УДК 343.1+004

Віталій Вікторович Носов,
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Гейміфіковане навчання кібербезпеки та цифрових криміналістичних досліджень у виші

Стрімкий розвиток кіберпростору суспільства призвів до зросту потреби у фахівцях в галузі кібербезпеки. Аналіз [1] показав, що у 2019 році в Україні 51 виш здійснює підготовку бакалаврів за спеціальністю 125 Кібербезпека. Суттєва специфіка навчання прикладним дисциплінам за цією спеціальністю полягає у постійній необхідності швидкого оновлення великого масиву знань разом із швидким розвитком інформаційних технологій, і якщо теоретичні відомості більш-менш залишаються актуальними тривалий період, то практичні аспекти потребують переробки і нової розробки кожен семестр навчання.

Комплексний підхід до розробки навчальних практичних задач із пов'язаними між собою курсами з тестового проникнення до комп'ютерних систем і цифрових криміналістичних досліджень (digital forensics) потребує постійного створення і модифікації мережі спеціальних віртуальних машин з різними операційними системами та застосунками, які містять або актуальні вразливості, або сліди несанкціонованого доступу. І це є значною проблемою.

Ефективність практичного навчання в цій галузі, окрім іншого, також залежить від способу стимуляції пізнавальної, мотиваційної та поведінкової діяльності студентів (курсантів) і одним із найбільш підходящих саме в цій царині є гейміфікація (використання ігрових практик та механізмів у контексті розв'язання практичних задач) [2, 3], яка спирається на природні людські інстинкти [4]: конкуренція, досягнення, винагорода і таке інше.

Впровадження гейміфікації у навчанні кібербезпеці і цифровим криміналістичним дослідженням можна здійснювати двома способами (одночасно або на вибір):

а) локальне або хмарне розгорнення фреймворка (інфраструктури програмних рішень) ігрового середовища;

б) реєстрація у провайдера спеціалізованої ігрової послуги і віддалене використання у навчанні актуальних ігрових сценаріїв.

Кожен спосіб має взаємодоповнюючі переваги і недоліки відносно організації навчання у виші:

спосіб а):

- переваги:
- контрольована доступність;
- гнучка зміна функціональності і параметрів роботи;
- наперед відомі для викладача варіанти розв'язання задач;
- недоліки:
- значні витрати ресурсів на розгортання, адміністрування і оновлення середовища;
- значні витрати ресурсів на безперервну розробку і оновлення ігрових сценаріїв-завдань;

спосіб б):

- переваги:
- провайдер здійснює розгортання, адміністрування і оновлення ігрового середовища;
- провайдер забезпечує систему безперервного оновлення ігрових сценаріїв-завдань від необмеженої кількості зацікавлених сторін;
- недоліки:
- залежність доступності середовища від надійності провайдера;
- значні витрати ресурсів для знаходження викладачем наперед невідомих варіантів розв'язання задач.

Наявні складові для реалізації обох способів гейміфікації у вигляді асоціативної карти наведені в [5] – для курсу тестового проникнення до комп'ютерних систем, і в [6] – для курсу цифрових криміналістичних досліджень.

Для впровадження гейміфікації за способом б) можна використовувати британський ресурс hackthebox.eu, де вже зареєстровано біля 100 вишів світу, а за способом а) Capture The Flag framework [7] та актуальну базу підготовлених віртуальних машин із різними завданнями-сценаріями vulnhub.com.

Досвід впровадження гейміфікації показує, що доцільна комбінація обох способів.

Список бібліографічних посилань

1. Вступ.ОСВІТА.UA : сайт. URL: https://vstup.osvita.ua/spec/1-40-1/0-100-1513-0-0-50 (дата звернення: 27.10.2019).
2. Sailer M. Does Gamification of Learning work? URL: http://gamification-research.org/2019/08/does-gamification-of-learning-work (дата звернення: 27.10.2019).
3. Sailer M., Homner L. The gamification of learning: a meta-analysis. *Educational Psychology Review.* 2019. https://doi.org/10.1007/s10648-019-09498-w (дата звернення 27.10.2019).
4. Hamari J., Eranti V. Framework for Designing and Evaluating Game Achievements // Proceedings of Digra 2011 Conference: Think Design Play, Hilversum, Netherlands, September, 14–17. URL: http://www.digra.org/dl/db/11307.59151.pdf (дата звернення 27.10.2019).
5. Aman Hardikar. Penetration testing practice lab – vulnerable apps/systems. URL: https://www.amanhardikar.com/mindmaps/Practice.html (дата звернення: 27.10.2019).
6. Aman Hardikar. Forensic challenges. URL: https://www.amanhardikar.com/mindmaps/ForensicChallenges.html (дата звернення: 27.10.2019).
7. Repository Capture The Flag framework. URL: https://github.com/CTFd (дата звернення: 27.10.2019).

Одержано 28.10.2019