



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Кафедра «Кібербезпека та захист інформації»

МЕТОДИЧНІ ВКАЗІВКИ
до лабораторних робіт
освітнього компонента (навчальної дисципліни)
СУЧАСНІ КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА
ЇХ ОСОБЛИВОСТІ

назва освітнього компонента (навчальної дисципліни)

обов'язковий компонент циклу професійної підготовки

Рівень вищої освіти

другий (магістерський)

перший (бакалаврський), другий (магістерський), третій (освітньо-науковий)

Форма здобуття
освіти

очна (денна)

очна (денна), заочна, дистанційна

Мова викладання

Українська

2025/2026 навчальний рік

Методичні вказівки до лабораторних робіт освітнього компонента (навчальної дисципліни) **«Сучасні КСЗІ та їх особливості»** для здобувачів очної (денної) форми здобуття освіти другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації галузі знань F Інформаційні технології / Укл.: Зоріло В.В. – Одеса, 2025. – 15 с.

Розробник: Зоріло Вікторія Вікторівна, доцент кафедри «Кібербезпека та захист інформації»

Схвалено на засіданні кафедри «Кібербезпека та захист інформації»
Протокол від №2 від 06.10.2025.

Схвалено на засіданні НМК ННІ ІТІП
Протокол від №2 від 14.10.2025

Зміст

Лабораторна робота 1. Аналіз загроз та вразливостей інформаційних систем.....	4
Лабораторна робота 2. Моделювання архітектури комплексної системи захисту інформації ..	5
Лабораторна робота 3. Дослідження міжнародних стандартів ISO/IEC 27001, NIST та порівняння з національними вимогами.....	6
Лабораторна робота 4. Розробка політики інформаційної безпеки організації	7
Лабораторна робота 5. Реалізація криптографічних методів захисту даних у прикладних задачах	8
Лабораторна робота 6. Використання засобів технічного захисту інформації від НСД та витоків	9
Лабораторна робота 8. Аналіз та реагування на інциденти кібербезпеки	15

Лабораторна робота 1. Аналіз загроз та вразливостей інформаційних систем

Мета роботи: Сформувати навички виявлення активів, загроз і вразливостей, оцінювання ризиків та обґрунтування заходів їх оброблення.

Короткі теоретичні відомості

Загроза інформаційній безпеці – потенційна причина небажаної події, яка може призвести до порушення конфіденційності, цілісності або доступності інформації. Вразливість – слабе місце системи, яке може бути використане для реалізації загрози. Ризик характеризує поєднання імовірності реалізації загрози та можливого впливу на активи й процеси організації.

Під час аналізу система розглядається як сукупність активів, користувачів, програмних і технічних засобів, мереж, даних та процесів. Спочатку визначаються критичні активи, потім джерела загроз, вразливості та сценарії атак. Рівень ризику можна визначати якісно за матрицею «імовірність × вплив». За результатами визначаються пріоритетні ризики та заходи їх оброблення.

Хід роботи

1. Обрати навчальну або умовну інформаційну систему та описати її призначення, користувачів і межі аналізу.
2. Скласти перелік активів: дані, облікові записи, сервери, робочі станції, мережеве обладнання, ПЗ та критичні процеси.
3. Для кожного активу визначити вимоги до конфіденційності, цілісності та доступності.
4. Визначити зовнішні й внутрішні джерела загроз та можливі сценарії їх реалізації.
5. Для кожної загрози визначити відповідні вразливості та можливі наслідки.
6. Скласти таблицю «актив – загроза – вразливість – наслідок – імовірність – вплив – ризик».
7. Оцінити ризики за трибальною шкалою і побудувати матрицю ризиків.
8. Виділити щонайменше п'ять пріоритетних ризиків та запропонувати для них заходи оброблення.
9. Сформулювати висновок про поточний стан захищеності та першочергові заходи.

Результат роботи

Звіт: опис системи, активи, таблиця загроз і вразливостей, матриця ризиків, заходи оброблення та висновок.

Контрольні запитання для самоперевірки

1. Чим відрізняються загроза, вразливість і ризик?
2. Які активи необхідно враховувати?
3. Як визначається вплив реалізації загрози?
4. Чому одна вразливість може мати різний ризик?
5. Які основні джерела загроз?
6. Що таке сценарій реалізації загрози?
7. Які існують варіанти оброблення ризику?
8. Для чого потрібна матриця ризиків?
9. Які ризики є пріоритетними?
10. Чому аналіз потрібно періодично повторювати?

