ТЕМА 8. ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ УСТАНОВ, ЩО ЗДІЙСНЮЮТЬ НАУКОВУ ДІЯЛЬНІСТЬ

Завдання 1. Розробка політики інформаційної безпеки для наукової установи

Створити комплексний документ, який регулює інформаційну безпеку у вищому навчальному закладі або дослідницькому інституті.

Етапи виконання завдання:

- аналіз міжнародних стандартів (ISO 27001, NIST, GDPR);
- розробка рекомендацій щодо захисту інформації в науковій організації;
- визначення механізмів моніторингу та контролю доступу.

Результати виконання завдання оформити у вигляді офіційного документу «Політика інформаційної безпеки» (6-8 сторінок).

Завдання 2. Оцінка механізмів Due Diligence для інформаційної безпеки

Виконати аудит цифрової безпеки наукової установи та оцінити потенційні ризики.

Етапи виконання завдання:

- збір інформації про інформаційні активи та їхню класифікацію (конфіденційні, відкриті, службові);
- проведення аналізу ризиків: можливі загрози та вразливості (кібератаки, витік даних, соціальна інженерія);
- розробка рекомендацій щодо усунення ризиків.

Результати виконання завдання оформити у вигляді звіту про аудит безпеки із таблицею ризиків.

Завдання 3. Політика кіберзахисту для університету або наукового центру

Розробити практичний кейс політики кібербезпеки для захисту критичних даних дослідницької установи.

Етапи виконання завдання:

- визначення зон безпеки (мережеві сегменти, доступ до серверів, рівень довіри користувачів);
- розробка механізмів шифрування даних, VPN-доступу та автентифікації користувачів;
- впровадження протоколів реагування на кіберінциденти.

Результати виконання завдання оформити у вигляді регламенту кібербезпеки та презентації рекомендацій.