DOI: 10.58254/viti.7.2025.21.232

УДК 681.35

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

ЗМЕНШЕННЯ НЕВИЗНАЧЕНОСТІ ОЦІНКИ ЧАСУ КОМПРОМЕТАЦІЇ SERVER-SIDE WEB APPLICATION ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

На сучасному етапі розвитку методів і способів організації кіберзахисту об'єктів критичної інфраструктури одним із дієвих підходів залишається систематичний пошук вразливостей таких об'єктів у формі тестування на проникнення (penetration testing). Основною формою тестування на проникнення слід вважати практичне доведення можливості несанкціонованого та віддаленого нав'язування виконання демонстраційної шкідливої програми з авторизованими повноваженнями у складі одного з компонентів системи об'єкта критичної інфраструктури. Показником ефективності організації процесу тестування на проникнення запропоновано використовувати часові витрати досягнення тактичної цілі Compromise System.

Оцінка часових витрат досягнення тактичної цілі Compromise System в реальних умовах виконання практичних завдань тестування на проникнення знаходиться під впливом багатьох факторів невизначеності. Для зменшення впливу невизначеності пропонується два підходи. Перший підхід – шляхом впровадження методів теорії інформаційної підтримки прийняття рішень, на етапах досягнення тактичних цілей Reconnaissance та Resource Development. Другий – застосування критеріїв прийняття рішень в умовах невизначеності для обробки результатів експериментальних випробувань демонстраційних шкідливих програм, при проходженні казуального ланцюжка Initial Access – Execution. Обґрунтування сформульованих положень здійснено шляхом дослідження структурно-казуальних відношень предметної області на основі аналізу The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology та таксономій експертних знань Adversarial Tactics, Techniques & Common Knowledge.

Викладено змістовний опис методики оцінки зменшення невизначеності, оцінки часу компрометації компонентів Server-side Web Application при проходженні казуального ланцюжка Initial Access – Execution (у контексті етапу досягнення тактичної цілі Gaining Access тестування на проникнення) за способом Exploit Public-Facing Application на основі застосування критеріїв прийняття рішень в умовах невизначеності.

Ключові слова: *тестування на проникнення, прийняття рішень, оцінка часу.*

P. Khusainov, Y. Chernysh, T. Tereshchenko. Decreasing an indetermination of evaluation of time to compromise Server-Side Web Application of Industrial Control System

At the present stage of development of methods and ways of organizing cyber defense of critical infrastructure facilities, one of the effective approaches is the systematic search for vulnerabilities of such facilities in the form of penetration testing. The main form of penetration testing should be considered practical proof of the possibility of unauthorized and remote imposition of a demonstration malware program with authorized powers as part of one of the components of the critical infrastructure system. As an indicator of the effectiveness of organizing the penetration testing process, it is proposed to use the time spent on achieving the tactical goal of the Compromise System.

Estimating the time required to achieve the Compromise System tactical objective in real-world penetration testing is subject to many uncertainty factors. Two approaches are proposed to reduce the impact of uncertainty. The first is by implementing methods of decision support information theory at the stages of achieving the tactical goals of Reconnaissance and Resource Development. The second is the use of decision-making criteria under uncertainty to process the results of experimental tests of demonstration malware, when passing the casual chain Initial Access - Execution. The substantiation of the formulated provisions was carried out by studying the structural and casual relations of the subject area based on the analysis of The Cyber Kill Chain, The Unified Kill Chain, Ethical Hacking Methodology and the taxonomies of expert knowledge Adversarial Tactics, Techniques & Common Knowledge.

A substantial description of the methodology for assessing the reduction of uncertainty, estimating the time of compromise of Server-side Web Application components during the passage of the casual chain Initial Access - Execution (in the context of the stage of achieving the tactical goal of Gaining Access penetration testing) by the Exploit Public-Facing Application method based on the application of decision-making criteria under conditions of uncertainty is presented.

Keywords: *penetration test, decision making, assessment of time.*

Постановка завдання. Об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури (ОКІ), кібератака, яка безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Кіберзахист ОКІ забезпечується шляхом впровадження на ньому комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю. Власник/керівник ОКІ зобов'язаний проводити перевірку ефективності заходів щодо захисту об'єкта критичної інформаційної інфраструктури від несанкціонованого втручання (зовнішнього проникнення) шляхом періодичного виконання (не рідше одного разу на рік) тестування на проникнення. Тестування на проникнення (*penetration testing*) уособлює комплекс заходів оцінки захищеності об'єкта кіберзахисту від кіберзагроз шляхом доведення або заперечення твердження про можливість компрометації системи (об'єкта кіберзахисту) із застосуванням способів і засобів здійснення кібератак. Поняття "компрометація системи" уособлює факт будь-якого порушення сталого, надійного та штатного режимів функціонування системи (об'єкта кіберзахисту), яка підлягає спостереженню, та/або порушення конфіденційності, цілісності, доступності оброблюваної інформації [1–5].

