DOI: 10.58254/viti.8.2025.20.257

УДК 681.35

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)
Череушенко В. Б. ORCID:0009-0006-2839-3637 (ВІТІ ім. Героїв Крут)

ФОРМУВАННЯ АЛЬТЕРНАТИВНИХ СТРАТЕГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ SERVER-SIDE WEB APPLICATION ІЗ ВРАХУВАННЯМ ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ

Тестування на проникнення (penetration testing) є одним із дієвих активних методів зниження ризиків компрометації системи шляхом експлуатації вразливості її програмних компонентів. В Україні поняття "тестування на проникнення" визначено як пошук та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. На сучасному етапі розвитку практики пошуку та виявлення вразливості системи (об'єкта кіберзахисту) цей процес базується на участі фахівця з тестування на проникнення. Понад усе він відповідає за правильне виявлення (доведення існування) вразливості системи (об'єкта кіберзахисту) на основі використання сучасного міжнародного досвіду для здійснення такої діяльності.

До розгляду пропонується постановка наукового завдання на розробку методичного апарату для вибору стратегій дій процесу тестування на проникнення. На основі використання запропонованого методичного апарату сформульовано задачу пошуку та виявлення вразливості системи (об'єкта кіберзахисту) за мінімальний (прийнятний) час за умови прийнятної (мінімальної) величини витрат ресурсів та визначеної ймовірності правильного виявлення вразливості системи (об'єкта кіберзахисту).

Оприлюднюються основні положення розробленого методичного апарату для вирішення задач тестування на проникнення: семантична мережа структурно-казуальних відношень між задачами досягнення тактичних цілей (тактик); обґрунтування на основі застосування підходів The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology, таксономій ATT&CK, CAPEC, CVE, CWE; інтерпретація в контексті логіко-психологічної схеми прийняття рішень; орієнтований граф граф-схеми дій фахівця; модель формування множини альтернативних стратегій. Надається змістовний метод стратегії дій фахівця з тестування на проникнення Server-Side Web Application системи (об'єкта кіберзахисту, в процесі якого здійснюється досягнення тактичної цілі (тактики) Initial Access на основі вирішення задачі Exploit Public-Facing Application.

Ключові слова: *тестування на проникнення, вибір рішень, альтернативні стратегії дій.*

P. Khusainov, T. Tereshchenko, V. Chereushenko. Formulation of alternative strategies for testing Server-Side Web Application penetration, taking into account the reduction of uncertainty

Penetration testing is one of the most effective active methods of reducing the risk of system compromise by exploiting vulnerabilities in its software components. In Ukraine, the concept of "penetration testing" is defined as the search for and identification of potential vulnerabilities in information (automated), electronic communication, information and communication systems, and electronic communication networks. At the current stage of development of the practice of searching for and identifying system vulnerabilities (cyber protection objects), this process is based on the participation of a penetration testing specialist. Above all, he is responsible for the correct identification (proving the existence) of system vulnerabilities (cyber protection objects) based on the use of modern international experience for carrying out such activities.

We propose to consider setting a scientific task to develop a methodological framework for selecting strategies for the penetration testing process. Based on the use of the proposed methodological apparatus, the task of searching for and detecting vulnerabilities in a system (cyber protection object) in a minimum (acceptable) amount of time has been formulated, subject to acceptable (minimum) resource costs and a defined probability of correctly detecting vulnera The main provisions of the developed methodological apparatus for solving penetration testing tasks are published: a semantic network of structural-causal relationships between tasks for achieving tactical goals (tactics); justification based on the application of The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology, ATT&CK, CAPEC, CVE, CWE taxonomies; interpretation in the context of a logical-psychological decision-making scheme; an oriented graph of a specialist's action scheme; a model for forming a set of alternative strategies. A meaningful method of a specialist's strategy for testing the penetration of a Server-Side Web Application system (cyber protection object) is provided, in the process of which the tactical goal (tactics) of Initial Access is achieved based on solving the Exploit Public-Facing Application task.bilities in the system (cyber protection object).

Keywords: *penetration testing, decision selection, alternative action strategies.*

Постановка завдання. Тестування на проникнення уособлює комплекс заходів оцінки захищеності об’єкта кіберзахисту від кіберзагроз, спрямований на доведення або заперечення твердження про можливість компрометації системи (об’єкта кіберзахисту) із застосуванням способів та засобів здійснення кібератак [1; 2]. Досягнення цілі тестування на проникнення уособлює методичний базис для здійснення:

пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж на основі публічної пропозиції [3];

перевірки ефективності здійснення заходів кіберзахисту об’єкта критичної інфраструктури від зовнішнього втручання не рідше одного разу на рік [4];

підтвердження відновлення штатного функціонування систем/мереж аудиту та перегляду діяльності, пов’язаної із реагуванням на кіберінциденти/кібератаки з використанням сил та засобів Держспецзв’язку або інших сил кіберзахисту [5].

Доведення можливості компрометації системи (об’єкта кіберзахисту) свідчить про її вразливість. Вразливість системи (об’єкта кіберзахисту) – властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи (об’єкта кіберзахисту), здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів. Дослідник потенційної вразливості (далі – Дослідник) – фізична або юридична особа, яка здійснює пошук потенційної вразливості системи. Застосування Дослідником тактик, методів (способів, технік) та засобів кібератак на відміну від діяльності зловмисника (хакера, суб’єкта кібератаки) здійснюється з дотриманням певного етичного кодексу правил, зокрема, відмови від нанесення реальної шкоди (через порушення режиму функціонування, знищення, шифрування інформації і т. ін.).

