Малік Данило Андрійович
слухач магістратури НАВС

Науковий керівник:
Школьніков Владислав Ігорович
доктор філософії, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ №1 НАВС, капітан поліції

ФІЗИЧНА БЕЗПЕКА

Фізична безпека комп'ютерних систем – це комплекс заходів, спрямованих на захист комп'ютерних систем, мобільних пристроїв, даних та програм від несанкціонованого доступу.

Фізична безпека комп'ютерних систем є важливою для захисту вашої особистої та ділової інформації. Вона може допомогти вам:

– Захистити ваші дані від крадіжки або втрати.

– Запобігти несанкціонованому доступу до вашого комп'ютера або мобільного пристрою.

– Захистити вашу особисту інформацію від розкриття.

– Зберегти цілісність ваших даних.

– Знизити ризик зараження вашого комп'ютера або мобільного пристрою вірусами.

1. Фізична безпека:

Контроль доступу:

– Встановіть замки на дверях та вікнах комп'ютерного приміщення.

– Використовуйте систему пропусків для контролю доступу до комп'ютерного приміщення.

– Встановіть камери спостереження для моніторингу комп'ютерного приміщення.

2. Захист обладнання:

– Зафіксуйте комп'ютери та монітори на столах.

– Використовуйте сейфи для зберігання носіїв інформації.

– Встановіть систему пожежогасіння в комп'ютерному приміщенні.

3. Безпека даних:

– Шифруйте дані на комп'ютерах та носіях інформації.

– Регулярно робіть резервні копії даних.

– Використовуйте програмні засоби для захисту даних (антивіруси, фаєрволи).

4. Інформаційна безпека:

Використання надійних паролів:

– Встановіть складні паролі для всіх облікових записів.

– Не використовуйте один і той же пароль для різних облікових записів.

– Регулярно змінюйте паролі.

– Оновлення програмного забезпечення:

– Встановлюйте останні оновлення операційної системи та програмного забезпечення.

– Використовуйте програмне забезпечення з відкритим кодом.

5. Навчання персоналу:

– Проведіть навчання персоналу з питань інформаційної безпеки.

– Слід ознайомити персонал з правилами та процедурами інформаційної безпеки.

– Навчіть персонал, як діяти у разі виникнення інциденту безпеки.

6. Регулярний перегляд:

– Регулярно переглядайте та оновлюйте план дій на випадок надзвичайних ситуацій.

– Регулярно проводьте аудит інформаційної безпеки.

– Регулярно оновлюйте програмне забезпечення для захисту даних.

Загальні рекомендації із дотримання фізичної безпеки комп’ютерних систем:

– Нагляд або блокування доступу до пристроїв.

– Блокування доступу для ОС Windows.

– Блокування доступу для MacOS.

– При введенні чутливих даних (паролі від облікових записів, банківські дані, персональна інформація тощо) слід прикривати другою рукою клавіші, що натискаються.

– Політика чистого столу – не залишати на столі носіїв з чутливими даними.

– Не використовувати невідомі або чужі комп’ютерні пристрої або носії даних.