Доведення можливості компрометації системи (об'єкта критичної інформаційної інфраструктури ОКІ) свідчить про її вразливість. Вразливість системи (об'єкта критичної інформаційної інфраструктури ОКІ) – властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режими функціонування системи (об'єкта критичної інформаційної інфраструктури ОКІ), здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів. Пошук та виявлення потенційної вразливості організовується Власником системи (об'єкта критичної інформаційної інфраструктури ОКІ) шляхом оголошення публічної пропозиції. Дослідник (фізична або юридична особа) потенційної вразливості надає відповідну послугу Власнику системи (об'єкта критичної інформаційної інфраструктури ОКІ) на основі договору. Зокрема, визначається величина граничного часу (директивного, обмеженого) протягом якого Дослідник повинен практично продемонструвати можливість компрометації системи (об'єкта критичної інформаційної інфраструктури ОКІ) шляхом здійснення віддаленої кібератаки у формі *penetration test* [6].

Аналіз публікацій. Сценарій здійснення Дослідником віддаленої кібератаки у формі *penetration test* розглядається як комбінація послідовності тактик (етапів досягнення тактичних цілей) та технік (способів, методів) відповідних експертних продуктів:

The Cyber Kill Chain – узагальнена односпрямована послідовність тактик кібератаки шляхом нав'язування виконання шкідливого програмного засобу [7];

The Unified Kill Chain – сукупність тактик у контексті здійснення трьох послідовних фаз (*In, Through, Out*) компрометації системи багатокомпонентного об'єкта (кіберзхисту) [8];

Ethical Hacking Methodology – взаємопов'язані етапи кібератаки за методологією *Certified Ethical Hacker (CEH)* [9];

Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) – опис тактик (*tactics*), технік (*techniques*) кібератак, які здійснювалися проти комунікаційних, технологічних систем та персональних мобільних комунікаційних пристроїв [10].

Формулювання мети статті. Одним із перспективних напрямів діяльності Дослідника на етапі *Initial Access* (несанкціоноване набуття авторизованих повноважень) слід вважати техніку *Exploit Public-Facing Application* через: відсутність потреби у привілеях; відсутність фізичного доступу до апаратних компонентів системи; складність (неможливість) впливу на ланцюги постачання та використання способів соціальної інженерії стосовно легітимних користувачів системи. Адекватність вибору цього способу підкреслюється тим, що близько

20 % категорій дефектів програм (196 із 940) таксономії *Common Weakness Enumeration (CWE)* та більше ніж 20 % вразливостей (63 324 з 273 728) таксономії *Common Vulnerabilities and Exposures (CVE)* відносяться до *Server-side Web Application* [11; 12].

Метою статті є викладення (оприлюднення) змістового опису методики зменшення невизначеності оцінки часу компрометації компонентів *Server-side Web Application* системи (об’єкта критичної інформаційної інфраструктури ОКІ) при проходженні Дослідником казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application* на основі застосування критеріїв прийняття рішень в умовах невизначеності.

Основна частина. Поняття та відношення між ними, які утворюють єдину основу для одноманітного розуміння необхідної для рішення задачі інформації, прийнято називати предметною областю. Множина понять про об’єкти, факти, процеси, події уособлює екстенсіональне представлення предметної області, а множина обумовлених ними відношень зв’язків та залежностей понять – інтенсіональне. Розрізняють структурний, функціональний, казуальний та семантичний типи відношень інтенсіонального представлення предметної області. Структурні відношення застосовуються для визначення ієрархій або мереж понять, функціональні відношення – для порядку перетворення декларативної інформації, казуальні відношення – для причинно-наслідкових зв’язків, ланцюгів зв’язків. Семантичний тип уособлює всі інші можливі типи відношень.

