у наступній послідовності:

- збір інформації;
- тестування конфігурації;
- тестування механізмів керування ідентифікацією;
- тестування процесу аутентифікації;
- тестування процесу авторизації;
- тестування механізмів керування сесіями;
- тестування обробки вхідних даних від користувача;
- обробка помилок;
- тестування механізмів, що реалізують криптографічні функції;
- тестування бізнес-логіки додатка;
- тестування клієнтської частини.

У кожному з етапів докладно описується інформація, яку необхідно зібрати під час виконання тестування, як обробляти отриману інформацію, які компоненти додатка необхідно перевірити, та програмні засоби, за допомогою яких можна провести тестування додатка на кожному з етапів з прикладами їх використання. В кінці кожного з етапів наведено посилання, які містять додаткову корисну інформацію про особливості проведення тестування. Найкраще застосування — тестування безпеки веб-додатків з акцентом на найбільш поширені вразливості та загрози.

Стандарт тестування на проникнення PTES описує 7 основних етапів проведення тестування на проникнення [10]:

- попередня взаємодія між сторонами;
- збір інформації;
- моделювання загроз;
- аналіз вразливостей;
- експлуатація вразливостей;
- пост-експлуатаційний період та оцінка можливих збитків від атак;
- формування звітів.

Окремою частиною стандарту PTES є розділ технічних рекомендацій, у якому описане необхідне програмне забезпечення і додаткова інформація для практичної реалізації тестування на проникнення. Його варто застосовувати для практично-орієнтованого підходу, який забезпечує детальні технічні рекомендації щодо проведення тестів на проникнення.

Методика ISAAF розроблена групою безпеки відкритих інформаційних систем (OSSIG – Open Information Systems Security Group). Згідно методики ISAAF тестування на проникнення складається з наступних 3 фаз [11]:

– планування та підготовка до тестування (підписання угоди між замовником та виконавцем тестування на проникнення, узгодження методики тестування та набору програм для проведення тестування на проникнення);

– проведення тестування на проникнення (збір інформації, складання схеми мережі, що тестується, ідентифікація вразливостей, заходи з проникнення у систему, отримання доступу до ресурсів, компрометування віддалених користувачів / сайтів, приховування слідів);

– формування звіту про проведене тестування на проникнення (перелік програм та методик, що були використані під час тестування, дата та час проведення тестування, список знайдених вразливостей, рекомендації для підвищення безпеки).

Методика ISAAF дозволяє проводити:

- оцінку захищеності паролів;
- оцінку захищеності мережевих пристроїв;
- оцінку захищеності міжмережевих екранів;
- оцінку захищеності систем виявлення вторгнень;
- оцінку захищеності веб – додатків;
- оцінку захищеності операційних систем;
- аудит програмного коду;
- аналіз захищеності баз даних.

Узагальнені результати аналізу вищевказаних методик тестування на проникнення за різними критеріями представлені в таблиці 1, в якій використані наступні позначення:

- «+» – є в повному обсязі;
- «±» – є у короткому викладі чи згадується;
- «–» – цей матеріал відсутній, або викладений таким чином, що не має цінності.

Таблиця 1

Результати порівняльного аналізу методик тестування на проникнення

Критерій	OSSTMM	NIST	OWASP	PTES	ISSAF
1	2	3	4	5	6
Рекомендації щодо обговорення із замовником цілей та завдань тестування	+	±	+	+	+
Рекомендації щодо підготовки договору на тестування	+	±	–	±	+
Законодавчі аспекти тестування	±	+	–	–	+
Рекомендації щодо збору інформації про об'єкт тестування	+	+	+	+	+
Детальні рекомендації щодо аналізу та оцінки вразливостей	±	±	+	+	+
Рекомендації щодо етапів тестування та їх змісту	+	+	+	+	+
Окремі рекомендації щодо тестування теле-комунікаційних мереж	+	+	±	+	+
Окремі рекомендації щодо тестування бездротових мереж	+	+	–	+	+
Окремі рекомендації щодо тестування веб-додатків	±	–	+	+	±
Окремі рекомендації щодо перевірки безпеки фізичної інфраструктури	+	–	–	+	+
Окремі рекомендації щодо перевірки безпеки паролів	–	+	±	+	+
Окремі рекомендації щодо перевірки безпеки баз даних	–	–	±	–	+
Окремі рекомендації щодо перевірки безпеки вихідного коду	–	–	±	–	+
Рекомендації щодо конкретного ПЗ, що використовується для тестування	–	–	±	+	+
Рекомендації щодо формування звіту про тестування	+	–	+	+	+
Аналіз та рекомендації щодо усунення знайдених вразливостей	–	+	–	–	+