На підставі викладеного пропонується змістовна постановка наукової задачі на розробку науково-методичного апарату вибору стратегії дій Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту), яка повинна забезпечувати:

мінімальну або допустиму величину часових витрат;

допустиму або мінімальну величини витрат ресурсів;

гарантовану ймовірність правильного виявлення вразливості за визначений час;

мінімальний вплив невизначеності.

Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення Дослідником у процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту) можуть бути: неможливість точного передбачення наслідків рішень; неможливість повторення або експериментальної перевірки рішення; особа, яка приймає рішення, не має можливості контролю всіх факторів; наявність множини альтернативних рішень та необхідність вибору одного з них; низька якість початкової інформації постановки задачі та вибору рішення. Аналіз результатів експериментальних випробувань показав, що стратегії діяльності Дослідника, які спрямовані на виявлення вразливості *Server-Side Web Application,* мають найменший вплив невизначеності.

Аналіз публікацій. Для ознайомлення з принципами будови, категоріями вразливості *Server-side Web Application* (об’єкта кіберзахисту) з оцінками *Common Weakness Scoring System* та *Common Vulnerability Scoring System*, а також і методикою застосування критеріїв зменшення невизначеності при виборі варіанту стратегії в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту) за величною часових витрат необхідно звернутися до [6–8]. Науково-методичний апарат, використаний для створення моделі формування множини альтернативних стратегій діяльності Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту), деталізується в [9; 10].

Формулювання мети статті. Метою статті є викладення постановки та напрямку вирішення наукової задачі вибору стратегії дій Дослідника в процесі пошуку та виявлення

вразливості системи (об'єкта кіберзахисту) на основі множини альтернативних стратегій за показниками величини часових витрат, величини витрат ресурсів та ймовірності правильного виявлення вразливості за визначений час. Центральним елементом викладення є обґрунтування моделі формування множини альтернативних стратегій діяльності Дослідника на основі зваженого ймовірнісно-часового орієнованого графа.

Основна частина. Виявлення вразливості системи (об'єкта кіберзахисту) є результатом психологічної діяльності Дослідника та її головною ціллю. Поняття "ціль" уособлює очікуваний (ідеалізований, уявний) результат психологічної діяльності людини на певному інтервалі часу. Формулювання цілі (постановка задачі) є наслідком певного стимулу змінити поточну ситуацію у потрібному напрямку з урахуванням набутого досвіду. Постановка задачі характеризується використанням кількісних даних (параметрів) очікуваного результату на відміну від більш ідеалізованого (уявного) формулювання цілі. Під поняттям "ситуація" розглядається деякий узагальнений стан (актуальний опис поточного стану предметної області, визначений на певному часовому інтервалі), що змінюється за результатом вирішення задачі. Вирішення задачі у загальному вигляді є послідовністю дій щодо формування варіантів рішення, вибору та реалізації одного з них.

Вибір рішення є прерогативою людини і принципово не може мати формального подання. Особа, яка приймає рішення (Дослідник потенційної вразливості), керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб'єктивними уявленнями, судженнями, емоціями. Прямий чи опосередкований вплив на вибір особи, яка приймає рішення, може мати психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формуються) залежно від конкретних суспільно-історичних умов: світогляду (система поглядів на суспільство та природу явищ); інтересів (спрямованість на певні предмети та явища); здібностей (індивідуальні особливості – умови успішного виконання якої-небудь однієї або кількох видів діяльності); темпераменту; характеру; уваги (спрямованість свідомості на певний предмет або діяльність: стійкість, перемикання, розподіл та об'єм).

Розрізняють два широких класи задач вибору рішень при неповній інформації про задачу та проблемну ситуацію. Перший клас задач відомий як "прийняття рішень в умовах ризику", другий – "прийняття рішень в умовах невизначеності". Неповнота інформації для вибору рішення 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 відома деяка кінцева кількість значень кожної величини, але без відповідних функцій розподілу ймовірностей.

Етап реалізації рішення полягає у виконанні операцій за планом обраної стратегії дій на етапі вибору рішення досягнення цілі (вирішення задачі). Реалізація рішення зазвичай здійснюється в умовах можливого прояву внутрішніх та зовнішніх дестабілізуючих факторів, що викликає певну невідповідність фактичного результату очікуваному. Визначення такої невідповідності, аналіз причин та вироблення рекомендацій щодо її усунення (зменшення) на наступному циклі управління уособлює етап оцінювання результату (вирішення задачі).

Сформулюємо наукову задачу пошуку та виявлення Дослідником потенційної вразливості (об'єкта кіберзахисту). *Необхідно* довести існування вразливості (об'єкта кіберзахисту) за найменшу $min\,T$ або граничну величину $T \le T_{\circ}$ сумарних часових витрат при обмеженні на витрату ресурсів $C \le C_{\circ}$ або їх мінімальну величину $min\,C$ за умови, що ймовірність правильного виявлення вразливості системи (об'єкта кіберзахисту) буде не менше певного граничного значення$P(T \le T_{\circ}) \ge P_{\circ}$.