Лабораторна робота 2. Моделювання архітектури комплексної системи захисту інформації

Мета роботи: Розробити логічну модель КСЗІ та показати взаємозв'язок активів, зон довіри, загроз і засобів захисту.

Короткі теоретичні відомості

КСЗІ поєднує організаційні, інженерно-технічні, програмно-апаратні та криптографічні заходи. Архітектура захисту повинна відповідати структурі системи, характеру інформації та ризикам. Основою проєктування є визначення меж системи, зон довіри та інформаційних потоків.

У корпоративній мережі доцільно виділяти зовнішню мережу, DMZ, внутрішній сегмент користувачів, серверний сегмент та зону адміністрування. Між зонами застосовують фільтрацію, сегментацію, контроль доступу, моніторинг та криптографічний захист. Архітектура має ґрунтуватися на багаторівневому захисті, мінімальних привілеях і відсутності неконтрольованих потоків.

Хід роботи

1. Використати систему з роботи 1 або типову організацію з локальною мережею, веб-сервісом, БД та віддаленим доступом.
2. Визначити межі системи й зовнішні взаємодії.
3. Виділити зони довіри та побудувати логічну схему.
4. Для кожної зони визначити активи, користувачів і дозволені потоки.
5. Нанести міжмережеві екрани, VPN, сегментацію, засоби захисту кінцевих точок та моніторинг.
6. Передбачити багатофакторну автентифікацію для критичних ресурсів.
7. Визначити захист даних під час передавання та зберігання.
8. Передбачити резервне копіювання та журналювання.
9. Для кожного компонента пояснити, яку загрозу він зменшує.
10. Перевірити модель на єдині точки відмови, надмірні привілеї та неконтрольовані потоки.

Результат роботи

Звіт: схема КСЗІ, опис зон і потоків та таблиця «загроза – засіб захисту – очікуваний результат».

Контрольні запитання для самоперевірки

1. Що таке архітектура КСЗІ?
2. Що таке зона довіри?
3. У чому полягає багаторівневий захист?
4. Для чого потрібна сегментація?
5. Яке призначення DMZ?
6. Що означає мінімальний привілей?
7. Які компоненти потрібно моніторити?
8. Як резервування підвищує стійкість?
9. Чому засіб захисту пов'язують із конкретною загрозою?
10. Які ознаки слабкої архітектури?

Лабораторна робота 3. Дослідження міжнародних стандартів ISO/IEC 27001, NIST та порівняння з національними вимогами

Мета роботи: Порівняти ISO/IEC 27001 і NIST із чинними національними вимогами та визначити спільні й відмінні підходи.

Короткі теоретичні відомості

ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою та орієнтується на ризик-орієнтований підхід, контроль результативності й постійне вдосконалення. NIST використовує рамки та спеціальні публікації для організації процесів кібербезпеки, управління ризиками, захисту, виявлення, реагування і відновлення.

Українські організації додатково працюють у межах законодавства, нормативно-правових актів і нормативних документів у сфері захисту інформації та кібербезпеки. Під час порівняння важливо розмежовувати міжнародну практику управління безпекою та конкретні національні вимоги, обов'язковість яких визначається статусом організації та характером інформації.

Хід роботи

1. Обрати організацію та сферу діяльності.
2. Опрацювати офіційні матеріали ISO/IEC 27001 і обраного документа NIST.
3. Визначити релевантні українські нормативні вимоги.
4. Скласти таблицю за критеріями: ризики, політика, доступ, криптографія, моніторинг, інциденти, безперервність, аудит.
5. Для кожного критерію описати підхід ISO, NIST і національних вимог.
6. Виділити спільні положення.
7. Виділити відмінності та потенційні труднощі адаптації.
8. Запропонувати щонайменше п'ять практичних заходів для організації.
9. Сформулювати аналітичний висновок.

Результат роботи

Звіт: нормативні джерела, порівняльна таблиця, відмінності та практичні рекомендації.

