МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інформаційних технологій та інноваційного підприємництва

Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

«ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Одеса – 2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувач кафедри «Кібербезпека та захист інформації»

Методичні вказівки схвалено на засіданні кафедри «Кібербезпека та захист інформації»
(Протокол від «06» жовтня 2025 р. № 2)

Методичні вказівки схвалено на засіданні НМК ННІ ІТІП
(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

Вступ	4
Лабораторна робота №1. ІНФОРМАЦІЙНА РОБОТА	5
Лабораторна робота №1. АНАЛІТИЧНА РОБОТА	13
Література	20
Додаток 1	21

ВСТУП

У сучасних умовах глобальної цифровізації, загострення геополітичного протистояння та стрімкого розвитку гібридних загроз забезпечення кібербезпеки та захисту інформації виходить за межі суто технічних і програмно-апаратних рішень. Ефективна протидія сучасним викликам у кіберпросторі вимагає від фахівців високого рівня стратегічного мислення, а також спроможності орієнтуватися у колосальних масивах інформації. Дисципліна «Інформаційно-аналітичне забезпечення інформаційної безпеки» є невіддільним складником підготовки магістрів спеціальності F5 Кібербезпека та захист інформації, оскільки вона формує фундаментальні знання та практичні навички, необхідні для виявлення, оцінювання та прогнозування ризиків безпеки на основі глибокого аналізу даних.

Практичний складник курсу орієнтований на опанування здобувачами двох взаємопов’язаних, але методологічно відмінних етапів: інформаційної та аналітичної роботи. Інформаційна робота закладає базис системи захисту, навчаючи майбутніх експертів здійснювати верифікований пошук у різноманітних джерелах, оцінювати достовірність отриманих відомостей, усувати дублювання та деструктивний інформаційний шум.

Логічним продовженням та інтелектуальним ядром дисципліни є аналітична робота. На цьому етапі магістранти вчаться перетворювати первинно оброблені, «сирі» факти у прикладні знання, що мають високу практичну цінність для керівництва організацій та державних інституцій. Застосовуючи методи причинно-наслідкового аналізу, інтеграції та розпізнавання шаблонів кібератак, здобувачі отримують досвід побудови багатоваріантних прогнозів розвитку кризових ситуацій та формулювання чітких, стратегічно обґрунтованих рекомендацій щодо мінімізації безпекових ризиків.

Ці методичні вказівки розроблені з метою надання чіткої інформаційної та методологічної підтримки здобувачам другого (магістерського) рівня вищої освіти спеціальності F5 Кібербезпека та захист інформації під час виконання лабораторних робіт. Матеріали містять детальні теоретичні основи, покрокові інструкції, практичні кейси (зокрема аналіз кіберінцидентів на кшталт витоку даних), а також вимоги до оформлення звітів із дотриманням принципів академічної доброчесності. Самостійне виконання запропонованих завдань сприятиме формуванню у майбутніх магістрів професійних компетентностей, необхідних для успішного вирішення складних задач у сфері забезпечення інформаційної та кібербезпеки України.

Лабораторна робота №1.

Тема: ІНФОРМАЦІЙНА РОБОТА

Мета роботи: Опанувати методи інформаційної роботи як етапу інформаційно-аналітичного забезпечення інформаційної безпеки шляхом отримання навичок праці з різними джерелами, відбору фактів, відсіювання недостовірних даних, отримання вмінь формувати структурований інформаційний масив, який стане основою для подальшого аналізу.

Очікуваний результат: Підготовлений структурований інформаційний масив (без інтерпретацій), який можна використати для подальшої аналітичної роботи.

1. Теоретичні основи інформаційної роботи

Інформаційна робота – це процес організованого пошуку, збору, перевірки та первинної обробки даних, які надходять із різних джерел. Її основне завдання – забезпечити аналітика достовірним та впорядкованим інформаційним масивом для подальшого аналізу та прийняття рішень. На відміну від аналітичної роботи, інформаційна не ставить собі за мету побудову прогнозів чи формування висновків, але вона є обов'язковим підґрунтям для будь-якої аналітики.

Основні етапи інформаційної роботи:

– *Інформаційний пошук.*

Пошук здійснюється у відкритих (ЗМІ, Інтернет, соціальні мережі, офіційні звіти), напівзакритих (галузеві бази даних, професійні спільноти) та закритих джерелах (внутрішні документи організації).

– *Перевірка достовірності.*

Достовірність інформації визначається ступенем її наближеності до першоджерела. Тут важливо відрізняти довіру до джерела від його реальної «чистоти».

– *Первинна обробка.*

Отримані дані сортуються, виділяються ключові слова, складаються базові категорії. На цьому етапі інформація ще не аналізується, але вже впорядковується для зручності подальшої роботи.

– *Зберігання та доступність*

Оброблені масиви інформації повинні бути організовані так, щоб до них міг звернутися будь-який аналітик, а не лише той, хто створив базу. Це забезпечує безперервність роботи в команді.

