Міністерство освіти і науки України
Карпатський національний університет імені Василя Стефаника
Кафедра комп’ютерних наук та інформаційних систем

А. В. Ізмайлов

Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи кібербезпеки»

Івано-Франківськ
2025

УДК 004
І37

Рекомендовано до друку Вченою радою факультету математики та інформатики Карпатського національного університету імені Василя Стефаника (протокол № 9 від 22 жовтня 2025р.)

Рецензенти:

Горєлов В.О., кандидат технічних наук, доцент кафедри КНІС (Карпатський національний університет імені Василя Стефаника)

Ровінський В.А., кандидат технічних наук, доцент кафедри КНІС (Карпатський національний університет імені Василя Стефаника)

І37 Ізмайлов А.В. Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи кібербезпеки». Івано-Франківськ : КНУВС, 2025. 19 с.

Наведено методичні вказівки і завдання до лабораторних робіт з дисципліни «Основи кібербезпеки». Призначено для проведення лабораторних занять з курсу «Основи кібербезпеки» та інших, у яких вивчається різні аспекти захисту інформаційних технологій.

Для здобувачів освіти за спеціальностями галузі F «Інформаційні технології». Може бути корисним для читачів, які займаються вивченням кібербезпеки.

Зміст

Лабораторна робота №1

Проектування системи IT-безпеки

***Мета роботи*:** Навчитись проектувати системи IT-безпеки.

1.1 Теоретичні відомості

Кібербезпека – це комплекс процесів, практичних порад і технологічних рішень, які допомагають захищати важливі системи та мережу від кібератак.

Ефективна програма з кібербезпеки включає фахівців, процеси та технологічні рішення, які разом зменшують ризик перерв у роботі компаній, фінансових втрат і підриву репутації внаслідок атак.

У комплексі заходів та рішень з кібербезпеки можна умовно виділити 4 основні складові, які на різних рівнях забезпечують захист від зовнішніх та внутрішніх загроз тієї чи іншої інформаційної системи:

- Управління ризиками та відповідність вимогам безпеки
- Безпечний цикл розробки програмного забезпечення та сервісів
- Безпекові операції
- Тести на проникнення

1.2 Хід роботи

1.2.1 Сформулюйте ідею деякої інформаційної системи у межах деякої організації (підприємство, навчальний заклад, медичний центр, банк, логістична компанія, IT-фірма, тощо), розробку та підтримку системи IT-безпеки якої Ви будете здійснювати:

- Охарактеризуйте ідею інформаційної системи (призначення, ключові технології, рівень взаємодії з користувачем, тощо) та її цілі у межах 5-10 речень і занесіть їх у звіт.

- Охарактеризуйте діяльність та структуру організації, у межах якої функціонуватиме запропонована інформаційна система у межах 5-10 речень і занесіть їх у звіт.
- Вкажіть типи інформації, що обробляються (персональні, фінансові, технічні тощо) у межах організації та інформаційної системи.

1.2.2 Побудуйте діаграми, що відображають організацію, систему та її безпекові аспекти:

1.2.2.1 Контекстна діаграма системи (DFD рівня 0 або контекстна UML-діаграма), яка містить:

– основну систему (у центрі);
– зовнішні сутності (користувачі, інші системи);
– потоки даних між ними.

1.2.2.2 Діаграма організаційної структури (Organizational Chart), на якій відображені основні підрозділи організації та їх роль у забезпеченні IT-безпеки:

– керівництво;
– відділ інформаційних технологій;
– служба безпеки;
– користувачі або клієнти.

1.2.2.3 Діаграма архітектури системи або мережевої топології, на якій відображені:

– сервери (веб, бази даних, файловий, поштовий тощо);
– клієнтські пристрої;
– мережеві з’єднання, шлюзи, VPN.

