Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №7

Соціальна інженерія та моделювання фішингу (SET)

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** вивчити підходи соціальної інженерії та навчитися виявляти ознаки фішингу.

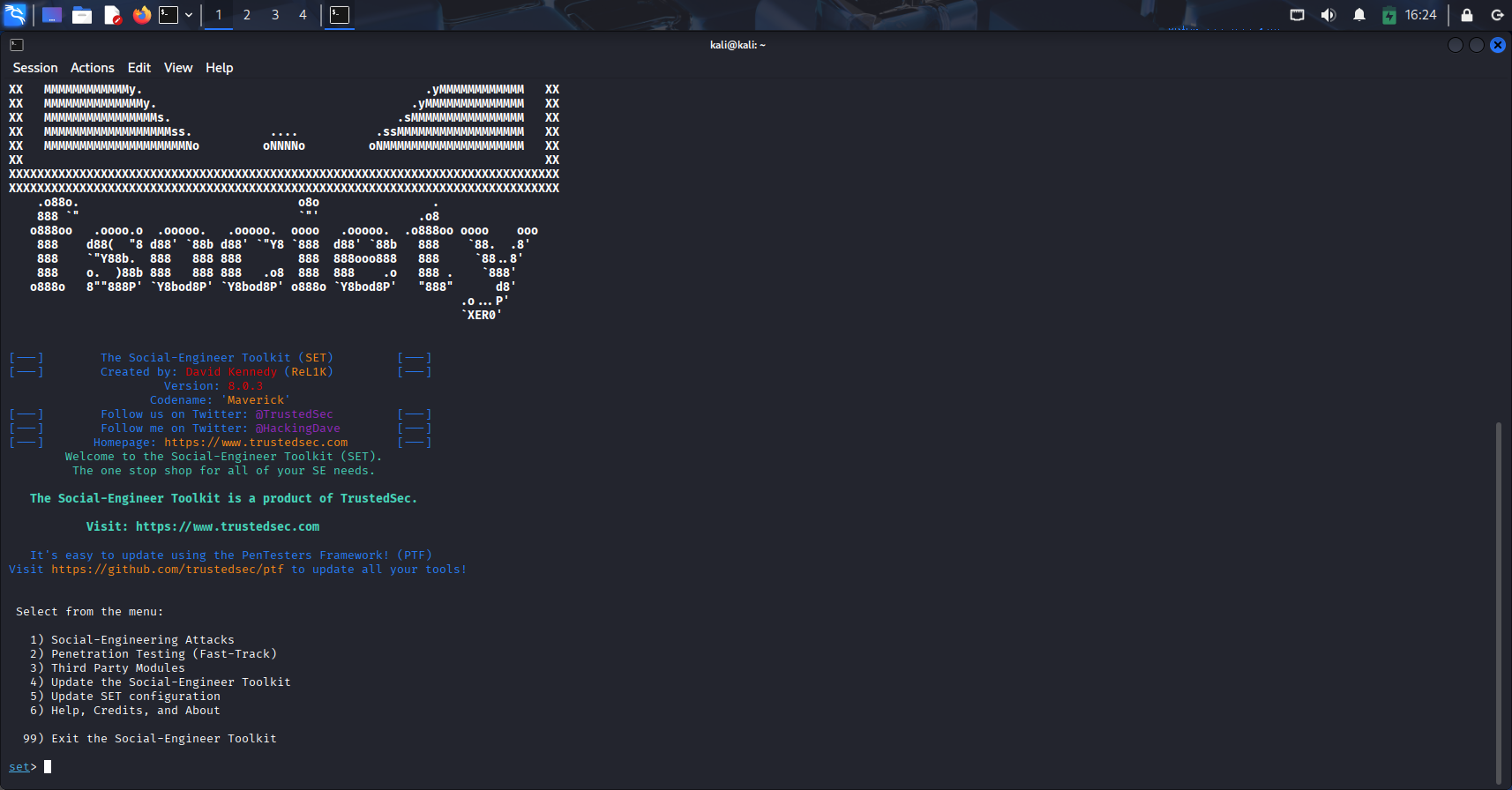
**Опис середовища:**

ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109, The Social-Engineer Toolkit (SET) Created by: David Kennedy (ReL1K) Version: 8.0.3, Local Kali ip: 192.168.135.130, Local Lubuntu ip: 192.168.135.133

