DOI: 10.58254/viti.6.2024.22.264

УДК 681.35

Черниш Ю. О. ORCID: 0000-0002-6626-5656 (ВІТІ ім. Героїв Крут)
канд. техн. наук Хусаінов П. В. ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
Терещенко Т. П. ORCID: 0000-0002-9659-7897 (ВІТІ ім. Героїв Крут)

ПРИЙНЯТТЯ РІШЕНЬ В ПРОЦЕСІ ПОШУКУ ВРАЗЛИВОСТІ SERVER-SIDE WEB APPLICATION

Процес пошуку вразливості складається з трьох етапів. На першому етапі здійснюється ідентифікація дефекту програмних та програмно-апаратних компонентів з оцінкою їх придатності для експлуатації. Другий етап присвячений вибору існуючого або розробці нового експлойту для ідентифікованого дефекту. На третьому етапі відбувається налагодження зручності використання та надійності експлойту. Вразливість (vulnerability) системи об'єкта кіберзахисту до здійснення негативного технічного ефекту (negative technical impact) завжди базується на експлуатації її дефектів. Ідентифікація дефекту з оцінкою придатності до застосування є багатоетапним процесом вибору рішення в умовах невизначеності. Ефективність процесу пошуку дефекту можна підвищити на основі застосування теорії прийняття рішень.

Ідея полягає у зменшенні невизначеності, використовуючи інформаційну модель для пошуку вразливості із можливістю її кількісного аналізу. Для кількісного аналізу застосовуються класичні критерії вибору рішень в умовах невизначеності. Інформаційна модель є ієрархічною, має чотири рівні та включає чотири типи елементів. Перший рівень складається з методів Initial Access, другий – з категорій вразливості Web Application. Третій та четвертий рівень оцінки, відповідно, дефектів та вразливості компонентів.

Доцільність, раціональність та обґрунтованість рішень з пошуку дефектів базується на застосуванні апробованих джерел експертного досвіду світового рівня. Так, Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) визначає, системи класу Server-side Web Application привабливим для хакерів об'єктом атак з найбільшою середньою кількістю потенційних дефектів у складі принаймні трьох компонентів: Web Server, Web Application Server, DBMS Server. Для з'ясування розподілу дефектів Server-side Web Application за характерними класами необхідно скористатися Open Worldwide Application Security Project (OWASP), для детального ознайомлення з ними – Common Weakness Enumeration (CWE). Застосування National Vulnerability Database (NVD) та Common Vulnerabilities and Exposures (CVE) доповнює оцінку знайденого дефекту.

Ключові слова: *прийняття рішень, пошук вразливостей, об'єкт кіберзахисту*

Y. Chernysh, P. Khusainov, T. Tereshchenko. Decision Making in the Searching Weakness Process of Server-Side Web Application.

The vulnerability search process consists of three stages. At the first stage, the weakness of software and firmware components is identified and their suitability for exploitation. The second stage is devoted to choosing an existing or developing a new exploit for the identified weakness. The third stage configures the usability and reliability of the exploit for the identified vulnerability. The vulnerability of the system of the cyber protection object to negative technical impact is always based on the exploitation of its defects. Weakness identification with applicability assessment is a multi-stage process of choosing solutions under conditions of uncertainty. The efficiency of the weakness search process can be improved by using decision making theory.

The idea is to reduce uncertainty by using an information model to search for weakness and to make it possible to process it quantitative analysis. For quantitative analysis, classical criteria for choosing solutions under uncertainty conditions were used. The information model is a hierarchy, has four levels and includes four types of elements. First level consists a techniques of Initial Access. First level consists a techniques of Initial Access, second – of category wekness Web Application. The third and fourth levels of assessment, respectively, of weaknesses and vulnerabilities.

The expediency, rationality and reasonableness of solutions for finding defects is based on the application of proven sources of world-class expert experience. Thus, Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) defines Server-side Web Application class systems as an attractive attack target for hackers with the highest average number of potential defects in at least three components: Web Server, Web Application Server, DBMS Server. To find out the distribution of Server-side Web Application defects by characteristic classes, it is necessary to use the Open Worldwide Application Security Project (OWASP), for a detailed study of them - Common Weakness Enumeration (CWE). The application of the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE) complements the evaluation of the found defect.

Keywords: *decision making, searching vulnerabilities, cyber protection object.*

Постановка завдання. Пошук вразливості системи (об'єкта кіберзахисту) є послідовним та багатоетапним процесом прийняття рішень, який розглядається у контексті можливостей застосування тактик, технік, процедур *Adversarial Tactics*, *Techniques & Common Knowledge (ATT&CK)*. Організація пошуку та виявлення потенційної вразливості здійснюється власником системи (далі – Власник) шляхом оголошення публічної пропозиції. У публічній пропозиції, зокрема, визначається інформація про систему, часові строки, початкові умови, обмеження та порядок звітування про виконання робіт (послуги) дослідником потенційної вразливості (далі – Дослідник). Вразливість системи – властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів [1, 2].