1.2.2.4 Діаграма потоків даних (Data Flow Diagram, DFD рівня 1-2), на якій відображені:

– внутрішні процеси, які обробляють дані;
– сховища інформації;
– напрями руху конфіденційних даних.

1.2.2.5 *За необхідності*, наведіть Use Case-діаграму для демонстрації взаємодії користувачів із системою.

1.2.3 Охарактеризуйте інтеграції з іншими системами (CRM, ERP, хмарні сервіси тощо).

1.2.4 *За наявності*, вкажіть (із занесенням у звіт) додаткові коментарі щодо заходів чи аспектів, пов'язаних із кібербезпекою запропонованої системи та організації, в межах якої ця система функціонує, які на Вашу думку повинні бути зафіксовані у, наприклад, звітній чи проектній документації.

1.2.5 Підведіть підсумки виконаної роботи та стисло окресліть своє бачення перспектив розвитку системи IT-безпеки запропонованого рішення (у довільній формі із занесенням у звіт). За необхідності можна навести посилання на додаткові джерела, які стосуються обраної тематики запропонованого рішення.

Примітка: обсяг «ходу роботи» у звіті не повинен перевищувати 5 сторінок при кеглі 14пт, без урахування діаграм та рисунків.

1.3 Зміст звіту

1. Титульна сторінка та тема роботи.
2. Мета роботи.
3. Короткі теоретичні відомості (обсягом до 1 сторінки).
4. Хід роботи (результати виконаної роботи).
5. Висновки.

1.4 Контрольні запитання

1.4.1 Що таке кібербезпека?

1.4.2 Які стандарти кібербезпеки Ви знаєте?

1.4.3 Які складові системи IT-безпеки довільної організації Ви можете назвати?

1.4.4 Які заходи щодо забезпечення індивідуальної інформаційної безпеки користувачів Ви знаєте?

Лабораторна робота №2

Управління ризиками та відповідність вимогам безпеки

***Мета роботи*:** Навчитись визначати потенційні ризики для організації та здійснювати оцінку відповідності вимогам безпеки.

1.1 Теоретичні відомості

У комплексі заходів та рішень з кібербезпеки можна умовно виділити 4 основні складові, які на різних рівнях забезпечують захист від зовнішніх та внутрішніх загроз тієї чи іншої інформаційної системи:

- Управління ризиками та відповідність вимогам безпеки
- Безпечний цикл розробки програмного забезпечення та сервісів
- Безпекові операції
- Тести на проникнення

Складова «Управління ризиками та відповідність вимогам безпеки» (Governance Risk & Compliance (GRC)) передбачає наступні заходи, процеси та рішення для кібербезпеки:

- Оцінка ризиків
- Аудит та перевірка на відповідність вимогам безпеки
- Політики та стандарти
- Програма тренінгів та загального підвищення обізнаності
- Процес сертифікації

Найбільш поширеними стандартами у сфері кібербезпеки є:

- ISO 27001
- NIST 800-53
- OWASP

На основі стандартів розробляються політики кібербезпеки на рівні компанії та підрозділів. Політики регулюють поведінку працівників у напрямі кібербезпеки, а також рівні, режими та правила доступу до інформації.

1.2 Хід роботи

1.2.1 При виконанні завдань лабораторної роботи слід вказувати конкретні пропозиції по регулярності та термінах проведення тих чи інших заходів, а також конкретні найменування програмних засобів, які будуть використовуватись. Слід чітко вказувати, хто проводить аудити, перевірки, тести та зазначати конкретне застосування стандартів.

1.2.2 Опишіть (із занесенням у звіт) стратегію реалізації складової **«Управління ризиками та відповідність вимогам безпеки»** системи IT-безпеки для запропонованого у лабораторній роботі №1 рішення у межах визначеної організації (стратегія повинна стосуватись як самої системи, так і організації) обов'язково зафіксувавши (виділивши) реалізацію наступних компонентів:

- Оцінка ризиків (обов'язково навести як наявні ризики, так і ті, які можуть виникнути у перспективі розвитку).
- Аудит та перевірка на відповідність вимогам безпеки.
- Політики та стандарти.
- Програма тренінгів та загального підвищення обізнаності.
- Процес сертифікації.

