ПОЛОЖЕННЯ ПРО ХАКАТОН З КІБЕРБЕЗПЕКИ

ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. **Хакатон з кібербезпеки** (далі – Хакатон) проводиться з метою популяризації знань з кібербезпеки, удосконалення практичних умінь, розвитку креативного мислення та навичок командної роботи серед учасників. Цей захід об'єднає учнів, вчителів, викладачів та експертів у галузі кібербезпеки для обговорення актуальних викликів та розробки інноваційних рішень. Умови участі у хакатоні додаються.

1.2. Завдання Хакатону:

- Стимулювання інтересу до знань і вмінь з кібербезпеки серед місцевих громад;
- Розвиток практичних навичок з кіберзахисту;
- Створення умов для обміну досвідом між учасниками;
- Виявлення та підтримка талановитої молоді в сфері кібербезпеки.

Організатор Хакатону:

virtual routes

ДРОГОБИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА

with support from Google.org

.

СТРУКТУРА ХАКАТОНУ

- Хакатон проводиться у два етапи.
  - І етап – дистанційний (підготовка симуляції) до 12 квітня 2026 р.
  - ІІ етап – очний (командний: презентація симуляції і вирішення практичних завдань з кіберзахисту) 21-23 квітня 2026 р.
  - У ІІ етапі буде 2 тури: півфінал і фінал.
    У 1-тур ІІ етапу буде відібрано кращі команди по результату підготовлених симуляцій. Відбудеться 2 півфінали.
    У 2-турі ІІ етапу буде відібрано кращі 6 команд, які отримають завдання на вирішення практичних завдань з кіберзахисту.

УЧАСНИКИ ХАКАТОНУ

- До участі у Хакатоні запрошуються команди у складі 4 осіб і вчитель.
- Категорії учасників: учні 8-11 класів.
- Кожна команда має призначити капітана, який буде представляти команду під час реєстрації та спілкування з організаторами.
- Максимальна кількість команд від одного закладу освіти – 5.

ПОРЯДОК ПРОВЕДЕННЯ ХАКАТОНУ

- Дата проведення: **21-23 квітня 2026 р. (об 09.30)**
- Місце проведення: **Дрогобицький державний педагогічний університет імені Івана Франка (Дрогобич, вул. Стрийська, 3)**
- Реєстрація команд здійснюється до 12.04.2026 р. шляхом заповнення онлайн-форми: https://docs.google.com/forms/d/e/1FAIpQLSf2U2s8ioh5coaL_2qf9pTIBZA0hS4SnOTgzI9X7p34aURvpQ/viewform?usp=dialog
- При реєстрації необхідно надати інформацію про всіх учасників команди
- До 12.04.2026р необхідно надіслати виконане завдання.

ПРЕЗЕНТАЦІЯ ІНТЕРАКТИВНИХ СИМУЛЯЦІЙ (ПРОЄКТІВ)

Інтерактивна гра-симуляція, у якій гравець потрапляє в ситуацію шахрайства й обирає, як реагувати. Кожна дія веде до іншого кроку або наслідку.

1. Загальні вимоги до завдання першого етапу

У межах дистанційного етапу Хакатону кожна команда повинна підготувати інтерактивну симуляцію кіберзагрози, яка моделює реалістичну ситуацію цифрового шахрайства або соціальної інженерії.

Інтерактивна симуляція — це навчальний цифровий сценарій у форматі гри, квесту або розгалуженої історії, у якій користувач потрапляє в ситуацію потенційної кіберзагрози та повинен обрати спосіб реагування. Кожне рішення повинно впливати на подальший розвиток подій та демонструвати можливі наслідки поведінки користувача.

Основною метою виконання завдання є формування практичних навичок розпізнавання кіберзагроз, розвитку критичного мислення та усвідомленої

поведінки користувачів у цифровому середовищі.

