УДК 004.415.538:004.056.5
DOI: 10.31673/2409-7292.2023.030909

**Легомінова С. В., Рабчун Д. І.,
Драгунцов Р. І., Запорожченко М. М.**

ТЕСТУВАННЯ ЗАХИЩЕНОСТІ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ: ВИБІР ЕФЕКТИВНИХ МЕТОДІВ ТА СЦЕНАРІЇВ ДЛЯ РІЗНИХ ОБ'ЄКТІВ ТЕСТУВАННЯ

Сучасні виклики у сфері кібербезпеки вимагають глибокого розуміння та ефективного застосування різних видів тестування захищеності. Тестування захищеності, як один із основних елементів стратегії кібербезпеки, вимагає систематичного підходу та вибору оптимальних сценаріїв тестування відповідно до конкретних потреб та особливостей IT інфраструктури організації. З ростом різноманітності кіберзагроз і технік атак, важливо розглядати та порівнювати різні види тестування захищеності для визначення їх ефективності у різних сценаріях. Метою статті є розробка рекомендацій для фахівців із кібербезпеки щодо вибору ефективних методів оцінювання рівня захисту, шляхом використання різних сценаріїв тестування захищеності IT інфраструктури. У статті виконано аналіз та класифікацію різних видів тестування захищеності з метою вибору найефективніших методів та сценаріїв для різних систем. Розроблено матрицю вибору, яка допомагає систематизувати процес вибору методів та сценаріїв тестування відповідно до конкретних об'єктів тестування. Кожен об'єкт має свої особливості та формує відповідні вимоги до тестування, і вибір методів повинен бути адаптований до цих унікальних аспектів для забезпечення максимальної ефективності заходів безпеки. Застосування відповідних методів, таких як сканування вразливостей, пентест, аналіз вразливостей, Red teaming та соціально-інженерне тестування, у поєднанні з конкретними сценаріями, дозволяє ефективно виявляти та усувати недоліки та вразливості IT інфраструктури та її компонентів. На основі виконаного аналізу, надаються практичні рекомендації щодо вибору оптимальних стратегій для конкретних сценаріїв тестування. Стаття розроблена для фахівців з кібербезпеки, дослідників та організацій, що прагнуть покращити ефективність своїх програм тестування захищеності та забезпечити високий рівень захисту в умовах незліченних кіберзагроз.

Ключові слова: тестування захищеності, кібербезпека, аналіз вразливостей, тестування додатків та веб-сервісів, black box, red teaming.

Вступ

У світі постійних технологічних інновацій, розмаїття кіберзагроз та обмеженої кількості ресурсів, забезпечення ефективної кібербезпеки стає необхідністю для усіх видів організацій та підприємств. Тестування захищеності, як один із основних елементів стратегії кібербезпеки, вимагає систематичного підходу та вибору оптимальних сценаріїв тестування відповідно до конкретних потреб та особливостей IT інфраструктури організації. З ростом різноманітності кіберзагроз і технік атак, важливо розглядати та порівнювати різні види тестування захищеності для визначення їх ефективності у різних сценаріях.

Постановка проблеми

Для вибору ефективних підходів до тестування захищеності, а також отримання релевантних результатів необхідно провести аналіз та огляд методів та різних видів тестування захищеності з метою визначення ефективних сценаріїв для оцінювання захищеності IT інфраструктури. Різноманітність послуг у сфері оцінювання захищеності потребує класифікації задач з тестування захищеності відповідно до методів та об’єктів тестування. Спираючись на високий рівень експертизи та відомостей у сфері кібербезпеки, необхідно визначити оптимальні стратегії тестування захищеності, які відповідають заданим вимогам до рівня безпеки та ефективності.

Аналіз публікацій

У статті [1] проведено аналіз методів тестування спеціального програмного забезпечення на етапі експлуатації, які відповідають регламентам міжнародних стандартів STANAG та ISO/ДСТУ і направлені на виявлення потенційної вразливості(vulnerability). Запропоновано шляхи удосконалення тестуванн спеціального програмного забезпеченняінформаційної системи управління оборонними ресурсами DRMIS (Defense Resources Management Information System) для впровадження на етапі експлуатації. У роботі [2] наведено інформацію про методологію тестів на проникнення, його методів і способів реалізації. Проаналізовано сучасні безкоштовні та з відкритим вихідним кодом програми. Розглянуто приклад тестування на проникнення в академічній сфері в навчальних цілях на базі Kali Linux і Metasploitable 2

Linux. Ці перевірки і методи показують проактивні методи захисту та повинні допомогти поліпшити безпеку комп'ютерних систем і корпоративних мереж. В публікації [3] наведено перелік найбільш розповсюджених міжнародних методологій проведення пентестінгу, надано їх короткий опис. Проаналізовано методи проведення пентестінгу, визначені основні переваги і недоліки таких методів.