Як видно з табл. 1, найбільш опрацьованою методикою тестування на проникнення як у теоретичному, так і практичному плані є методика ISSAF. Методики OSSTMM та NIST мають більшою мірою теоретичний характер. Методика PTES є практико-орієнтованою та містить широкий набір технічних рекомендацій та конкретних вразливостей, які необхідно перевіряти під час тестування на проникнення.

Оскільки у кожній з методик тестування на проникнення є багато правил та рекомендацій, за якими потрібно слідкувати під час їх використання, виникає потреба у написанні спеціалізованого програмного забезпечення, яке допоможе автоматизувати аналіз та впровадження вищезгаданих методик. У цьому контексті виникає необхідність у розгляді та використанні програмних фреймворків, які допомагають ідентифікувати потенційні загрози та впроваджувати ефективні контрзаходи. Один з найбільш популярних фреймворків для цього – Mitre ATT&CK [12], який аналізує тактики та методи атак, дозволяючи організаціям розуміти, як саме зловмисники можуть використовувати дефекти в системі. Ще один широко використовуваний фреймворк – CIS Controls [13], фокусується на конкретних контролях безпеки, які можуть застосовуватися для мінімізації ризиків усіма видами організацій. Для розуміння їхньої ефективності та придатності для конкретних потреб слід провести детальне

порівняння, враховуючи різні аспекти, такі як охоплення атак, складність використання, практичність застосування та підтримка спільноти. Крім того, важливо розглянути і Cyber Kill Chain [14], який надає відомості для аналізу та захисту від кібератак, описуючи етапи кібератаки та допомагаючи розібратися в тому, як саме зловмисники можуть проникнути в систему. Узагальнені результати аналізу ви популярних фреймворків за різними критеріями представлені в таблиці 2.

Таблиця 2

Результати порівняльного аналізу популярних фреймворків

Критерії порівняння	Mitre ATT&CK	CIS Controls	Cyber Kill Chain
1	2	3	4
Охоплення атак	Широке, описує різні тактики та методи атак	Менш широке, фокусується на конкретних контролях	Описує етапи кібератаки
Складність використання	Висока, потребує досвіду та розуміння	Низька, прості та зрозумілі рекомендації	Залежить від рівня експертизи користувача
Практичність застосування	Висока, надає конкретні дії для захисту	Висока, прямий зв'язок із захистом систем	Надає відомості для аналізу та захисту від кібератак
Підтримка спільноти	Є, активна спільнота експертів та оновлення	Є, спільнота експертів із практичними порадами	Відомості доступні для аналізу, але менша активність спільноти
Потреба у постійній актуалізації	Так, оновлюється з урахуванням нових загроз	Так, але менше частоти оновлень	Так, з урахуванням розвитку кіберзагроз

За результатами порівняльного аналізу Mitre ATT&CK та CIS Controls можна зробити кілька важливих висновків. Обидва фреймворки є корисними інструментами для забезпечення безпеки веб-додатків та інформаційних систем загалом. Mitre ATT&CK відзначається широким охопленням атак та глибоким аналізом тактик та методів атак, що робить його цінним ресурсом для дослідження загроз та визначення стратегій захисту. З іншого боку CIS Controls зосереджуються на конкретних контролях безпеки, які можна безпосередньо застосувати для забезпечення захисту систем.