Вирішення сформульованої наукової задачі полягає у виборі такого варіанта стратегії діяльності Дослідника (потенційної вразливості) в процесі пошуку та виявлення потенційної вразливості (об'єкта кіберзахисту) з множини альтернативних стратегій A, при якому буде

забезпечено $min\,T$при обмеженні $C \le C_\circ$ або $min\,C$ при обмеженнях $T \le T_\circ$ із забезпеченням $P(T \le T_\circ) \ge P_\circ$. Під поняттям "стратегія дій Дослідника" уособлюється один із можливих варіантів виконання Дослідником дій для забезпечення послідовності операцій рішення задач, спрямованих на досягнення головної цілі у формі доведення вразливості системи (об'єкта кіберзахисту) через досягнення сукупності тактичних цілей (тактик).

Потужність множини A визначається можливістю Дослідника здійснити застосування всієї сукупності комбінацій технік (методів, способів) кібератак для одержання результатів (вирішення задач) досягнення тактичних цілей (тактик) і доведення факту існування вразливості як головного результату процесу пошуку та виявлення вразливості системи (об'єкта кіберзахисту). Методичний базис предметної області (відношення між поняттями, що утворюють єдину основу для одноманітного розуміння рішення задачі), який обумовлює утворення множини альтернативних стратегій A діяльності Дослідника:

The Cyber Kill Chain – узагальнена послідовна схема кібератаки спрямована на нав'язування виконання шкідливого програмного засобу [11];

The Unified Kill Chain – узагальнена послідовна схема кібератаки за трьома циклічними фазами (*In, Through, Out*) її реалізації [12];

Ethical Hacking Methodology – схема кібератаки за методологією *Certified Ethical Hacker (CEH)* [13];

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) – тактики (*tactics*), технік (*techniques*) кібератак на системи *Enterprise, Industrial Control System, Mobile* [14];

Common Attack Pattern Enumerations and Classifications (CAPEC) – система відношень понять абстрактного, стандартного та конкретно-технологічного рівня деталізації опису типових (шаблонних) механізмів технік (методів, способів) кібератак [15].

При ієрархічному представленні структурних відношень між поняттями утворюється деревоподібний граф, при мережевому представленні – граф типу "мережа". Структурні відношення понять застосовуються для визначення ієрархій або мереж понять, казуальні – причинно-наслідкові зв'язків (ланцюгів зв'язків), семантичні – для всіх інших можливих типів відношень. Семантична мережа є найбільш повною моделлю представлення знань про предметну область з використанням різнотипних відношень.

Діяльність людини характеризується деревом цілей. Дерево цілей є відображенням декомпозиції головної цілі в систему часткових цілей. Коренева вершина ієрархічного графа дерева цілей асоціюється з головною ціллю, вузлові вершини – з проміжними (частковими, тактичними) цілями, кінцеві (термінальні) вершини є відображенням первинних (елементарних) цілей. Лінійно-впорядкована послідовність дій людини спрямована на досягнення головної цілі, будемо називати її траєкторією діяльності.

Траєкторія діяльності утворюється сукупністю структурованих казуальних відношень, що визначають просування до головної цілі від первинних (елементарних) через проміжні (часткові, тактичні). Типовим фрагментом траєкторії діяльності є частково-впорядкована послідовність дій досягнення (головної, проміжної, первинної) цілі з деякої фіксованої початкової ситуації. Така частково-впорядкована послідовність дій розпочинається від перебування у відомому стані початкової ситуації, подібна казуальному сценарію та може розглядатися у контексті застосування стереотипних знань.

При використанні на семантичній мережі тільки структурних відношень вона перетворюється у мережу класифікації, при використанні тільки казуальних відношень – у сценарій. Сценарій – формалізований опис стандартної послідовності взаємозв'язаних фактів типової ситуації предметній області, послідовності дій або процедур досягнення цілей, тобто стереотипних знань. Під поняттям "стереотипні знання" розглядається такий опис ситуації у предметній області у формі послідовності фактів опису, який дозволяє передбачати та відновлювати значення пропущених фактів. Казуальний сценарій є типовою послідовністю дій (процедур), що підлягає структуризації у формі казуального ланцюжка (сценарію), в якому

кожна чергова дія створює умови для здійснення наступної. Сценарій класифікації призначений для структурованого відображення результатів узагальнення знань про предметну область. Для структуризації знань в сценаріях класифікації найчастіше застосовуються відношення типу “причина – наслідок”, “ціль – підціль”, “частина – ціле”, “засіб – результат”, “інструмент – дія” і т.д. Під поняттям “узагальнення” розглядається процес здобуття нових знань, які пояснюють і класифікують вже відомі факти предметної області, а також можуть передбачувати нові. Узагальнення передбачає застосування моделей класифікації, формування понять, розпізнавання образів, виявлення закономірностей. Здатність людини до узагальнення є базисом для одержання нових знань.

Успішним результатом доведення Дослідником існування вразливості є здійснення запуску на виконання демонстраційної шкідливої програми в обчислювальному середовищі будь-якого компонента (об’єкта кіберзахисту) з повноваженнями авторизованого користувача (рис. 1). Під поняттям “демонстраційна шкідлива програма” розглядається спеціальна форма реалізації в принципі широкого спектра функціональних можливостей абстрактної шкідливої програми без деструктивної частини її алгоритму (*payload*).