Принципи інформаційної роботи

- *Об'єктивність* – збір даних без спотворень і відбору «під потрібну картину».
- *Однозначність* – формулювання інформації має виключати подвійне тлумачення.
- *Повнота* – охоплення всіх релевантних джерел.

– *Доступність* – будь-який фахівець може працювати з масивом незалежно від того, хто його зібрав.

Важливість інформаційної роботи

Якість інформаційної роботи прямо визначає ефективність подальшого аналізу. Навіть найсильніший аналітик не зможе зробити якісні висновки, якщо вихідний масив даних неповний, зашумлений або недостовірний.

2. Завдання

1. Обрати тему, запропоновану викладачем або самостійно за згодою викладача.
2. Провести пошук інформації у різних типах джерел (3-5 чи більше незалежних джерел):
   - офіційні джерела (державні структури, компанії, міжнародні організації);
   - ЗМІ (різного рівня: міжнародні, національні, локальні);
   - соціальні мережі та неофіційні канали.

   Завдання: показати, що один факт може мати різні інтерпретації залежно від джерела.
3. Зібрати та зафіксувати всі знайдені дані у вигляді таблиці 1:
   - Обов'язково зазначати джерело, дату публікації, тип (офіційне, ЗМІ, соцмережі).
   - Важливо вказати оцінку достовірності (висока, середня, низька).

Таблиця 1. Приклад фрагмента таблиці джерел

№	Джерело	Тип	Дата публікації	Достовірність	Коментар
1	Сайт CERT-UA	офіційне	15.03.2022	висока	першоджерело про атаку
2	BBC News	ЗМІ	16.03.2022	середня	вторинне підтвердження
3	Telegram-канал «... »	соцмережі	16.03.2022	низька	чутки, не підтверджено

4. Усунути дублювання та інформаційний шум.
   - Дублювання: коли один і той самий факт підтверджують кілька джерел - залишити першоджерело.
   - Шум: чутки, неперевірені повідомлення, перебільшення - позначити як недостовірне або відкинути.

   Мета: залишити лише «чистий» інформаційний масив.
5. Побудувати структурований масив даних (хронологію подій).
   - Всі факти розташувати в послідовності за часом.
   - Використати схему: дата - подія - підтверджене джерело.
   - Якщо є прогалини (невідомі деталі), то позначити це.

Структурований масив даних (хронологія подій) - це таблиця або список, де події розташовані за часом. Такий підхід дозволяє:

- бачити розвиток ситуації крок за кроком;
- розрізняти підтверджені факти і неперевірені чутки;
- швидко виявляти прогалини (де бракує інформації).

Форма подання: Дата – Подія – Джерело (посилання чи назва)

Приклад побудови хронології подій див.табл.2 (тема: витік даних в енергетичній компанії).

Таблиця 2. Приклад хронології подій

Дата	Подія	Джерело
12.04.2023	У даркнеті з'являється анонс про продаж бази клієнтів компанії.	Форум на Darknet (скріншот)
14.04.2023	Українське ЗМІ повідомляє про можливий витік.	«Економічна правда»
15.04.2023	Компанія публікує офіційний пресреліз: "Ми перевіряємо ситуацію".	Сайт компанії
18.04.2023	CERT-UA підтверджує факт витоку 50 тис. записів.	CERT-UA
20.04.2023	Невідомо, чи дані включають фінансову інформацію.	- (Прогалина)

Зауваження: Для опрацювання прогалин скористайтеся наступними порадами:

– Якщо факт ще не підтверджено - написати «невідомо», «інформація перевіряється»;
– Якщо джерело сумнівне - вказати його, але зробити примітку: «непідтверджене».
– Якщо кілька джерел кажуть різне - подати обидва факти й вказати суперечність.

6. Провести оцінку повноти інформації.
    - Які факти встановлені достеменно?
    - Які дані залишаються сумнівними?
    - Яких відомостей бракує для цілісної картини?

    Для проведення оцінки треба:

    - Зіставлення фактів із завданням: подивіться, що саме треба було встановити (наприклад: «чи стався витік?», «який обсяг даних?», «хто причетний?»).
    - Класифікація фактів. Усі зібрані дані розділіть на три категорії: достеменно встановлені (є кілька незалежних підтверджень, офіційні джерела); сумнівні (є лише одне джерело або джерело має низьку довіру); відсутні (інформація, яка потрібна для відповіді на завдання, але її немає).

    Форма подання: таблиця (приклад див. табл.3).

