Конспект лекції «Кібергігієна та правила безпеки. роль ШІ у створенні контенту та діяльності».

Два критично важливі аспекти взаємодії у сучасному цифровому світі: забезпечення кібербезпеки через дисципліну (кібергігієну) та використання кібертворчості як ресурсу для підтримки ментального здоров'я в умовах інформаційного тиску.

1.4 Кібергігієна та правила безпеки (паролі, оновлення, приватність)

1. **Кібергігієна** (або **цифрова гігієна**) — це комплекс практик, правил і звичок, які допомагають захистити ваші особисті дані, пристрої та цифрову репутацію від кіберзагроз. Якщо порівнювати з особистою гігієною, то кібергігієна для наших даних — це те ж саме, що миття рук для фізичного здоров'я.

Основні елементи кібергігієни включають:

1. Паролі та автентифікація

Надійні унікальні паролі та двофакторна автентифікація є основою кібергігієни.

- ✓ Пароль повинен містити **більше восьми символів**, маленькі та великі літери, спеціальні символи та числа. В ідеалі це має бути максимально випадкова комбінація всіх елементів.
- ✓ Пароль не повинен містити жодних особистих даних, таких як повне ім'я, вік, адреса, дата народження чи стать, оскільки ця інформація часто доступна в соціальних мережах і робить пароль менш надійним.
- ✓ Використання одного пароля для кількох сервісів є критичною помилкою, оскільки компрометація одного акаунту відкриває доступ до всіх інших. Рекомендовано використовувати менеджери паролів (наприклад, Bitwarden, 1Password), які зберігають паролі та аналізують їхню надійність.
- ✓ Обов'язково підключайте двофакторну автентифікацію (Multi-Factor Authentication) для кожного акаунту (якщо така можливість є), оскільки це значно підвищує захист.
- ✓ Ніколи не записуйте паролі і не зберігайте їх у телефоні. Ніколи не діліться паролями, навіть із найкращими друзями (за винятком дорослих членів родини, яким ви довіряєте).

2. Оновлення та антивірусний Захист

- ✓ Регулярне оновлення програмного забезпечення є критично важливим. Встановлюйте оновлення операційної системи негайно, оскільки більшість із них містить важливі патчі безпеки. Відкладання оновлень є типовою помилкою, яку активно експлуатують кіберзлочинці. Регулярно оновлюйте прошивку IoT-пристроїв (розумних телевізорів, камер).
- ✓ Використовуйте антивірусні рішення, які можуть використовувати машинне навчання для виявлення нових загроз. Регулярно оновлюйте антивірус.
- ✓ Для смартфонів використовуйте біометричну автентифікацію, дублюючи її надійним PIN-кодом. Регулярно переглядайте, які дозволи надані додаткам.

LIVEWORKSHEETS

- ✓ Уникайте відкритих мереж у громадських місцях або використовуйте VPN для всього трафіку. Використовуйте лише **захищену мережу Wi-Fi** (на яку встановлено пароль).

3. Приватність та захист персональних даних

Приватність — це право контролювати інформацію про себе, заборона на збір і поширення особистих даних без згоди.

- Персональні дані- це інформація, за допомогою якої можна ідентифікувати особу (ПІБ, адреса, дата народження, банківські дані, псевдонім тощо). Діти та підлітки часто поширюють свої персональні дані та залишають багато цифрових слідів.
- Налаштування приватності- рекомендовано встановлювати закритий (приватний) акаунт у соціальних мережах, щоб уникнути небажаних контактів, хейтспічу та кібербулінгу.
- Мінімізація інформації- вказуйте мінімальну кількість інформації про себе. Не публікуйте особисті дані (номер телефону, адресу, геолокацію).
- Геолокація під час війни- будьте обережні, оскільки за позначкою геолокації на фотографії чи відео може ховатися справжня небезпека, особливо під час війни, коли окупанти можуть використовувати цю інформацію для планування нападів.
- Інформаційна гігієна та недовіра-необхідно критично та обачливо ставитися до всього, що ви бачите та чуєте в Інтернеті, оскільки інформація, як правило, ніким не перевіряється. Не відкривайте файли, які надіслали невідомі вам люди, бо вони можуть містити віруси або агресивний зміст.
- Звернення по допомогу- якщо хтось пише з проханням допомоги або намагається шантажувати чи примусити до отримання інформації, варто разом із дорослими зробити скріншот та звернутися до кіберполіції через онлайн-форму.