Контрольні запитання для самоперевірки

1. Що таке ISMS?
2. Яке призначення ISO/IEC 27001?
3. Що вирішує NIST Cybersecurity Framework?
4. Чим стандарт відрізняється від нормативної вимоги?
5. Що спільного в ISO та NIST?
6. Яке місце займає оцінювання ризиків?
7. Чому враховують національні вимоги?
8. За якими критеріями порівнювати підходи?
9. Що означає постійне вдосконалення?
10. Які переваги міжнародних практик?

Лабораторна робота 4. Розробка політики інформаційної безпеки організації

Мета роботи: Розробити проєкт політики інформаційної безпеки для умовної організації.

Короткі теоретичні відомості

Політика інформаційної безпеки – документований набір принципів, правил і вимог, що визначає підхід організації до захисту інформації. Вона встановлює цілі, сферу дії, ролі та відповідальність, правила доступу, роботи з даними і реагування на порушення.

Політика має відповідати цілям організації, законодавству та результатам оцінювання ризиків. Для ключових процесів встановлюються конкретні правила щодо облікових записів, автентифікації, корпоративних пристроїв, резервного копіювання, передавання даних та повідомлення про інциденти. Документ регулярно переглядається.

Хід роботи

1. Описати організацію, її бізнес-процеси та інформаційні ресурси.
2. Визначити область дії політики.
3. Сформулювати цілі щодо конфіденційності, цілісності та доступності.
4. Визначити ролі: керівництво, адміністратори, користувачі, відповідальні за безпеку.
5. Розробити правила керування обліковими записами та доступом.
6. Встановити вимоги до пристроїв, електронної пошти, Інтернету, носіїв і віддаленого доступу.
7. Визначити вимоги до резервування, криптографії та журналювання.
8. Визначити порядок повідомлення про інциденти та відповідальність.
9. Передбачити процедуру перегляду й затвердження політики.
10. Зіставити політику з ризиками роботи 1 та оформити як цілісний документ.

Результат роботи

Результат: завершений проєкт політики з метою, сферою дії, ролями, правилами, відповідальністю та порядком перегляду.

Контрольні запитання для самоперевірки

1. Що таке політика інформаційної безпеки?
2. Які розділи вона повинна містити?
3. Чому політика враховує ризики?
4. Які ролі визначаються?
5. Що означає мінімальний привілей?
6. Які правила потрібні для віддаленого доступу?
7. Чому регламентують повідомлення про інциденти?
8. Як часто переглядати політику?
9. Чим політика відрізняється від інструкції?
10. Які наслідки відсутності політики?

Лабораторна робота 5. Реалізація криптографічних методів захисту даних у прикладних задачах

Мета роботи: Закріпити навички застосування симетричного шифрування, хешування та цифрового підпису.

Короткі теоретичні відомості

Криптографія використовує математичні перетворення для забезпечення конфіденційності, цілісності, автентичності та, у відповідних сценаріях, неспростовності. Основні класи механізмів – симетричне шифрування, асиметрична криптографія, хешування та цифровий підпис.

Симетричні алгоритми використовують спільний секретний ключ і ефективні для великих обсягів даних. Асиметричні використовують пару ключів та застосовуються для автентифікації, обміну ключами й підпису. Хеш-функція створює дайджест і не є шифруванням. У практиці слід використовувати перевірені бібліотеки та не реалізовувати криптографічні примітиви самостійно.

Хід роботи

1. Взяти навчальний текстовий файл або повідомлення.
2. Визначити потрібну властивість безпеки.
3. Обрати відповідний стандартний криптографічний механізм.
4. Створити ключ або пару ключів засобами бібліотеки.
5. Зашифрувати дані та зберегти результат окремо.
6. Розшифрувати дані й перевірити повне відновлення.
7. Обчислити хеш вихідного повідомлення, змінити один символ і повторити обчислення.
8. За наявності завдання створити та перевірити цифровий підпис.
9. Перевірити реакцію механізму на змінене повідомлення.
10. Описати захист ключів і наслідки їх компрометації.
11. Сформулювати висновок щодо відповідності механізму задачі.

Результат роботи

Результат: працездатний навчальний приклад криптографічного захисту з описом параметрів та перевірок.