Казуальний сценарій пошуку та виявлення Дослідником потенційної вразливості системи (об’єкта кіберзахисту) розпочинається (рис. 1, П) з вирішення задач досягнення тактичної цілі (тактики) *Reconnaissance* (за методологією *ATT&CK*). Тактична ціль *Reconnaissance* полягає в одержанні (здобутті) Дослідником якомога повної інформації про систему (об’єкт кіберзахисту). Зокрема, визначається призначення, завдання, умови та штатний режим функціонування системи (об’єкта кіберзахисту), складові її інфраструктури (інтерфейси, структура мережного сегмента, сервіси, операційні системи і т.д.).

Успішним результатом досягнення тактичної цілі *Reconnaissance* є одержання (здобуття) Дослідником повної інформації для вирішення задач досягнення тактичної цілі (тактики) *Resource Development*, спрямованої на:

вибір методу (способу, техніки) запуску демонстраційної шкідливої програми шляхом вирішення задач досягнення тактичної цілі (тактики) *Initial Access*;

врахування можливості виконання демонстраційної шкідливої програми у складі вразливого компонента системи (об’єкта кіберзахисту) шляхом вирішення задач досягнення тактичної цілі (тактики) *Execution*;

забезпечення достатності умов для технічного ефекту доведення уразливості системи (об’єкта кіберзахисту) внаслідок виконання демонстраційної шкідливої програми шляхом вирішення задач досягнення тактичної цілі (тактики) *Penetration Testing Impact* (рис. 1, К).

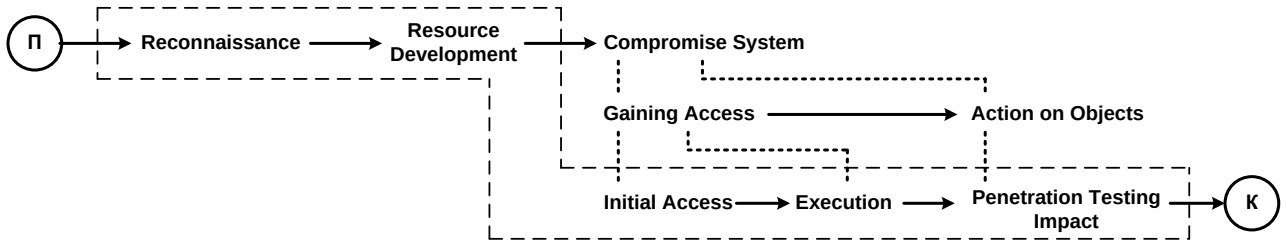

Рис. 1. Семантична мережа структурно-казуальних відношень цілеспрямованої діяльності Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту)

Для формування повного уявлення про предметну область семантична мережа структурно-казуальних відношень процесу пошуку та виявлення вразливості системи (об’єкта кіберзахисту) доповнена такими означеннями та співставленнями:

початок фази *Compromise System* за методологією *The Unified Kill Chain* та фази *Gaining Access*, відповідно, за методологією *CEH* співвідноситься з початком вирішення задач досягнення тактичної цілі (тактики) *Initial Access*;

початок фази *Action on Objects* за методологією *CEH* співвідноситься з початком вирішення задач досягнення тактичної цілі (тактики) *Penetration Testing Impact.*

Логіко-психологічна схема вирішення задачі за участю людини, яка приймає рішення (Дослідник потенційної вразливості), у загальному вигляді є послідовністю етапів інформаційної підготовки, вибору та реалізації рішення задачі. Етап інформаційної підготовки рішення уособлює сукупність операцій здобуття, обробки, аналізу інформації для ідентифікації ситуації вироблення множини альтернативних рішень.

Функціонально-динамічний підхід спрямований на дослідження комплексу психологічних механізмів вибору рішення людиною. 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 вибору рішення.

Розглядаючи представлену семантичну мережу структурно-казуальних відношень предметної області як процес вирішення задачі пошуку та виявлення вразливості системи (об’єкта кіберзахисту) за участю людини (Дослідника), необхідно зазначити (рис. 2):

загальна тривалість вирішення задач досягнення тактичної цілі (тактики) *I.Reconnaissance* справедливо проінтерпретувати як етапи *інформаційної підготовки* і *вибору рішення*, вирішення комплексу взаємопов’язаних задач у процесі послідовного досягнення тактичних цілей (тактик) *II.Resource Development, III.Initial Access, IV.Execution, V.Penetration Testing Impact* як чотири послідовних фази етапу реалізації рішення доведення існування вразливості системи (об’єкта кіберзахисту);

можливість повернення до вирішення задач етапів інформаційної підготовки і вибору рішення (*I.Reconnaissance*) при недостатності (неповноті, невизначеності) інформації для якісної технічної підготовки реалізації рішення (рис. 2, *а*);

наявність принципової невизначеності другої (*III.Initial Access*) та третьої (*IV.Execution*) фаз етапу реалізації рішення обумовлює відповідного повернення та уточнення вирішення задач фази (*II.Resource Development*) технічної підготовки реалізації рішення (рис. 2, *б*).