Що ж до практичної застосовності, CIS Controls відзначаються своєю простотою та прямим зв'язком із практикою захисту, що робить їх ефективними для використання на практиці. У той же час, Mitre ATT&CK вимагає більшої експертизи та дослідницької роботи для його використання.

Обидва фреймворки мають активні спільноти експертів, які надають підтримку та оновлення. Проте, важливо враховувати, що Mitre ATT&CK вимагає більшої частоти оновлень з урахуванням кіберзагроз, що швидко змінюються.

Загалом, вибір між цими двома фреймворками залежить від конкретних потреб та контексту організації, проте обидва вони можуть бути корисними інструментами для підвищення рівня безпеки та захисту інформаційних систем.

Щодо Cyber Kill Chain, вона надає відомості для аналізу та захисту від кібератак, описуючи етапи кібератаки та допомагаючи розібратися в тому, як саме зловмисники можуть проникнути в систему. Цей фреймворк може доповнити аналіз Mitre ATT&CK та CIS Controls, надаючи більш повну картину загроз та способів їх виявлення та запобігання.

Зі збільшенням складності та поширеності цифрових платформ, питання їх надійності та безпеки набувають першочергового значення. Вивчення та впровадження машинного навчання для підтримки та вдосконалення процесів тестування на проникнення стає критично важливим завданням. Так, наприклад, у роботі [15] для вирішення завдання аналізу дерева атак автори застосували метод машинного навчання. При цьому за основу взяли Q-навчання

для пошуку траєкторії атак. Проте незначність простору дій та простору вибірки знизили практичну цінність зазначеної розробки. На думку авторів [15] корисним удосконаленням у питаннях аналізу дерева атак для тестування на проникнення стала технологія глибокого машинного навчання з підкріпленням.

Технології штучного інтелекту, такі як навчання з підкріпленням, все частіше використовуються для тестування на проникнення. Вже існує ряд фреймворків, які використовують ці технології, що допомагає значно підвищити ефективність та точність тестування. Наприклад, PentestGPT [16] є одним з таких фреймворків, що інтегрує технології штучного інтелекту для виявлення та аналізу вразливостей у web-додатках. У майбутньому ці підходи можуть стати стандартом у галузі кібербезпеки, забезпечуючи більш надійний захист інформаційних систем. Використання методів машинного навчання дозволяє автоматизувати процес тестування, зменшити людський фактор та покращити виявлення нових та невідомих вразливостей [17].

Висновки

Захищеність веб-додатків від атак зловмисників залежить від технологій та компонентів, які використовуються при побудові веб-додатків, а також від можливих вразливостей у цих компонентах. Було проведено аналіз технологій тестування на проникнення web-додатків. Широкий вибір засобів дозволяє проводити пошук вразливостей, проте ефективність їх використання залежить від алгоритму дій, за яким необхідно проводити цей пошук. Згідно досліджень, існують міжнародні стандарти обробки інформації про вразливості, бази даних вразливостей, та засоби їх пошуку. Окремі організації займаються розробкою методик тестування на проникнення. Проте, більшість методик охоплюють широке коло питань кібербезпеки, отже виникає необхідність додаткових витрат часу на аналіз вразливостей згідно наявних методик та обрання тих складових, зокрема, які підходять для тестування веб-додатків.

Для досягнення оптимальних результатів, незалежно від використовуваних методів тестування на проникнення, важливо, щоб тестувальник дотримувався певної методології. Найбільш відомими з них є OSSTMM, NIST, OWASP, PTES та ISAAF.

OSSTMM є експертною методологією з виконання тестів та метрик безпеки, що пройшла рецензування. Якщо ж говорити про її практичне застосування, то вона підходить для всебічного тестування безпеки, яке вимагає глибокого аналізу захищеності організації у сферах комунікаційної безпеки, фізичної безпеки та безпеки спектрів, ідеально підходить для організацій, які прагнуть детально оцінити свою безпекову інфраструктуру, особливо коли комунікаційна та фізична безпека є такими ж важливими, як і безпека.