Контрольні запитання для самоперевірки

1. Чим відрізняється симетрична криптографія?
2. Чим відрізняється асиметрична криптографія?
3. Які властивості забезпечує хешування?
4. Чому хеш не є шифруванням?
5. Для чого цифровий підпис?
6. Що станеться при компрометації ключа?
7. Чому не пишуть власні криптоалгоритми?
8. Що таке відкритий і закритий ключ?
9. Як захищають ключі?
10. Як зміна символу впливає на хеш?

Лабораторна робота 6. Використання засобів технічного захисту інформації від НСД та витоків

Мета роботи: Дослідити налаштування технічних засобів захисту від НСД і витоків та оцінити їх ефективність.

Короткі теоретичні відомості

Технічний захист охоплює засоби протидії несанкціонованому доступу, шкідливому ПЗ, мережевим атакам і витоку технічними каналами. До них належать міжмережеві екрани, контроль доступу, захист кінцевих точок, сегментація, шифрування каналів і фізичні засоби.

Захист від витоку має враховувати мережеві, фізичні та побічні канали: візуальні, акустичні, електромагнітні, через лінії зв'язку, живлення або неправильне поводження з носіями. Навчальні випробування виконуються лише в ізольованому середовищі або на власному обладнанні.

Хід роботи

1. Підготувати ізольовану тестову систему.
2. Визначити активи та канали доступу.
3. Зафіксувати базовий стан: служби, правила доступу, захист і журналювання.
4. Налаштувати міжмережевий екран за принципом необхідного трафіку.
5. Створити безпечне контрольне правило й перевірити його.
6. Увімкнути засіб захисту кінцевої точки.
7. Обмежити доступ до критичних ресурсів за мінімальними привілеями.
8. Перевірити захищене передавання даних.
9. Проаналізувати можливі фізичні та побічні канали витоку.
10. Порівняти стан до і після захисту та визначити залишкові ризики.

Результат роботи

Результат: опис налаштувань, результати контрольних перевірок, журнальні записи та перелік залишкових ризиків.

Контрольні запитання для самоперевірки

1. Що таке НСД?
2. Які засоби належать до технічного захисту?
3. Яке призначення міжмережевого екрана?
4. Чому «дозволити все» небезпечно?
5. Що таке мінімальні привілеї?
6. Які фізичні канали витоку існують?
7. Чому захист від витоку не обмежується мережею?
8. Яке значення журналювання?
9. Чому потрібне ізольоване середовище?
10. Як перевірити ефективність заходу?

Лабораторна робота №7. Моніторинг та аудит безпеки з використанням інструментів NirSoft

Мета роботи

Набути практичних навичок моніторингу та аудиту безпеки операційної системи Windows шляхом аналізу журналів подій, інформації про сеанси користувачів, мережевої активності та подій засобу Windows Defender. Навчитися виявляти ознаки потенційно підозрілої активності, встановлювати часову послідовність подій та формувати результати аудиту.

Теоретичні відомості

Моніторинг безпеки є одним із важливих елементів комплексної системи захисту інформації. Його призначення полягає у своєчасному виявленні подій, які можуть свідчити про порушення встановлених правил безпеки, помилки конфігурації, несанкціоновані дії або спроби отримання доступу до інформаційних ресурсів.

У сучасних інформаційних системах основним джерелом відомостей для моніторингу є журнали подій. Операційна система Windows реєструє значну кількість подій, пов'язаних з автентифікацією користувачів, роботою служб і програм, змінами системної конфігурації, мережевою активністю та роботою засобів захисту.

Для аналізу таких даних у лабораторній роботі використовуються утиліти NirSoft. Це набір невеликих інструментів для Windows, багато з яких не потребують традиційного встановлення та можуть працювати у portable-режимі.

Основним засобом роботи є FullEventLogView. Програма відображає події журналів Windows у табличному вигляді, дає змогу здійснювати фільтрацію за часом, каналом, ідентифікатором та іншими параметрами, переглядати детальний опис події та експортувати результати у текстові, CSV, HTML, XML та інші формати. Утиліта підтримує роботу з журналами локального комп'ютера, файлами .evtx та, за наявності відповідних прав, журналами віддаленого комп'ютера.

Для дослідження активності користувачів застосовується WinLogOnView. Програма аналізує журнал безпеки Windows і визначає час входу та виходу користувачів, тривалість сесії, обліковий запис та мережеву адресу, якщо відповідні дані наявні в журналі.