Таблиця 3. Ситуація: витік даних у банку

Категорія	Факти	Коментар
Достеменно встановлені	CERT-UA підтвердив витік клієнтських e-mail	Надійне джерело
Сумнівні	Telegram-канал пише про викрадення паролів	Немає підтвердження від офіційних джерел
Відсутні	Обсяг викрадених даних (кількість записів)	Немає інформації навіть у офіційних повідомленнях

Висновки:

- Якщо достеменної інформації достатньо, можна завершувати інформаційну роботу (далі працює аналітик).
- Якщо багато сумнівних чи відсутніх даних, необхідно продовжити роботу, попередньо вказавши, що, наприклад, «Потрібно додатково перевірити джерела X, Y» або «Слід звернути увагу на офіційні звіти компанії/держорганів».

7. Скласти звіт за встановленою структурою.

Структура звіту:

- Назва.
- Джерела інформації (таблиця: джерело, тип, дата, достовірність).
- Фактичний масив даних – усі зібрані повідомлення.
- Усунення дублювання та шуму – короткий опис того, що відкинуто.
- Хронологія подій (структурований масив) – таблиця.
- Оцінка повноти – що відомо, що не підтверджено.
- Висновки – стан інформаційного масиву (але без інтерпретацій і прогнозів).

8. Правила оформлення лабораторної роботи

8.1. Робота виконується у письмовій формі (друкований текст у Word). Обсяг – за необхідністю. Шрифт – Times New Roman, кегль 14, інтервал 1,5. Поля: зліва 30 мм, справа 15 мм, зверху та знизу – по 20 мм.

8.2. Структура роботи.

Титульний аркуш (див. Додаток 1).

Розділи у відповідності з п.3. Форма звітності.

8.3. Вимоги до оформлення таблиць і схем.

Кожна таблиця має заголовок («Таблиця 1. Хронологія подій кейсу»).

Джерела даних зазначаються у таблиці або у примітках.

Схеми (графи, карти подій) повинні мати підпис і нумерацію.

8.4. Академічна доброчесність.

Забороняється плагіат.

При використанні чужих матеріалів обов’язково давати посилання на джерело.

Якщо дані взято з відкритих ресурсів (ЗМІ, офіційні сайти, аналітичні звіти), потрібно зазначити точне посилання.

3. Рекомендації щодо роботи з джерелами

- Офіційні заяви (уряд, компанії, CERT, ООН, ЄС) - мають найвищий рівень достовірності, але інколи неповні або тенденційні.
- ЗМІ (важливо порівнювати кілька незалежних медіа, щоб уникнути перекручень)
- Соціальні мережі (мають найнижчий рівень достовірності, але можуть дати перші сигнали про подію).
- Аналітичні звіти та дослідження (є цінними, але слід зважати на інтереси авторів).

***Рекомендації щодо оцінки достовірності джерела*:**

- Перевіряйте наближеність до першоджерела: чим ближче джерело до події, тим вищий рівень достовірності (приклад: повідомлення на офіційному сайті Держспецзв'язку про кібератаку достовірніше, ніж стаття в телеграм-каналі, який просто передруковує чужі пости);
- Звертайте увагу на репутацію джерела: відомі медіа або державні інституції мають редакційну політику і не можуть поширювати фейки (приклад: Reuters чи BBC у випадку міжнародних новин будуть більш надійним джерелом, ніж маловідомий блог);
- Перевіряйте сталість та послідовність інформації: якщо джерело сьогодні пише одне, а завтра – протилежне, це сигнал для обережності (приклад: якщо сайт публікує одночасно «атака була відбита» і «атака вивела систему з ладу», то рівень довіри низький);
- Шукайте підтвердження у незалежних джерелах: якщо одна й та ж інформація повторюється у кількох незалежних джерелах, її достовірність зростає (приклад: якщо про витік даних повідомили одразу кілька видань (Forbes, Financial Times, «Економічна правда»), це серйозніший сигнал, ніж поява інформації лише в одному телеграм-каналі);
- Враховуйте можливу упередженість: деякі джерела мають власні політичні, економічні чи ідеологічні інтереси (приклад: пресреліз самої компанії після інциденту завжди намагатиметься мінімізувати масштаб проблеми, тоді як незалежні розслідування можуть давати повнішу картину);
- Оцінюйте формат і якість подання: чіткі цифри, документи, скріни логів чи фото підвищують рівень достовірності (загальні формулювання «кажуть, що…», «можливо…» – ознака низької достовірності).

Оцінку джерела зручно робити, використовуючи таблицю 4.

Таблиця 4. Оцінка достовірності джерела

Критерій	Що перевіряти?	Приклад (висока достовірність)	Приклад (низька достовірність)
Наближеність до події	Чи є джерело прямим учасником або офіційною структурою?	Повідомлення CERT-UA про кібератаку	Анонімний пост у Telegram
Репутація	Чи має джерело історію надійності?	Reuters, «Економічна правда»	Невідомий блог без контактів
Послідовність	Чи суперечить джерело саме собі або іншим фактам?	Регулярні офіційні звіти з кіберінцидентів	Сайт, де новини змінюються щогодини на протилежні
Незалежні підтвердження	Чи підтверджується інформація кількома незалежними джерелами?	Витік даних описаний у кількох відомих ЗМІ	Інформація є лише в одному джерелі
Можлива упередженість	Чи може джерело мати власний інтерес?	Звіт незалежного розслідування	Пресреліз компанії після інциденту
Якість подання	Чи є конкретні факти, цифри, документи?	Звіт з логами, скрінами та датами	«Кажуть, що була атака» без деталей

Приклади аналізу достовірності джерела за таблицею.