2. Кібертворчість і саморегуляція: використання медіа-арту та мемотворчості для гармонізації емоційного стану

Кібертворчість та **медіа-арт** розглядаються як важливий інструмент для самовираження та антистресової смислової саморегуляції, особливо в умовах воєнних викликів та інформаційного тиску.

1. Медіа-арттерапія та саморегуляція

Медіа-арттерапія — це новітній різновид арттерапії, який передбачає використання сучасних систем комунікації та кіберпростору як засобів та простору для зцілення особистості.

- ✓ Створення власних медіапродуктів сприяє антистресовій смисловій саморегуляції, допомагаючи покращити психологічний стан під час війни. Це також забезпечує збереження психічного здоров'я та психологічного добробуту.
- ✓ Зцілювальна дія медіа-арттерапії ґрунтується на художній експресії (знімаються бар'єри перед творчістю завдяки звичності медіа-засобів), побудові терапевтичних

LIVEWORKSHEETS

стосунків (отримання емоційної підтримки та прийняття через поширення продуктів у соціальних мережах) та зворотному зв'язку (формування нових смислів та усвідомлення).

- ✓ Вона включає різні форми, такі як колаж, відео, анімаційні фільми, сторітелінг. Раніше відомі кінотерапія та фототерапія також увійшли до складу медіа-арттерапії.
- ✓ Для зняття стресу та релаксації активно застосовуються інформаційні технології, що ґрунтуються на віртуальній реальності (VR-тренінги та медитаційні застосунки), які допомагають знижувати рівень напруги та покращувати якість сну.
- ✓ Сьогодні користувачі можуть створювати картини та малюнки за текстовим описом за допомогою застосунків штучного інтелекту. Це є корисним інструментом, особливо для клієнтів, які не мають можливості використовувати традиційні художні матеріали через фізичні обмеження чи певні умови перебування.

2. Мемотворчість як засіб гармонізації

Мемотворчість є різновидом кібертворчості, який використовується для **гармонізації емоційного стану**.

- ✓ Інтернет-мем завжди є результатом спільної творчості.
- ✓ Гумор є одним із зрілих (адаптивних) механізмів психологічного захисту, які мають значний вплив на психічне благополуччя. Роль гумору у підвищенні інформаційної стійкості також є важливою.
- ✓ Створення мему на медіаповідомлення, яке зачепило почуття, є однією з форм творчого домашнього завдання.
- ✓ У контексті війни використання нецензурної мови в публічному просторі може розглядатися як реакція на ненормальні обставини і є показником того, що людина вже не може діяти іншими культурними способами.

3. Комплексний підхід до саморегуляції

Саморегуляція в кіберпросторі також передбачає:

- ✓ Ціннісно-смислова саморегуляція-визначення смислу і цінності того, що відбувається, чому і навіщо, заради чого використовуються медіа.
- ✓ Свідома активність- усвідомлене вибудовування захисних ланцюжків за допомогою зрілих механізмів (гумор, сублімація) та набуття навичок саморегуляції.
- ✓ Баланс між світами- важливо навчитися шукати баланс між реальним та цифровим світом. Треба обмежувати час на перегляд новин до 15–20 хвилин на день.
- ✓ Тілесна релаксація- дуже корисно хоча б 15–20 хвилин на день гуляти або споглядати природу, що знімає психоемоційне напруження. Також рекомендується робити тілесні релаксації та вправи на заземлення для роботи з тілесним напруженням.

LIVEWORKSHEETS

Конспект лекції «Кібергігієна та правила безпеки. роль ШІ у створенні контенту та діяльності».

Штучний інтелект (ШІ) та нейронні мережі докорінно змінюють сучасний інформаційний простір, впливаючи як на створення контенту, так і породжуючи нові, більш витончені кіберзагрози.

Роль штучного інтелекту у створенні контенту та діяльності

Штучний інтелект і алгоритми персоналізованого контенту є ключовими чинниками, що формують новий тип суспільної свідомості — мережеву свідомість. ШІ дедалі більше впливає на інформаційне середовище, починаючи від персоналізованого контенту і закінчуючи автоматизованим створенням новин.

