Індивідуальне дослідницьке завдання

Дослідження комп’ютерних вірусів:

- **ILOVEYOU**
- **Stuxnet**
- **WannaCry**

Мета

1. Розвинути навички критичного аналізу кіберінцидентів.
2. Зрозуміти механізми інфікування, дії шкідливого коду та наслідки для суспільства/інфраструктури.
3. Навчитись формулювати рекомендації щодо запобігання та реагування.

Обов’язкові вимоги з кібербезпеки (читати першими!)

- **Категорично заборонено** намагатися запускати справжні зразки вірусу на робочому ПК.
- Аналіз виконується **виключно** на основі публічних технічних звітів.
- Для загальної інформації: технічні дослідження (dynamic analysis) виконуються виключно у спеціалізованих комп’ютерних лабораторіях із захищеним програмним та мережевим середовищем, часто для цього використовуються знімки коду (snapshots, dumps) і обмежують та контролюють трафік.
- Використовуйте тільки **авторитетні джерела** (аналізи антивірусних вендорів, CERT, наукові статті, офіційні звіти).

Завдання та кроки виконання

1) Загальна інформація про об’єкти

- ILOVEYOU (соціально-орієнтований масовий вірус/черв’як, 2000)
- Stuxnet (цільовий саботажний worm/зловмисний код проти промислових систем, ~2010)
- WannaCry (ransomware, глобальна хвиля 2017)

2) Збір джерел

- Збір 5–10 авторитетних джерел (технічні звіти вендорів, CERT-аналізи, наукові публікації, статті журналістів-аналітиків) для кожного об’єкту.

- Коротка бібліографія (посилання, рік, короткий опис що в джерелі).

3) Історичний та контекстний опис

Включити:

- Коли і як виявлено; регіональні вогнища; масштаби (кількість жертв, постраждалих організацій).
- Політичний/соціальний/економічний контекст (наприклад, Stuxnet і промисловий саботаж; WannaCry і старі вразливості в SMB; ILOVEYOU і соціальна інженерія).

4) Загальний технічний аналіз (у рамках фахового рівня Вашої спеціальності)

Фактичні деталі:

- Вектор інфікування (як вірус потрапляв у системи: e-mail, USB, мережа, оновлення).
- Механізм розповсюдження (самореплікація, черв’як, поширення через мережеві сервіси).
- Payload (що саме робив вірус: шифрування файлів, шпигунство, модифікація ПЛК тощо).
- Використані вразливості/техніки.
- Технічні індикатори (IOC): домени, IP, хеші (за наявності у відкритих джерелах) — просто перерахувати (**не завантажуйте зразки!**).

Обов’язково надайте тлумачення термінів та скорочень (наприклад, «SMB» - мережевий протокол для спільного доступу до файлів).

5) Соціальні, економічні і правові наслідки

- Фінансові збитки, вплив на бізнес/державні установи, людські наслідки (перервані послуги), юридичні/регуляторні/політичні реакції (за наявності певних видів).

6) Реакція та контрзаходи

- Які кроки зробили організації, вендори і держави (патчі, оновлення, ботнет-відключення, закони).
- Короткострокові (patch, block C2) і довгострокові (архітектурні зміни, процеси) заходи.

7) Уроки та рекомендації

- Практичні поради для користувачів, організацій та політиків (наприклад, політика резервного копіювання, оновлення, сегментація мережі, освіта персоналу) по кожному типу досліджуваних об’єктів окремо.

Формат і результати

1. **Загальний об’єм звіту не має перевищувати** 10 сторінок і має бути структурованим за пунктами 2–7 по кожному об’єкту досліджень.
2. **Окремо підготувати презентацію** (5–8 слайдів) — коротко: проблема, механізм інфікування, наслідки, висновки.
3. **Інфографіка / timeline** — візуальне відтворення етапів інфікування та відповідей на кіберзагрозу по кожному об’єкту.

Контрольні запитання для перевірки якості звіту з ІДЗ

1. Хто і коли виявив вірус?
2. Який був первинний вектор інфікування?
3. Як вірус розповсюджувався далі?
4. Які технічні механізми використовував (вразливості, експлойти, методи приховування)?
5. Який був payload і які системи/сервіси зачепив?
6. Які були наслідки (технічні, економічні, соціальні)?
7. Які заходи були вжиті для припинення поширення і відновлення?
8. Які уроки можна винести та які рекомендації для сьогодення?

Критерії оцінювання (всього 20 балів)

- **Збір джерел і їх якість** — 4 бали
- **Повнота історичного контексту** — 3 бали
- **Ясність технічного аналізу (у межах своєї спеціальності)** — 5 балів
- **Аналіз наслідків і рекомендацій** — 4 бали
- **Оформлення звіту та презентації** — 2 бали
- **Креативність (інфографіка, timeline)** — 2 бали