У статті [4] запропонований загальний алгоритм проведення тестування на проникнення IT-інфраструктури (аналіз вразливостей та захищеності інформаційних ресурсів) у вигляді етапів: ініціалізації, пасивної і активної розвідки, експлуатації і пост-експлуатації, систематизація і презентація результатів оцінки безпеки, оцінки ризиків та вразливостей, рекомендацій щодо їх усунення. У роботі [5] запропоновано програмне забезпечення, яке розроблено на основі мови програмування Java, включає графічну оболонку Java FX, для пошуку сервісів хосту використовується Shodan REST API, для ідентифікації враз-ливостей ресурси NVD і CVE details. Зібрані дані використовує окремий програмний модуль, що працює зі створен-ням моделі на основі мережі Петрі.

Незважаючи на наявні підходи, у технічній літературі залишається не розкритим питання щодо вибору ефективного методу та сценаріїв для різних об'єктів тестування.

Постановка завдання: розробити рекомендації для фахівців із кібербезпеки, для вибору ефективних методів оцінювання рівня захисту, шляхом використання різних сценаріїв тестування захищеності IT інфраструктури.

Сучасні стандарти інформаційної безпеки ISO 27001, NIST SP 800-115, SWIFT Customer Security Controls Framework (CSCF), PCI DSS 4.0 визначають процедури тестування захищеності як важливий елемент оцінювання безпеки інформації. Вони визначають регулярність проведення тестів, а також важливість оцінки не лише технічних аспектів, а й процесів та організаційних заходів.

Найкращі практики та методології щодо виконання тестувань захищеності, такі як PTES, OSSTMM, OWASP (WSTG), надають цілісну та структуровану інформацію, описують методи та стратегії тестування захищеності інформаційних систем та додатків [6, 7].

Основна частина

Тестування захищеності – це процес активного аналізу та оцінювання системи, програмного забезпечення, сервісу чи IT інфраструктури на предмет виявлення потенційних вразливостей та слабких місць, які можуть бути використані для несанкціонованого доступу, атаки чи компрометації. Цей вид тестування є одним із основних елементів стратегії забезпечення інформаційної безпеки та має на меті визначення рівня стійкості та готовності системи до різних видів кіберзагроз.

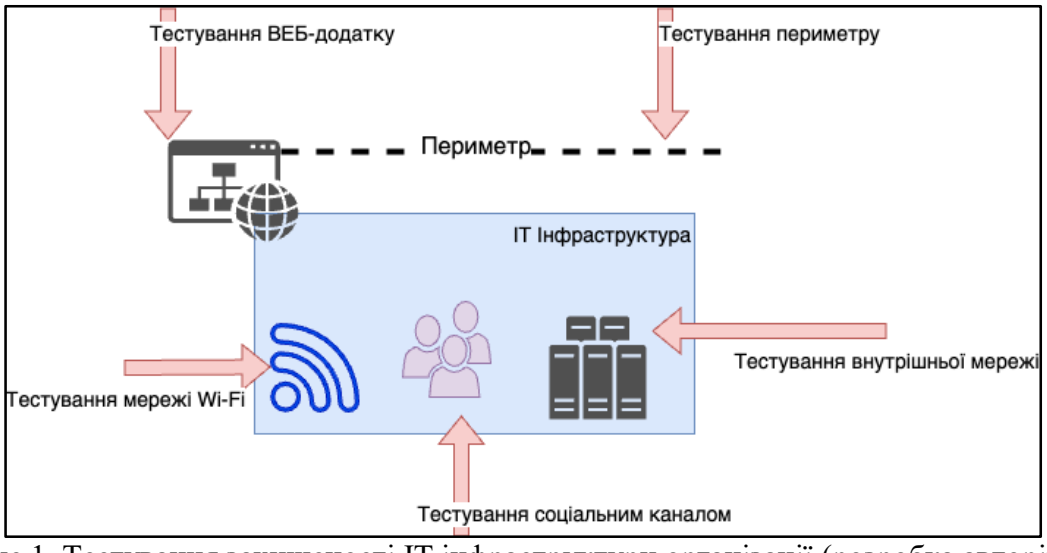

Рис.1. Тестування захищеності IT інфраструктури організації (розробка авторів)