При ієрархічному представленні множина структурних відношень понять є деревоподібним графом, при мережевому представленні – графом типу “мережа”. Семантична мережа – найбільш узагальнена модель представлення знань про предметну область із використанням різнотипних зв’язків. При однорідності типів зв’язків семантичної мережі відокремлюють мережі класифікації (відображення структури відношень понять предметної області), функціональні мережі (опис процедур визначення понять через інші поняття) та сценарії.

Сценарій – формалізований опис стандартної послідовності взаємозв’язаних фактів типової ситуації у предметній області, послідовності дій або процедур досягнення цілей, 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. За типами відношень розрізняють казуальні сценарії, дерева цілей та сценарії класифікації.

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. Дерево цілей є відображенням декомпозиції головної цілі в системі часткових цілей. Сценарії класифікації призначені для відображення результатів узагальнення структурованих знань про предметну область. Для структуризації знань у 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, 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 будь-якого наукового дослідження, одержання нових знань.

Діяльність людини характеризується деревом цілей. Коренева вершина графу такого дерева асоціюється з головною ціллю, вузлові вершини – з проміжними цілями, кінцеві (термінальні) вершини є відображенням первинних (елементарних) цілей. Досягненню цілі відповідає значення певної оціночної функції. 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 [13].

Типовим фрагментом траєкторії діяльності є частково-впорядкована послідовність дій досягнення (головної, проміжної, первинної) цілі з деякої фіксованої початкової ситуації. Під поняттям “ситуація” розглядається деякий узагальнений стан (актуальний опис середовища, визначений на певному часовому інтервалі), що змінюється за результатом виконання дій. Така частково-впорядкована послідовність дій розпочинається від перебування у відомому стані початкової ситуації, подібна казуальному сценарію та може розглядатися у контексті застосування стереотипних знань.

Предметна область процесу компрометації системи (об’єкта критичної інформаційної інфраструктури ОКІ) є семантичною мережею казуальних і структурних відношень між етапами (фазами, кроками) кібератаки. Казуальні відношення відображають існуючу повноту експертних знань про типові послідовності варіантів дій та процедур суб’єкта кібератаки (порушника, хакера) для компрометації системи цільового об’єкта, зокрема системи (об’єкта критичної інформаційної інфраструктури ОКІ) або компонентів її технологічних майданчиків (локацій). Структурні відношення визначають взаємозв’язок етапів досягнення тактичних цілей (тактик) для компрометації системи (*Compromise System*).

Основним акцентом доведення Дослідником можливості компрометації системи є авторизоване виконання демонстраційної шкідливої програми в обчислювальному середовищі одного з компонентів системи (об’єкта критичної інформаційної інфраструктури ОКІ) за визначений час. Під поняттям “демонстраційна шкідлива програма” розглядається спеціальна форма реалізації функцій шкідливої програми щодо несанкціонованого створення (нелегітимним користувачем) авторизованого обчислювального процесу (потоку) в одному з компонентів системи (об’єкта критичної інформаційної інфраструктури ОКІ), але без впровадження типової деструктивної частини алгоритму (*payload*) відомих шкідливих програм. Відповідно, під поняттям “шкідлива програма” розглядається одна з можливих форм реалізації алгоритму здійснення порушення режиму функціонування, безпеки та процедур обробки критичної технологічної інформації, який забезпечується шляхом несанкціонованого створення авторизованого обчислювального процесу (потоку) у певному компоненті системи. Несанкціоноване створення авторизованого обчислювального процесу (потоку) є результатом етапу досягнення тактичної цілі (рис. 1) *Gaining Access* (за методологією *CEH*) та/або *Initial Access* (за методологією *ATT&CK*).