**Команди:**

1) Запустити setoolkit:

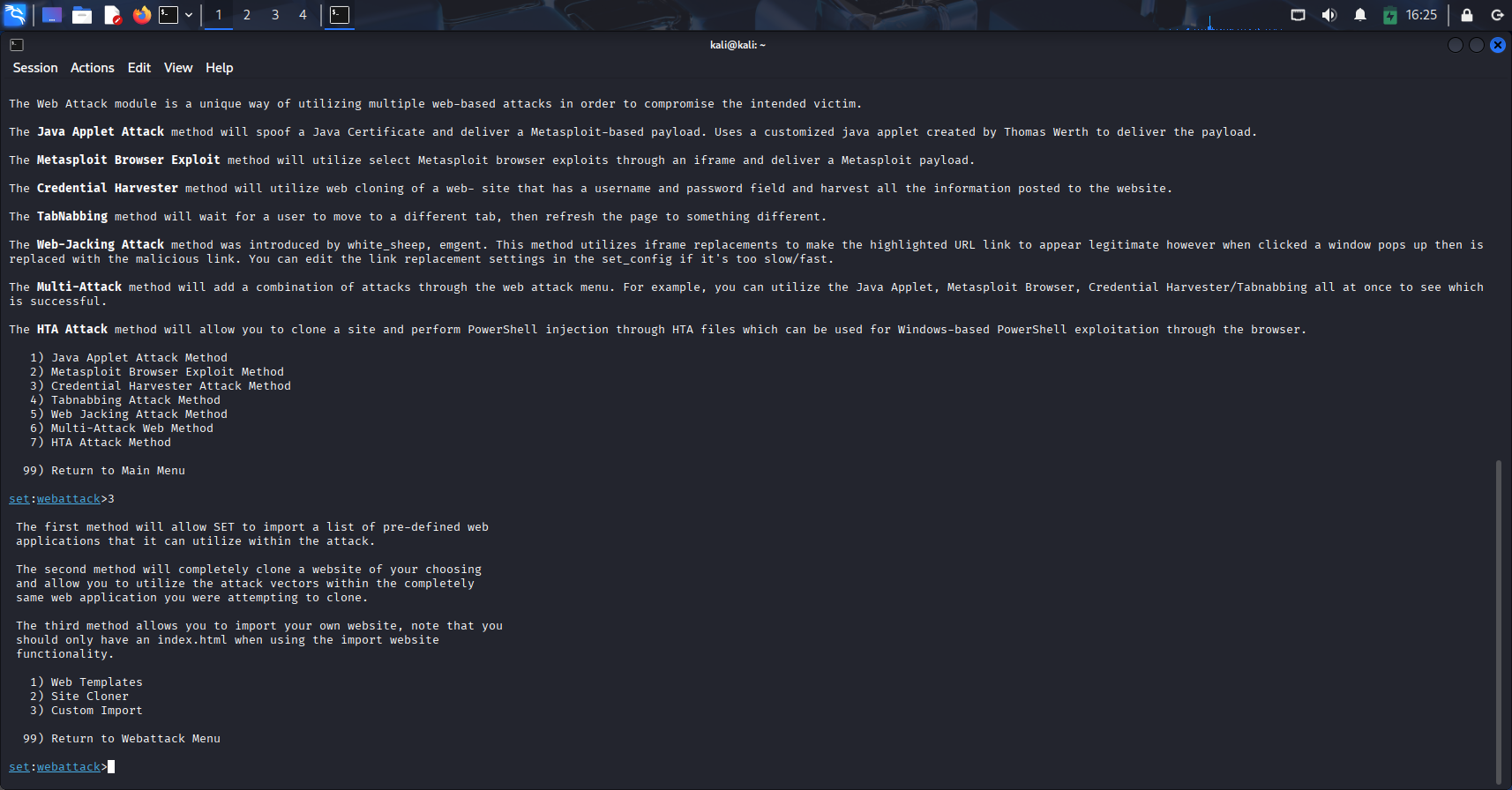
sudo setoolkit



2) Вибрати Website Attack Vectors -> Credential Harvester, налаштувати локальну

сторінку.