Визначення вимог до тестування захищеності

Основні проблеми тестування захищеності інформаційних систем включають в себе декілька аспектів:

Складність систем: Інформаційні системи можуть бути складними, містити багато компонентів та підсистем, що ускладнює процес тестування. Велика кількість взаємодіючих елементів може зробити труднощі при виявленні уразливостей та ризиків безпеки. *Різноманітність уразливостей*: Захищеність системи потребує виявлення широкого спектру можливих уразливостей, таких як вразливості програмного забезпечення, слабкі точки в мережевих протоколах, недоліки в конфігурації системи, соціальну інженерію та інші. Тестувальник повинен бути здатний охопити цей різноманітний спектр проблем. *Обмежені ресурси*: Часто існують обмежені ресурси, доступні для тестування. Це може включати обмежений час, бюджет або доступ до необхідних інструментів та технологій. *Змінність оточення*: Інформаційні системи постійно зазнають змін у вигляді нового програмного забезпечення, патчів, оновлень та інших змін, що може вплинути на їхню безпеку. Тестування потребує постійного оновлення та адаптації до цих змін. *Питання етики та конфіденційності*: Під час тестування можуть виникнути етичні дилеми та проблеми з конфіденційністю даних, особливо при проведенні тестування реальних систем. Необхідно дотримуватися етичних стандартів і забезпечувати безпеку інформації під час процесу тестування. *Пошук "невідомих невідомих"*: Інколи можуть існувати уразливості або потенційні загрози, про які немає повного розуміння або які не відомі тестувальникам. Це може бути складно виявити, оскільки ці проблеми не підпадають під зону знань тестувальників. *Слабкість методів тестування*: Існують ситуації, коли наявні методи тестування можуть бути недостатніми для виявлення всіх уразливостей. Це може призвести до пропуску певних загроз або недоліків в безпеці. Управління цими проблемами вимагає комплексного підходу, що включає в себе використання різноманітних методів тестування, постійне вдосконалення процесів та використання найновіших технологій для виявлення та виправлення уразливостей в інформаційних системах.

Для забезпечення релевантних результатів та визначення стану захищеності систем, який відповідатиме дійсності, фахівці із захисту інформації мають обрати види та сценарії тестування відповідно до особливостей ІТ інфраструктури, цілей та об’єкта тестування [8].

До основних цілей, що впливатимуть на вибір способу тестування захищеності можна віднести:

1) **Виявлення та ідентифікація вразливостей.** Забезпечення виявлення усіх реальних та потенційних вразливостей в інфраструктурі, програмному забезпеченні та мережевих пристроях.

2) **Перевірка ефективності системи захисту.** Оцінка працездатності та ефективності існуючих заходів безпеки, включаючи антивіруси, фаєрволи, системи виявлення вторгнень, а також механізмів і процедур реагування на інциденти ІБ.

3) **Аналіз відповідності вимогам стандартів та регуляторів (compliance).** Перевірка відповідності системи вимогам стандартів безпеки, таких як ISO 27001, NIST, PCI DSS, SWIFT та інших регуляторних норм.

4) **Визначення слабких місць у захисті мережі.** Ідентифікація та усунення слабких місць у мережевій інфраструктурі, включаючи неправильну конфігурацію та поганий контроль доступу.

5) **Аудит веб-додатків.** Оцінка безпеки веб-додатків та виявлення можливих вразливостей та проблем безпеки, таких як SQL-ін'єкції, XSS, IDOR та інші.

6) **Оцінка спроможності системи витримувати атаки.** Перевірка стійкості системи до різних типів атак, включаючи атаки відмови в обслуговуванні (DoS) та розподілені атаки відмови в обслуговуванні (DDoS).

© Легомінова, С. В., Рабчун, Д. І., Драгунцов, Р. І., & Запорожченко, М. М. (2023). Тестування захищеності сучасних інформаційних систем: вибір ефективних методів та сценаріїв для різних об'єктів тестування. Сучасний захист інформації, 4(56), 84–90. https://doi.org/10.31673/2409-7292.2023.030909.