Приклад 1 (Новина про витік даних у банку):

Джерело: Telegram-канал з 10 тис. підписників написав, що «великі клієнти банку Y втратили персональні дані».

Аналіз:

Наближеність до події: канал не є учасником інциденту і не має офіційного статусу, тому - низька.

Репутація: канал відомий публікаціями на різні теми без верифікації, тому - середня/низька.

Послідовність: за останні місяці у постах зустрічалися суперечності, тому - низька.

Незалежні підтвердження: на момент перевірки новина не підтверджена жодним офіційним джерелом чи ЗМІ, тому - низька.

Можлива упередженість: канал може працювати на «хайп», аби збільшити кількість переглядів, тому - середня.

Якість подання: жодних доказів (логів, документів, скрінів), тому - низька.

Висновок: джерело має ***низький рівень достовірності***. Цю інформацію не можна використовувати без підтвердження з офіційних джерел (наприклад, повідомлення НБУ чи CERT-UA).

Приклад 2 (Офіційне повідомлення CERT-UA про фішингову кампанію):

Джерело: CERT-UA (урядова команда реагування на комп'ютерні надзвичайні події України) опублікувала звіт на своєму сайті про масову розсилку фішингових листів.

Аналіз:

Наближеність до події: CERT-UA безпосередньо отримує звіти від організацій

та має власні сенсори, тому - висока.
Репутація: офіційна державна структура, що давно працює у сфері кібербезпеки, тому - висока.
Послідовність: усі публікації мають однакову структуру (опис атаки, IOC (Indicator of Compromise - індикатор компрометації), рекомендації), тому - висока.
Незалежні підтвердження: аналогічні повідомлення згодом підтверджують у міжнародних звітах (наприклад, ESET, Microsoft Threat Intelligence), тому - висока.
Можлива упередженість: низька, оскільки завдання CERT-UA - інформувати про загрози, а не просувати інтереси приватної компанії.
Якість подання: наведені приклади шкідливих листів, IP-адреси та хеші файлів для перевірки, тому - висока.

Висновок: джерело має ***високий рівень достовірності***. Інформацію можна використовувати для побудови заходів захисту без додаткових перевірок (але бажано співставити з іншими джерелами для повноти картини).

Приклад 3 (Публікація у виданні Forbes Україна про кібератаку на логістичну компанію)

Джерело: Forbes Україна опублікував статтю про можливий витік даних клієнтів у великій логістичній компанії.

Аналіз:
Наближеність до події: журналісти не є учасниками інциденту, але мають доступ до коментарів постраждалої компанії, тому - середня.
Репутація: відоме економічне видання з високою репутацією, але не спеціалізується на кібербезпеці, тому - середня/висока.
Послідовність: у статтях видання трапляються різні джерела та думки, іноді суперечливі, тому - середня.
Незалежні підтвердження: інформація базується на словах представника компанії, але немає технічних доказів чи підтвердження від CERT, тому - середня.
Можлива упередженість: публікація орієнтована на бізнес-аудиторію, тому може акцентувати економічні ризики, недооцінюючи технічні деталі, тому - середня.
Якість подання: наведені коментарі керівництва компанії, але відсутні будь-які технічні артефакти (логі, хеші, IP), тому - середня.

Висновок: джерело має ***середній рівень достовірності***. Інформацію можна брати до уваги, але для роботи в сфері інформаційної безпеки вона має бути перевірена за офіційними джерелами (CERT-UA, технічні звіти).

5. Перелік питань для підготовки до захисту лабораторної роботи

1. Що таке інформаційна робота і які її основні завдання?
2. У чому полягає різниця між первинними та вторинними джерелами інформації?
3. Як визначити достовірність джерела? Наведіть приклад.
4. Чому важливо оцінювати повноту інформації під час збору даних?

5. Що таке однозначність інформації і як її відсутність впливає на подальшу роботу?
6. Які основні вимоги висуваються до інформаційного масиву (доступність, інваріантність, можливість коригування)?
7. Як правильно будувати хронологію подій? Для чого вона потрібна?
8. Що таке концептуальний моніторинг і чи є він частиною інформаційної роботи?
9. Які критерії використовуються для відбору найбільш інформативних джерел?
10. Чому інформаційна робота є необхідним етапом перед аналітичною роботою?