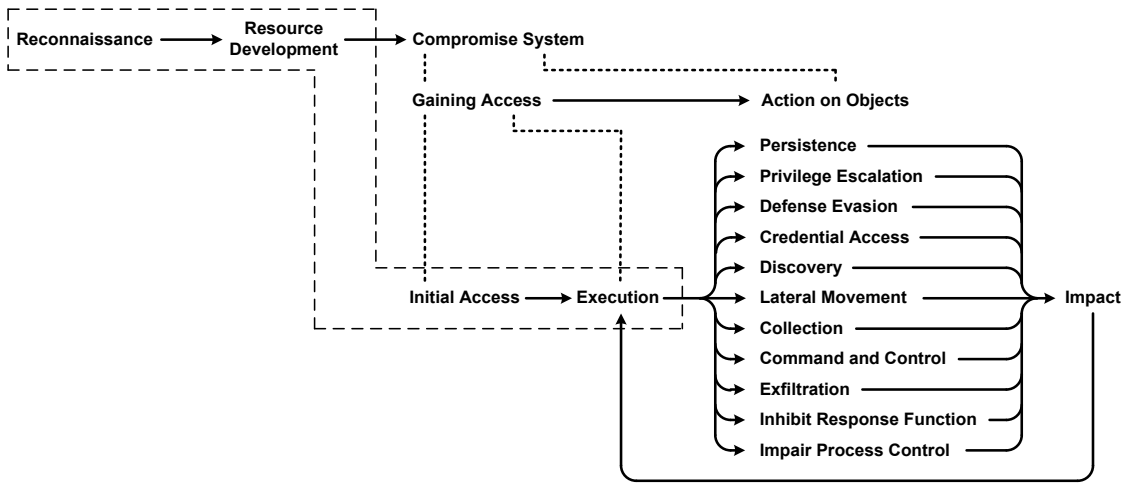

Рис. 1. Структурно-казуальна модель компрометації системи (об’єкта критичної інформаційної інфраструктури ОКІ) у контексті діяльності Дослідника

За методологією *CEH* успішний результат *Gaining Access* полягає у тому, що Дослідник одержав принципову можливість віддаленого (через комп'ютерну мережу) управління певним авторизованим обчислювальним процесом (потоком) демонстраційної шкідливої програми в одному з компонентів системи (об'єкта критичної інформаційної інфраструктури ОКІ) шляхом виконання (з повноваженнями авторизації) передбаченого набору команд деструктивного характеру на етапі досягнення тактичної цілі *Action on Objects* (за методологіями *The Cyber Kill Chain, The Unified Kill Chain*). Загальною недостатністю такого підходу є неврахування факторів невизначеності на оцінку часових витрат очікування успішного результату застосування демонстраційної шкідливої програми у контексті доведення Дослідником можливості компрометації системи (казуальне відношення *Gaining Access – Action on Objects*). Множина варіантів *Action on Objects* утворюється комбінуванням способів (технік) дій досягнення тактичних цілей (тактик) за методологією *ATT&CK*:

Persistence (забезпечення постійності набутих повноважень *Initial Access*);

Privilege Escalation (розширення/зміна набутих повноважень *Initial Access*);

Defense Evasion (запобігання виявлення несанкціонованого використання авторизованих повноважень *Initial Access* та *Privilege Escalation*);

Credential Access (одержання облікових та автентифікаційних даних для легітимного набуття повноважень поза контекстом тактичних цілей *Initial Access* та *Privilege Escalation*);

Discovery (одержання відомостей про внутрішню структуру та компоненти системи);

Lateral Movement (набуття авторизованих повноважень у середовищі компонента системи за результатами *Discovery*, але поза контекстом *Initial Access*);

Collection (акумулювання критичної технологічної інформації системи як етап її подальшого витоку);

Command and Control (утворення прихованого каналу управління компонентом системи з повноваженнями авторизованого користувача);

Exfiltration (здійснення витоку критичної технологічної інформації системи);

Inhibit Response Function (блокування процедур реагування на небезпечні стани технологічного процесу);

Impair Process Control (модифікація процедур реагування на небезпечні стани технологічного процесу та обробки критичної технологічної інформації);

Impact (порушення функціонування системи об'єкта критичної інформаційної інфраструктури ОКІ та безпеки критичної технологічної інформації).

Успіх доведення Дослідником можливості компрометації системи (об'єкта критичної інформаційної інфраструктури ОКІ) за визначений час є функціоналом від:

якості прийняття рішення на етапі одержання/узагальнення/аналізу інформації для ідентифікації вразливості системи (як узагальнення етапів *Footprinting*, *Scanning*, *Enumeration*, *Vulnerability Analysis* за методологією *CEH*; етап *Reconnaissance* за методологіями *The Cyber Kill Chain, The Unified Kill Chain, ATT&CK*);

якості прийняття рішення на етапі здійснення вибору/підготовки/створення/придбання засобів експлуатації вразливості системи (етап *Weaponization* за методологіями *The Cyber Kill Chain, The Unified Kill Chain*; етап *Resource Development* за методологією *ATT&CK*);

застосування критеріїв прийняття рішень в умовах невизначеності або в умовах ризику при обґрунтуванні вибору (на основі експериментальних даних) демонстраційної шкідливої програми (експлойту) для компрометації системних компонентів *Server-side Web Application* (при проходженні казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application*).