Розглянемо діяльність Дослідника за умови його неприналежності до множини користувачів системи, розташування поза адміністративними межами інфраструктури об'єкта кіберзахисту, а також без полягання на дію фактора "соціальної інженерії" стосовно легітимних користувачів. Процес пошуку потенційної вразливості складається з трьох послідовних етапів. На першому етапі здійснюється ідентифікація дефекту (проєктування, реалізації та/або налаштування) програмних (програмно-апаратних) компонентів з оцінкою її придатності для експлуатації вразливості системи (об'єкта кіберзахисту). Другий етап присвячений вибору існуючого або розробці нового експлойта для ідентифікованого дефекту. На третьому етапі відбувається налагодження працездатності та надійності (у системному оточенні) програмної реалізації експлойта для ідентифікованого (і найбільш перспективного, з точки зору Дослідника) дефекту системи (об'єкта кіберзахисту).

На кожному з етапів вирішення задачі пошуку потенційної вразливості Дослідник знаходиться під впливом невизначеності. Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення можуть бути:

неможливість точного передбачення наслідків рішень;

неможливість повторення або експериментальної перевірки рішення;

особа, яка приймає рішення (ОПР) немає можливості контролю всіх факторів;

наявність множини альтернативних рішень та необхідність вибору одного з них;

низька якість початкової інформації формулювання задачі та вибору рішення.

На підставі викладеного, пропонується розглянути підхід до інформаційного забезпечення вибору рішення в умовах невизначеності Дослідником потенційної вразливості компонентів *Server-Side Web Application* системи (об'єкта кіберзахисту) у контексті науково-методичного апарату прийняття рішень.

Аналіз публікацій. Тактики (тактичні цілі) *ATT&CK for Enterprise* уособлюють експертні знання про відношення понять "ціль – спосіб – результат" для кожного з кроків можливих сценаріїв кібератаки. Доведення Дослідником вразливості системи (об'єкта кіберзахисту) на предмет можливості її компрометації цілком відповідає досягненню тактичної цілі (тактики) *Initial Access* з використанням, принаймні, однієї з десяти незалежних технік (методів, способів). Вибір Дослідником техніки (методу, способу дії) досягнення тактичної цілі (тактики) *Initial Access* обумовлено початковим умовам задачі [3].

Вразливість (*vulnerability*) системи (об'єкта кіберзахисту) призводить до нав'язування йому непередбаченого негативного технічного впливу (*negative technical impact*). Іншими словами, нав'язування негативного технічного впливу базується на можливості непередбаченого використання (експлуатації) певного дефекту (*weakness*) програмних, апаратних, програмно-апаратних чи системних компонентів, які при певних умовах призводять до вразливого стану (вразливості) системи (об'єкта кіберзахисту). Атака (*attack*) –

спроба експлуатації дефекту системи з метою нав'язування їй вразливого стану для прояву негативного технічного ефекту шляхом застосування програмного експлойта (*exploit*) [4].

Дефекти програмних (програмно-апаратних) компонентів, які при певних умовах можуть призвести до вразливості *Server-side Web Application* за версією *Top 10 Web Application Security Risks*, розподілені на десять категорій [5].

Формулювання мети статті. Найбільш широкий спектр практичних задач діяльності Дослідника потенційної вразливості системи (об'єкта кіберзахисту) обмежений необхідністю дотримання таких умов:

відсутність або найменший рівень повноважень при спробі експлуатації дефекту будь-якого програмного (програмно-апаратного) компонента системи (об'єкта кіберзахисту);

відсутність фізичного доступу до апаратних засобів системи (об'єкта кіберзахисту);

відсутність можливостей або недоцільність впливу на ланцюги постачання програмних (програмно-апаратних) компонентів, апаратних засобів для інфраструктури;

відсутність можливостей або недоцільність використання способів соціальної інженерії стосовно легітимних користувачів системи (об'єкта кіберзахисту);

підключення інфраструктури системи (об'єкта кіберзахисту) до Інтернет або інших глобальних систем передачі даних.

За таких умов діяльність Дослідника, щодо компрометації системи (об'єкта кіберзахисту), повинна бути спрямована на досягнення тактичної цілі (тактики) *Initial Access* і є застосуванням техніки (методу, способу дії) *Exploit Public-Facing Application.* При цьому найбільш популярним видом організації інфраструктури *Public-Facing Application* є *Server-Side Web Application* [6].

Ідентифікація Дослідником дефекту (проєктування, реалізації та/або налаштування) програмних (програмно-апаратних) компонентів з оцінкою його придатності для експлуатації вразливості *Server-Side Web Application* багатокроковий процес з багатьма актами вибору рішень в умовах невизначеності. Зменшення впливу невизначеності і, відповідно, підвищення ефективності процесу пошуку Дослідником потенційної вразливості системи (об'єкта кіберзахисту), зокрема, у компонетах *Server-Side Web Application* може бути зроблено на основі науково-методичного апарату прийняття рішень. Ключовими елементами запропонованого результату дослідження: структура інформаційної моделі предметної області та забезпечення її придатності для обробки із застуванням відомих критеріїв (мінімаксний, Лапласа, Севіджа, Гурвіца, Ходжа-Лемана, Гермейера).