Лабораторна робота №2

Тема: АНАЛІТИЧНА РОБОТА

Мета роботи: отримання навичок перетворення інформаційних фактів у знання шляхом засвоєння і використання основних методів аналітичної роботи, отримання навичок формулювати практичні рекомендації на основі аналізу.

1. **Теоретичні основи**

Аналітична робота є логічним продовженням інформаційної роботи. Якщо інформаційна діяльність зосереджена на зборі, систематизації та верифікації даних, то аналітична спрямована на осмислення цих даних, виявлення закономірностей, побудову прогнозів та вироблення рекомендацій для прийняття рішень.

Сутність аналітичної роботи. Аналітика - це перетворення «сирих» фактів у знання, що мають практичну цінність. Її завдання - не лише дати опис ситуації, а пояснити, чому подія відбулася, що вона означає в ширшому контексті, які наслідки можливі, які дії потрібно здійснити. Наприклад, якщо в інформаційній роботі (Лабораторна робота №1) студент зібрав факти про кібератаку на компанію, то в аналітичній частині він має виявити причини атаки (слабкі паролі, людський фактор), оцінити ризики (втрата клієнтів, витік даних) і надати рекомендації (посилення політики доступу, навчання персоналу).

Основні принципи аналітичної роботи.

Інтегративність: аналітик ніколи не працює з одним фактом у відриві від інших. Його завдання - інтегрувати інформацію з різних джерел. Наприклад: повідомлення про збої в мережі можуть бути підтверджені як технічними логами, так і скаргами клієнтів у соцмережах.

Верифікація та зіставлення. Робота з різними джерелами дозволяє відділити правдиву інформацію від чуток. Наприклад: новина в Telegram-каналі може бути перевірена через офіційні прес-релізи або незалежні медіа.

Причинно-наслідковий аналіз. Аналітик шукає не лише факти, а й зв’язки між ними. Наприклад: «витік бази даних» може бути наслідком «фішингової атаки на співробітників», яка у свою чергу стала можливою через «відсутність багатофакторної автентифікації».

Прогностичність. Будь-який аналіз неповний без прогнозу. Наприклад: якщо хакерська група атакувала одну енергетичну компанію, велика ймовірність, що наступною стане інша компанія в тій же сфері.

Аргументованість рекомендацій. Аналітичний продукт завжди має вихід у практичні дії, але ці дії повинні бути логічно обґрунтовані, а не ґрунтуватися на припущеннях.

Методи аналітичної роботи.

Інтеграція. Визначення зв’язків між подіями та фактами з побудовою «інтегральної схеми». Приклад: аналітик може показати, як інформаційна кампанія в соцмережах пов’язана з політичними подіями та економічними

санкціями.

Розпізнавання. Зіставлення нової проблеми з уже відомими шаблонами. Приклад: серія атак за допомогою шкідливого ПЗ може нагадувати тактику відомої хакерської групи, що дозволяє зробити висновки про ймовірного противника.

Зіставлення та нарощування похідної інформації. Порівняння незалежних джерел дозволяє не лише підтвердити факт, а й виявити «похідну інформацію» - знання, яких прямо не було в жодному з джерел. Приклад: якщо два джерела називають різні дати події, але вони співпадають із відключенням серверів, можна зробити висновок про реальний час атаки.

Прогнозування. Передбачення розвитку ситуації на основі вже виявлених закономірностей. Приклад: після санкцій проти певних компаній можна очікувати кібератак з боку акторів, пов'язаних із країною-противником.

Особливості аналітичної роботи у сфері інформаційної безпеки.

Аналітична робота в ІБ має свою специфіку:

Висока динамічність: ситуація може змінюватися щогодини (атака триває в реальному часі).

Технічна насиченість: більшість даних надходить з автоматизованих систем (логи, трафік, телеметрія), що вимагає вміння працювати з «сирими» цифровими масивами.

Фактор невизначеності: часто немає повної інформації, і аналітик має працювати з прогалинами.

Ціна помилки: неправильний прогноз чи рекомендація може призвести до мільйонних збитків, репутаційних втрат, загибелі людей.

2. Завдання

- Оберіть тему, яку ви опрацьовували в Лабораторній роботі №1 («Інформаційна робота»).
- Перегляньте свій структурований масив даних (хронологію подій).
- Побудова інтегральної схеми:
  - Визначте ключові події та факти.
  - Побудуйте граф зв'язків: причини – наслідки, використовуючи для цього будь-яку зручну форму (малюнок від руки, схему у PowerPoint тощо).

<u>Рекомендації, які допоможуть визначати ключові події та факти</u>:

- Орієнтуватися на причинно-наслідкові зв'язки: подія є ключовою, якщо вона запускає ланцюг інших подій або суттєво впливає на розвиток ситуації, наприклад: у ситуації з кібератакою на «Київстар» - саме момент відключення зв'язку є ключовим, бо він викликав лавину наслідків (паніка, реакція ЗМІ, офіційні заяви).
- Виділяти точки ескалації чи перелому: важливими є факти, після яких ситуація перейшла в інший якісний стан, наприклад: якщо компанію спочатку лише критикували у соцмережах, але після статті у Forbes почалися офіційні перевірки - саме ця стаття стає ключовим фактом.