1.2.3 *За наявності*, вкажіть (із занесенням у звіт) додаткові коментарі щодо заходів чи аспектів, пов'язаних із запропонованою стратегією, які на Вашу думку повинні бути зафіксовані у, наприклад, звітній чи проектній документації.

1.2.4 Підведіть підсумки виконаної роботи. За необхідності можна навести посилання на додаткові джерела, які стосуються обраної тематики запропонованого рішення.

Примітка: обсяг «ходу роботи» у звіті не повинен перевищувати 8 сторінок при кеглі 14пт, без урахування діаграм та рисунків.

1.3 Зміст звіту

1. Титульна сторінка та тема роботи.
2. Мета роботи.
3. Короткі теоретичні відомості (обсягом до 1 сторінки).
4. Хід роботи (результати виконаної роботи).
5. Висновки.

1.4 Контрольні запитання

1.4.1 Що таке кібербезпека?

1.4.2 Які стандарти кібербезпеки Ви знаєте?

1.4.3 Які складові системи IT-безпеки довільної організації Ви можете назвати?

1.4.4 У чому полягає оцінка ризиків у кібербезпеці?

1.4.5 Коли є доцільними внутрішні, а коли зовнішні аудити? Відповідь обґрунтуйте

1.4.6 Яке призначення політик щодо кібербезпеки?

1.4.7 Які загальні рекомендації щодо програми тренінгів та загального підвищення обізнаності у організації?

1.4.8 Що таке фішинг?

1.4.9 Які загальні рекомендації щодо програми сертифікації працівників організації?

Лабораторна робота №3

Безпечний цикл розробки програмного забезпечення та сервісів

***Мета роботи*:** Навчитись розробляти стратегію безпечного циклу розробки програмного забезпечення та сервісів.

1.1 Теоретичні відомості

У комплексі заходів та рішень з кібербезпеки можна умовно виділити 4 основні складові, які на різних рівнях забезпечують захист від зовнішніх та внутрішніх загроз тієї чи іншої інформаційної системи:

- Управління ризиками та відповідність вимогам безпеки
- Безпечний цикл розробки програмного забезпечення та сервісів
- Безпекові операції
- Тести на проникнення

Складова «Безпечний цикл розробки програмного забезпечення та сервісів» (Secure SDLC (Software (Services) Development LifeCycle)) передбачає наступні заходи, процеси та рішення для кібербезпеки:

- Безпечне конфігурування
- Оцінка ризиків
- Моделювання загроз
- Статистичний аналіз
- Перегляд коду

Під час розробки програмного забезпечення та сервісів слід застосовувати конфігурації, які забезпечують високий рівень захисту на рівні стандартів. Окрім цього сюди відносять дотримання «елементарних» правил побудови застосунків, які дозволяють убезпечитись, наприклад, від SQL-ін’єкцій, перехоплення паролів через незахищений канал (http), тощо. Окрім самого програмного забезпечення, яке розробляється, слід тестувати і конфігурувати усі залучені до його роботи зовнішні бібліотеки.

1.2 Хід роботи

1.2.1 При виконанні завдань лабораторної роботи слід вказувати конкретні пропозиції по регулярності та термінах проведення тих чи інших заходів, а також конкретні найменування програмних засобів, які будуть використовуватись. Слід чітко вказувати, хто проводить аудити, перевірки, тести та зазначати конкретне застосування стандартів.

