Концептуальна модель проєктування CTF-завдань та методика її застосування для формування компетентностей з мережевої безпеки

УДК 621.395.7 (043.2)

Олександр Черепов[1], Богдан Неймет[2]

Ужгородський національний університет,
[1]oleksandr.cherepov@uzhnu.edu.ua, [2]bohdan.neimet@uzhnu.edu.ua

Війна змусила переоцінити, наскільки готові українські випускники зі сфери інформаційної безпеки до викликів сучасності. CERT-UA фіксує нові інциденти щодня; класичні лабораторні роботи в університеті за ними не встигають. Capture the Flag — формат, який давно зарекомендував себе як ефективний для практичної підготовки [1, 2]. Біда в іншому. У ЗВО CTF-задачі здебільшого з'являються як ініціатива окремого викладача. Вони робляться під конкретну лекцію або набір практичних задач, без явного зв'язку з компетентностями, що має закрити освітня програма. У свою чергу можливість скласти послідовний курс CTF орієнтованих задач, що можна було б відтворювати в іншому університеті чи навіть у наступному році, виявляється важкою задачею.

Мета роботи — побудувати модель проєктування CTF-задач з мережевої безпеки, яка прив'язує таксономію MITRE ATT&CK [1] до фахових компетентностей чинного стандарту вищої освіти спеціальності 125 (F5) «Кібербезпека та захист інформації» та до міжнародних рамок ENISA ECSF [3] і NIST NICE; а також запропонувати методику, як цю модель використовувати на практиці.

Серед наявних рішень виокремлюються три гілки. Платформи на кшталт CTFd чи kCTF дають інфраструктуру для розгортання задач — і нічого більше. Кіберполігони з декларативними мовами опису сценаріїв (KYPO [2], CyRIS, CRACK з мовою VSDL [4]) теж зосереджені на розгортанні. Фреймворк URSID [5], свіжіший і дотичніший за духом, переводить технічний сценарій ATT&CK у множину процедурних варіантів. Проте і він не передбачає зв'язку з освітніми компетентностями. Узагальнені моделі знань (наприклад, A4CKGE [6]) служать радше для аналізу багатокрокових атак, ніж для проєктування навчальних задач.

Запропонована модель забезпечує те, чого бракувало: можливість простежити від рядка освітньої програми до конкретної техніки ATT&CK, з якою працює студент за клавіатурою. Саме у цьому ми вбачаємо наукову новизну, що відрізняє наш підхід від наявних CTF-платформ і від додаткових практик окремих викладачів.

Модель складається з чотирьох шарів. Компетентнісний шар виконує роль точки входу: проєктувальник обирає фахову компетентність з освітньої програми, та додатково зіставляє її з ECSF або NICE, потім розкладає на елементи KSA і фіксує очікуваний рівень за НРК. Онтологічний шар працює нижче: тут MITRE ATT&CK, CWE і CAPEC зведено у спільну мережу знань. Для кожної компетентності у цій мережі видно, які техніки атак вона має закривати і які слабкості становлять її предмет. Сценарний шар бере зв'язки з онтології і перетворює їх у шаблон CTF-задачі — з точками альтернатив (де технік кілька, обираємо одну) і точками параметризації (де налаштування

варіюються між варіантами). Останній шар, інфраструктурний, відповідає за матеріальне втілення: Docker, Vagrant, Terraform або інший фреймворк. Перехід між шарами реалізовано як типізовані функції відображення; саме завдяки їм з'являється той зв'язок «компетентність — техніка — задача», заради якого все це вибудовується.

Методика застосування моделі складається з п'яти послідовних кроків: 1) декомпозиція цільової фахової компетентності з освітньої програми на KSA-елементи з урахуванням рівня НРК; 2) картування KSA на множину технік MITRE ATT&CK; 3) вибір сценарного шаблону з бібліотеки або проєктування нового; 4) генерація варіантів задачі за допомогою параметризації вхідних точок; 5) оцінювання навчальних результатів, а саме: успішність, час виконання, кількість спроб.

Модель було перевірено на групах студентів ДВНЗ «Ужгородський національний університет» освітньої програми «Кібербезпека та захист інформації». Цільова компетентність - здатність виконувати тестування на проникнення (близька за змістом до ECSF Penetration Tester). Акцент був зосереджений саме на активній розвідці. Зіставлення з ATT&CK дало техніки T1595, T1046, T1018 і T1083. За шаблон взяли трирівневу мережу: DMZ, внутрішній і серверний сегменти. У внутрішньому сегменті було прихований цільовий ресурс, доступ до якого можливий лише через проміжний хост. Альтернативні точки у шаблоні (Apache або Nginx, MySQL або PostgreSQL) дозволили породити більше 10 дидактично рівноцінних варіантів задачі. Кожен зі студентів отримав свій варіант. Результатом є те, що час підготовки набору задач скоротився приблизно вдвічі порівняно з ручним проєктуванням, а можливість обміну розв'язками між студентами мінімізувалась через варіативність.