7) Тестування спроможностей протидії соціальному інжинірингу. Визначення рівня обізнаності персоналу та його вразливості до атак, методом соціальної інженерії.

Правильно обрані цілі (мета) допомагають забезпечити повноцінний та систематичний підхід до тестування захищеності, з метою максимальної ефективності та забезпечення високого рівня безпеки систем та даних.

Об'єкти тестування захищеності включають різні аспекти інфраструктури, які можуть бути піддані аналізу та перевірці для визначення їх стійкості до потенційних атак. Нижче перераховані деякі з основних об'єктів тестування захищеності:

1) Мережева інфраструктура.
a. Роутери, комутатори та інші мережеві пристрої.
b. Протоколи зв'язку та мережеві служби.
c. Мережеві архітектури та конфігурації.
2) Операційні системи.
a. Операційні системи на серверах, комп'ютерах та інших пристроях.
b. Системи управління даними та файлові системи.
3) Програмне забезпечення.
a. Додатки та програми, які використовуються в організації.
b. Системи управління базами даних (DBMS).
4) Веб-додатки.
a. Веб-сайти та інтернет-портали.
b. Системи керування вмістом та електронна комерція.
5) Інфраструктура хмарних обчислень:
a. Хмарні сервіси та інфраструктура.
b. Сховища даних та ресурси обчислень у хмарі.
6) Пристрої інтернету речей (IoT):
a. Розумні пристрої та сенсори.
b. Мережі зв'язку та протоколи обміну даними.
7) Соціально-інженерне тестування:
a. Обізнаність персоналу та його реакція на соціальні атаки.
b. Процеси навчання та підвищення обізнаності в питаннях кібербезпеки серед персоналу.

Ці об'єкти представляють різноманітні складові інфраструктури підприємства, які можуть бути включені до тестування захищеності для виявлення вразливостей, оцінювання рівня захищеності та підвищення загального рівня безпеки.

Для забезпечення релевантних результатів оцінювання рівня захисту, фахівцям із кібербезпеки необхідно визначити вид тестування відповідно до мети та об’єкту, перечислених вище. Відомі види тестування захищеності пропонується класифікувати за об’єктом тестування та за способом проведення робіт.

Класифікація тестування захищеності за об'єктом тестування може бути визначена наступним чином:

1. Тестування програмного забезпечення.
a. **Статичний аналіз коду**: Оцінка безпеки за допомогою аналізу вихідного коду програми.
b. **Динамічний аналіз**: Визначення вразливостей в режимі виконання програми.
2. Тестування мережі.
a. **Сканування мережі**: Визначення активних пристроїв та вразливостей у мережевій інфраструктурі.
b. **Тестування безпеки протоколів**: Аналіз протоколів для виявлення слабких місць та потенційних загроз.
3. Тестування Веб-додатків.

a. **Пентест Веб-додатків**: Визначення вразливостей веб-додатків через спроби активного проникнення.

b. **Аналіз безпеки API**: Оцінка безпеки інтерфейсів програмування застосунків (API).

4. Тестування системи керування ідентифікацією та доступом (IAM).

Перевірка ефективності механізмів аутентифікації та контролю доступу.

5. Соціально-інженерне тестування.

Симуляція атак, спрямованих на маніпуляцію користувачами та отримання доступу до конфіденційної інформації.

6. Тестування Інтернету речей (IoT).

Оцінка захищеності підключених пристроїв та їх взаємодії у мережі.

7. Тестування інфраструктури хмарних обчислень.

Визначення можливих ризиків та вразливостей у хмарних сервісах.

Така класифікація дозволяє розглядати тестування захищеності з різних точок зору та підходити до конкретних елементів IT інфраструктури з урахуванням їх унікальних характеристик, вимог до тестування та відповідних загроз [9].

Класифікація тестування захищеності за способом проведення робіт може включати такі види тестування:

1. Сканування вразливостей (Vulnerability Scanning):

a. Здійснюється перевірка доступних систем, ідентифікуються та оцінюються відомі вразливості.

2. Пентест (Penetration testing):

a. Чорний ящик (Black Box): фахівці не мають інформації про систему та мають за мету визначити вразливості, які можуть бути використані зловмисниками.

b. Сірий ящик (Grey Box): фахівці мають часткову інформацію про архітектуру та особливості роботи системи, мають облікові дані для доступу до обмежених функцій, тощо.

c. Білий ящик (White Box): фахівцям надається повна інформація про систему для аналізу внутрішніх механізмів безпеки.