1.2.2 Опишіть (із занесенням у звіт) стратегію реалізації складової **«Безпечний цикл розробки програмного забезпечення та сервісів»** системи ІТ-безпеки для запропонованого у лабораторній роботі №1 рішення у межах визначеної організації (стратегія повинна стосуватись як самої системи, так і організації) обов'язково зафіксувавши (виділивши) реалізацію наступних компонентів:

- Безпечне конфігурування.
- Оцінка ризиків (обов'язково навести як наявні ризики, так і ті, які можуть виникнути у перспективі розвитку).
- Моделювання загроз.
- Статистичний аналіз.
- Перегляд коду.

1.2.3 *За наявності*, вкажіть (із занесенням у звіт) додаткові коментарі щодо заходів чи аспектів, пов'язаних із запропонованою стратегією, які на Вашу думку повинні бути зафіксовані у, наприклад, звітній чи проектній документації.

1.2.4 Підведіть підсумки виконаної роботи. За необхідності можна навести посилання на додаткові джерела, які стосуються обраної тематики запропонованого рішення.

Примітка: обсяг «ходу роботи» у звіті не повинен перевищувати 8 сторінок при кеглі 14пт, без урахування діаграм та рисунків.

1.3 Зміст звіту

1. Титульна сторінка та тема роботи.
2. Мета роботи.
3. Короткі теоретичні відомості (обсягом до 1 сторінки).
4. Хід роботи (результати виконаної роботи).
5. Висновки.

1.4 Контрольні запитання

1.4.1 Що таке кібербезпека?

1.4.2 Які стандарти кібербезпеки Ви знаєте?

1.4.3 Які складові системи IT-безпеки довільної організації Ви можете назвати?

1.4.4 У чому полягає оцінка ризиків при розробці програмного забезпечення та сервісів?

1.4.5 Які «елементарні» правила побудови застосунків з точки зору кібербезпеки Вам відомі?

1.4.6 Які компоненти модулювання загроз для довільного застосунку Вам відомі?

1.4.7 У чому полягає статистичний аналіз застосунку на предмет кібербезпеки?

Лабораторна робота №4

Безпекові операції

***Мета роботи*:** Навчитись розробляти стратегію безпекових операцій.

1.1 Теоретичні відомості

У комплексі заходів та рішень з кібербезпеки можна умовно виділити 4 основні складові, які на різних рівнях забезпечують захист від зовнішніх та внутрішніх загроз тієї чи іншої інформаційної системи:

- Управління ризиками та відповідність вимогам безпеки
- Безпечний цикл розробки програмного забезпечення та сервісів
- Безпекові операції
- Тести на проникнення

Складова «Безпекові операції» (Security Operations (SecOps)) передбачає наступні заходи, процеси та рішення для кібербезпеки:

- Управління інцидентами / подіями
- Сканування вразливостей
- Детектування втручань
- Захист від шкідливого програмного забезпечення
- Аудит доступу
- Шифрування

Збір та аналіз вмісту журналів (логів (logs)) роботи системи та її компонентів (наприклад, журнал фаєрвола) передбачає обробку різних типів журналів, як на постійній основі, так і журналів за період кібератаки або підозр на спробу її організувати. Аналіз вмісту проводиться як для виявлення вразливостей так і фактів успішного чи неуспішного проходження кібератак.

Intrusion Detection Systems (IDS) передбачають «слухання» мережевого трафіку у точці входу в систему на предмет несанкціонованих втручань та повідомлення про зафіксовані втручання (у вигляді подій певного типу). Intrusion

Prevention Systems (IPS) – на відміну від IDS дозволяє здійснити автоматичне блокування зафіксованого втручання, або доступу до системи взагалі.

Endpoint Detection and Response (EDR) системи передбачають регулярний моніторинг пристрою користувача для виявлення та відповіді на кіберзагрози, зокрема шкідливе програмне забезпечення (malware) та програми для вимагання (ransomware). До EDR часто відносять антивіруси, проте сам EDR містить ширший комплекс засобів, а антивірус є однією з його основних складових.