Основна частина. Прийняття рішень (ПР) людиною завжди є результатом складних психологічних процесів. Розрізняють функціонально-динамічний та логіко-психологічний підхід до дослідження процесів ПР [7].

Функціонально-динамічний підхід спрямований на дослідження комплексу психологічних механізмів ПР. Розумова діяльність людини розглядається як багаторівнева сукупність взаємозв'язаних процесів психофізичного, психологічного, гносеологічного та програмного характеру. Основні форми розумової діяльності: емпіричне, аксіоматичне, діалектичне. Емпіричне мислення базується на узагальненні попереднього досвіду, аксіоматичне – на застосуванні початкових знань про правила вирішення задачі. Діалектичне мислення є вищою формою психічних процесів людини, забезпечує позитивний прояв багатоваріантності, адаптації, самоорганізації, вибір рішення в умовах як повної, так і неповної інформації для ПР.

Логіко-психологічний підхід базується на представленні процесів ПР у формі послідовності етапів: постановки задачі; здобуття та обробка інформації для ПР; аналіз та ідентифікації проблемної ситуації; вироблення множини альтернативних рішень; вибір рішення; реалізація рішення. Сукупність дій, щодо забезпечення етапів ПР, розглядається

як композиція множин операцій інформаційної підготовки ПР, вибору та реалізації рішення (як результату процесів ПР).

Вибір рішення є прерогативою людини і принципово не може мати формального подання. Особа, яка приймає рішення (ОПР) керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями. Прямий чи опосередкований вплив на вибір рішення ОПР можуть мати психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формуються) залежно від конкретних суспільно-історичних умов:

світогляд (система поглядів на суспільство та природу явищ);

інтереси (спрямованість на певні предмети та явища);

здібності (індивідуальні особливості – умови успішного виконання якої-небудь однієї або кількох видів діяльності);

темперамент;

характер;

увага (спрямованість свідомості на певний предмет або діяльність: стійкість, перемикання, розподіл та об’єм).

Традиційними показниками оцінки ефективності широкого спектра процесів людської діяльності є величина середньої тривалості, матеріальні або фінансові витрати. Аналіз особливостей (з урахуванням визначених вище умов) процесу пошуку потенційної вразливості системи (об’єкта кіберзахисту) показав значну залежність від рівня кваліфікації Дослідника щодо реалізації складних форм експлуатації можливих дефектів.

Розрізняють два широких класи задач вибору рішень при неповній інформації про задачу та проблемну ситуацію ПР. Перший клас задач відомий як “прийняття рішень в умовах ризику”, другий – “прийняття рішень в умовах невизначеності”. Неповнота інформації ПР в умовах ризику передбачає існування функцій розподілу ймовірностей для всіх досліджуваних величин, в умовах невизначеності – функції розподілу невідомі або не можуть бути визначені. На практиці невизначеність не означає повної відсутності інформації про задачу. Можуть бути відомими деяка кінцева кількість значень кожної величини, але без відповідних функцій розподілу ймовірностей. Розгляд проблематики вирішення задач прийняття рішень в умовах ризику можливо при наявності експериментальних даних необхідного об’єму для визначення функцій розподілу кожної з досліджуваних величин. Для предметної області пошуку потенційної вразливості системи (об’єкта кіберзахисту) такі властивості непритаманні, що робить недоцільним розгляд умов ризику.

Розглянемо задачу вибору рішення в умовах невизначеності у контексті пошуку потенційної вразливості системи (об’єкта кіберзахисту) на етапі *Initial Access* шляхом *Exploit Public-Facing Application* у формі інфраструктури *Server-Side Web Application* (рис. 1). Успішний результат діяльності Дослідника полягає у доведенні вразливості системи (об’єкта кіберзахисту) шляхом демонстрації нав’язування їй певного негативного технічного впливу.

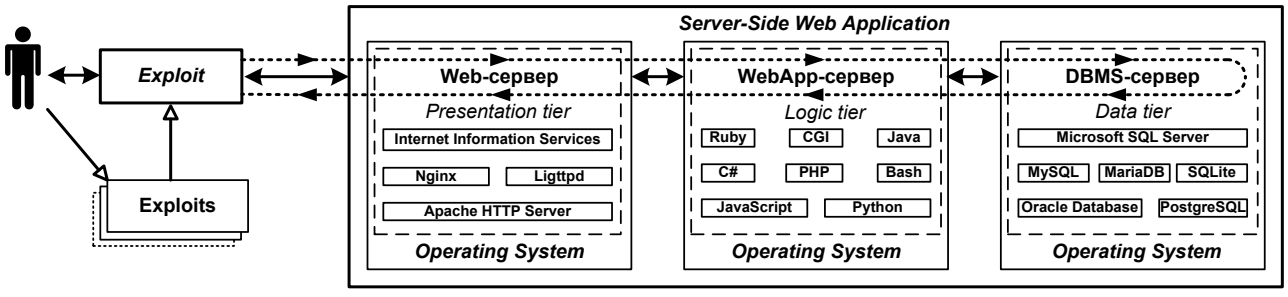

Рис. 1. Інтерпретація задачі пошуку потенційної вразливості *Server-Side Web Application*

Вибір рішень в умовах невизначеності здійснюється із застосуванням критеріїв ПР. Нагадаємо, що критерієм називається необхідна і достатня ознака оцінки або вибору рішення. Розрізняють прості (із застосуванням одного показника) та складні (комбінування кількох показників) критерії. Показник – кількісна характеристика досліджуваного об'єкта, яка має назву та діапазон можливих значень. Критерії ПР відображають більш або менш оптимістичну (песимістичну) суб'єктивну стратегію ОПР при виборі рішення.