А. ШІ як інструмент творчості (Кібертворчість)

- ✓ Засоби ШІ активно використовуються в медіатворчості та медіа-арті. В межах постмодерної культури зображення, створені ШІ, вважаються творчими продуктами, оскільки нове розташування готових предметів або елементів у просторі є творчістю.
- ✓ Штучний інтелект дозволяє користувачам створювати картини та малюнки за текстовим описом. Продукт, створений ШІ, розглядається як співтворчість. Людина виступає «замовником» малюнка, створюючи опис (промт), а ШІ здійснює компіляцію зображень, що вже існують у всесвітній мережі, використовуючи алгоритми глибокого навчання та генеративно-змагальні мережі (GAN).
- ✓ ШІ може бути використаний для створення мемів і гіфок, картинок для листівок, музичних фрагментів та навіть для добору подарунків.
- ✓ Картини, «намальовані» ШІ, зазвичай є більш майстерно виконаними та складними порівняно з малюнками, створеними людиною, проте їхній аналіз утруднений через відсутність спільних символів, властивих творчості певної соціальної групи.

Б. ШІ у підтримці ментального здоров'я та освіті

- ✓ Штучний інтелект відкриває нові можливості для підтримки людини та навчання, особливо в умовах стресу та війни:
- ✓ Створення малюнків за допомогою ШІ може бути корисним у роботі з клієнтами, які не можуть використовувати традиційні художні матеріали через фізичні обмеження (наприклад, ампутація кінцівок, знерухомлення) чи певні умови перебування (як то військові на «нулі»).
- ✓ Методи ШІ, зокрема машинне навчання та аналіз даних, використовуються для надання персоналізованих рекомендацій, спрямованих на підтримку ментального здоров'я користувачів.
- ✓ ШІ може виступати як індивідуальний асистент (тютор) з практично необмеженими знаннями, що покращує навчання та розвиток. Адекватне використання генеративних мовних моделей, наприклад ChatGPT, може осучаснити спроєктований віртуальний освітній простір. Також існують ШІ-ресурси для вибору професії.

2. Кіберзагрози та етичні виклики, пов’язані зі ШІ

LIVEWORKSHEETS

Конспект лекції «Кібергігієна та правила безпеки. роль ШІ у створенні контенту та діяльності».

Зростаюче застосування ШІ в усіх сферах життя, включаючи створення контенту, породжує нові виклики та загрози, особливо в контексті кібербезпеки та маніпулювання свідомістю.

А. Використання ШІ у кіберзлочинності

- ✓ Штучний інтелект дедалі частіше використовується у кіберзлочинності. Це призводить до того, що атаки стають значно досконалішими.
- ✓ Соціальна інженерія та Фішинг: Кіберзлочинці використовують комбінацію тактик, включаючи ШІ, для створення фішингових атак нового покоління, які використовують персоналізовані дані із соціальних мереж і виглядають абсолютно легітимними.
- ✓ Deepfake-технології: Вони входять до переліку головних загроз інформаційного простору і використовуються, поряд із бот-мережами, для впливу на масову свідомість.

Б. Маніпуляції та втрата критичного мислення

ШІ впливає на формування світогляду, але його вплив не завжди позитивний.

- ✓ **Інформаційні «бульбашки» (Filter Bubbles):** алгоритми соціальних мереж та персоналізації контенту, керовані ШІ, створюють інформаційні «бульбашки», які можуть обмежувати доступ до альтернативних думок, що, у свою чергу, знижує рівень критичного мислення. Це створює ширші можливості для контролю та обмеженості отриманої інформації.
- ✓ ШІ є одним із чинників, що посилює маніпуляції. Зростає роль фейкових новин та інформаційних маніпуляцій, які стають частиною політичних кампаній.
- ✓ Технології ШІ можуть сприяти фальсифікації інформації та творенню «альтернативної реальності» («фейків»).

В. Етичні проблеми та Відповідальність ШІ

З розвитком ШІ виникають питання щодо його етичного використання та правового статусу.

- ✓ Використання рекомендаційних систем для підтримки ментального здоров'я, що застосовують ШІ, може містити загрози, пов'язані з безпекою особистих даних. Виникають етичні проблеми, пов'язані з компромісом між конфіденційністю та персоналізованими даними, а також контролем даних.
- ✓ Стоїть питання відповідальності AI за вплив на свідомість суспільства. Навіть генеративні моделі, як-от ChatGPT, не можуть нести повну відповідальність за свої відповіді, оскільки вони базуються на алгоритмах і можуть допустити помилки, недостатність даних або неправильну інтерпретацію запиту. Самі ШІ-системи визначають себе як інструмент для забезпечення інформаційних послуг, а не як суб'єкт.
- ✓ Користувачам, які приймають рішення на основі відповідей ШІ, необхідно провести власний аналіз та здійснити відповідні перевірки.

LIVEWORKSHEETS

Конспект лекції «Кібергігієна та правила безпеки. роль ШІ у створенні контенту та діяльності».

LIVEWORKSHEETS