HEI-TRAIN. HEI Transformation for Entrepreneurship and AI-Driven Innovation

eit Food

Funded by the European Union – NextGenerationEU

Part of EIT Higher Education Initiative

eit-hei.eu

Роль **AI** у кібербезпеці

Володимир Хлівецький

ШІ для кібербезпеки

Основні сфери застосування ШІ в безпеці:

- виявлення аномалій;
- виявлення шкідливого ПЗ;
- виявлення вторгнень;
- запобігання шахрайству;
- узагальнення інцидентів;
- створення звітів;
- моделювання та реконструкція подій.

Еволюція ШІ в кібербезпеці

Сфера кібербезпеки використовує ШІ з кінця 1980-х років. Перші системи працювали на основі правил і видавали попередження за наперед визначених умов.
З початку 2000-х розвиток машинного навчання дозволив розпізнавати моделі трафіку та поведінку користувачів, виявляти аномалії та реагувати на загрози.
Сучасний етап - генеративний ШІ, здатний створювати контент на основі наявних даних і спілкуватися з користувачами природною мовою.
З'являються також ШІ-агенти, які можуть автономно виконувати завдання в сфері безпеки та ІТ.

Основні компоненти ШІ для кібербезпеки

- Машинне навчання
- Глибоке навчання
- Генеративний ШІ
- ШІ-агенти

Приклади застосування ШІ в кібербезпеці

- Управління ідентифікацією та доступом (IAM)
- Безпека кінцевих пристроїв
- Хмарна безпека
- Захист даних
- Виявлення загроз (XDR, SIEM)
- Розслідування та реагування

ШІ для кібербезпеки та безпека самого ШІ

Варто розрізняти:

ШІ для кібербезпеки - використання ШІ для захисту систем, виявлення та реагування на загрози.

Безпека ШІ - захист моделей, алгоритмів і даних самого ШІ від атак, маніпуляцій і викрадення.

Практичні рекомендації з впровадження ШІ

- **Розробіть стратегію.** Інструменти мають інтегруватися з вашою інфраструктурою.
- **Інтегруйте системи безпеки.** ШІ найкраще працює з цілісною картиною загроз.
- **Контролюйте якість даних.** Неточні або упереджені дані призведуть до хибних висновків.
- **Дотримуйтеся етики.** ШІ не повинен самостійно ухвалювати критичні рішення.
- **Постійно тестуйте системи.** Виявляйте упередженість та інші проблеми.
- **Встановіть політику використання генеративного ШІ.** Захищайте конфіденційні дані.

Нові тенденції в галузі ШІ для кібербезпеки

- Фахівці переходять до стратегічних завдань, а ШІ бере на себе операційні.
- Поява гібридних ролей - спеціаліст з безпеки + експерт з ШІ.
- Центри операцій з безпеки працюватимуть у режимі проактивного пошуку загроз.
- Інтеграція ШІ в системи безпеки як стандарт.
- Використання ШІ у відеоаналізі, дронах, роботах для фізичної безпеки.
- Технології обману (deception) на базі ШІ - динамічні пастки для хакерів.
- Системи прогнозування атак за допомогою ШІ.
- ШІ-агенти зможуть автономно виконувати завдання безпеки.