- Враховувати реакцію суспільства та інституцій: якщо інформація викликала широкий резонанс (ЗМІ, політики, міжнародні організації) - це сигнал, що подія має ключове значення.
- Дивитися на часові маркери: ключові події часто стають опорними точками в хронології. Це може бути перший публічний факт, найбільший інформаційний сплеск, офіційне підтвердження або перша реакція влади/компанії.
- Відрізняти «шум» від значущих фактів: якщо дані повторюють одне й те саме без нової суті - це інформаційний шум, не ключові події. Якщо ж новина додає новий елемент (новий актор, підтвердження джерела, технічна деталь атаки), то її можна вважати ключовою.

<u>Практична порада</u>:

- Коли ви аналізуєте хронологію, задайте собі три питання:
- Чи могло б без цього факту розгортання подій бути іншим?
- Чи цей факт змінив хід розвитку ситуації?
- Чи викликав він помітну реакцію від суспільства, органів влади, компаній?

Якщо хоча б на одне з цих питань відповідь «так» - це ключова подія або факт.

Розглянемо приклад. Ситуація: міжнародна IT-компанія «CyberTech» зазнала кібератаки.
Зібрані факти (інформаційна робота):
10 березня — користувачі скаржаться на збої у доступі до сервісів.
11 березня — на Reddit з'явився пост від невідомого, який заявляє про злам «CyberTech».
11 березня — офіційний акаунт компанії в Twitter пише: «Ми розслідуємо інцидент».
12 березня — незалежний дослідник підтвердив, що в даркнеті продаються дані користувачів.
13 березня — ЗМІ повідомляють, що серед даних є паролі та номери кредитних карток.
14 березня — CEO компанії вибачається публічно та оголошує про компенсаційні заходи.
15 березня — Європейська комісія починає перевірку відповідності GDPR.
16 березня — в соцмережах шириться хештег #DeleteCyberTech.
18 березня — акції компанії впали на 12%.
Визначення ключових фактів (аналітична робота)
Ключові події:
10 березня: перші збої — старт інциденту, «нульова точка».
12 березня: підтвердження витоку даних незалежним дослідником — надає достовірність.
14 березня: публічні вибачення та компенсаційна програма — офіційна реакція компанії.
15 березня: початок перевірки ЄС — ескалація на рівень міжнародного регулювання.
18 березня: падіння акцій на 12% — економічний наслідок.
Другорядні події:
Пост на Reddit (не підтверджений, тому шум, поки немає інших даних).
Твіти та соцмережеві кампанії (#DeleteCyberTech) — важливі як контекст, але вони не «зламують» розвиток подій.

- Виявлення основних проблем і чинників:
  - Визначте «тригери» (що стало початковим поштовхом).
  - Вкажіть фактори, які посилили розвиток ситуації.

<u>Рекомендації для виявлення основних проблем і чинників:</u>

- Шукайте «вузлові точки» подій: якщо певна подія радикально змінює розвиток ситуації (наприклад, підтвердження витоку даних незалежним дослідником), це сигнал, що тут прихована основна проблема.
- Визначайте, що повторюється у різних джерелах: якщо кілька незалежних джерел говорять про одне й те саме (наприклад, про затримку доставки чи витік паролів), - це не випадковість, а ключовий чинник ситуації.

- Аналізуйте наслідки для різних сторін, подумайте, хто постраждав, хто виграв? Якщо від події страждає компанія, клієнти і ще й регулятор реагує, значить це не «дрібниця», а центральна проблема.
- Відрізняйте симптоми від причин, наприклад, падіння акцій - симптом. Справжня причина — втрата довіри клієнтів через витік даних. Завжди ставте собі запитання: «Чому це сталося?»
- Виділяйте «людський фактор» і «технічний фактор»: проблеми бувають технічні (злам, уразливість у софті) й організаційні (повільна реакція компанії, відсутність прозорості). Розділіть їх, щоб розуміти, де джерело головної загрози.
- Шукайте чинники, які впливають на майбутнє. Не все однаково важливо: скандальний пост у соцмережах може швидко забутися, а регуляторна перевірка може призвести до мільйонних штрафів. Значить, перевірка ЄС - ключовий чинник майбутнього розвитку подій.