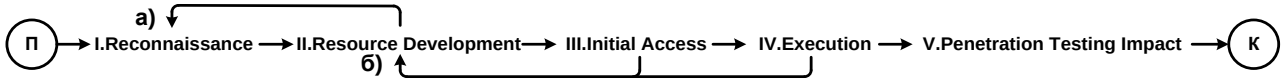

Рис. 2. Логіко-психологічна схема інформаційної підтримки вибору та реалізації рішень Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту)

Відповідно до визначеного напрямку вирішення наукової задачі сформуємо орієнтований граф граф-схеми алгоритму діяльності Дослідника. Вершини орієнтованого графа граф-схеми (рис. 2) уособлюють сукупність задач, спрямованих на досягнення тактичних цілей (тактик), відповідно, на етапах інформаційної підготовки, вибору та реалізації рішення (рис. 3) Дослідником (потенційної вразливості) у процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту).

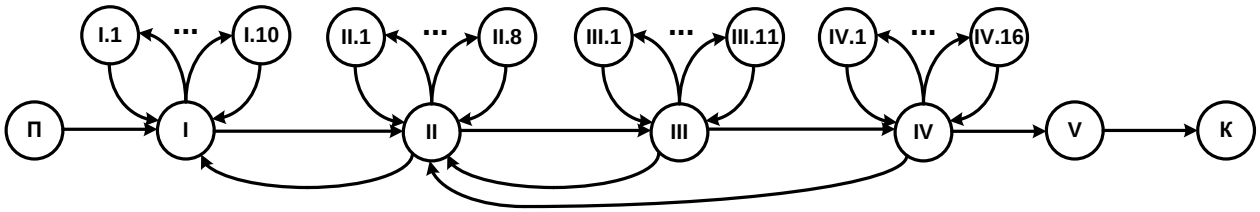

Рис. 3. Орієнтований граф граф-схеми алгоритму діяльності Дослідника в процесі пошуку та виявлення вразливості системи (об’єкта кіберзахисту)

Так, одержання (здобуття) необхідної Досліднику інформації з використанням специфічних засобів визначає десять категорій можливих методів (способів, технік) вирішення задач (рис. 3, I, I.1–I.10) досягнення Дослідником тактичної цілі (тактики) *Reconnaissance* (інформаційна підготовка і вибір рішень):

I.1. *Active Scanning* (сканування);

I.2. *Gather Victim Host Information* (ідентифікація хоста);

I.3. *Gather Victim Identity Information* (ідентифікація персоналій користувачів);

I.4. *Gather Victim Network Information* (ідентифікація мережної інфраструктури);

I.5. *Gather Victim Org Information* (ідентифікація організації);

I.6. *Phishing for Information* (фішинг);

I.7. *Search Closed Sources* (ідентифікація в приватних базах даних);

I.8. *Search Open Technical Databases* (ідентифікація в технічних базах даних);

I.9. *Search Open Websites/Domains* (ідентифікація зв’язаних вебресурсів/доменів);

I.10 *Search Victim-Owned Websites* (ідентифікація персоналій власників вебресурсів).

Відсутність необхідних засобів і/або незабезпечення необхідних умов визначає вісім категорій (рис. 3, II, II.1–II.8) можливих методів (способів, технік) вирішення задач досягнення Дослідником потенційної вразливості тактичної цілі (тактики) *Resource Development* (перша фаза етапу реалізації рішення, технічна підготовка):

II.1. *Acquire Access* (придбання легітимних повноважень);

II.2. *Acquire Infrastructure* (придбання легітимної інфраструктури);

II.3. *Compromise Accounts* (компрометація допоміжних легітимних облікових записів);

II.4. *Compromise Infrastructure* (попередня компрометація допоміжної інфраструктури);

II.5. *Develop Capabilities* (вибір, розробка засобів);

II.6. *Establish Accounts* (легітимізація облікових записів);

II.7. *Obtain Capabilities* (придбання засобів);

II.8. *Stage Capabilities* (розміщення засобів).

Впровадження одного з можливих методів (способу, техніки) запуску демонстраційної шкідливої програми має одинадцять категорій (рис. 3, III, III.1–III.11) вирішення такої задачі досягнення тактичної цілі *Initial Access* (друга фаза етапу реалізації рішення):

III.1. *Content Injection* (під час обробки *Specially Crafted Input* через канал клієнт-серверної комунікації);

III.2. *Drive-by Compromise* (під час обробки *Specially Crafted Input* при завантаженні з неконтрольованого джерела та використання за ініціативою користувача);

III.3. *Exploit Public-Facing Application* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами публічних інформаційних сервісів);

III.4. *External Remote Services* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами сервісів видаленої роботи);

III.5. *Hardware Additions* (під час обробки *Specially Crafted Input* в процесі підключення зовнішнього апаратного засобу за ініціативою користувача або технічного працівника);

III.6. *Phishing* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами оманних інформаційних сервісів та сервісів видаленої роботи за ініціативою користувача);

III.7. *Replication Through Removable Media* (під час обробки *Specially Crafted Input* в процесі підключення зовнішнього носія інформації за ініціативою користувача або технічного працівника);

III.8. *Supply Chain Compromise* (під час обробки *Specially Crafted Input* в процесі підключення апаратного засобу, і/або зовнішнього носія інформації, і/або використання програмного засобу, для якого не визначена безпека походження та надходження за ініціативою користувача або технічного працівника);

III.9. *Trusted Relationship* (під час обробки *Specially Crafted Input* в процесі клієнт-серверної комунікації з програмними засобами інформаційних сервісів та сервісів видаленої роботи, підключенні та використанні апаратного засобу, і/або зовнішнього носія інформації, і/або використання програмного засобу, для якого визначена неконтрольована категорія довіри, у тому числі за ініціативою користувача або технічного працівника);

III.10. *Valid Accounts* (шляхом використання повноважень авторизованого користувача через діючий обліковий запис для запуску на виконання програмних засобів);

III.11. *Wi-Fi Networks* (шляхом використання повноважень авторизованого комунікаційного пристрою бездротової локальної мережі).