Нагадаємо, що під поняттям "вразливість" (*vulnerability*) розглядається така властивість системи (об'єкта критичної інформаційної інфраструктури ОКІ), яка призводить до негативного технічного ефекту (*negative technical impact*). Нав'язування негативного

технічного ефекту базується на можливості непередбаченого використання (експлуатації) певного дефекту (*weakness*) програмних, апаратних, програмно-апаратних компонентів системи, які при певних умовах призводять до її вразливості.

Перші два аспекти відносяться до понятійного апарату теорії інформаційної підтримки прийняття рішень [14]. Прийняття рішень (ПР) Дослідником (у ролі особи, яка приймає рішення) є результатом складних психологічних процесів. Логіко-психологічний підхід базується на представленні процесів ПР у формі послідовності етапів, а саме: постановка задачі; здобуття та обробка інформації для ПР; аналіз та ідентифікація проблемної ситуації; вироблення множини альтернативних рішень; вибір рішення; реалізація рішення. Сукупність дій етапів ПР розглядається як композиція множин операцій інформаційної підготовки ПР, вибору та реалізації рішення (результат процесу ПР). Вибір рішення Дослідником принципово не може мати формального подання. Він керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями.

По-перше, розумова діяльність особи, яка приймає рішення (ОПР) розглядається як багаторівнева сукупність взаємозв’язаних процесів психофізичного, психологічного, гносеологічного та програмного характеру. Основні форми розумової діяльності: емпіричне, аксіоматичне, діалектичне мислення. 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.

По-друге, 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).

Зокрема, невизначеність або неповна визначеність початкової ситуації для здійснення цілеспрямованої діяльності заперечує можливість застосування стереотипних знань. За такої умови постає необхідність пошуку можливих варіантів траєкторії діяльності та вибору одного з них за критеріями на основі значення оціночної функції. Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення можуть бути: неможливість точного передбачення наслідків рішень; неможливість повторення або експериментальної перевірки рішення; неможливість контролю всіх факторів; наявність множини альтернативних рішень та необхідність вибору одного з них; низка якість початкової інформації формулювання задачі та вибору рішення.

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. Може бути відома деяка кінцева кількість значень кожної величини, але без відповідних функцій розподілу ймовірностей. Розгляд проблематики вирішення задач ПР в умовах ризику можливо при наявності експериментальних даних необхідного об’єму для визначення функцій розподілу кожної з досліджуваних величин.

Базові стратегії зменшення впливу невизначеності та суб'єктивізму при вирішенні задач ПР в умовах невизначеності реалізуються шляхом застосування критеріїв максиміну, Байеса-Лапласа та Севіджа. Хоча не існує загальних підходів для визначення придатності до застосування згадуваних критеріїв в тих чи інших ситуаціях, але все ж можна навести з цього приводу деякі евристичні правила: критерій максиміну спрямований на вибір найбільш обережного передбачуваного результату для всіх комбінацій умов експериментів до моменту необхідності обґрунтування кінцевого рішення; критерій Байєса-Лапласа заснований на більш оптимістичних передбаченнях ніж критерій максиміну, але є менш оптимістичним за критерій Севіджа. Згадувані критерії є базисом для усунення невизначеності, шляхом зменшення суб'єктивізму особистих міркувань та передбачень ОПР, а також протиріч, які їх обумовлюють. Практичне застосування критеріїв ПР в умовах невизначеності базується на обробці матриці рішень, яка сформована зі значень оціночної функції (без знання функції розподілу її величини) за результатами проведених експериментальних випробувань.

Розглянемо змістовний опис методики оцінки зменшення невизначеності, оцінки часу, компрометації компонентів *Server-side Web Application* системи (об'єкта критичної інформаційної інфраструктури ОКІ) при проходженні Дослідником казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application* на основі застосування критеріїв ПР в умовах невизначеності.

Досліджуваною величиною (значення оціночної функції) є експериментальне вимірювання (оцінка) часового інтервалу до настання успішного результату роботи демонстраційної шкідливої програми. Застосування демонстраційної шкідливої програми здійснюється у формі експлойта, який для компонентів *Server-side Web Application* виступає в ролі *Web*-клієнта легітимного користувача (рис. 2, *а*). Нагадаємо, що під поняттям "експлойт" (*exploit)* розглядається спеціальний програмний засіб, призначений для віддаленої (через комп'ютерну мережу) експлуатації дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application*, що призводить до їх вразливості (вразливого стану) та прояву негативного технічного ефекту демонстративної шкідливої програми. Основною функціональною рисою досягнення успішного результату демонстративної шкідливої програми шляхом застосування експлойта з існуючої колекції експлойтів (*expoloits*) Дослідника (рис. 2, *б*) є утворення прихованого каналу управління вразливим компонентом (*Gaining Access*) з авторизованими повноваженнями технічного персоналу *Server-side Web Application*, де T_{GA} – показник часового інтервалу, витрачений на досягнення тактичної цілі *Gaining Access*.