Вибираємо Site Cloner

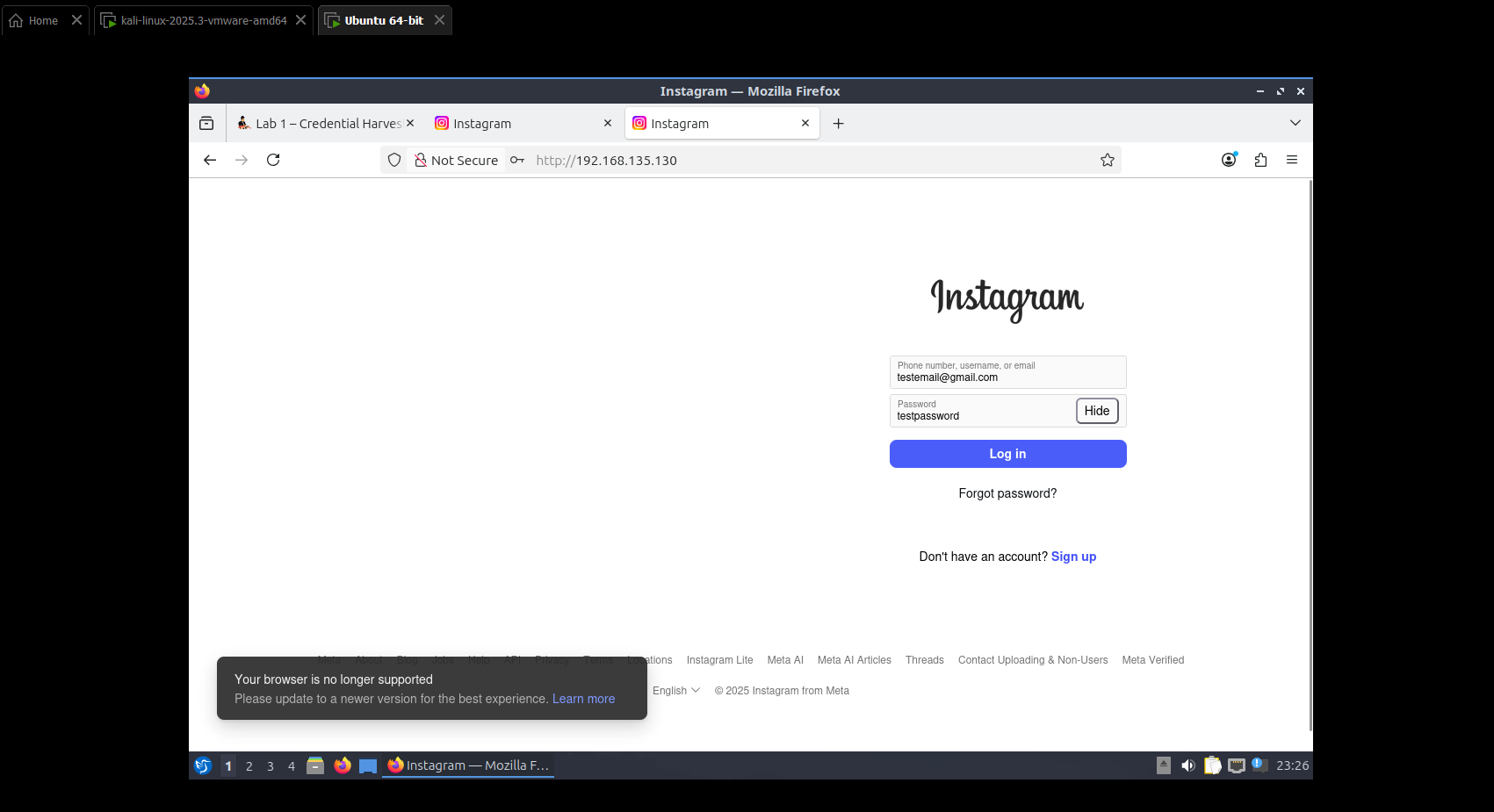


Вводимо IP адресу(можна лишити за замовчуванням).

