ТЕМА 8

Завдання 1. Отримайте приклад політики інформаційної безпеки університету чи наукової установи (можна з відкритих джерел).

1. Визначте ключові розділи:
- загальні положення;
- організаційна структура;
- класифікація інформації;
- контроль доступу;
- заходи реагування на інциденти.

2. Порівняйте зі стандартами ISO/IEC 27001.

3. Запропонуйте рекомендації щодо покращення структури.

Завдання 2. Здобувач отримує 3 документи: наказ, регламент, внутрішній інструктаж.

1. Потрібно визначити:
- які документи є обов'язковими для виконання;
- які регламентують конкретні дії працівників;
- які носять рекомендаційний характер.

2. Визначити, чи є прогалини в документації, що можуть створити ризики для наукових даних.

Результати дослідження оформити в аналітичну таблицю з коментарями.

Завдання 3. Університет отримав пропозицію про міжнародний проєкт із комерційними партнерами.

1. Проведіть оцінку ризиків (Due Diligence) за критеріями:
- надійність партнерів;
- відповідність законодавству;
- ризики витоку інформації;
- ризики порушення інтелектуальної власності.

2. Складіть короткий висновок з рекомендаціями.

Завдання 4. Співпраця з іноземним дослідником включає обмін конфіденційними даними через месенджери.

Потрібно:

1. Визначити загрози інформаційній безпеці.

2. Запропонувати заходи щодо захисту даних.

3. Вказати, які правила політики ІБ порушено.

Завдання 5. Створіть короткий план політики інформаційної безпеки для своєї лабораторії або наукового підрозділу:

- класифікація інформації;
- доступ до даних;
- резервування та архівування;
- контроль за використанням програмного забезпечення;
- реагування на інциденти.

1. Обґрунтуйте вибір заходів відповідно до сучасних стандартів і законодавства.

Ситуаційні завдання

1. Науковець випадково виклав непублічну статтю в публічному репозиторії.
   - Які загрози та наслідки?
   - Які дії політики ІБ мали б запобігти цьому?
2. Партнерський університет надає доступ до хмарного сховища без шифрування.
   - Оцінка ризиків.
   - Алгоритм дій для безпечного використання даних.
3. Університет підписав меморандум про співпрацю, але не перевірив наявність санкцій проти партнера.
   - Що треба було зробити у процесі Due Diligence?

Теми для доповідей

1. Основні принципи політики інформаційної безпеки в наукових установах.
2. Документальне забезпечення політики ІБ: стандарти та практика.
3. Використання Due Diligence у міжнародних наукових проектах.
4. Ризики цифрової комунікації у науковій діяльності.
5. Контроль доступу та резервування наукових даних.
6. Політика ІБ в університетах: міжнародний досвід та українська практика.
7. Роль внутрішніх регламентів у забезпеченні академічної доброчесності.