Сірик А.В., магістрант,
Єфіменко А. А., к.т.н., доцент,
Державний університет «Житомирська політехніка»

МЕТОДИКА РОЗРОБКИ ЗАВДАНЬ З КРИПТОГРАФІЇ ТА СТЕГАНОГРАФІЇ ДЛЯ СТУДЕНТСЬКИХ CTF-ЗМАГАНЬ

Зростання кількості та складності кіберзагроз вимагає від сучасних фахівців постійного вдосконалення навичок у галузі інформаційної безпеки. Одним із найефективніших методів підготовки спеціалістів є CTF-змагання (Capture The Flag), які дозволяють перевірити знання та вміння в умовах, наближених до реальних. Завдяки духу суперництва, CTF-змагання стимулюють учасників застосовувати свої знання на практиці та дають можливість здобути необхідний досвід у вирішенні кібербезпекових завдань різної складності.

Метою цього дослідження є розробка методики створення освітніх завдань з криптографії та стеганографії для CTF-змагань, яка дозволить студентам ефективно застосовувати отримані теоретичні знання та вдосконалювати практичні навички у вирішенні завдань з кібербезпеки. Запропонована методика сприяє формуванню фундаментальних знань та розвитку навичок, необхідних для розуміння й аналізу кіберзагроз, а також для ефективного застосування технік криптографії та стеганографії.

CTF-змагання активно використовують завдання з криптографії та стеганографії для перевірки знань та вмінь учасників. Однак, враховуючи неоднаковий рівень підготовки студентів, виникає необхідність адаптації складності та типів завдань для різних груп учасників. Крім того, поступове ускладнення завдань забезпечує можливість для розвитку критичного мислення та творчого підходу, що є невід'ємними якостями фахівця з кібербезпеки.

Розробка завдань з криптографії та стеганографії для студентських CTF-змагань включає декілька етапів:

1. **Аналіз цільової аудиторії:** Для створення ефективних завдань важливо враховувати рівень підготовки учасників. Для новачків доцільно пропонувати завдання з класичними криптографічними методами, такими як шифр Цезаря чи шифр Віженера, тоді як досвідченим учасникам варто включати сучасні алгоритми, наприклад, RSA та AES, або криптоаналітичні завдання.
2. **Структура завдань:** Розробка багаторівневої системи завдань з різною складністю, від простих завдань з дешифрування до виявлення прихованих даних у мультимедійних файлах. Це сприяє глибшому зануренню в предмет та розвиває в учасників здатність до розв'язання складних технічних завдань.
3. **Визначення вимог до завдань:** Завдання мають бути захоплюючими та поступово ускладнюватися, що стимулює учасників до застосування дедуктивного мислення. Ключовим аспектом є наявність чітких інструкцій та підказок, що полегшують процес розв'язання.
4. **Використання інструментів:** Для криптографії та стеганог-р]рафії використовуються інструменти на зразок CyberChef, Cryptool, DeepSound, Steghide, Audacity. Наприклад, Steghide дозволяє приховувати дані в зображеннях, а DeepSound — в аудіофайлах, що надає учасникам можливість практичного освоєння відповідних технологій.
5. **Оцінка ефективності:** Після розробки завдань проводиться їх тестування на групі студентів. Аналіз результатів і зворотний зв'язок допоможуть коригувати та вдосконалити методику, зробивши її максимально ефективною для освітніх цілей.

Запропонована методика розробки завдань з криптографії та стеганографії для студентських CTF-змагань має як теоретичну, так і практичну цінність. Теоретично вона формує системний підхід до створення завдань з поступовим ускладненням, враховуючи різний рівень підготовки учасників, що сприяє поглибленню знань студентів та розвитку їхніх навичок у галузі інформаційної безпеки. Практична значимість полягає у можливості впровадження розроблених завдань в освітній процес, що підвищить рівень підготовки студентів до реальних кіберзагроз та забезпечить їм практичний досвід у розв'язанні складних проблем з інформаційної безпеки.

Перспективи наступних досліджень включають розробку більш складних завдань з криптоаналізу, а також дослідження нових стеганографічних технік, які можуть бути використані в майбутніх CTF-змаганнях. Подальший розвиток методики дозволить удосконалити освітній процес та забезпечити глибше засвоєння матеріалу учасниками, розвиваючи навички, необхідні для ефективного реагування на кіберзагрози.

Список використаних джерел

1. Palriwala S. Composing CTF challenge. Medium. URL: https://medium.com/techloop/composing-ctf-challenge-b5828dba0feb (date of access: 02.12.2024).
2. Beginner's Guide – SANReN Cyber Security Challenge. SANReN Cyber Security Challenge. URL: https://www.csc.ac.za/?page_id=555 (date of access: 24.12.2024).