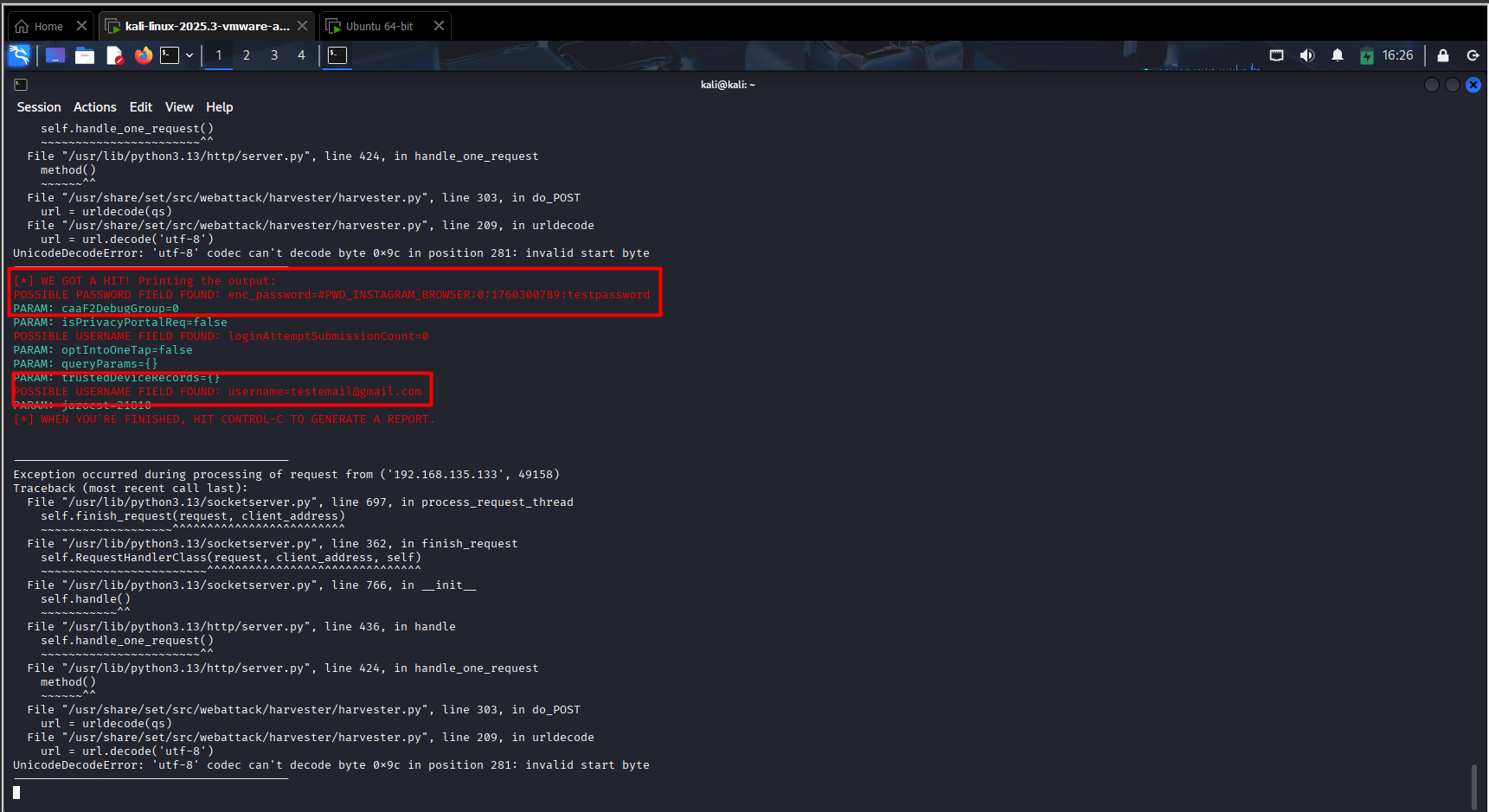
Вводимо адресу сайту, який будемо копіювати.