Для дослідження мережевої активності може використовуватися NetworkTrafficView. Засіб відображає статистику мережевого трафіку з групуванням за протоколами, адресами та портами, а для TCP-з'єднань може відображати інформацію про процес, пов'язаний із з'єднанням. Для частини режимів захоплення трафіку потрібен відповідний драйвер захоплення пакетів.

Додатково може використовуватися WinDefLogView для перегляду подій журналу Windows Defender. Це дає можливість доповнити аудит інформацією про спрацювання вбудованого засобу захисту операційної системи.

На відміну від повноцінних SIEM-систем, утиліти NirSoft не утворюють єдину централізовану платформу збору та кореляції подій. Тому в цій лабораторній роботі виконується аналіз подій окремими засобами та самостійно встановлюється зв'язок між отриманими даними. Такий підхід дає змогу зрозуміти принципи аудиту безпеки та підготовки даних, які в SIEM-системах надалі можуть використовуватися для автоматичного виявлення підозрілої активності.

Обладнання та програмне забезпечення

Для виконання роботи необхідні:

1. Комп'ютер або віртуальна машина з операційною системою Windows 10 або Windows 11.

2. Права користувача, достатні для перегляду локальних журналів подій.
3. Утиліта FullEventLogView.
4. Утиліта WinLogOnView.
5. Утиліта NetworkTrafficView.
6. За можливості — утиліта WinDefLogView.
7. Табличний редактор для оформлення результатів, наприклад Microsoft Excel або LibreOffice Calc.

Програми рекомендується завантажувати безпосередньо з офіційного сайту NirSoft. Перед виконанням роботи студент повинен переконатися, що використовує актуальну версію відповідної утиліти та розуміє призначення кожного інструмента.

Порядок виконання роботи

1. Підготовка робочого середовища

- 1.1. Підготувати комп'ютер або віртуальну машину з Windows 10/11.
- 1.2. Створити на робочому столі або в іншому зручному місці каталог для лабораторної роботи, наприклад:

Lab7_NirSoft

- 1.3. Завантажити та розпакувати у цей каталог FullEventLogView, WinLogOnView, NetworkTrafficView та, за можливості, WinDefLogView.

- 1.4. Перевірити запуск кожної програми.

- 1.5. Зафіксувати у звіті версію операційної системи та назви використаних утиліт.

2. Дослідження журналів подій Windows

- 2.1. Запустити FullEventLogView.

- 2.2. Ознайомитися з основним вікном програми та доступними полями подій.

- 2.3. Визначити, які канали журналів присутні на досліджуваній системі.

- 2.4. Знайти події журналу Security.

- 2.5. Переглянути декілька подій, пов'язаних з автентифікацією користувачів.

- 2.6. Для однієї з подій відкрити детальну інформацію та визначити:

- дату і час події;
- назву каналу;
- джерело події;
- Event ID;
- рівень події;
- користувача, якщо він зазначений;
- опис події;
- додаткові дані події.

- 2.7. Повторити аналіз для журналів System та Application.

- 2.8. Порівняти призначення журналів Security, System та Application.

- 2.9. Зробити висновок щодо того, які журнали можуть бути корисними під час розслідування інциденту інформаційної безпеки.

3. Фільтрація та пошук подій

- 3.1. У FullEventLogView відкрити розширені параметри фільтрації.

- 3.2. Встановити обмеження за часовим інтервалом.

- 3.3. Виконати пошук подій за конкретним Event ID.

- 3.4. Виконати пошук подій за назвою каналу.

- 3.5. Виконати пошук за іменем користувача або іншою характерною ознакою події.

- 3.6. Порівняти кількість подій до та після застосування фільтра.

- 3.7. Вибрати декілька подій, які мають відношення до безпеки системи.

- 3.8. Експортувати результати пошуку у формат CSV або HTML.

- 3.9. Відкрити отриманий файл і перевірити правильність експорту.

4. Дослідження активності користувачів

4.1. Запустити WinLogOnView.

4.2. Переглянути список зареєстрованих сеансів користувачів.

4.3. Визначити:

- ім'я користувача;
- час входу;
- час виходу;
- тривалість сеансу;
- мережеву адресу, якщо вона доступна.

4.4. Визначити, які облікові записи використовувалися для входу в систему протягом досліджуваного періоду.

4.5. Зіставити отриману інформацію з подіями Security, які були знайдені за допомогою FullEventLogView.