NIST надає конкретні рекомендації щодо тестування на проникнення для підвищення точності тестів. Його найкраще застосовувати для створення послідовних процедур тестування безпеки, що відповідають американським федеральним регуляціям та стандартам. Підходить для організацій, яким необхідно дотримуватись американських урядових стандартів безпеки або використовувати широко визнаний фреймворк, що інтегрується з наявними вимогами щодо відповідності.

OWASP розвивається спільнотою, яка враховує останні загрози та логічні помилки процесів, окрім вразливостей програмного забезпечення. Найкраще застосування — тестування безпеки веб-додатків з акцентом на найбільш поширені уразливості та загрози. Особливо підходить для команд розробників під час життєвого циклу розробки програмного забезпечення (SDLC), щоб інтегрувати тестування безпеки у процес розробки, зокрема на ранніх стадіях, щоб своєчасно виявити вразливості.

PTES націлений на створення сучасного стандарту для тестування на проникнення та підвищення обізнаності бізнесу щодо очікувань від такого тестування. Варто застосовувати для практично-орієнтованого підходу, який забезпечує детальні технічні рекомендації щодо проведення тестів на проникнення. Корисно для постачальників послуг безпеки та внутрішніх

безпекових команд, які регулярно проводять тести на проникнення і потребують структурованої методології з ясними вказівками на кожну фазу тестування.

ISAAF надає докладну методику тестування на проникнення та дозволяє оцінити захищеність різних компонентів інформаційних систем, включаючи веб-додатки. Підходить для детального оперативного тестування різних компонентів інформаційних систем, включаючи мережеві пристрої, брандмауери та веб-додатки. Ідеально підходить для великих організацій та IT-відділів, які потребують надійного фреймворку для проведення ретельних безпекових оцінок і тестів на проникнення, які охоплюють багато аспектів їхньої IT-інфраструктури.

Програмні фреймворки допомагають виявляти загрози та захищати системи. Маючи на увазі різні потреби та особливості організацій, проведений аналіз демонструє, що Mitre ATT&CK та CIS Controls можуть бути корисними інструментами. Mitre ATT&CK відомий своїм широким охопленням атак та глибоким аналізом, в той час як CIS Controls спрямовані на конкретні контролі безпеки. Додатковий порівняльний аналіз показує, що вибір між цими фреймворками залежить від таких чинників, як складність використання, практична застосовність та частота оновлень. Обидва фреймворки мають активні спільноти експертів, які надають підтримку та оновлення, проте Mitre ATT&CK вимагає більшої експертизи та частіших оновлень. Щодо аналізу Cyber Kill Chain, він доповнює розуміння загроз та допомагає виявити стратегії захисту від кібератак. Цей фреймворк, в поєднанні з іншими методологіями та фреймворками, може забезпечити більш повну картину кіберзахисту для веб-додатків та інших інформаційних систем.

Mitre ATT&CK та Cyber Kill Chain корисні для організацій, які зосереджені на розумінні та пом'якшенні загроз від стійких і тривалих атак. Ці фреймворки підходять краще для команд безпеки, які аналізують тактику, техніки загроз і готують захисні стратегії відповідно, у той час, як CIS Controls надає набір дієвих контролів і найкраще підходить для організацій, які потребують прямих, зрозумілих рекомендацій, які безпосередньо впливають на захист систем від загальнопоширених загроз.

Таким чином, вибір методології та методів тестування та їх наступна реалізація є ключовими для забезпечення високого рівня безпеки будь-якої інформаційної системи.

При виборі стандарту тестування на проникнення або фреймворку важливо враховувати специфічні потреби конкретної організації, критичність систем, які беруть участь, кваліфікацію команди безпеки, а також будь-які регуляторні вимоги, які мають бути виконані. Комбінування елементів з різних методологій та фреймворків також може бути ефективним для створення індивідуальної стратегії оцінки безпеки, яка охоплює всі необхідні аспекти.