Так, традиційними (відображають найбільш широко вживані стратегії) критеріями ПР в умовах невизначеності являються мінімаксний (максиміний), Лапласа (Байеса-Лапласа), Севіджа. Розширення спектра можливих стратегій здійснюється шляхом введення похідних критеріїв ПР Гурвіца, Ходжа-Лемана, Гермейера. Матриця рішень формується на підставі значень оціночної функції. Формалізоване подання оціночної функції відображає залежність між початковими умовами, факторами та результатом, яка визначається у термінах залежних та незалежних змінних. Можливі варіанти значень залежних та незалежних змінних утворюють відповідний набір значень оціночної функції для всієї множини альтернативних рішень. Вибір змінних (залежні, незалежні) та відношень між ними для створення оціночної функції уособлює сутність якості урахування особливостей предметної області ПР.

Обов'язковою умовою доведення вразливості є наявність (існування) працездатної програмної реалізації експлойта. Іншими словами, демонстрація нав'язування негативного технічного впливу шляхом експлуатації дефектів компонентів *Server-Side Web Application* без застосування відповідного експлойта не є дійсною і не може бути здійснена. Множина альтернативних рішень визначається кількістю окремих засобів у колекції вже відомих і/або розроблених експлойтів (exploits), вибір одного з альтернативних рішень – уособлюється з вибором експлойта, що найбільш придатний для практичного нав'язування негативного технічного впливу в інфраструктурі компонентів *Server-Side Web Application.*

Розглянемо проблемні питання вразливості *Server-side Web Application* за версією *The Open Worldwide Application Security Project (OWASP)*. Вразливості *Server-side Web Application* розподілені за категоріями *Top 10 Web Application Security Risks*, а їх формулювання здійснено на основі асоційованих записів *Common Weakness Enumeration (CWE)* та *Common Vulnerabilities and Exposures (CVE)*. Опис категорій *Top 10 Web Application Security Risks* доповнюються оцінками загальної кількості асоційованих записів *CWEs Mapped* та *Total CVEs* зі складу відповідного вектора кількісних характеристик.

1. Контроль доступу (*A01:2021 Broken Access Control*). Стислий опис дефектів: недотримання принципу найменших привілеїв; відсутність (недостатність, некоректність, неправильна реалізація) контролю (перевірки) розширення (зміни) повноважень та використання маркерів доступу (функцій інтерфейсу прикладного програмування, посилань на об'єкти). *CWEs Mapped* = 34. *Total CVEs* = 19013.

2. Криптографічні перетворення (*A02:2021 Cryptographic Failures)*. Стислий опис дефектів: використання менш стійких криптографічних елементів (ключів, векторів ініціалізації, гамм шифру) при неможливості утворення захищеного каналу; відсутність (недостатність, некоректність, неправильна реалізація) контролю (перевірки) автентичності та дійсності (ключів, цифрових підписів, програмних компонентів, ідентифікаційних сертифікатів); надлишкова інформативність реакції компонентів при обробці некоректних (неправильних) комбінацій криптографічних даних. *CWEs Mapped* = 29. *Total CVEs* =3075.

3. Коректність вхідних даних (*A03:2021 Injection*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю та усунення небезпечних (некоректних) вхідних даних (співставлень, інтерпретацій об'єктів); надлишкова інформативність реакції компонентів при обробці некоректних (неправильних) запитів до системи керування базою даних. *CWEs Mapped* = 33. *Total CVEs* = 32078.

4. Безпечний дизайн (*A04:2021 Insecure Design*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур *OWASP Software Assurance Maturity Model (SAMM)* на всіх етапах розробки компонентів *Server-side Web Application* із застосуванням апробованих програмних елементів. *CWEs Mapped* = 40. *Total CVEs* = 2691.

5. Неправильні налаштування безпеки (*A05:2021 Security Misconfiguration*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур безпеки використання хмарних сервісів; використання компонентів (облікових записів) з налаштуваннями за замовчанням; надлишкова інформативність відповідей на некоректні (недоречні) запити до компонентів *Server-side Web Application*; відсутність (недостатність, некоректність, неправильна реалізація) контролю (перевірки) використання актуальних версій оновлень безпеки та аналізу ризиків. *CWEs Mapped* = 20. *Total CVEs* =789.

6. Контроль вразливих та застарілих версій компонентів (*A06:2021 Vulnerable and Outdated Components*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю та оновлення застарілих (неактуальних) версій компонентів *Server-side Web Application*. *CWEs Mapped = 3. Total CVEs* = 0.

