Урок 68. Тема уроку: Роль медіа та штучного інтелекту в інформаційній війні. Кібербезпека в умовах інформаційної війни.

План

1. Роль медіа в інформаційній війні
2. Роль штучного інтелекту (ШІ) в інфовійні
3. Кібербезпека в умовах інформаційної війни

Медіа та штучний інтелект є ключовою зброєю та інструментами захисту в сучасній інформаційній війні, де головна мета полягає у формуванні потрібної суспільної думки, деморалізації супротивника та захисту власного інформаційного й цифрового простору. Поєднання штучного інтелекту (ШІ) з медіаресурсами створює безпрецедентну динаміку протистояння, що вимагає жорстких заходів кібербезпеки. [1, 2, 3]
.

---

1. Роль медіа в інформаційній війні

Медіа (телебачення, онлайн-видання, соціальні мережі та месенджери) виступають головним полем бою та інструментом впливу. Вони виконують такі функції: [1]

- **Формування суспільного наративу:** Держави використовують медіаплатформи для мобілізації власного суспільства та залучення міжнародної підтримки. [1]
- **Поширення пропаганди та дезінформації:** Супротивник застосовує підконтрольні ресурси та координовані мережі для поширення фейків, маніпуляцій і панічних настроїв. [1, 2]
- **Психологічні операції (ІПсО):** Через таргетовану інформацію в соцмережах здійснюється тиск на військових та цивільних з метою зниження бойового духу та створення розколу в суспільстві. [1, 2]

---

2. Роль штучного інтелекту (ШІ) в інфовійні

Штучний інтелект кардинально змінив швидкість і масштаби ведення інформаційних операцій. Його використовують як для атаки, так і для оборони. [1]
Наступальний потенціал та ризики ШІ:

- **Генерація дипфейків (Deepfakes):** Створення високореалістичних фальшивих відео, фото чи аудіозаписів із лідерами думок чи політиками для дезорієнтації населення.
- **Автоматизовані бот-мережі:** Алгоритми ШІ здатні керувати тисячами акаунтів одночасно, імітуючи поведінку реальних людей, поширюючи пропаганду й адаптуючи тексти під конкретні аудиторії. [1]
- **Генерація пропагандистських матеріалів:** Використання великих мовних моделей (як-от ChatGPT) для масового та швидкого створення текстів маніпулятивного характеру або фейкових новин. [1]

Оборонний потенціал ШІ (на прикладі досвіду України):

- **Моніторинг настроїв та аналіз медіапростору:** Платформи на базі ШІ (наприклад, SemanticForce або українські системи Mantis Analytics та Let's Data) у реальному часі аналізують мільйони повідомлень, виявляючи бот-мережі, адаптовані пропагандистські наративи та маніпуляції.
- **Розвідка на основі відкритих джерел (OSINT) та геопросторова аналітика:** ШІ обробляє супутникові знімки, відео та дописи у соцмережах для виявлення переміщень чи логістичних проблем ворога (як це робить аналітична агенція Molfar).
- **Виявлення колаборантів та контррозвідка:** Спеціалізовані системи ШІ аналізують перехоплені розмови або координати для блокування діяльності навідників та зрадників. [1, 2, 3, 4]

---

3. Кібербезпека в умовах інформаційної війни

Кібератаки є невіддільною частиною інформаційної війни. Злам державних сайтів, витік персональних даних або відключення критичної інфраструктури використовуються для підсилення панічних настроїв у медіа. [1]

Ключові правила цифрового захисту:

1. **Використання безпечного зв'язку:** Надавайте перевагу мобільному інтернету або захищеним, перевіреним Wi-Fi мережам. Завжди використовуйте надійні сервіси VPN (наприклад, NordVPN, Surfshark, ProtonVPN) для шифрування трафіку.
2. **Заборона на вороже ПЗ:** Категорично заборонено використовувати російські чи білоруські антивіруси та програмне забезпечення, оскільки вони збирають дані на користь спецслужб ворога.
3. **Цифрова гігієна в соцмережах:** Уникайте публікації фотографій із прив'язкою до місцевості (геолокацією), не викладайте військову техніку, наслідки обстрілів чи об'єкти критичної інфраструктури.
4. **Контроль конфіденційності під час роботи з ШІ:** Ніколи не завантажуйте секретні документи, паролі чи персональні дані у публічні ШІ-моделі (ChatGPT тощо).
5. **Критичне мислення та медіаграмотність:** На тлі загрози дипфейків та автоматизованої дезінформації критично важливо перевіряти будь-яку сенсаційну новину через офіційні джерела та аналізувати інформацію. [1, 2, 3, 4]