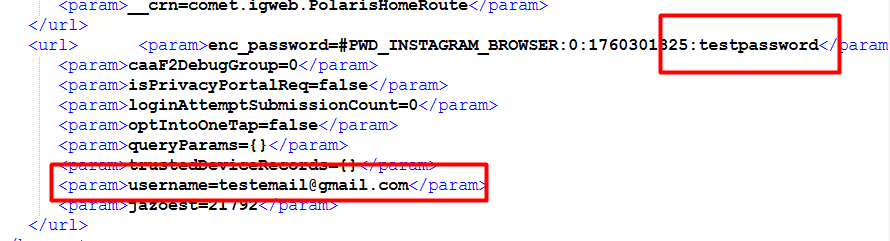


Об'єктом фішингової атаки буде друга віртуальна машина з встановленим дистрибутивом Lubuntu. На ній відкриваю веб-браузер. В рядок пошуку пишу IP адресу Kali Linux машини. Заповняю поля.



Як бачимо, SET перехопив POST-запити і результат виводиться в консоль. Ми перехопили дані, які користувач вводив в поля на фішинговому сайті. Звіт доступний по шляху /root/.set/reports







3) Аналіз заголовків емейлів та URL, створити чекліст виявлення фішингу

**Чекліст для виявлення фішингу**

1. Аналіз адреси сайту (URL):

Чи це IP-адреса? Справжні сайти майже ніколи не використовують IP-адресу (наприклад, 192.168.1.10) замість доменного імені (наприклад, instagram.com).

Чи захищене з'єднання (HTTPS)? Легітимні сайти, які працюють з логінами та паролями, завжди використовують захищений протокол https:// (із замком у адресному рядку). Відсутність s (http://) є тривожним сигналом.

Чи правильне доменне ім'я? Зловмисники часто реєструють схожі домени, використовуючи друкарські помилки (наприклад, instagrarn.com замість instagram.com) або додаючи слова (наприклад, instagram-login.com).

Чи підозрілі субдомени? Шахраї можуть використовувати справжній домен як субдомен для фейкового сайту (наприклад, instagram.secure-auth.com). Тут основний домен — secure-auth.com, а не instagram.com.

2. Аналіз джерела (електронного листа або повідомлення):

Адреса відправника. Чи збігається адреса з офіційною? Чи немає в ній помилок? Часто адреса може виглядати схожою, але бути з іншого домену (наприклад, support@mail-instagram.com).

Заголовки листа. Необхідно аналізувати технічні заголовки емейлів. Перевіряйте розбіжності у полях From та Return-Path та результати перевірок SPF/DKIM/DMARC.

**Аналіз фішингової сторінки, використаної в лабораторній роботі:**

В адресному рядку вказано http://192.168.135.130. Це локальна IP-адреса, а не офіційний домен www.instagram.com. Це найбільш очевидна ознака фішингу. Використовується протокол http://, а не https://. Сам браузер попереджає про це, показуючи напис "Not Secure" зліва від адреси. Справжня сторінка входу в Instagram завжди буде захищена.

Візуально сторінка є точною копією справжньої сторінки входу в Instagram. Логотип, поля для введення даних, кнопки та посилання в нижній частині сторінки повністю імітують оригінал. Це демонструє, наскільки ефективними можуть бути інструменти для клонування сайтів, як-от SET. Будь-які дані (номер телефону, ім'я користувача, пароль), введені на цій сторінці та надіслані через кнопку "Log in", не потраплять до Instagram. Натомість вони будуть перехоплені вебсервером, запущеним на машині з IP-адресою 192.168.135, і збережені у лог-файл, як це передбачено лабораторною роботою.

**Висновки:** Під час виконання лабораторної роботи було на практиці освоєно методику проведення атаки соціальної інженерії за допомогою інструментарію Social-Engineer Toolkit (SET). Було успішно створено клон вебсайту для збору облікових даних (Credential Harvester Attack), що дозволило наочно зрозуміти механізм фішингових атак. На основі отриманого досвіду було розроблено чекліст для виявлення фішингу, що є важливим практичним навиком для захисту від подібних кіберзагроз.