7. Ідентифікація та автентифікація (*A07:2021 Identification and Authentication Failures*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю за проявом нестійкості до угадування (прогнозування) можливих значень одноразових паролів (маркерів, ідентифікаторів) та їх повторного використання; критичне порушення логіки процесу двофакторної автентифікації та відновлення паролів; можливість витоку незашифрованих (зашифрованих з використанням нестійких криптографічних алгоритмів) значень паролів через діагностичні повідомлення або у відповідях на некоректні (недоречні) запити до компонентів *Server-side Web Application*. *CWEs Mapped = 22. Total CVEs =3897.*

8. Цілісність компонентів і даних (*A08:2021 Software and Data Integrity Failures*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю автентичності (цілісності, безпечності) даних у складі серіалізованих об’єктів (конвеєрів обробки даних за замовчуванням) та програмних компонентів *Server-side Web Application*, що інсталюються (оновлюються) з репозиторіїв (зовнішніх носіїв). *CWEs Mapped* = 10. *Total CVEs* =1152.

9. Реєстрація подій та моніторинг (*A09:2021 Security Logging and Monitoring Failures*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур реєстрації, обліку, архівування (резервування) та систематичного (ретроспективного) аналізу повідомлень про події функціонування компонентів *Server-side Web Application*; низька інформативність (прагматична цінність) повідомлень про події; неузгодженість форматів повідомлень від різних джерел; потрапляння критичної технологічної інформації (ідентифікаторів, параметрів автентифікації) до вмісту повідомлень про події з можливістю її витоку. *CWEs Mapped* = 4. *Total CVEs* = 242.

10. Коректність запитів *Web*-сервера (*A10:2021 Server-Side Request Forgery*). Стислий опис дефектів: відсутність (недостатність, некоректність, неправильна реалізація) процедур контролю (перевірки) та запобігання (усунення) запитів *Web*-сервера до інших компонентів *Server-side Web Application* від запитів *Web*-клієнта. *CWEs Mapped* = 1. *Total CVEs* = 387.

Сукупність асоційованих з категоріями *Top 10 Web Application Security Risks* записів *CWE* та *CVE* утворюють інформаційну модель вибору рішення в умовах невизначеності в процесі пошуку вразливості *Server-Side Web Application* (рис. 2). Під поняттям “інформаційна модель” зазвичай розуміють організовану за певними правилами сукупність інформації про властивості об’єкта (системи, процесу), який підлягає спостереженню (керуванню). Інформаційна модель повинна відображати залежні та незалежні змінні оціночної функції предметної області, мати раціональну інформативність, форму та композицію.

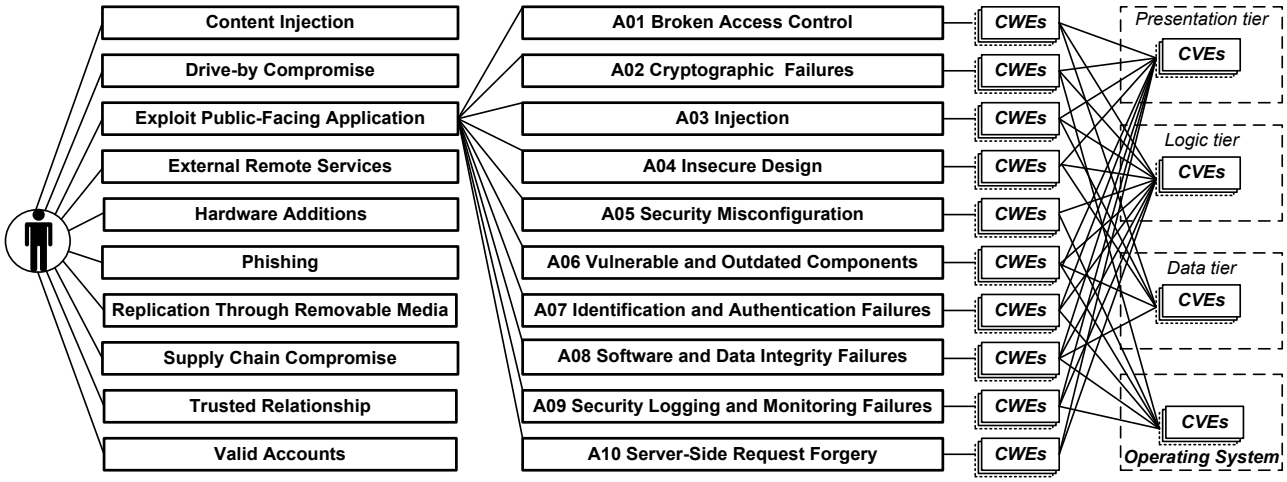

Рис. 2. Порядок утворення інформаційної моделі вибору рішення в задачах пошуку потенційної вразливості *Server-Side Web Application* для тактичної цілі *Initial Access*

Інформаційна модель вибору рішення в процесі пошуку вразливості *Server-Side Web Application* є ієрархією, яка складається з чотирьох рівнів та містить чотири типи інформаційних елементів. На практиці не існує встановленої процедури генерування ієрархій. Зазвичай ця процедура починається з вивчення літератури для збагачення думками. Знайомлячись із чужими працями, ми нібито проходимо через стадію мозкового штурму для складання переліку всіх концепцій, істотних для завдання, незалежно від їхнього співвідношення чи порядку. Далі, здійснюється спроба створення деякої ієрархічної системи понять та відношень між ними на основі застосування таких аксіом:

зв’язані з поняттям інформаційні елементи утворюють незалежні множини;

елементи однієї множини визначають групу елементів рівня ієрархії;

елементи груп різних зв’язаних рівнів ієрархії функціонально впливають один на одного через інтерпретацію відношень між поняттями відповідних незалежних множин;

кожен елемент ієрархії може бути функціонально-зв’язаним з кількома поняттями;

роль елемента відносно іншого, може бути головною, підлеглою або нейтральною.