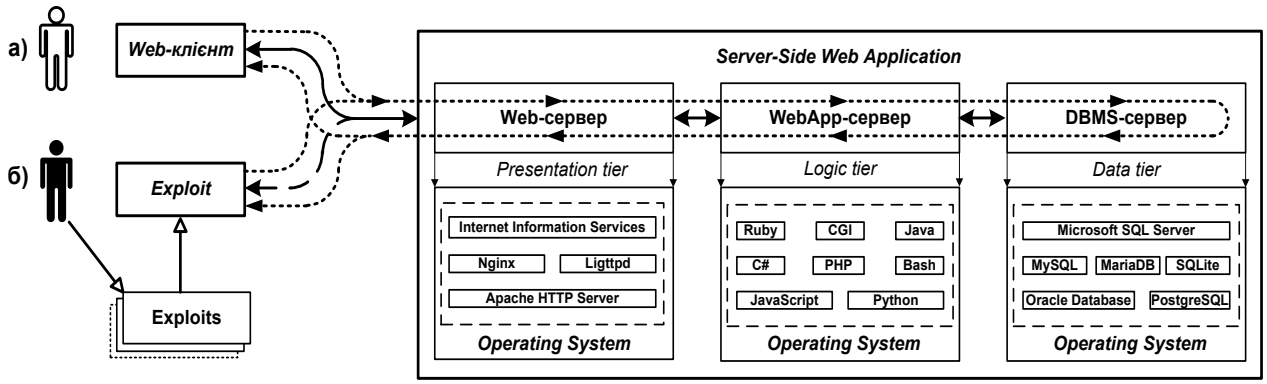

Рис. 2. Організація одержання експериментальних даних для оцінки часових витрат *Gaining Access* (*Initial Access – Execution*) за напрямом впливу *Exploit Public-Facing Application*

Розглянемо можливі інтерпретації T_{GA} за категоріями дефектів (проєктування, реалізації, налаштування) *Server-side Web Application* [15; 16]:

A01:2021 Broken Access Control – некоректна зміна повноважень (недотримання принципу найменших привілеїв), маркерів доступу (функцій інтерфейсу прикладного програмування, посилань на об'єкти), $T_{GA} = T_{A01}$, *Total CVEs* = 19013;

A02:2021 Cryptographic Failures – некоректна перевірка дійсності параметрів автентифікації, цифрових підписів програмних компонентів, запобігання надлишкової інформативності при обробці некоректних комбінацій криптографічних даних (ключів, векторів ініціалізації) при утворенні менш стійких захищених каналів комунікації, $T_{GA} = T_{A02}$, *Total CVEs* =3075;

A03:2021 Injection – передавання на обробку небезпечних (некоректних) вхідних даних (об'єктів), надлишкова інформативність при обробці некоректних (неправильних) запитів до системи керування базою даних, $T_{GA} = T_{A03}$, *Total CVEs* = 32078;

A04:2021 Insecure Design – недотримання порядку *OWASP Software Assurance Maturity Model (SAMM)* при розробці компонентів *Server-side Web Application* із застосуванням апробованих колекцій програмних компонентів, $T_{GA} = T_{A04}$, *Total CVEs* = 2691;

A05:2021 Security Misconfiguration – використання хмарних сервісів (облікових записів) з налаштуваннями за замовчанням, надлишкова інформативність при обробці некоректних запитів до компонентів *Server-side Web Application*, несистематичне застосування оновлень безпеки та аналізу ризиків, $T_{GA} = T_{A05}$, *Total CVEs* =789;

A06:2021 Vulnerable and Outdated Components – використання застарілих версій програмних компонентів *Server-side Web Application*, $T_{GA} = T_{A06}$, *Total CVEs* = 0;

A07:2021 Identification and Authentication Failures – 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) *Server-side Web Application*, $T_{GA} = T_{A07}$, *Total CVEs =3897*;