Симуляція повинна не лише демонструвати приклади кіберзагроз, але й навчати учасників правильної поведінки в подібних ситуаціях.

2. Основні вимоги до симуляції

Кожна команда повинна підготувати одну завершену інтерактивну симуляцію, яка відповідає таким вимогам:

1. Симуляція повинна містити від 8 до 12 змістовних кроків (ситуацій).
2. Кожен крок повинен описувати окрему ситуацію, у якій користувач отримує певне повідомлення, дзвінок, файл, посилання або інший елемент цифрової взаємодії.
3. У кожному ключовому кроці повинно бути не менше двох і не більше чотирьох варіантів дій.
4. Кожен варіант вибору повинен мати чітко визначений наслідок, який впливає на подальший розвиток подій.
5. Симуляція повинна містити не менше трьох різних завершень, які відображають різні результати дій користувача (успішне вирішення ситуації, частково правильну поведінку або помилкові дії).
6. Після завершення симуляції повинні бути подані пояснення правильних і помилкових рішень, а також практичні рекомендації щодо безпечної поведінки в інтернеті.
7. Симуляція повинна бути логічно побудованою, зрозумілою для користувача та мати чітку структуру розвитку подій.

3. Рекомендована структура симуляції

Симуляція повинна складатися з таких логічних етапів:

3.1. Вступ

Короткий опис ситуації, у якій опиняється користувач. Необхідно пояснити контекст події, описати цифрове середовище та обставини, що передують виникненню кіберзагрози.

3.2. Початкова взаємодія

Користувач отримує перший сигнал про потенційну загрозу (повідомлення, лист, дзвінок, посилання, файл тощо).

3.3. Прийняття рішень

Користувач повинен обрати один із запропонованих варіантів дій. Вибір впливає на подальший розвиток сценарію.

3.4. Розвиток ситуації

Події ускладнюються, з’являються додаткові ознаки шахрайства, психологічний тиск або нові елементи взаємодії.

3.5. Перевірка інформації

Користувач отримує можливість перевірити достовірність інформації через альтернативні джерела або інші канали зв'язку.

3.6. Реакція на загрозу

Користувач повинен обрати спосіб реагування після усвідомлення ризику.

3.7. Завершення

Симуляція завершується одним із можливих результатів залежно від прийнятих рішень.

3.8. Підсумки та рекомендації

У фінальній частині симуляції повинні бути подані висновки та рекомендації щодо безпечної поведінки в подібних ситуаціях.

4. Тематика симуляцій

Тематика симуляції повинна стосуватися актуальних загроз у цифровому середовищі.

Рекомендовані теми:

- шахрайство у соціальних мережах;
- фішингові електронні листи;
- SMS-шахрайство (смишинг);
- телефонне шахрайство (вішинг);
- підроблені сайти авторизації;
- шахрайство через QR-коди;
- фейкові інтернет-магазини;
- шахрайські повідомлення в месенджерах;
- шкідливі вкладення у листах;
- встановлення підозрілих програм;
- маніпуляції в онлайн-іграх або чатах;
- інші приклади соціальної інженерії.

Команди можуть запропонувати власну тему симуляції за умови, що вона відповідає тематиці кібербезпеки та цифрової безпеки користувачів.

5. Формат виконання роботи

Симуляція може бути створена у будь-якому цифровому інструменті, який дозволяє реалізувати розгалужену структуру сценарію.

Рекомендовані інструменти:

- Google Slides;
- Google Forms;
- Canva;

- PowerPoint;
- PDF-документ з інтерактивними переходами;
- веб-сторінка або мінісайт;
- програмний застосунок.

Команди можуть використовувати й інші інструменти за умови, що робота буде доступною для перегляду журі.

6. Матеріали, які подає команда

Для участі в першому етапі команда повинна подати такі матеріали:

1. Основний файл або посилання на інтерактивну симуляцію.
2. Короткий опис проєкту (обсяг до 2 сторінок), у якому зазначається:
   - назва команди;
   - назва симуляції;
   - обрана тема;
   - мета створення симуляції;
   - короткий опис сценарію;
   - використаний інструмент.
3. Інструкцію щодо перегляду або запуску симуляції (за потреби).