Розглянемо ієрархію запропонованої інформаційної моделі (відлік рівнів ієрархії здійснюється зліва направо).

Перший рівень ієрархії відображує можливі тактики (способи дії) Дослідника для досягнення тактичної цілі *Initial Access* (за версію *MITRE ATT&CK for Enterprise*). Досягнення тактичної цілі *Initial Access* полягає у нав’язуванні Дослідником виконання власного алгоритму негативного технічного впливу з повноваженнями вразливого програмного компоненту об’єкта кіберзахисту. Досвід історії дослідження фахівцями корпорації *MITRE* відомих кіберінцидентів (кібератак) дозволив визначити десять незалежних методів нав’язування. Вибір способу дії з множини альтернативних варіантів першого рівня ієрархії обумовлені інтерпретацією сформульованих раніше початкових умов процесу пошуку Дослідником потенційної вразливості *Exploit Public-Facing Application*:

відсутність або найменший рівень повноважень суб’єкта доступу до інфраструктури, який керується Дослідником;

відсутність фізичного доступу Дослідника до апаратних засобів інфраструктури;

відсутність можливостей або недоцільність (велика вартість, висока невизначеність досягнення успіху) впливу Дослідника на ланцюги постачання програмних (програмно-апаратних) компонентів та апаратних засобів для інфраструктури;

відсутність у Дослідника можливостей використання способів соціальної інженерії стосовно легітимних користувачів інфраструктури;

суб'єкт доступу, який керується Дослідником, може взаємодіяти з компонентами *Server-Side Web Application* через вхідний маршрутизатор його інфраструктури, політика фільтрації маршрутизатора немає жодних обмежень.

Другий рівень ієрархії відображає множину альтернативних варіантів спрямування зусиль Дослідника в процесі пошуку потенційної вразливості *Server-Side Web Application* за десятьма категоріями *Top 10 Web Application Security Risks*. Числовий ідентифікатор категорії вразливості є порядковою ранговою оцінкою її значущості для компрометації системи компонентів *Server-Side Web Application.* Рангова оцінка визначається на підставі оціночної функції ваги категорії вразливості. Вхідними даними для обчислення значення оціночної функції є сукупність кількісних значень таких часткових показників:

CWEs Mapped (кількість типових дефектів, що мали місце для прояву вразливості);

Max Incidence Rate, Avg Incidence Rate (максимальний та середній процент існуючих *Web Application*-продуктів, які мають дефекти з переліку *CWE* для цієї категорії вразливості);

Max Coverage, Avg Coverage (максимальний та середній процент *Web Application*-продуктів, які мають хоча б один дефект з переліку *CWE* для цієї категорії вразливості відносно всіх *Web Application*-продуктів всіх організацій);

Total Occurrences (загальна кількість ідентифікованих *Web Application*-продуктів, які мають хоча б один дефект з переліку *CWE* для цієї категорії вразливості);

Total CVEs (загальна кількість *CVE* для яких є характерним згадування хоча б одного з переліку *CWE* для цієї категорії вразливості).

Третій рівень ієрархії містить ідентифікатори підмножин записів класифікатора *CWE*, які асоційовані з відповідними категоріями вразливості *Top 10 Web Application Security Risks*. Система оцінки *Common Weakness Scoring System (CWSS)* забезпечує механізм для визначення пріоритетності у дефектів (проєктування, реалізації та/або налаштування) програмних (програмно-апаратних) та апаратних компонентів цільового об'єкта [8, 9]. Значення результуючої оцінки *CWSS* базується на застосуванні трьох груп показників.

Перша, за порядком згадування, група показників *Base Finding metric group* (основні пошукові характеристики дефекту) уособлюють величину ризику визначеного дефекту, впевненість у точності його ідентифікації та достовірність засобів контролю. Значення метрик *Base Finding metric group* визначають:

результат успішної ідентифікації та експлуатації дефекту (*Technical Impact, TI*);

необхідний рівень повноважень для експлуатації дефекту (*Acquired Privilege, AP*);

набутий рівень повноважень після експлуатації дефекту (*Acquired Privilege Layer, AL*);

можливість запобігання експлуатації дефекту на основі використання існуючих захисних механізмів (*Internal Control Effectiveness, IC*);

впевненість у можливості успішної експлуатації дефекту (*Finding Confidence, FC*).