4.6. Визначити, чи відповідають дані двох засобів один одному.

4.7. За наявності відмінностей пояснити можливі причини таких розбіжностей, наприклад відсутність необхідних записів у журналі або особливості реєстрації окремих типів подій.

4.8. Експортувати результати WinLogOnView у CSV або інший доступний формат.

5. Аналіз мережевої активності

5.1. Запустити NetworkTrafficView.

5.2. Вибрати активний мережевий адаптер та доступний метод захоплення трафіку.

5.3. За необхідності виконати програму з правами адміністратора.

5.4. Протягом декількох хвилин виконувати звичайні дії на навчальному комп'ютері: відкрити дозволений вебресурс, запустити програму, яка використовує мережу, або виконати іншу штатну мережеву операцію.

5.5. Проаналізувати отримані записи.

5.6. Для декількох з'єднань визначити:

- протокол;
- локальну IP-адресу;
- віддалену IP-адресу;
- локальний порт;
- віддалений порт;
- кількість пакетів;
- обсяг переданих даних;
- час початку та завершення з'єднання;
- процес, якщо така інформація доступна.

5.7. Визначити декілька найбільш активних мережевих з'єднань.

5.8. Визначити, які процеси створюють мережеву активність.

5.9. Зробити висновок про можливості використання мережевого моніторингу під час аудиту безпеки.

5.10. Зберегти результати дослідження у файл.

6. Аналіз подій Windows Defender

6.1. Запустити WinDefLogView, якщо він доступний у робочому середовищі.

6.2. Ознайомитися з подіями, які реєструє Windows Defender.

6.3. Визначити, чи є в журналі записи про виявлені загрози або інші події, пов'язані із засобом захисту.

6.4. Для наявних подій визначити дату і час, тип події, назву загрози або об'єкта, рівень та виконану системою дію.

6.5. Не створювати реальне шкідливе програмне забезпечення та не завантажувати небезпечні файли лише для отримання тестової події.

6.6. Якщо в журналі немає подій виявлення загроз, зафіксувати цей факт у звіті та проаналізувати доступні штатні події Windows Defender.

7. Формування часової послідовності подій

7.1. Вибрати певний часовий інтервал, наприклад останню годину або останній робочий сеанс.

7.2. За допомогою FullEventLogView визначити основні події цього періоду.

7.3. За допомогою WinLogOnView визначити активність користувачів.

7.4. За допомогою NetworkTrafficView визначити мережеву активність у відповідний період.

7.5. За наявності відповідних записів додати до аналізу події Windows Defender.

7.6. Розташувати вибрані події у хронологічному порядку.

7.7. Побудувати коротку часову послідовність, наприклад:

час → подія автентифікації → активність користувача → запуск/робота програми → мережеве з'єднання → подія засобу захисту.

7.8. Визначити, які події є звичайними, а які можуть потребувати додаткової перевірки.

8. Аналіз підозрілої активності

8.1. Вибрати одну ситуацію, яка може розглядатися як потенційно підозріла.

Прикладом може бути декілька невдалих спроб автентифікації протягом короткого проміжку часу.

8.2. За допомогою FullEventLogView знайти відповідні події у журналі Security.

8.3. Визначити час, користувача, тип події та інші доступні параметри.

8.4. Перевірити, чи існувала в цей період активна сесія користувача за допомогою WinLogOnView.

8.5. Перевірити, чи спостерігалася відповідна мережна активність за допомогою NetworkTrafficView, якщо такі дані доступні.

8.6. Сформулювати критерій, за яким виявлену послідовність можна вважати потенційно підозрілою.

8.7. Запропонувати, які додаткові дані необхідно отримати для остаточного підтвердження або спростування підозри.

9. Експорт результатів та підготовка аудиторських матеріалів

9.1. Експортувати результати пошуку подій із FullEventLogView.

9.2. Експортувати результати аналізу сеансів із WinLogOnView.

9.3. Зберегти результати мережевого моніторингу NetworkTrafficView.

9.4. Вибрати не менше п'яти подій, які мають значення для аналізу безпеки.

9.5. Для кожної події зазначити:

- дату і час;
- джерело;
- тип або Event ID;
- короткий опис;
- оцінку події;
- необхідність подальшої перевірки.