A08:2021 Software and Data Integrity Failures – некоректна перевірка автентичності (цілісності, безпечності, дійсності) даних у складі серіалізованих об'єктів (конвеєрів обробки даних) компонентів *Server-side Web Application*, що інсталюються (оновлюються) з репозиторіїв (зовнішніх носіїв) за замовчанням, $T_{GA} = T_{A08}$, *Total CVEs* =1152;

A09:2021 Security Logging and Monitoring Failures – неузгодженість форматів повідомлень про події функціонування компонентів *Server-side Web Application,* потрапляння критичної технологічної інформації (ідентифікаторів, параметрів автентифікації) до вмісту повідомлень про події, $T_{GA} = T_{A09}$, *Total CVEs* = 242;

A10:2021 Server-Side Request Forgery – потрапляння запитів *Web*-клієнта у запити *Web*-сервера до інших компонентів *Server-side Web Application*, $T_{GA} = T_{A10}$, *Total CVEs* = 387.

Придатність наведених категорій дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application* до експлуатації визначається на основі обробки вмісту матриці рішень, де $T_{ij} = T_{GA}$:

$$\begin{array}{cccccc} & w_1 & \cdots & w_j & \cdots & w_m \\ d_1 & T_{11} & \cdots & T_{1j} & \cdots & T_{1m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ d_i & T_{i1} & \cdots & T_{ij} & \cdots & T_{im} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ d_n & T_{n1} & & T_{nj} & & T_{nm} \end{array} \quad (1)$$

Множина значень величини показника $T_{ij} = T_{GA}$, розташованих по елементах матриці рішень $\|T_{ij}\|$, залежно від умов експериментального випробування, характеризуються перетинами доданих означень множин комбінацій незалежних змінних $W = \{w_j\}$ (верхній рядок) та залежних змінних $D = \{d_i\}$ (крайній лівий стовпчик). Кожний елемент $w_j \in W$ уособлює одну з можливих комбінацій значень незалежних змінних, $j = \overline{1,m}$, а кожний елемент $d_i \in D$ – одну з можливих комбінацій залежних (контрольованих) змінних опису умов певної ітерації експериментального випробування, $i = \overline{1,n}$.

Результатом обробки матриці рішень (1) у термінах понятійного апарату теорії ПР в умовах невизначеності є вибір одного з можливих альтернативних рішень або альтернативи. Поняття альтернативного рішення (альтернативи) відповідає $\underline{i}$-му порядковому номеру елемента $d_i \in D$ (i-го рядка матриці рішень), а обґрунтування його вибору є результатом застосування критеріїв максиміну, Байєса-Лапласа та Севіджа з урахуванням особливостей постановки задачі. Вибір одного з альтернативних рішень уособлюється з вибором експлойту (з існуючої колекції експлойтів), який є найбільш придатним для компрометації одного з компонентів *Server-Side Web Application* системи (об'єкта критичної інформаційної інфраструктури ОКІ) при проходженні Дослідником казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application*.

Орієнтовна розмірність матриці рішень для кожної з категорії дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application* може бути оцінена на підставі відповідного значення *Total CVEs* – загальна кількість *CVE* в категорії *Top 10 Web Application Security Risks*. Необхідно зазначити, що значення *Total CVEs* = 0 у категорії *A06:2021 Vulnerable and Outdated Components* відображає практично несуттєву ймовірність успіху Дослідника для казуального ланцюжка *Initial Access – Execution* за способом *Exploit Public-Facing Application.*

Застосування критерію максиміну базується на припущенні, що обране на його основі рішення не може бути гіршим за будь-яке інше з множини альтернатив. Правило вибору альтернативного рішення $d_i = min\ \ T_{ik}$, де $T_{ik} = \underset{j}{max} T_{ij}$, передбачає доповнення матриці $\|T_{ij}\|$ стовпчиком із найбільшими значеннями T_{ij} у кожному рядку. Рішенням є вибір j-го рядка $\|T_{ij}\|$, для якого $d_i = min\ \ \underset{j}{max} T_{ij}$.

