ТЕМА 3

Завдання 1. Підготуйте наукове есе, у якому:

– обґрунтуйте місце апаратного рівня у багаторівневій системі захисту інформації;

– проаналізуйте співвідношення апаратних і програмних механізмів безпеки;

– оцініть ризики ігнорування фізичного захисту в наукових установах;

– сформулюйте авторське визначення «апаратної безпеки» з урахуванням сучасних викликів (цифровізація, гібридні загрози, кіберфізичні системи).

Завдання 2. Порівняйте ефективність:

– біометричних систем контролю доступу;

– апаратних токенів автентифікації;

– смарт-карт;

– багатофакторної аутентифікації на апаратному рівні.

Оцінювання здійсніть за такими критеріями:

– стійкість до компрометації;

– економічна доцільність;

– масштабованість;

– застосовність у наукових лабораторіях.

Результати представити у вигляді аналітичної таблиці з пояснювальною запискою.

Завдання 3. Уявіть, що ви є членом комісії з безпеки науково-дослідного центру, який працює з чутливою інформацією.

Необхідно:

1. Провести аудит потенційних апаратних вразливостей.

2. Визначити ризики фізичного несанкціонованого доступу.

3. Запропонувати модель інтеграції:

– систем контролю доступу;

– відеоспостереження;

– сигналізації;

– апаратного шифрування носіїв.

4. Розробити алгоритм реагування на інцидент.

Завдання 4. Розробіть модель зонування наукової інфраструктури:

– відкрита зона;

– обмежена зона;

– зона підвищеного доступу;

– критична зона зберігання даних.

Для кожної зони визначте:

– типи апаратного контролю;

– механізми журналювання доступу;

– обмеження інтерфейсів введення-виведення.

Завдання 5. Проаналізуйте відповідність системи фізичного захисту наукової установи міжнародним стандартам управління інформаційною безпекою, зокрема вимогам International Organization for Standardization.

Необхідно:

– визначити прогалини;

– запропонувати план удосконалення;

– оцінити ресурсні потреби.

Завдання 6. Ризик-матриця

Побудуйте ризик-матрицю для наукової установи, враховуючи:

– несанкціонований фізичний доступ;

– крадіжку обладнання;

– підключення несанкціонованих пристроїв;

– саботаж;

– техногенні загрози.

Теми для доповідей

1. Апаратні засоби автентифікації як елемент нульової довіри (Zero Trust).
2. Фізична безпека наукової інфраструктури в умовах гібридних загроз.
3. Біометричні системи контролю доступу: етичні та правові аспекти.
4. Захист апаратних носіїв інформації від несанкціонованого копіювання.
5. Апаратне шифрування даних: переваги та обмеження.
6. Інсайдерські загрози та механізми їх мінімізації на фізичному рівні.
7. Захист серверних приміщень і дата-центрів дослідницьких установ.
8. Блокування портів введення-виведення як метод протидії витоку інформації.
9. Інтеграція систем відеоспостереження та аналітики доступу.
10. Кіберфізичні атаки та їх вплив на наукову інфраструктуру.