9.6. Підготувати короткий висновок про стан моніторингу досліджуваної системи.

10. Формування висновків

У висновку необхідно зазначити:

- які джерела інформації були досліджені;
- які інструменти NirSoft використовувалися;
- які типи подій вдалося виявити;
- які параметри подій є найбільш інформативними для аудиту;
- чи були виявлені потенційно підозрілі події;
- які додаткові засоби контролю доцільно впровадити;

- які переваги та обмеження має підхід на основі окремих утиліт порівняно з повноцінною SIEM-системою.

Вимоги до звіту

Звіт повинен містити:

1. Назву та мету лабораторної роботи.
2. Характеристики досліджуваного середовища.
3. Перелік використаних програм.
4. Результати аналізу журналів Windows.
5. Результати аналізу сеансів користувачів.
6. Результати мережевого моніторингу.
7. Результати аналізу Windows Defender, якщо відповідний інструмент використовувався.
8. Часову послідовність вибраних подій.
9. Приклад потенційно підозрілої активності та її аналіз.
10. Скріншоти основних етапів роботи.
11. Таблиці з отриманими результатами.
12. Висновки.

Рекомендована таблиця для аналізу подій

№	Дата і час	Джерело	Event ID / тип	Користувач	Опис	Оцінка події

Рекомендована таблиця для часової послідовності

Час	Джерело	Подія	Пов'язаний об'єкт	Оцінка

Контрольні питання

1. Що таке моніторинг інформаційної безпеки та яке його призначення в КСЗІ?
2. Які типи інформації реєструються в журналах подій Windows?
3. Яке призначення має журнал Security?
4. Яку інформацію дозволяє отримати FullEventLogView?
5. Які переваги дає фільтрація подій за часом, джерелом та Event ID?
6. Які відомості про користувацькі сесії можна отримати за допомогою WinLogOnView?
7. Які параметри мережевої активності можна досліджувати за допомогою NetworkTrafficView?
8. Чому декілька окремих подій самі по собі не завжди свідчать про інцидент інформаційної безпеки?
9. Що таке кореляція подій та чим вона відрізняється від простого перегляду журналу?
10. Які переваги та обмеження має використання окремих утиліт NirSoft порівняно з повноцінною SIEM-системою?

Лабораторна робота 8. Аналіз та реагування на інциденти кібербезпеки

Мета роботи: Відпрацювати послідовність аналізу та реагування на умовний інцидент і сформулювати звіт.

Короткі теоретичні відомості

Інцидент кібербезпеки – подія або сукупність подій, що можуть негативно впливати на конфіденційність, цілісність чи доступність інформації. Реагування має бути формалізованим процесом.

Типовий цикл охоплює підготовку, виявлення й аналіз, локалізацію, усунення причини, відновлення та аналіз після інциденту. Важливо встановити часову послідовність, уражені активи, масштаб і докази, документувати дії та зберігати цілісність матеріалів. Результати аналізу першопричини використовують для вдосконалення захисту.

Хід роботи

1. Отримати опис навчального інциденту.
2. Зафіксувати час, джерело повідомлення та потенційно уражені системи.
3. Визначити, чи є подія інцидентом, та оцінити критичність.
4. Зібрати пов'язані журнали й артефакти у навчальному середовищі.
5. Побудувати часову шкалу подій.
6. Визначити уражені активи та вплив на К, Ц, Д.
7. Запропонувати заходи локалізації.
8. Запропонувати усунення причини та відновлення.
9. Визначити критерії повернення до штатної роботи.
10. Оформити звіт: опис, шкала, докази, вплив, дії, залишкові ризики.
11. Провести аналіз першопричини та запропонувати щонайменше п'ять профілактичних заходів.

Результат роботи

Результат: звіт про інцидент із часовою шкалою, оцінкою впливу, локалізацією, відновленням, аналізом першопричини та рекомендаціями.

Контрольні запитання для самоперевірки

1. Що таке інцидент?
2. Які основні етапи реагування?
3. Чим подія відрізняється від інциденту?
4. Що фіксують на початку?
5. Для чого потрібна часова шкала?
6. Що таке локалізація?
7. Чому потрібно зберігати докази?
8. Що таке аналіз першопричини?
9. Як визначити критичність?
10. Як результати розслідування впливають на КСЗІ?