Усі подані матеріали повинні бути доступними для відкриття та перегляду.

7. Загальні вимоги до якості роботи

Симуляція повинна:

- бути правдоподібною та відображати реальні ситуації кіберзагроз;
- містити логічну послідовність подій;
- демонструвати наслідки кожного вибору користувача;
- сприяти формуванню навичок безпечної поведінки в інтернеті;
- бути зрозумілою та зручною для проходження.

Особлива увага приділяється навчальній цінності, реалістичності сценарію та якості пояснення правильних рішень.

Що важливо:

- Симуляція має бути правдоподібною: таке могло б статися з будь-ким у класі.
- Кожен вибір має мати наслідок, а не бути "правильна/неправильна" відповідь.
- Гравець має відчути, що вчиться мислити, а не просто здогадуватись.
- Додайте емоції, гумор, трохи напруги — зробіть це цікаво.
- Найголовніше: пояснюйте кожен вибір. Це навчання!

ВИЗНАЧЕННЯ ПЕРЕМОЖЦІВ ТА НАГОРОДЖЕННЯ

- Для відзначення досягнень учасників журі встановлює спеціальні номінації, щоб кожна команда отримала відзнаку та визнання.

КОНТАКТНА ІНФОРМАЦІЯ

- Додаткову інформацію можна отримати:

  Телефон: 050 430 27 63; 067 89 24 912
  Електронна пошта: **cybersecurity@dspu.edu.ua**

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

- Організатори залишають за собою право вносити зміни до даного Положення, повідомляючи про це учасників заздалегідь.
- Подання заявки на участь у Хакатоні означає повну згоду з умовами цього Положення.
- Усі спірні питання вирішуються організаторами Хакатону.

Приклади можливих сценаріїв

СЦЕНАРІЙ: «Посилка, яка може коштувати ваших даних»

Вступна ситуація

Після школи ти перевіряєш телефон і бачиш нове SMS-повідомлення:
"Вашу посилку затримано на митниці. Для отримання необхідно сплатити митний платіж 52 грн. Перейдіть за посиланням: delivery-support.site"
Ти не пам’ятаєш, щоб замовляв посилку, але нещодавно справді купував щось в інтернеті.

КРОК 1. Перше рішення

Що ти зробиш?
A) Натиснеш на посилання
B) Перевіриш номер відправника
C) Проігноруєш повідомлення
Наслідки
A → Перехід до КРОКУ 2
B → Перехід до КРОКУ 3
C → Перехід до КРОКУ 4

КРОК 2. Сторінка оплати

Після переходу відкривається сторінка, схожа на сайт служби доставки.
Там потрібно ввести:

- номер картки
- CVV код
- одноразовий SMS-код

Що ти зробиш?
A) Введеш дані картки
B) Перевіриш адресу сайту
C) Закриєш сторінку
Наслідки
A → ГРА ЗАВЕРШЕНА (викрадення банківських даних)
B → Перехід до КРОКУ 3
C → Перехід до КРОКУ 4

КРОК 3. Перевірка повідомлення

Ти звертаєш увагу, що номер відправника виглядає дивно.
Крім того, посилання не схоже на офіційний сайт служби доставки.
Що ти зробиш?
A) Знайдеш офіційний сайт доставки
B) Зателефонуєш у службу підтримки
C) Повернешся на сайт і оплатиш
Наслідки
A → Перехід до КРОКУ 5
B → Перехід до КРОКУ 5
C → ГРА ЗАВЕРШЕНА (шахрайство)

КРОК 4. Сумніви

Ти не переходиш за посиланням, але повідомлення викликає занепокоєння.
Що ти зробиш?
A) Перевіриш свої інтернет-замовлення
B) Пошукаєш інформацію про номер відправника

