

Завдання модуля 6 – Кейс-стаді для різних профілів студентів

Кейс-стаді 1: Вчитель (Легка складність) – Сприяння цифровому благополуччю в класі

Сценарій: Контроль екранного часу та технологічних звичок учнів

Ви — вчитель старших класів, і помічаєте, що ваші учні часто виглядають розсіяними, втомленими та тривожними. Багато хто з них повідомляє, що проводить понад 7 годин на день перед екранами, включаючи час удома. Вас просять допомогти сприяти здоровішим цифровим звичкам через навчання.

Завдання:

- Оцініть, як цифровий стрес і час перед екраном впливають на учнів (проведіть неформальне опитування або спостереження).
- Розробіть три стратегії або види діяльності в класі для сприяння здоровому використанню цифрових технологій.
- Порекомендуйте інструменти або додатки, які учні можуть використовувати для моніторингу та контролю екранного часу.
- Створіть односторінковий посібник або інфографіку для учнів з назвою “Як взяти під контроль своє цифрове життя”.

Чого навчаються студенти: Розпізнавання ознак цифрового перевантаження, формування здорових цифрових звичок та застосування практик цифрового благополуччя в освіті.

Кейс-стаді 2: Студент медсестринства (Середня складність) – Конфіденційність пацієнтів та онлайн-етика

Сценарій: Захист конфіденційності пацієнтів онлайн Ви — студент медсестринства, який проходить практику в лікарні. Один з ваших одногрупників публікує фото в Instagram, зроблене в лікарні, на якому випадково видно конфіденційну інформацію пацієнта (ім'я та діагноз на

дошці). Журналіст знаходить це фото і звертається до вашого одногрупника із запитаннями про медичну допомогу в лікарні. Одногрупник не знає, як правильно відповісти.

Завдання:

1. Визначте ризики, пов'язані зі слабкими пароллями та спільними логінами в медичній сфері.
2. Підготуйте перелік правил «можна / не можна» щодо захисту пацієнтських даних.
3. Створіть короткий плакат або візуальну пам'ятку про найкращі практики управління пароллями.
4. Напишіть короткий poradnik у вигляді електронного листа про те, як фішингові атаки можуть бути спрямовані на медичних працівників, і як їх розпізнати.

Чого навчаються студенти: Обізнаність щодо кібербезпеки в охороні здоров'я, професійна відповідальність та гігієна цифрового середовища.

Кейс-стаді 3: Студент з кібербезпеки (Висока складність) – Сприяння кібербезпеці та обізнаності про ШІ на робочому місці

Сценарій: Навчання співробітників безпечним цифровим звичкам і використанню ШІ Ви — фахівець з кібербезпеки в середній компанії, яка нещодавно запровадила інструменти з використанням ШІ для внутрішніх комунікацій, підбору персоналу та клієнтського обслуговування. Проте багато працівників: • Не знайомі з основами цифрової гігієни • Використовують однакові паролі • Діляться конфіденційною інформацією з генеративними ШІ

Керівництво просить вас створити кампанію підвищення обізнаності для покращення кібергігієни, обізнаності про ризики ШІ та підтримки цифрового благополуччя.

Завдання:

- Оцініть основні зони ризику на робочому місці • Визначте три головні ризики: (наприклад, слабкі паролі, фішинг, неправильне використання ШІ)
- Створіть інформаційний ресурс для працівників • Плакат, сценарій відео або презентація, яка охоплює:
- Основи управління пароллями
- Як розпізнавати фішинг

- Етичне та безпечне використання ШІ
- Поради щодо цифрового благополуччя (наприклад, обмеження екранного часу)
- Запропонуйте три правила для робочого середовища • Напишіть коротку «Політику цифрової відповідальності» для співробітників, що включає:
- Захист даних
- Захист облікових записів
- Належне використання ШІ (наприклад, не вводити конфіденційні дані в публічні ШІ-сервіси)
- Оцініть ефект • Проаналізуйте, як кампанія змінить звички працівників і зменшить ризики • Запропонуйте спосіб оцінки результатів (опитування, чекліст, тест)

Чого навчаються студенти:

- Як застосовувати знання з кібербезпеки на практиці
- Як пояснювати цифрові ризики неспеціалістам
- Як просувати відповідальне використання технологій і зменшувати цифровий стрес

Фінальні вимоги та очікування від студентів:

Студенти обирають один кейс за своїм профілем і подають короткий звіт (1–2 сторінки), який містить:

- Покроковий аналіз етичних і приватних аспектів
- Інструменти, рішення або дії, які були застосовані
- Рефлексію або елемент професійного спілкування