3. Аналіз конфігурацій (Configuration Analysis):

a. Оцінка Конфігурації Систем: здійснюється аналіз відповідності та рівня безпеки налаштувань систем та програмного забезпечення.

b. Аудит конфігурації мережі: перевіряється безпека мережевих налаштувань та обладнання.

4. Тестування безпеки Веб-додатків:

a. Тестування вихідного коду: визначення вразливостей вихідного коду веб-додатків.

b. Тестування захищеності додатку: ідентифікація, аналіз та оцінювання проблем Веб-додатку які можуть призвести до компрометації самого додатку або його користувачів.

5. Red Teaming:

a. Моделювання реальних атак для перевірки ефективності внутрішніх протоколів по реагуванню на інциденти ІБ та заходів безпеки. Цей підхід дозволяє імітувати дії потенційного зловмисника та виявляти частини IT інфраструктури, які не покриті контролями кібербезпеки та зрозуміти, яким технікам і тактикам зловмисників IT інфраструктура не в змозі протистояти.

6. Соціально-інженерне тестування:

a. Фішингові та вішингові кампанії: виявлення рівня обізнаності персоналу та його вразливості до атак методом соціальної інженерії.

7. Тестування інтернету речей (IoT):

a. Аналіз протоколів та комунікацій: виявлення вразливостей у протоколах та засобах зв'язку пристроїв IoT.

8. Тестування фізичної безпеки:

а. Аудит безпеки приміщень: оцінка безпеки фізичного доступу до контрольованої зони, приміщень, обладнання та точок підключення до внутрішньої мережі.

9. Тестування інфраструктури хмарних обчислень:

а. Аналіз захисту даних: Визначення можливих загроз, вразливостей та слабких конфігурацій у хмарних сервісах.

Ця класифікація враховує різні аспекти тестування захищеності та вказує на методи, які можуть бути використані для виявлення потенційних загроз та вразливостей у різних областях інформаційної безпеки організації [10, 11].

Рекомендації по вибору ефективного методу та сценарію тестування захищеності з урахуванням цілей. Для вибору методу та сценарію тестування який буде ефективним та надасть релевантну оцінку рівня захисту, ключовим є зв'язок між об'єктом тестування, обраним методом та конкретними сценаріями, які відображають унікальні ризики та вразливості для кожного об'єкта. Важливо адаптувати методи та сценарії до конкретних потреб та характеристик інфраструктури організації.

Для типових задач по тестуванню захищеності пропонується використовувати матрицю «Вибору методів та цілей тестування захищеності» у таблиці 1.

Таблиця 1

Вибір методів та цілей тестування захищеності (розробка авторів)

Об'єкт	Метод	Сценарій	Ціль
Мережева інфраструктура	Сканування вразливостей	Тестування мережі	Виявлення та ідентифікація вразливостей
Операційні системи	Аналіз конфігурацій	Аналіз конфігурацій	Аналіз відповідності вимогам стандартів та регуляторів
Внутрішня інфраструктура	Тестування мережі	Red Teaming	Моделювання реальних атак для перевірки протоколів реагування на інциденти ІБ
Веб-додатки	Тестування Веб-додатків	Тестування захищеності додатку	Аудит веб-додатків
Конфігурація та	Аналіз конфігурації	Перевірка налаштувань систем	Забезпечення правильної конфігурації та ефективного контролю доступу
Соціальний інженерінг	Соціально інженерне тестування	Фішингові та вішингові кампанії	Підвищення обізнаності персоналу та захист від соціального інженерінгу
	Аналіз безпеки пристроїв IoT	Аналіз протоколів та комунікацій	Виявлення та ідентифікація вразливостей
Фізична безпека	Фізична безпека	Аудит безпеки приміщень та контроль доступу	Забезпечення фізичної безпеки об'єктів та контролю доступу
Інфраструктура хмарних обчислень	Аналіз захисту даних в хмарі	Тестування інфраструктури хмарних обчислень	Захист даних у хмарних сервісах та впровадження ефективних заходів захисту

Запропонована матриця допомагає систематизувати процес вибору методів та сценаріїв тестування відповідно до конкретних об'єктів тестування. Кожен об'єкт має свої особливості та формує відповідні вимоги до тестування, і вибір методів повинен бути адаптований до цих унікальних аспектів для забезпечення максимальної ефективності заходів безпеки.