СПИСОК ЛІТЕРАТУРИ

1. An overview of penetration testing [Electronic resource] / Aileen G. Bacudio, 1Xiaohong Yuan, 2Bei-Tseng Bill Chu [et al.] // International journal of network security & its applications (IJNSA). – 2011. – Vol. 3, № 6. – P. 19 – 38. – Access mode: https://doi.org/10.5121/ijnsa.2011.3602.

2. НД ТЗІ 3.6-004-21. Нормативний документ системи технічного захисту інформації. – Чинний від 2008-01-01. – Вид. офіц. – Київ : [б. в.], 2021. – 23 с.

3. Захист веб-додатків: чому це важливо? [Електронний ресурс] // Компанія ITBIZ. – Режим доступу: https://itbiz.ua/statti-ta-obzori/zaxist-veb-dodatkiv-chomu-ce-vazhlivo/.

4. Аналіз проблем безпеки веб-застосунків [Електронний ресурс] / А. Притула, Л. Куперштейн // Матеріали Всеукраїнської науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи» : Міжнар. наук. конф., Вінниця, 20 трав. 2024 р. – Вінниця, 2024. – Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/19523/16190.

5. НД ТЗІ 1.1-003-99. Нормативний документ системи технічного захисту інформації. – Чинний від 1999-04-28. – Вид. офіц. – Київ : [б. в.], 1999. – 22 с.

6. Types of penetration testing | black box vs white box vs grey box [Electronic resource] / Mark Nicholls // Redscan. – Acces mode : https://www.redscan.com/news/types-of-pen-testing-white-box-black-box-and-everything-in-between/.

7. OSSTMM 3 | the open source security testing methodology manual contemporary security testing and analysis [Electronic resource] / P. Herzog // ISECOM. – Access mode : https://www.isecom.org/OSSTMM.3.pdf.

8. Technical guide to information security testing and assessment. recommendations of the national institute of standards and technology [Electronic resource] / Karen Scarfone, Murugiah Souppaya, Amanda Cody [et al.] // NIST Technical Series Publications. – Access mode : https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.

9. OWASP testing guide [Electronic resource] // OWASP. – Access mode : https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf.

10. The penetration testing execution standard [Electronic resource] // PTES. – Access mode : http://www.pentest-standard.org/index.php/Main_Page.

11. Information systems security assessment framework (ISSAF) draft 0,2.1 [Electronic resource] // Untrusted Network. – Access mode : https://untrustednetwork.net/files/issaf0.2.1.pdf.

12. Mitre att&ck [Electronic resource] // MITRE ATT&CK. – Access mode : https://attack.mitre.org/.

13. CIS controls [Electronic resource] // CIS. – Access mode : https://www.cisecurity.org/controls.

14. Cyber kill chain [Electronic resource] // Lockheed Martin. – Access mode : https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

15. Tvoroshenko I. Research of regression and modular testing of web applications [Electronic resource] / Irina Tvoroshenko, Heorhii Maksimenko // Science, theory and practice : Міжнародна наукова конференція, Tokyo, 12–15 October 2021. – London, 2021. – P. 406 – 411. – Access mode : https://openarchive.nure.ua/handle/document/17929.

16. Pentest Gpt: evaluating and harnessing large language models for automated penetration testing [Electronic resource] / Gelei Deng [et al.]. – Access mode : https://arxiv.org/pdf/2308.06782.

17. Притула А. Застосування штучного інтелекту для тестування на проникнення / А. Притула, Л. Куперштейн // Матеріали LIII науково-технічної конференції підрозділів Вінницького національного технічного університету (НТКП ВНТУ-2024) : Всеукр. наук. конф., Вінниця, 20–22 берез. 2024 р. – Вінниця, 2024. – С. 345 – 349.

Стаття надійшла до редакції 22.06.2024.
Стаття пройшла рецензування 26.06.2024.

Куперштейн Леонід Михайлович – канд. техн. наук, доцент кафедри захисту інформації.

Притула Андрій Вікторович – аспірант кафедри захисту інформації, e-mail: andrik.pritula@gmail.com.

Маліновський Вадим Ігоревич – канд. техн. наук, доцент кафедри захисту інформації.

Вінницький національний технічний університет.