За наявності статистично вичерпної вибірки результатів експериментальних випробувань наявної колекції експлойтів для кожної категорії дефектів (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application* доцільно розглянути застосування критерію Байеса-Лапласа. Правило вибору одного з альтернативних рішень $d_i = max\ \ \overline{T}_{ik}$, $\overline{T}_{ik} = \sum_{j=1}^{n} T_{ij} \cdot p_j$, $\sum_{j=1}^{n} p_j = 1$, де $\overline{T}_{ik}$– середні значення показника T_{ik}, p_j – ймовірність здійснення спроби експлуатації дефекту (проєктування, реалізації, налаштування) компонентів (програмних, програмно-апаратних) *Server-side Web Application,* яка відповідає умовам експерименту w_j. Ймовірності здійснення експерименту з умовами w_j відомі та не залежать від часу спостереження. Критерій Байеса-Лапласа передбачає доповнення матриці $\|T_{ij}\|$ стовпчиком із величиною математичного очікування величини значень $\overline{T}_{ik}$ у кожному рядку. Обирається j-й рядок $\|T_{ij}\|$, який відповідає альтернативі d_i, для якої величина T_{ij} (у додатковому стовпчику зі значеннями математичного очікування) є найменшою. Застосування критерію Байеса-Лапласа передбачає зростання достовірності результату при збільшенні множини результатів експериментів (теоретично до нескінченності) і ризику неправильного рішення при їх відносно невеликій кількості. Поява умов ризику для критерію Байеса-Лапласа доцільна

за принципом "недостатності обґрунтування" та на практиці має більш широке розповсюдження. За відсутності достатньо повної, великої та репрезентативної вибірки значень результатів експериментів замість математичного очікування величини $\overline{T}_{ik}$ пропонується використовувати середнє математичне $\hat{T}_{ik} = \frac{1}{n}\sum_{j=1}^{n} T_{ij}$.

Критерій Севіджа використовує поняття додаткової втрати при виборі альтернативи d_i для умов w_j, яка має відмінне від найкращого значення оціночної функції. Правило вибору одного з альтернативних рішень базується на використанні величини залишків $d_i = \min_i \max_j (\max_i T_{ij} - T_{ij})$. Обчислення залишків $\Delta T_{ij} = \max_i T_{ij} - T_{ij}$ здійснюється стовпцями $\|T_{ij}\|$ шляхом віднімання від максимального значення T_{ij} у стовпчику від значення кожного його елемента. Для зручності оперування значеннями залишків при виборі рішення утворюють матрицю залишків $\|\Delta T_{ij}\|$ всіх елементів $\|T_{ij}\|$. Критерій Севіджа передбачає доповнення $\|\Delta T_{ij}\|$ стовпчиком максимальних залишків у рядку $\max_j \Delta T_{ij}$. Далі обирається j-й рядок $\|T_{ij}\|$, який відповідає альтернативі d_i, для якої величина $\max_j \Delta T_{ij}$ (у додатковому стовпчику $\|\Delta T_{ij}\|$) є найменшою.

Висновки. Взагалі, вибір рішень із кількох можливих (на основі матриці рішень) не є однозначним, оскільки найкраще значення оціночного показника може спостерігатися у кількох альтернатив. Наявність лише однієї альтернативи притаманно, зазвичай, досить простим (елементарним) та детермінованим процедурам вибору рішення.

Подальші дослідження здійснюються за напрямком забезпечення розв'язання більш складних (структурованих, багатоетапних) задач діяльності Дослідника вразливості системи (об'єкта критичної інформаційної інфраструктури ОКІ), які досить органічно конструюються з елементарних процедур застосування критеріїв ПР в умовах невизначеності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. С. 42. Ст. 403.

2. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX // Офіційний вісник України. 2021. № 98. С. 23. Ст. 6341.

3. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: постанова Каб. Міністрів України від 19.06.2019 № 518 // Офіційний вісник України. 2019. № 50. С. 53. Ст. 1697.

4. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.

5. Про затвердження Методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03.07.2023 № 570.

6. Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: постанова Каб. Міністрів України від 16.052023 № 497 // Офіційний вісник України. 2023. № 52. С. 72. Ст. 2911.

7. The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

8. The Unified Kill Chain. URL: https://www.unifiedkillchain.com.

9. Certified Ethical Hacker. URL: https://cert.eccouncil.org/certified-ethical-hacker.html.

10. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.

11. Common Weakness Enumeration. URL: https://cwe.mitre.org.

12. Common Vulnerabilities and Exposures. URL: https://cve.mitre.org.

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

14. 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.

15. 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. Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 2024. № 5. 240 с. DOI: 10.58254/viti.5.2024. С. 204–214.

16. 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. Київ: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2024. № 6. 280 с. DOI: 10.58254/viti.6.2024. С. 264–274.