Висновки. Запропонована модель і методика дають викладачеві інструмент, що допомагає зв'язати рядки фахових компетентностей освітньої програми «Кібербезпека та захист інформації» (F5) з конкретними технічними задачами, які студент розв'язує у віртуальному середовищі. Це робить процес осяжним, а навчальний результат повторюваним між дисциплінами та між закладами. Подальша робота включає у себе формальний розвиток сценарного шару (композиційна алгебра і метрика складності варіантів), формування корпусу TTP за матеріалами CERT-UA та відкритих звітів про кіберінциденти проти інформаційної інфраструктури України 2022–2026 років, та експериментальну верифікацію методики у форматі контрольної й експериментальної груп серед студентів освітньої програми.

1. Strom B. E., Applebaum A., Miller D. P. та ін. MITRE ATT&CK: Design and philosophy. MITRE Technical Report MP180360. Bedford, MA : The MITRE Corporation, 2020. p. URL : https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.
2. Vykopal J., Vizváry M., Ošlejšek R. та ін. Lessons learned from complex hands-on defence exercises in a cyber range. Proceedings of the 2017 IEEE Frontiers in Education Conference (FIE). – Indianapolis : IEEE, 2017. – P.

1–8. DOI: 10.1109/FIE.2017.8190713.
3. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework (ECSF). – Athens : ENISA, 2022. URL: https://www.enisa.europa.eu/topics/skills-framework/ecsf.
4. Russo E., Costa G., Armando A. Building next generation cyber ranges with CRACK. Computers & Security. – 2020. – Vol. 95. – Article 101837. DOI: 10.1016/j.cose.2020.101837.
5. Besson P.-V., Viet Triem Tong V., Guette G. та ін. URSID: Automatically refining a single attack scenario into multiple cyber range architectures. Foundations and Practice of Security (FPS 2023). Lecture Notes in Computer Science. Cham : Springer, 2024. DOI: 10.1007/978-3-031-57537-2_8.
6. Xiang X., Ma C., Zeng L. та ін. Uncovering multi-step attacks with threat knowledge graph reasoning. Security and Safety. – 2025. – Vol. 4. – Article 2024019. DOI: 10.1051/sands/2024019.

Удосконалення процедур цифрової криміналістики в системах реагування на інциденти кібербезпеки

УДК 004.056.55

Мар'яна Мельник[1], Віктор Чешун[2], Дмитро Чешун[3]

[1,2]Хмельницький національний університет, [3]Хмельницький фаховий економіко-технологічний коледж Університету економіки і підприємництва
[1]melnyk.masia@gmail.com, [2]cheshunvn@khmnu.edu.ua,
[3]dmytro.cheshun@gmail.com

Сучасний етап розвитку цифрового суспільства характеризується тотальною інтеграцією інформаційних технологій у процеси державного управління та функціонування критичної інфраструктури, що водночас створює безпрецедентні ризики для національної безпеки.

Аналіз поточної ситуації [1-3] дозволяє виявити суттєві недоліки в існуючих підходах до реагування, серед яких найгострішими є низький рівень автоматизації моніторингу подій безпеки та відсутність єдиної методології збору цифрових доказів. Більшість установ сьогодні стикаються з проблемою фрагментарності журналів подій та невідповідністю процедур вилучення артефактів міжнародним стандартам, що часто унеможливлює проведення глибокого технічного аналізу та встановлення реальних причин інцидентів. Досвід масштабних атак останніх років підтверджує, що без впровадження проактивних методів виявлення та структурованих алгоритмів розслідування об'єкти критичної інфраструктури залишаються вразливими до тривалої прихованої присутності зловмисників у їхніх внутрішніх мережах.

Мета дослідження полягає у розробці та практичному обґрунтуванні системного підходу до розслідування кіберінцидентів, який би забезпечував цілісність процесу криміналістики від моменту первинної фіксації аномалії до формування підсумкової аналітичної звітності. Автори поставили за ціль створити гнучку модель, що поєднує сучасні технічні засоби автоматизованого аналізу телеметрії з чіткими організаційними регламентами взаємодії між