Поняття “*Specially Crafted Input*” уособлює сукупність спеціально сформованих даних, які надаються для обробки алгоритму цільового програмного засобу (прикладного чи системного призначення) з метою прояву його вразливості (*vulnerability*) для нав’язування виконання негативного технічного ефекту (*negative technical impact*). Нав’язування негативного технічного впливу базується на можливості непередбаченого використання (експлуатації) певного дефекту (*weakness*) цільового програмного (програмно-апаратного) засобу, який за певних умов призводить до її вразливого стану (вразливості). Спробу експлуатації дефекту цільового програмного (програмно-апаратного) засобу з метою нав’язування йому вразливого стану для прояву негативного технічного ефекту прийнято називати атака (*attack*).

Дані *Specially Crafted Input* можуть бути заздалегідь підготовлені, розташовані у складі легітимного логічного об’єкта (файл даних, завантажувальний модуль, бібліотека, командний рядок, команда протоколу обміну даними, змінна, аргумент, структура, метод класу і т. ін.) та надані для обробки цільовим програмним (програмно-апаратним) засобом (прикладного чи системного призначення) з використанням певного носія інформації або у пам’яті апаратного пристрою. Іншою формою надання даних *Specially Crafted Input* для обробки є їх генерування в процесі комунікації з цільовим програмним (програмно-апаратного) засобом (прикладного чи системного призначення). Спеціальний програмний засіб, який здійснює генерування даних *Specially Crafted Input* в процесі комунікації прийнято називати експлойт (*exploit*).

Відомо понад 938 типових класів дефектів на етапах проєктування, реалізації, введення в експлуатацію, супроводження та завершення роботи програмних (програмно-апаратних) продуктів. Станом на 22.10.2025 обліковано 298 000 вразливостей за одинадцятьма категоріями: *Overflow* (перевищення ємності місць для розміщення даних) – 20 %; *Memory Corruption* (пошкодження пам’яті) – 20 %; *Sql Injection* (поява в запитах мовою *Structured Query Language* зовнішніх даних) – 9 %; *Cross-Site Scripting* (компрометація гіперпосилань) – 25 %; *Directory Traversal* (некоректна інтерпретація шляху у файловій системі) – 5 %; *File Inclusion* (нав’язування оброблення файлу з неконтрольованого джерела) – 1,5 %; *Cross-Site Request Forgery* (підміна суб’єкта доступу за запитом) – 6 %; *XML External Entity* (обробка зовнішніх об’єктів *eXtensible Markup Language*) – 1,5 %; *Server-side Request Forgery* (підміна суб’єкта доступу до довіреного сервісу) – 1,5%; *Open Redirect* (модифікація шляху доступу) – 1,5%; *Input Validation* (порушення фільтрації вхідних даних) – 9 %. Найбільш

характерні наслідки практичної експлуатації вразливості програмних (програмно-апаратних) продуктів та технологічних рішень (за останні 10 років обліковано 69833 кіберінциденти): *Code Execution* (виконання команд, програм із зовнішніх джерел) – 27 %; *Bypass* (подолання захисних механізмів) – 10 %; *Privilege Escalation* (розширення повноважень) – 14 %; *Denial of Service* (припинення функціонування) – 33 %; *Information Leak* (порушення конфіденційності інформації) – 16 %.

Близько 20 % категорій дефектів програм (196 із 940) таксономії *Common Weakness Enumeration (CWE)* та більше ніж 20 % вразливостей (63 324 з 298 000) таксономії *Common Vulnerabilities and Exposures (CVE)* відносяться до *Server-side Web Application* [16; 17].

Врахування придатності вразливого компонента (об’єкта кіберзхаисту) для виконання демонстраційної шкідливої програми визначає шістнадцять категорій (рис. 3, IV, IV.1–IV.16) можливого розширення обсягу технічної підготовки реалізації рішення шляхом необхідності додавання вирішення задач досягнення тактичної цілі (тактики) *Execution* (третя фаза етапу реалізації рішення):

IV.1. *Cloud Administration Command* (адміністрування хмарних сервісів);

IV.2. *Command and Scripting Interpreter* (командні інтерпретатори);

IV.3. *Container Administration Command* (адміністрування середовища контейнерізації);

IV.4. *Deploy Container* (розгортання контейнерної інфраструктури);

IV.5. *ESXi Administration Command* (адміністрування віртуальних машин);

IV.6. *Exploitation for Client Execution* (експлуатація вразливості клієнтських програм);

IV.7. *Input Injection* (використання інтерфейсу користувача);

IV.8. *Inter-Process Communication* (використання інтерфейсу взаємодії процесів);

IV.9. *Native API* (використання інтерфейсу системних викликів операційної системи);

IV.10. *Scheduled Task/Job* (адміністрування сервісів виконання за розкладом);

IV.11. *Serverless Execution* (використання інтерфейсу хмарних сервісів);

IV.12. *Shared Modules* (нав’язування виконання подільних бібліотек);

IV.13. *Software Deployment Tools* (адміністрування сервісів розгортання програм);

IV.14. *System Services* (використання сервісів виконання команд);

IV.15. *User Execution* (нав’язування користувачу виконання програм);

IV.16. *Windows Management Instrumentation* (експлуатація можливостей *WMI*).