Для наочності розгляньте таблицю «Виявлення основних проблем і чинників» для попереднього прикладу з міжнародною ІТ-компанією «CyberTech».Виявлення основних проблем і чинників

Подія/Факт	Основна проблема	Ключові чинники
10 березня — збої у сервісах	Початок інциденту, відсутність швидкої реакції	Наявність технічної уразливості, брак моніторингу
11 березня — пост на Reddit про злам	Недостатня інформаційна політика компанії (чутки випереджають офіційні заяви)	Соцмережі як канал формування громадської думки
12 березня — підтвердження витоку незалежним дослідником	Достовірний факт витоку даних	Наявність даних у даркнеті, відсутність захисту паролів
14 березня — публічні вибачення CEO	Запізніла реакція керівництва	Репутаційні ризики, комунікаційні прорахунки
15 березня — перевірка ЄС щодо GDPR	Можливі штрафи та юридичні наслідки	Невідповідність стандартам захисту персональних даних
18 березня — падіння акцій на 12%	Економічні наслідки скандалу	Втрата довіри інвесторів, фінансові ризики

- Встановлення причинно-наслідкових зв’язків:
  - Вкажіть, які події стали прямими наслідками інших.
  - Позначте, чи існує ланцюжок розвитку (кілька подій одна за одною).
- Прогноз розвитку подій:
  - Опишіть два сценарії: оптимістичний; песимістичний.
  - За можливості додайте найбільш імовірний варіант.

<u>Рекомендації для складання прогнозу розвитку подій:</u>

- Виходьте з ключових фактів, прогноз завжди має ґрунтуватися на перевірених подіях і чинниках.
- Прогноз не обов’язково один (декілька сценаріїв).
- Виділяйте рушійні фактори: фактори, які найбільше вплинуть на подальший розвиток. У кіберінциденті це можуть бути результати перевірки регуляторів,
- реакція клієнтів і медіа, технічна здатність компанії швидко закрити уразливість.
- Позначайте індикатори майбутніх змін: що підкаже, який сценарій починає реалізовуватися? Наприклад, якщо кількість негативних згадок у

соцмережах зменшується, то це ознака стабілізації; якщо регулятори готують позови, то це сигнал до погіршення ситуації.

- Обмежуйте прогноз часовими рамками: прогноз завжди «живе» у конкретному часовому горизонті (короткостроковий (дні/тижні), середньостроковий (місяці), довгостроковий (рік і більше)). Для кризових подій (наприклад, кібератака) зазвичай достатньо коротко- і середньострокових прогнозів.
- Враховуйте ефект «ланцюгової реакції»: подія може викликати вторинні наслідки. Наприклад: витік даних - розслідування - падіння акцій - звільнення керівництва. Якщо ви бачите можливість такого ланцюга, зазначте його в прогнозі.
- Формулюйте прогноз чітко і нейтрально.

Для наочності розглянемо приклад трьох сценаріїв прогнозу розвитку подій для ситуації «Кібератака на CyberTech».

Оптимістичний сценарій (ймовірність низька):

Компанія швидко локалізує витік і підтверджує, що масштаби менші, ніж повідомляли ЗМІ. Вибачення CEO та компенсаційна програма знижують хвилю критики в соцмережах. Перевірка ЄС виявляє лише дрібні порушення, які можна швидко виправити. За місяць негативна хвиля згасає, акції відновлюють більшість втрат.

Умова: сильна технічна та PR-команда, оперативна прозора комунікація.

Базовий сценарій (ймовірність середня, найбільш реалістичний):

Масштаб витоку підтверджується: мільйони записів, але без найбільш критичних даних (наприклад, без PIN-кодів карток). Перевірка ЄС триває, але справа не доходить до максимальних штрафів. Клієнти частково втрачають довіру, однак завдяки знижкам і новій кампанії компанія утримує більшість. Упродовж 3–6 місяців компанія поступово стабілізує репутацію, хоча фінансові показники залишаються нижчими, ніж до атаки.

Умова: контрольоване управління кризою, але не без втрат.

Песимістичний сценарій (ймовірність невисока, але можливий):

Витік виявляється масовим і включає критичні персональні дані. ЄС накладає штрафи за GDPR, компанія потрапляє в судові процеси. В соцмережах поширюється кампанія #DeleteCyberTech, і починається відтік клієнтів. Інвестори масово продають акції, вартість компанії падає на 40%. Через рік компанія втрачає значну частину ринку і стає об'єктом для поглинання конкурентами.

Умова: компанія не контролює кризу, інформаційна політика слабка, витік дійсно великий.

Таким чином, прогноз завжди має кілька сценаріїв. У кожному сценарії вказуються ключові фактори, що впливають на його реалізацію.

- Формування рекомендацій:
  - Розробіть 2–3 пропозиції для керівництва.
  - Кожна рекомендація має бути: конкретною; виконуваною; спрямованою на усунення причин або мінімізацію наслідків.