Висновок

У сучасному світі, де зростаюча кількість загроз та атак на інформаційну безпеку вимагає від підприємств та компаній побудови надійного захисту своїх систем, тестування захищеності стає ключовим елементом стратегії кібербезпеки. Вибір ефективних методів та сценаріїв тестування є важливим завданням для досягнення високого рівня безпеки. З точки зору об'єктів тестування, таких як мережева інфраструктура, операційні системи, програмне забезпечення, веб-додатки, інфраструктура хмарних обчислень, пристрої Інтернету речей та соціально-інженерне тестування, виявляється важливість вибору сценаріїв та методів до кожного з них. Застосування відповідних методів, таких як сканування вразливостей, пентест, аналіз вразливостей, Red teaming та соціально-інженерне тестування, у поєднанні з конкретними сценаріями, дозволяє ефективно виявляти та усувати недоліки та вразливості IT інфраструктури та її компонентів. Забезпечення безпеки охоплює багатоаспектний підхід, який враховує технічні, організаційні та людські аспекти. Тестування захищеності є важливим інструментом у цьому процесі, який дозволяє не лише виявляти вразливості, а й розробляти стратегії для їх усунення та попередження подібних проблем у майбутньому.

У статті надано рекомендації щодо вибору методів та сценаріїв тестування з урахуванням конкретних об'єктів, визначаючи основні цілі для кожного з них. Гнучкість та адаптивність у виборі методів стають ключем до успішного забезпечення безпеки, адже кожна організація має свої унікальні характеристики та потреби. Отже, впровадження комплексної програми тестування захищеності, спрямованої на різні об'єкти, є важливим етапом у забезпеченні стійкості інформаційної інфраструктури та захисті від сучасних кіберзагроз.

Перелік посилань

1. Руденська, Г. В. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, No 1(71), 2021. С. 93-98. https://doi.org/10.33099/2304-2745/2021-1-71/93-98

2. Стефінко, Я. Я., & Піскозуб, А. З. (2014). Використання відкритих операційних систем для тестування на проникнення в навчальних цілях. Вісник Національного університету Львівська політехніка. Комп'ютерні системи та мережі, (806), 258-263.

3. Kalchenko, V. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем / V. Kalchenko // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2018. – Т. 4 (50). – С. 109-114. – doi:https://doi.org/10.26906/SUNZ.2018.4.109.

4. Якименко, Ю., Рабчун, Д., Мужанова, Т., Запорожченко, М., & Щавінський, Ю. (2023). Технічний аудит захищеності інформаційно - телекомунікаційних систем підприємств. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(20), 45–61. https://doi.org/10.28925/2663-4023.2023.20.4561

5. Стеценко, І. В., & Савчук, В. В. (2021). Метод автоматизації тестування на проникнення вебатак. Технічні науки та технології, (1(19), 098–103. https://doi.org/10.25140/2411-5363-2020-1(19)-98-103

6. "Penetration testing execution standard". URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

7. "OWASP Web Security Testing Guide" URL: https://owasp.org/www-project-web-security-testing-guide/

8. Drahuntsov R., Rabchun D. Potential disguising attack vectors on security operation centers and siem systems. Cybersecurity: Education, Science, Technique. 2021. 2(14). p. 6-14. https://doi.org/10.28925/2663-4023.2021.14.614

9. Bacudio, Aileen & Yuan, Xiaohong & Chu, Bill & Jones, Monique. An Overview of Penetration Testing. International Journal of Network Security & Its Applications. 2011. № 3. pp.19 - 38. DOI:10.5121/ijnsa.2011.3602

10. Jai Narayan Goel, B.M. Mehtre, Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology, Procedia Computer Science. 2015. Vol. 57. pp. 710-715, https://doi.org/10.1016/j.procs.2015.07.458

11. Мужанова, Т. М., Лавровський, І. М. Аналіз сучасних засобів для тестування на проникнення. Сучасний захист інформації. 2023. 2(54). с. 35–40. https://doi.org/10.31673/2409-7292.2023.020005

Надійшла: 12.11.2023 Рецензент: д.т.н., професор Гайдур Г.І.