Забезпечення достатності умов для технічного ефекту доведення уразливості системи (об’єкта кіберзахисту) внаслідок виконання демонстраційної шкідливої програми (*Penetration Testing Impact*) пропонується розглядати (рис. 3, V) у формі вирішення задачі досягнення тактичної цілі (тактики) *Command and Control* (за методологією *ATT&CK*), тобто утворення прихованого каналу обміну даними між командним інтерпретатором (з повноваженнями деякого авторизованого користувача) в обчислювальному середовищі вразливого компонента системи (об’єкта кіберзахисту) та терміналом автоматизованого робочого місця Дослідника.

Дуги орієнтованого графа граф-схеми алгоритму діяльності Дослідника в процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту) визначають напрямки переходів між вершинами (рис. 3), які:

уособлюють вирішення задач Дослідником у контексті досягнення відповідних тактичних цілей (тактик);

уособлюють етапи інформаційної підготовки і вибору та реалізації рішення Дослідника при наявності інформації необхідної якості для технічної підготовки реалізації рішення за напрямком завершення процесу або у зворотному напрямку у разі її неповноти.

Елементарними структурними елементами забезпечення зв’язності вершин є ланцюг, циклічний та паралельний контур. В якості прикладів ілюстрації таких елементарних структурних елементів можна розглянути, відповідно (рис. 3):

односпрямовану зв’язність вершин I, II та III (ланцюг);

циклічну зв’язність вершин I, I.1 або II, II.8 і т. д. (циклічний контур);

паралельну зв’язність вершин IV, II і III, II за умови паралельного об’єднання вершин III та IV (паралельний контур).

Перетворимо орієнтований граф граф-схеми у модель для формування множини альтернативних стратегій A діяльності Дослідника в процесі пошуку та виявлення потенційної вразливості (об’єкту кіберзахисту) шляхом означення її вершин показниками, де $i = \overline{1,n}$, $j = \overline{1,m}$, n – кількість задач, $m = 5$ – фази етапів інформаційної підготовки і вибору та реалізації рішення (рис. 2, 3):

середнього значення τ_{ij}та дисперсії $D(\tau_{ij})$величини часових витрат;

ймовірності одержання якісного результату вирішення задачі q_{ij} (у контексті досягнення відповідної тактичної цілі);

прогнозованою величиною необхідних ресурсів c_{ij}.

Дуги зв’язності вершин ізоморфні переходам між операціями вирішення задач Дослідником у процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту) і зважуються ймовірностями p_{lk} їх використання при побудові можливих шляхів просування граф-схемою, де $l,k = \overline{1,v}$, $l \neq k$, v– кількість вершин граф-схеми.

Формування множини альтернативних стратегій A здійснюється у два кроки. Перший крок реалізується шляхом імітаційного моделювання всіх можливих шляхів просування граф-схемою на основі оперування можливими значеннями ймовірностей q_{ij} та похідних від неї значень ймовірностей p_{lk} (в частині, яких стосується). Другий крок полягає у здійсненні перетворень елементарних структурних елементів (ланцюг, циклічний контур, паралельний контур) орієнтованого підграфа можливого шляху просування граф-схемою з обчисленням еквівалентних значень T, C та $P(T \leq T_{\circ})$для кожної альтернативної стратегії множини A. Науково-методичним апаратом побудови та перетворення орієнтованого графа граф-схеми процесу пошуку та виявлення Дослідником вразливості системи (об’єкта кіберзахисту) є:

структурно-алгоритмічний метод аналізу і синтезу діяльності;

функціонально-структурна теорія функціонування ергатичних систем;

ймовірнісно-часовий граф алгоритму діяльності оператора системи.

Рішенням буде вибір такої стратегії дій Дослідника (потенційного вразливості) в процесі пошуку та виявлення потенційної вразливості (об’єкта кіберзахисту) з таким еквівалентними значеннями T, C та $P(T \leq T_{\circ})$, які будуть задовольняти умовам сформульованої постановки наукової задачі. При наявності у зазначених показниках для множини альтернативних рішень ознак неоднозначності вибору використовуються критерії прийняття рішень в умовах невизначеності: мінімаксний (максимінний), Лапласа (Байеса-Лапласа), Севіджа, а також похідних від них Гурвіца, Ходжа-Лемана, Гермейера.

