Практичне заняття № 8

Тема «Технології захисту інформації та результатів наукових досліджень»

Мета заняття:

Ознайомлення студентів з основними технологіями захисту інформації в наукових дослідженнях, методами забезпечення конфіденційності, цілісності та доступності даних. Розвиток навичок застосування сучасних засобів захисту інформації для охорони результатів наукових досліджень.

Основні питання заняття:

1. **Основи захисту інформації**:
    - Поняття і значення захисту інформації в наукових дослідженнях.
    - Загрози для інформації в процесі наукової діяльності: несанкціонований доступ, модифікація даних, знищення інформації.
    - Види захисту інформації: технічний, програмний, організаційний.
2. **Основні принципи захисту даних**:
    - Конфіденційність, цілісність, доступність — основні принципи захисту.
    - Методики шифрування інформації для забезпечення конфіденційності.
    - Аутентифікація та авторизація доступу до наукових даних.
3. **Методи захисту результатів наукових досліджень**:
    - Захист результатів за допомогою авторських прав, патентів і ліцензій.
    - Технології криптографії для захисту даних на етапах збору, зберігання та передачі.
    - Засоби цифрового підпису для верифікації результатів наукових досліджень.
4. **Інформаційна безпека в наукових установах**:
    - Організаційні аспекти безпеки: політики безпеки, внутрішні процедури, інцидентний менеджмент.
    - Програми та інструменти для моніторингу інформаційної безпеки.

- Захист від шкідливого програмного забезпечення та вірусів.

5. **Захист результатів наукових досліджень в умовах онлайн-середовища**:
    - Проблеми захисту даних в Інтернеті, використання хмарних технологій для зберігання наукових результатів.
    - Безпечне зберігання та обмін науковими даними за допомогою зашифрованих каналів зв'язку.
    - Використання двофакторної аутентифікації та інші сучасні методи захисту.

Практичні завдання:

1. **Аналіз загроз інформаційній безпеці наукових досліджень**:
    - Студенти проводять аналіз можливих загроз для інформації в науковому дослідженні: несанкціонований доступ, витік даних, втручання в процес обробки даних тощо. Для цього вони можуть використовувати сценарії реальних загроз.
2. **Шифрування даних**:
    - Студенти застосовують методи симетричного (AES) та асиметричного (RSA) шифрування для захисту результатів наукових досліджень. Вони створюють зашифровані файли, передають їх та дешифрують.
3. **Створення цифрового підпису для наукових результатів**:
    - Студенти генерують цифровий підпис для наукових звітів або статей за допомогою сучасних інструментів, таких як OpenSSL чи GnuPG, і перевіряють підпис на цілісність документа.
4. **Розробка політики безпеки для наукового проєкту**:
    - Студенти створюють просту політику безпеки для наукового проєкту, що містить рекомендації щодо захисту даних, процедури аутентифікації та доступу до наукової інформації.
5. **Захист результатів наукових досліджень у хмарному середовищі**:
    - Студенти використовують хмарні сервіси для зберігання наукових результатів (Google Drive, OneDrive, Dropbox) і застосовують додаткові засоби захисту даних (шифрування, двофакторна аутентифікація) для забезпечення безпеки.
6. **Тестування на проникнення**:

- Студенти виконують тестування на проникнення для простих інформаційних систем наукових досліджень з використанням інструментів для тестування безпеки, таких як Kali Linux, з метою оцінки вразливості системи.

Очікувані результати:

1. Студенти мають навички застосування основних технологій захисту інформації в наукових дослідженнях.
2. Вміння використовувати криптографічні методи для захисту даних, а також створювати та перевіряти цифрові підписи.
3. Студенти навчаються створювати політики безпеки для наукових проєктів та реалізовувати їх у практиці.
4. Оволодіння основами захисту результатів наукових досліджень у хмарному середовищі.
5. Розвиток навичок аналізу та управління ризиками для забезпечення інформаційної безпеки.

Література:

1. **Шевченко В.І.** «Основи інформаційної безпеки» — К.: Вища школа, 2018.
2. **Руденко Ю.М.** «Методи і засоби захисту інформації» — М.: Техніка, 2019.
3. **Савченко О.П.** «Інформаційна безпека в наукових проєктах» — К.: Наукова думка, 2020.
4. **Stallings W.** «Cryptography and Network Security: Principles and Practice» — 7th ed., Pearson, 2017.
5. **Bertino E., Sandhu R.** «Database Security: Concepts, Approaches, and Challenges» — Springer, 2005.

Ресурси:

- **OpenSSL** — інструмент для шифрування та генерації цифрових підписів: https://www.openssl.org
- **GnuPG** — програмне забезпечення для створення цифрових підписів: https://gnupg.org
- **Kali Linux** — дистрибутив для тестування безпеки та проникнення: https://www.kali.org
- **Google Drive** — хмарний сервіс для зберігання файлів: https://www.google.com/drive

- **OneDrive** — хмарне сховище від Microsoft: https://onedrive.live.com
- **Dropbox** — хмарний сервіс для зберігання та обміну файлами: https://www.dropbox.com
- **LastPass** — менеджер паролів для забезпечення безпеки: https://www.lastpass.com