Друга група показників *Attack Surface metric group* (характеристики умов "поверхні" реалізації атаки для експлуатації дефекту) відображає якість бар'єрів (захисних механізмів). Значення метрик *Attack Surface metric group* визначають:

необхідний рівень повноважень суб'єкта атаки для доступу до програмної реалізації функціональних можливостей компонента, що містить дефект (*Required Privilege, RP*);

необхідний рівень повноважень суб'єкта атаки в системному операційному середовищі для успішної експлуатації дефекту (*Required Privilege Layer, RL*);

канал комунікації, який надає суб'єкту атаки доступ до функціональних можливостей результату успішної експлуатації дефекту (*Access Vector, AV*);

надійність процедури захисту доступу до функціональних можливостей результату успішної експлуатації дефекту (*Authentication Strength, AS*);

участь легітимного користувача при експлуатації дефекту (*Level of Interaction, IN*);

поширеність успішної експлуатації дефекту (*Deployment Scope, SC*).

Третя група показників *Environmental metric group* описує характеристики системного операційного оточення компонентів цільового об'єкта, в якому ідентифіковано дефект:

ступінь негативного впливу результату успішної експлуатації дефекту на процеси використання цільового об'єкта за призначенням (*Business Impact, BI*);

ймовірність ідентифікації дефекту суб'єктом атаки (*Likelihood of Discovery, DI*);

ймовірність успішної експлуатації дефекту суб'єктом атаки (*Likelihood of Exploit, EX*);

можливість запобігання експлуатації дефекту з використанням засобів системного операційного оточення компонента, який містить дефект (*External Control Effectiveness, EC*);

частота ідентифікації дефекту даного типу у інших компонентах (*Prevalence, P*).

Розрізняють цільовий, узагальнений, контекстний та агрегований метод застосування *CWSS.* Цільовий метод спрямований на оцінювання окремої вразливості, що була виявлена при розробці конкретного програмного пакета компонентів. Предметом узагальненого методу є клас вразливості незалежно від конкретного програмного пакета. Величина узагальненої оцінки визначається на підставі аналізу прояву класу вразливості у конкретному програмному пакеті компонентів. Узагальнені та цільові оцінки можуть суттєво відрізнятися. Контекстний метод базується на врахуванні особливостей процесів діяльності, системного оточення, ризиків тощо. Цей метод може застосовуватися в комбінації з методами цільового та узагальненого оцінювання або доповнюючи їх. Агрегований метод спрямований на одержання загальної оцінки кількох вразливостей. Хоча агрегування може бути найбільш застосовним для цільового методу, його також можна використовувати для узагальненого оцінювання, цільової та контекстної оцінки.

Четвертий рівень ієрархії відображає розподіл записів *CVE* за компонентами *Server-Side Web Application,* які забезпечують функції *Presentation tier, Logic tier, Data tier* та *Operating System*.

Система оцінки вразливостей *Common Vulnerability Scoring System (CVSS)* базується на застосуванні сукупності чотирьох груп показників. Група показників *Base* (базові) призначена для опису незмінних властивостей у часі та у різних системних середовищах. Група *Threat* (загрози) відображає зміни характеристики з плином часу, а група *Environmental* (оточення) – змінні характеристики з урахуванням особливостей системного операційного середовища. Четверта група показників *Supplemental* (додаткова) застосовується для уточнення характеристик [10-11].

Величина результуючого кількісного значення оцінки *CVSS* визначає серйозність вразливості, яка розраховується на основі стандартизованої формули *CVSS* на основі метрик, утворених відповідно до груп показників *Bas*e, *Threat* та *Environmental*. Базова метрична оцінка (*Base Metrics*) уособлює величину серйозності вразливості як розумний найгірший вплив у будь-якому операційному системному середовищі, незалежно від плину часу. Тимчасові метрики (*Temporal Metrics*) коригують базовий рівень вразливості на основі факторів, які змінюються з часом, наприклад, доступність коду для експлойта. Метрики середовища (*Environmental Metrics*) уточнюють базовий та тимчасовий ступені серйозності до конкретного системного операційного середовища, наприклад, наявність засобів захисту.

Група факторів оцінювання величини *Base Metrics* (*Base metric group*) має внутрішній поділ на метрики можливостей експлуатації вразливості (*Exploitability metrics*) та метрики наслідків впливи (*Impact metrics*). Склад підгрупи *Exploitability metrics*:

вектор атаки (*Attack Vector, AV*);

повторюваність атаки (*Attack Complexity, AC*);

необхідний рівень привілеїв суб'єкта атаки (*Privileges Required, PR*);

необхідність взаємодії з користувачем, який працює в системі (*User Interaction, UI*);

умови масштабування атаки (*Scope, S*).

Показники факторів підгрупи *Impact metrics* відображають прямий наслідок успішної експлуатації вразливості у формі негативного впливу, відповідно, на конфіденційність (*Confidentiality, C*), цілісність (*Integrity, I*) та доступність (*Availability, A*) інформації, яка циркулює в інфраструктурі цільового об'єкта.

