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:

.

СТРУКТУРА ХАКАТОНУ

- Хакатон проводиться у два етапи.
  - І етап – дистанційний (підготовка симуляції) 1-15 травня 2025 р.
  - ІІ етап – очний (командний: презентація симуляції і вирішення практичних завдань з кіберзахисту) 20-22 травня 2025 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 2-4 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.

ПОРЯДОК ПРОВЕДЕННЯ ХАКАТОНУ

- Дата проведення: **20-22 травня 2025 р. (об 09.30)**
- Місце проведення: **Дрогобицький державний педагогічний університет імені Івана Франка (Дрогобич, вул. Стрийська, 3)**
- Реєстрація команд здійснюється до 01.05.2025 р. шляхом заповнення онлайн-форми: https://docs.google.com/forms/d/e/1FAIpQLScELxBEzMcFW6u2ouNdhIdNeDUMlGGg_3U82ERs7IuvXN6GjA/viewform?usp=header
- При реєстрації необхідно надати інформацію про всіх учасників команди
- До 15.05.2025р слід 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.

- **Завдання для команди:**

Ваша команда має створити **власну симуляцію** кіберзагрози — це гра або тест, у якому гравець потрапляє у типовий випадок інтернет-шахрайства (наприклад, фейкове повідомлення чи дзвінок) і має зробити вибір. Кожне рішення впливає на розвиток подій. Ваш симулятор має не лише показати загрозу, а й навчити уникати її. В межах 1 етапу команда готує 4 симуляції.

- **Структура симуляції:**

Кілька ситуацій-кроків (4 і більше) — кожна з них містить повідомлення або діалог і варіанти дій. Один із них правильний, інші — помилкові або небезпечні.

Алгоритми дій та наслідки:

- Кожна дія веде до наступного кроку або до завершення гри;
- Можливе "відновлення" після помилки або одразу поразка;
- Чим глибше проходить гравець — тим більше дізнається про шахрайські методи.

Фінал:

- Висновки та поради;
- Підсумкова оцінка (кібергерой / уважний користувач / у зоні ризику);

Теми для симуляторів:

- Шахрай у соцмережах (Instagram, Telegram — просить гроші, надсилає підозріле фото/файл)
- SMS про виграш, доставку, митні платежі (смишинг)
- Дзвінок від "банку", "Google", "техпідтримки" (вішинг)
- Підроблений сайт авторизації / підміна адреси (фішинг)
- QR-код, наклеєний у громадському місці
- Лист з вкладенням від невідомого адресата (фішинг + шкідливе ПЗ)
- Повідомлення про "акцію" або "приз" — треба ввести особисті дані
- Шахрай у шкільному чаті — просить терміново щось зробити (приклад фейкового педагога/учня)
- Фейковий інтернет-магазин із суперзнижками (збір даних карток)
- Запит на встановлення шкідливого додатку "для безпеки"
- Соціальні маніпуляції у грі/дискорд-чаті — змушують передати дані акаунту
- Лист щастя: "Ваш комп'ютер зламано, ми бачимо вашу камеру, скиньте гроші"
- Псевдовідео від YouTube-акаунту знайомого з лінком на фішинговий сайт
- Інші теми що стосуються соціальної інженерії

Як оформити симулятор:

1. **Оберіть формат:**

- Google Slides (слайди з гіперпосиланнями);
- Google Forms (із гілками залежно від вибору);
- Canva (імітація чату);
- PowerPoint / PDF (історія з варіантами дій);

2. **Побудуйте сценарій:**

- Від 4 ситуацій-кроків і більше (залежно від теми);
- Кожна ситуація має 2–3 варіанти дій;

- Вкажіть, що буде після кожного вибору;
- Додайте коротке пояснення: чому варіант безпечний або ні;

3. **Після проходження гри:**

- Напишіть 5–7 порад з кібергігієни за темою;
- Додайте коротку підсумкову оцінку: скільки правильних рішень, висновки.

4. **Підготуйте коротку презентацію для проєкту:**

- Як обрали теми?
- Що хотіли донести до гравців?
- Що було складно/цікаво?
- Час презентації проєкту – до 10 хвилин.

Як подати роботу:

- Завантажте архів або файл із симуляцією (PDF, презентація, посилання);
- Додайте короткий опис проєкту (Word або Google Docs);
- Упевніться, що всі посилання відкриваються та файли працюють.

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: "Привіт, це я... чи ні?"

КРОК 1: Несподіване повідомлення

Ти отримуєш повідомлення в Instagram: "Привіт! Це Ігор. Я зараз із чужого акаунта, бо свій зламали. Мені терміново потрібні гроші — допоможеш?"

Варіанти:

- A) Погодитися надіслати гроші — він же друг!
- B) Попросити уточнення — наприклад, спитати, про що ви говорили вчора в школі.
- C) Написати Ігорю на Viber або Telegram, щоб перевірити.

Дії при виборі варіанту

- A → Перехід до КРОКУ 2A (довіра без перевірки)
- B або C → Перехід до КРОКУ 2B (перевірка, але шахрай не здається)

КРОК 2A: Фальшивий номер картки

Фейковий "Ігор" надсилає номер картки з чужим прізвищем і тисне: "Кидай сюди. Дуже терміново!"

Варіанти:

- A) Надіслати 200 грн
- B) Звернути увагу на інше прізвище
- C) Сказати, що передзвониш, і перевірити

Дії при виборі варіанту

- A → ГРА ЗАВЕРШЕНА: втрачено кошти (ПОРАЗКА)
- B або C → Перехід до КРОКУ 3 (перехід на шлях безпеки)

КРОК 2B: Спроба обійти перевірку

Фейковий Ігор відповідає: "Ну серйозно, у мене зараз немає часу грати в загадки. Просто допоможи!"

Варіанти:

- A) Вибачитися і скинути гроші
- B) Сказати, що без перевірки нічого не зробиш
- C) Повідомити в кіберполіцію або класному керівнику

Дії при виборі варіанту

- A → ГРА ЗАВЕРШЕНА: поразка
- B → Перехід до КРОКУ 3
- C → Перехід до КРОКУ 3 із бонусом

КРОК 3: Звірка фактів

Ти перевіряєш справжнього Ігоря в Telegram. Він каже: "Мене ніхто не ламав. Я взагалі вдома!"

Варіанти:

- A) Повідомити адміністрацію Instagram про фейковий акаунт
- B) Заблокувати профіль
- C) Надіслати скріншоти іншим друзям, щоб не повелись

Дії при виборі варіанту

Усі три — правильні кроки. Перехід до КРОКУ 4

КРОК 4: Реакція на загрозу

Ти хочеш захистити себе й інших:

Варіанти:

- A) Створити короткий пост з попередженням
- B) Надіслати скаргу на фейковий акаунт
- C) Проігнорувати — це не твоя справа

Дії при виборі варіанту

- A або B → Перехід до КРОКУ 5 (правильна відповідальна поведінка)
- C → Закінчення без активних дій (НЕПОРАЗКА, але слабкий результат)

КРОК 5: Підсумок і поради

На екрані з’являється підсумок:

"Ти правильно розпізнав(-ла) загрозу. Такі ситуації трапляються щодня — завдяки твоїй уважності ще менше людей стануть жертвами."

- Завжди перевіряй, хто тобі пише.
- Не реагуй на тиск або терміновість.
- Перевір дані через інший канал.
- Запитуй те, що знає лише справжній знайомий.
- Не надсилай гроші без підтверджень.
- Повідомляй про фейкові акаунти.
- Допомагай друзям бути обережними.