1.2 Хід роботи

1.2.1 При виконанні завдань лабораторної роботи слід вказувати конкретні пропозиції по регулярності та термінах проведення тих чи інших заходів, а також конкретні найменування програмних засобів, які будуть використовуватись. Слід чітко вказувати, хто проводить аудити, перевірки, тести та зазначати конкретне застосування стандартів.

1.2.2 Опишіть (із занесенням у звіт) стратегію реалізації складової **«Безпекові операції»** системи IT-безпеки для запропонованого у лабораторній роботі №1 рішення у межах визначеної організації (стратегія повинна стосуватись як самої системи, так і організації) обов’язково зафіксувавши (виділивши) реалізацію наступних компонентів:

- Управління інцидентами / подіями.
- Сканування вразливостей.
- Детектування втручань.
- Захист від шкідливого програмного забезпечення.
- Аудит доступу.
- Шифрування.

1.2.3 *За наявності*, вкажіть (із занесенням у звіт) додаткові коментарі щодо заходів чи аспектів, пов’язаних із запропонованою стратегією, які на

Вашу думку повинні бути зафіксовані у, наприклад, звітній чи проектній документації.

1.2.4 Підведіть підсумки виконаної роботи. За необхідності можна навести посилання на додаткові джерела, які стосуються обраної тематики запропонованого рішення.

Примітка: обсяг «ходу роботи» у звіті не повинен перевищувати 8 сторінок при кеглі 14пт, без урахування діаграм та рисунків.

1.3 Зміст звіту

1. Титульна сторінка та тема роботи.
2. Мета роботи.
3. Короткі теоретичні відомості (обсягом до 1 сторінки).
4. Хід роботи (результати виконаної роботи).
5. Висновки.

1.4 Контрольні запитання

1.4.1 Що таке кібербезпека?

1.4.2 Які стандарти кібербезпеки Ви знаєте?

1.4.3 Які складові системи IT-безпеки довільної організації Ви можете назвати?

1.4.4 Які типи журналів слід аналізувати у довільній системі кібербезпеки?

1.4.5 Які методи та засоби сканування вразливостей Вам відомі?

1.4.6 У чому ключова відмінність між IDS та IPS засобами для детектування втручань?

1.4.7 Що таке EDR?

1.4.8 Які відмінності між сигнатурним та безсигнатурним антивірусом?

1.4.9 Які методи та засоби шифрування Вам відомі?

Лабораторна робота №5

Тести на проникнення

***Мета роботи*:** Навчитись розробляти стратегію тестів на проникнення для перевірки цілісності системи кібербезпеки.

1.1 Теоретичні відомості

У комплексі заходів та рішень з кібербезпеки можна умовно виділити 4 основні складові, які на різних рівнях забезпечують захист від зовнішніх та внутрішніх загроз тієї чи іншої інформаційної системи:

- Управління ризиками та відповідність вимогам безпеки
- Безпечний цикл розробки програмного забезпечення та сервісів
- Безпекові операції
- Тести на проникнення

Складова «Тести на проникнення» (Penetration Testing) передбачає наступні заходи, процеси та рішення для кібербезпеки:

- Зовнішній / внутрішній тест на проникнення
- Оцінка безпеки бездротового зв’язку
- Тестування веб-застосунків
- OWASP (безпековий фреймворк та рекомендації)
- NIST 800-53 (стандарт та безпековий фреймворк)

«Етичний хакінг», «Білі капелюхи» – спроби зламу системи відділом кібербезпеки (або фаховою компанією чи волонтерами) з метою виявлення та усунення вразливостей. Аналізуються варіанти атак зсередини та зовні різними каналами зв’язку.

При виявленні вразливостей при доступі по бездротовому зв’язку важливою особливістю є наявність певної територіальної зони, у межах якої може відбутись спроба несанкціонованого доступу, наприклад, з-поза меж будівлі, яка охороняється і т.д.