Група факторів оцінювання величини *Temporal Metrics* (*Temporal metric group*) призначені для оцінювання поточного стану придатності способів експлуатації вразливості, доступності тексту програмної реалізації цільового компонента для дослідження, здійснення виправлень та існування деяких можливостей обходу захисних механізмів. Склад підгрупи *Temporal metric group*:

показник ймовірності експлуатації вразливості із застосуванням існуючого практичного експлойта (*Exploit Code Maturity, E*);

рівень усунення вразливості (*Remediation Level, RL*);

ступінь впевненості у вразливості та її технічних деталях (*Report Confidence, RC*).

Група факторів оцінювання величини *Environmental Metrics* (*Environmental metric group*) відображає унікальні вимоги щодо впливу вразливості системного операційного середовища на конфіденційність (*Confidentiality Requirement, CR*), цілісність (*Integrity Requirement, IR*) та доступність (*Availability Requirement, AR*) інформації, що циркулює у інфраструктурі цільового об'єкта. Сукупність показників *Environmental metric group* є модифікованим еквівалентом *Base metric group* з урахуванням особливостей цільового об'єкта. Ідентифікатори модифікованих показники мають на початку назви слово *Modified*.

Векторний рядок *CWSS* та *CVSS* є текстовим представленням значень показників у стислій формі. Оцінки *CWSS* і *CVSS* не обов'язково порівнюються. Не всі фактори *CWSS* можна описати символічно за допомогою дискретних значень. Використання *CWSS* та *CVSS,* в умовах невизначеності, обумовлено проявом неповної інформація у звітах про вразливості (не містять усіх відповідних деталей, необхідних для оцінки). Якщо інформація відсутня, застосовується консервативний підхід, який полягає у виборі найбільшої величини оцінок.

Концептуально *CVSS* і *CWSS* дуже схожі. Однак у *CVSS* є деякі важливі переваги та обмеження. Однією з сильних сторін *CVSS* є її простота. Відмінності між *CVSS* та *CWSS*:

CVSS для оцінювання вразливості в інстальованих програмних компонентів;

CVSS розглядає вразливості, які вже виявлені та перевірені;

CWSS можна застосувати до того, як будуть доведені будь-які вразливості;

CVSS не можна масштабувати для оцінки програмного пакета компонентів;

CWSS придатний для оцінювання в умовах невизначеності;

CVSS непридатна до використання за умов неповної інформації;

CWSS надає оцінку дефекту до того як він сприяв вразливості;

CVSS має ухил врахування впливу на фізичну систему;

CWSS має невелике упередження на користь програми, яка містить дефекти;

CVSS може використовуватися як вхідні дані для управління ризиками організації;

CVSS не залежить від постачальника та платформи;

CWSS можуть бути розраховані автоматично.

На практиці оцінки *CVSS* не мають регулярного розподілу, як правило, з перекосом у бік високих оцінок; цілком можливо, що *CWSS* може мати кращий розподіл. Однак, оскільки оцінки *CWSS* можна розрахувати в ранніх сценаріях з низьким рівнем інформації, багато факторів є "тимчасовими" за своєю природою, незалежно від того, до якої групи вони належать. Спрощена модель конфіденційності/цілісності/доступності не забезпечує глибини та гнучкості *CVSS* забезпечує узгодженість, корисну для системних і мережевих адміністраторів, які не є фахівцями, для встановлення пріоритетів вразливості.

Висновки. Запропонований підхід до ПР, в умовах невизначеності, який супроводжує діяльність Дослідника потенційної вразливості, базується на використанні інформаційної

моделі для ПР, яка придатна для обробки із застосуванням критеріїв ПР. Ухил ОПР на більш чи менш оптимістичну (песимістичну) суб’єктивну стратегію досягається застосуванням відповідного критерію ПР. В якості прикладу вирішення задачі розглядається пошук вразливості компонентів інфраструктури *Server-Side Web Application* при виборі Дослідником техніки (способу дії) *Exploit Public-Facing Application* на етапі *Initial Access.*

Подальші дослідження щодо перевтілення науково-методичного апарату теорії ПР в діяльність фахівців з кібербезпеки спрямовані на врахування особливостей відношень між інформаційними елементами *CWSS* та *CVSS.*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про основні засади забезпечення кібербезпеки України”.
2. Постанова Кабінету Міністрів України від 16 травня 2023 року № 497 “Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж”.
3. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.
4. Common Attack Pattern Enumerations and Classifications. URL: https://capec.mitre.org.
5. Open Worldwide Application Security Project. URL: https://owasp.org.
6. Терещенко Т. П., Остапчук В. М., Хусаінов П. В., Черниш Ю. О. Оцінка та запобігання прояву вразливості Server-Side Web Application / за заг. ред. Г. Д. Радзівілова // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць. Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2024. № 5. 240 с. DOI: 10.58254/viti.5.2024. С. 204–214.
7. Герасимов Б. М., Локазюк В. М., Оксіюк О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень: навч. посібник. К.: Вид-во Європ. ун-ту, 2007. 335 с.
8. Common Weakness Enumeration. URL: https://cwe.mitre.org.
9. Common Weakness Scoring System. URL: https://cwe.mitre.org/cwss/cwss_v1.0.1.html.
10. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org.
11. Common Vulnerability Scoring System. URL: https://www.first.org/cvss/.