Поради до формування рекомендацій в аналітичній роботі

- Орієнтуватися на практичність: рекомендація має бути не абстрактною («посилити захист»), а конкретною й такою, що піддається виконанню («запровадити MFA для всіх акаунтів до кінця кварталу»).
- Виходити з аналізу проблем: кожна порада повинна напряму відповідати на виявлені ризики чи слабкі місця. Якщо проблема - витік даних, то рекомендація має зосереджуватися на заходах для зменшення наслідків і запобігання повторення.
- Враховувати ресурси організації: не варто радити «побудувати власний дата-центр», якщо мова про середню компанію. Рекомендації мають бути реалістичними для умов конкретного суб'єкта.
- Розділяти за пріоритетністю: корисно позначати рекомендації як термінові (впровадити негайно) і довгострокові (стратегічні кроки). Це допомагає керівництву структурувати план дій.

- Формулювати зрозумілою мовою.
- Давати варіанти: іноді варто показати кілька можливих шляхів: мінімальний (дешевий), оптимальний (баланс), максимальний (повний захист). Це залишає простір для управлінського рішення.
- **Обґрунтовувати** рекомендацію (вигоду).

Приклад рекомендацій для ситуації «Кібератака на CyberTech»:
Терміново: повідомити клієнтів про інцидент і запровадити безкоштовний моніторинг їхніх акаунтів.
Середньостроково: впровадити багатофакторну автентифікацію для всіх користувачів.
Довгостроково: створити окремий підрозділ SOC для постійного моніторингу атак.

3. Форма звітності

Звіт повинен містити:

- Тему.
- Інтегральну схему (схематичний граф).
- Опис основних проблем і чинників.
- Встановлені причинно-наслідкові зв’язки.
- Прогноз (мінімум два сценарії).
- Конкретні рекомендації.
- Висновки по роботі.

4. Правила оформлення лабораторної роботи

4.1. Робота виконується у письмовій формі (друкований текст у Word). Обсяг – за необхідністю. Шрифт – Times New Roman, кегль 14, інтервал 1,5. Поля: зліва 30 мм, справа 15 мм, зверху та знизу – по 20 мм.

4.2. Структура роботи.

Титульний аркуш (див.Додаток 1).

Розділи у відповідності з п.3. Форма звітності.

4.3. Вимоги до оформлення таблиць і схем.

Кожна таблиця має заголовок («Таблиця 1. Хронологія подій кейсу»).

Джерела даних зазначаються у таблиці або у примітках.

Схеми (графи, карти подій) повинні мати підпис і нумерацію.

4.4. Академічна доброчесність.

Забороняється плагіат.

При використанні чужих матеріалів обов’язково давати посилання на джерело.

Якщо дані взято з відкритих ресурсів (ЗМІ, офіційні сайти, аналітичні звіти), потрібно зазначити точне посилання.

5. Перелік питань для підготовки до захисту лабораторної роботи:

- Що відрізняє інформаційну роботу від аналітичної?
- Які основні етапи аналітичної роботи ви можете назвати?
- Чому важливо виділяти ключові факти у процесі аналітики?
- Які існують тактичні методи аналітичної роботи (інтеграція, розпізнавання) та як вони застосовуються?
- Які підходи до визначення причинно-наслідкових зв’язків ви знаєте?
- У чому полягає мета прогнозування під час аналітичної роботи?

- Які фактори потрібно враховувати при складанні рекомендацій?
- Чому аналітик має працювати навіть із суперечливою інформацією?
- Як можна оцінити якість та повноту аналітичного звіту?
- Наведіть приклад ситуації, коли неправильний аналіз призводить до хибних висновків, і поясніть, як цього уникнути.

Література

Базова

1. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.
2. Інформаційна безпека : підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін. ; під ред. В. В. Остроухова. – К. : Видавництво Ліра-К, 2021. – 412 с.
3. Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України: матеріали Науково-практичної конференції (Львів, 22 грудня 2023) / упорядник: Т.В.Магеровська. – Львів : ЛьвДУВС, 2024. –192 с.

Допоміжна

4. Маковій В. П. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави / Морська безпека та оборона, N 1, 2023, с.62-68.

Інтернет ресурси

1. https://pidru4niki.com/16520415/politologiya/sutnist_informatsiyno-analitichnogo_zabezpechennya_derzhavnogo_upravlinnya_sferi_bezpeki
2. https://vestnik-pravo.mgu.od.ua/archive/juspradenc42/part_2/15.pdf
3. https://pidru4niki.com/15830523/politologiya/viznachennya_tsili_zavdannya_informatsiyno-analitichnogo_zabezpechennya_iaz

Додаток 1

Міністерство освіти і науки України

Одеський національний морський університет
Навчально-науковий інститут інформаційних технологій та інноваційного підприємництва
Кафедра кібербезпеки та захисту інформації

Лабораторна робота № ___

з дисципліни: «Інформаційно-аналітичне забезпечення інформаційної безпеки»

Тема: «Інформаційна робота / Аналітична робота»

Виконав(ла):
студент(ка) групи _____
Прізвище Ім’я По батькові

Перевірила:
Кобозєва Алла Анатоліївна,
зав.каф.КБЗІ

м. Одеса – 2025