1.2 Хід роботи

1.2.1 При виконанні завдань лабораторної роботи слід вказувати конкретні пропозиції по регулярності та термінах проведення тих чи інших заходів, а також конкретні найменування програмних засобів, які будуть використовуватись. Слід чітко вказувати, хто проводить аудити, перевірки, тести та зазначати конкретне застосування стандартів.

1.2.2 Опишіть (із занесенням у звіт) стратегію реалізації складової **«Тести на проникнення»** системи IT-безпеки для запропонованого у лабораторній роботі №1 рішення у межах визначеної організації (стратегія повинна стосуватись як самої системи, так і організації) обов'язково зафіксувавши (виділивши) реалізацію наступних компонентів:

- Зовнішній / внутрішній тест на проникнення.
- Оцінка безпеки бездротового зв'язку.
- Тестування веб-застосунків.
- OWASP (безпековий фреймворк та рекомендації). Чітко вказати як налагоджена протидія принаймні 2 пунктам з актуального списку OWASP Top 10.
- NIST 800-53 (стандарт та безпековий фреймворк).

1.2.3 *За наявності*, вкажіть (із занесенням у звіт) додаткові коментарі щодо заходів чи аспектів, пов'язаних із запропонованою стратегією, які на Вашу думку повинні бути зафіксовані у, наприклад, звітній чи проектній документації.

1.2.4 Підведіть підсумки виконаної роботи. За необхідності можна навести посилання на додаткові джерела, які стосуються обраної тематики запропонованого рішення.

Примітка: обсяг «ходу роботи» у звіті не повинен перевищувати 8 сторінок при кеглі 14пт, без урахування діаграм та рисунків.

1.3 Зміст звіту

1. Титульна сторінка та тема роботи.
2. Мета роботи.
3. Короткі теоретичні відомості (обсягом до 1 сторінки).
4. Хід роботи (результати виконаної роботи).
5. Висновки.

1.4 Контрольні запитання

1.4.1 Що таке кібербезпека?

1.4.2 Які стандарти кібербезпеки Ви знаєте?

1.4.3 Які складові системи IT-безпеки довільної організації Ви можете назвати?

1.4.4 У чому полягає основна суть «етичного хакінгу»?

1.4.5 У чому полягає особливість виявлення вразливостей при доступі по бездротовому зв’язку?

1.4.6 Які основні вразливості визначено для веб-застосунків?

1.4.7 Що таке OWASP Top Ten?

1.4.8 У чому особливість безпекового стандарту NIST 800-53?

Рекомендовані джерела

1. 11 Strategies of a World-Class Cybersecurity Operations Center / K. Knerler, I. Parker, C. Zimmerman. – The MITRE Corporation, 2022. – 452 p. / Режим доступу: https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
2. Основи кібербезпеки: навч. посібник [електронний ресурс] / Є.С. Сілін, О.А. Кадубовський. – Дніпро.: ДонДПУ, 2023. − 200 с. / Режим доступу: https://ddpu.edu.ua/fmk/publications/manuals/manual_18.pdf
3. Безпека вебдодатків: навч. посібн. / О.В. Пірог. – Електронні дані. – Житомир: Житомирська політехніка, 2025. – 290 с. / Режим доступу: http://eztuir.ztu.edu.ua/123456789/8813
4. World’s Biggest Data Breaches & Hacks [Електронний ресурс] / Режим доступу: https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
5. Matrix – Enterprise | MITRE ATT&CK® [Електронний ресурс] / Режим доступу: https://attack.mitre.org/matrices/enterprise/
6. NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC [Електронний ресурс] / Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
7. Izmailov A., Petryshyn L. Analysis of modern encryption methods – Analiza nowoczesnych metod szyfrowania informacji. Zeszyty Studenckiego Towarzystwa Naukowego AGH; Issue 25. Wydawnictwo Studenckiego Towarzystwa Naukowego AGH – ISSN 1732-0925; 2012. – S. 123-129.