Адекватність запропонованого науково-методичного апарату вирішення поставленої задачі підтверджується результатами експериментальних випробувань класу стратегій діяльності Дослідника в процесі пошуку та виявлення вразливості *Server-side Web Application* (рис. 4) системи (кіберзахисту), які в якості обов’язкової фази реалізації рішення включають досягнення тактичної цілі (тактики) *Initial Access* на основі вирішення задачі *Exploit Public-Facing Application* (рис. 4, III.3). Достатня репрезентативність експериментальної бази підкреслюється охопленням більше ніж 63 324 категорій дефектів (проєктування, реалізації, налаштування) *Server-side Web Application* (більше 20 % записів *CVE*):

53 % – передавання на обробку небезпечних (некоректних) вхідних даних (об’єктів), надлишкова інформативність під час обробки некоректних (неправильних) запитів до системи керування базою даних;

30 % – некоректна зміна повноважень (недотримання принципу найменших привілеїв), маркерів доступу (функцій інтерфейсу прикладного програмування, посилань на об’єкти);

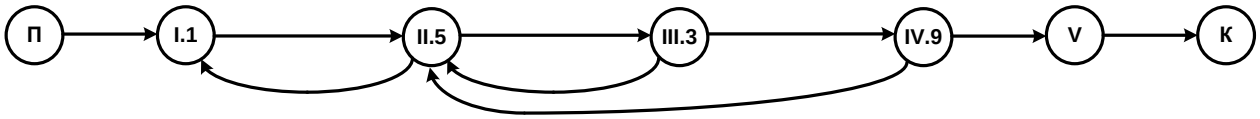

Рис. 4. Приклад орієнтованого графа граф-схеми діяльності Дослідника потенційної вразливості *Server-Side Web Application*

6 % – можливість угадування (прогнозування) та повторного використання значень одноразових паролів (маркерів, ідентифікаторів), критичне порушення логіки двофакторної автентифікації (відновлення паролів), потрапляння незашифрованих (зашифрованих нестійкими криптографічними алгоритмами) значень паролів у діагностичні повідомлення (відповіді на некоректні запити до компонентів);

5 % – некоректна перевірка дійсності параметрів автентифікації, цифрових підписів програмних компонентів, запобігання надлишкової інформативності під час обробки некоректних криптографічних даних (ключів, векторів ініціалізації) при утворені менш стійких захищених каналів комунікації;

5 % – недотримання порядку *OWASP Software Assurance Maturity Model* під час розробки компонентів із застосуванням апробованих колекцій програмних компонентів).

Результати експериментальних випробувань в основному збігаються з положеннями та оцінками рейтингу *Top 10 Web Application Security Risks* під егідою *The Open Worldwide Application Security Project* [18].

Висновки. Необхідність ефективної організації пошуку та виявлення вразливості системи (об’єкта кіберзахисту) обумовило актуальну необхідність постановки наукового завдання на розробку науково-методичного апарату вибору стратегій діяльності Дослідника (потенційної вразливості) в умовах невизначеності. Основним напрямком вирішення наукового завдання є формування множини альтернативних рішень з оцінкою кожного з них за показниками часових, ресурсних витрат та ймовірністю правильного виявлення вразливості за визначений час. Надання Досліднику можливості вибору найкращої раціональної стратегії з автоматичним генеруванням послідовності операцій доведення існування вразливості є передумовою суттєвого покращення ефективності задач тестування на проникнення шляхом скорочення часового інтервалу етапу інформаційної підготовки.

Подальші дослідження здійснюються у напрямку розробки комплексу імітаційного моделювання множини альтернативних стратегій діяльності Дослідника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.10.2025).

2. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment. URL: https://www.nist.gov/privacy-framework/nist-sp-800-115.

3. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: Постанова Каб. Міністрів України від 16.05.2023 № 497. URL: https://zakon.rada.gov.ua/laws/show/497-2023-п#Text (дата звернення: 28.10.2025).

4. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова Каб. Міністрів України від 19.06.2019 № 518: станом на 7 верес. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 28.10.2025).

5. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі від 03.07.2023 № 570. URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text.

6. Терещенко Т. П., Остапчук В. М., Хусаінов П. В., Черниш Ю. О. Оцінка та запобігання прояву вразливості Server-Side Web Application // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2024. № 5. С. 204–214. DOI: 10.58254/viti.5.2024.

7. Черниш Ю. О., Хусаінов П. В., Терещенко Т. П. Прийняття рішень в процесі пошуку вразливості Server-Side Web Application // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць // за заг. ред. Г. Д. Радзівілова. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2024. № 6. С. 264–274. DOI: 10.58254/viti.6.2024.

8. Хусаінов П. В., Черниш Ю. О., Терещенко Т. П. Зменшення невизначеності оцінки часу компрометації Server-Side Web Application об’єкта критичної інфраструктури // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2025. № 7. С. 232–242. DOI: 10.58254/viti.7.2025.21.232.

9. Герасимов Б. М., Локазюк В. М., Оксіюк О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень: навч. посіб. К.: Вид-во Європ. ун-ту, 2007. 335 с.

10. Герасимов Б. М., Камишин В. В. Організаційна ергономіка: методи і алгоритми дослідження та проєктування. К.: Інфосистем, 2009. 212 с.

11. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/cyber/cyber-kill-chain.html.
12. The Unified Kill Chain. URL: https://www.unifiedkillchain.com.
13. Certified Ethical Hacker. URL: https://cert.eccouncil.org/certified-ethical-hacker.html.
14. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.
15. Common Attack Pattern Enumerations and Classifications. URL: https://capec.mitre.org.
16. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org.
17. Common Weakness Enumeration. URL: https://cwe.mitre.org.
18. Open Worldwide Application Security Project. URL:https://owasp.org.