C) Натиснеш на посилання пізніше
Наслідки
A → Перехід до КРОКУ 5
B → Перехід до КРОКУ 5
C → Перехід до КРОКУ 2

КРОК 5. Нове повідомлення

Через кілька хвилин приходить нове SMS:
"Останнє попередження. Якщо оплата не буде здійснена протягом 10 хвилин, посилка буде повернена."
Що ти зробиш?
A) Натиснеш на посилання
B) Перевіриш інформацію через офіційний сайт
C) Проігноруєш повідомлення
Наслідки
A → Перехід до КРОКУ 2
B → Перехід до КРОКУ 6
C → Перехід до КРОКУ 6

КРОК 6. Перевірка фактів

Ти знаходиш офіційний сайт служби доставки.
Там немає жодної інформації про посилку.
Що ти зробиш?
A) Зателефонуєш у службу підтримки
B) Пошукаєш у Google інформацію про подібні SMS
C) Повернешся до SMS і натиснеш на посилання
Наслідки
A → Перехід до КРОКУ 7
B → Перехід до КРОКУ 7
C → Перехід до КРОКУ 2

КРОК 7. Викриття схеми

Ти дізнаєшся, що це **поширена схема SMS-шахрайства (смишинг)**.
Мета шахраїв — змусити людей перейти на підроблений сайт і ввести банківські дані.
Що ти зробиш?
A) Заблокуєш номер
B) Повідомиш про шахрайство службі доставки
C) Видалиш повідомлення
Наслідки
A або B → Перехід до КРОКУ 8
C → Перехід до КРОКУ 8 (пасивна реакція)

КРОК 8. Захист інших

Ти вирішуєш попередити інших людей.
Що ти зробиш?
A) Напишеш у шкільний чат
B) Надішлеш скріншот друзям
C) Нічого не скажеш
Наслідки
A або B → Перехід до КРОКУ 9
C → Перехід до КРОКУ 9

КРОК 9. Нова спроба шахраїв

Через годину надходить повідомлення у Telegram:
"Ми помітили, що ви не оплатили доставку. Перейдіть за новим посиланням."
Що ти зробиш?
A) Проігноруєш повідомлення
B) Поскаржишся на акаунт
C) Натиснеш на посилання

Наслідки

A або B → Перехід до КРОКУ 10
C → ГРА ЗАВЕРШЕНА (шахрайство)

КРОК 10. Усвідомлення загрози

Ти розумієш, що шахраї використовують кілька каналів:

- SMS
- підроблені сайти
- месенджери

Це типова схема соціальної інженерії.
Що ти зробиш?
A) Перевіриш налаштування безпеки телефону
B) Розповіси батькам або вчителю
C) Нічого не робитимеш

Наслідки

A або B → Перехід до КРОКУ 11
C → Перехід до КРОКУ 11 (але без додаткового захисту)

КРОК 11. Безпечна поведінка

Ти виконав кілька важливих дій:

- не перейшов за підозрілим посиланням
- перевірив інформацію
- попередив інших

Це допомогло уникнути шахрайства.

КРОК 12. Підсумок симуляції

На екрані з’являється результат:
Результат може бути різним:

Кібергерой

Ти правильно перевірив інформацію та допоміг іншим уникнути шахрайства.

Уважний користувач

Ти уникнув шахрайства, але міг би активніше попередити інших.

У зоні ризику

Ти майже став жертвою шахраїв. Наступного разу будь уважнішим.

Поради з кібергігієни

• Не переходьте за підозрілими посиланнями
• Перевіряйте адресу сайту
• Не вводьте дані банківських карток на невідомих сторінках
• Перевіряйте інформацію через офіційні джерела
• Не піддавайтеся на повідомлення з відчуттям терміновості
• Блокуйте шахрайські номери
• Попереджайте інших користувачів