Вразливості в кібербезпеці

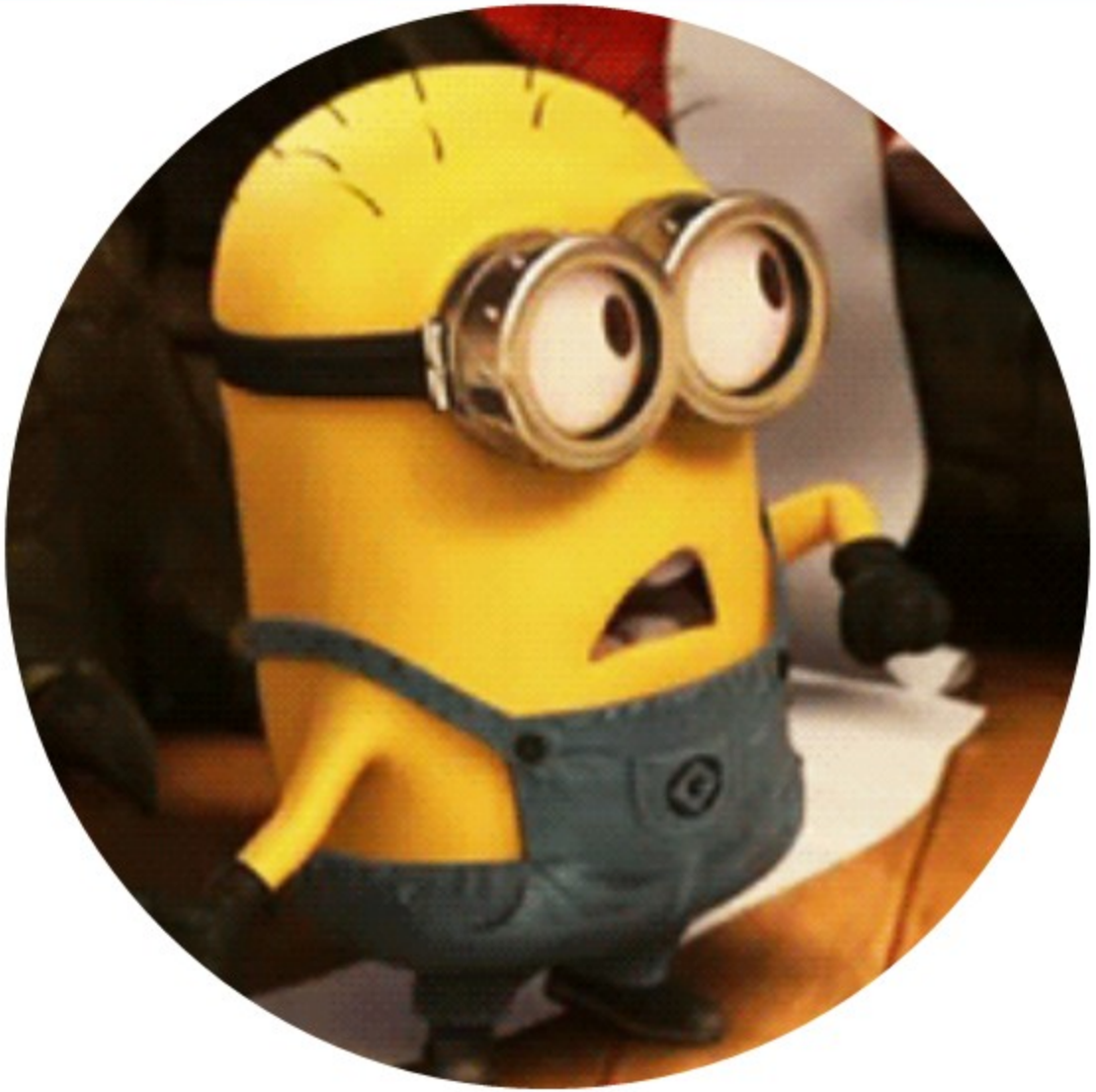
- OWASP Top 10
- Рівні критичності
- CVSS
- CVE
- CWE
- Bug Bounty

Нормативна база про кібербезпеку в Україні

- Закон України «Про основні засади забезпечення кібербезпеки України» — № 2163-VIII від 05.10.2017.
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» — № 80/94-ВР від 05.07.1994
- Закон України «Про захист персональних даних» — № 2297-VI від 01.06.2010.
- Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» — № 3475-IV від 23.02.2006.
- Закон України № 681-IX "Про внесення змін до Закону України 'Про захист інформації в інформаційно-телекомунікаційних системах' щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації"

Приклади кібератак на підприємства в Україні

- Атака на дата-центр «Парковий» (січень 2024)
- Кібератака на Kyivstar (грудень 2023)
- Атака на агрохолдинг МХП (січень 2025)
- Інформаційні атаки на компанію «Мономах» (жовтень 2025)
- Спроба фішингової атаки на оборонні підприємства (грудень 2024)



Основні компоненти ШІ для кібербезпеки

- Захист даних, систем і мереж від атак
- Маркетологи — клієнтська база
- Фінансисти — платежі
- Виробництво — лінії, автоматизація

Що таке ШІ у безпеці

- ШІ = «пильний охоронець»
- Аналізує поведінку
- Виявляє аномалії
- Блокує загрози автоматично
- Навчається на досвіді

Як ШІ бачить загрози

- Аналіз часу, геолокації, типу пристрою
- Порівняння з історичними шаблонами
- Виявлення «нестандартної поведінки»

Роль людини: цифрова гігієна

- Обережність з листами
- Складні паролі
- Оновлення ПЗ
- Не передавати доступи
- Резервне копіювання
- Тренінги з безпеки

Перспективи

- Прогнозування атак
- Повна автоматизація реагування
- Інтеграція з іншими технологіями
- Розвиток українських рішень

Підсумок

- Кібербезпека - справа кожного
- ШІ - потужний інструмент
- Загрози стають розумнішими
- Людина + ШІ = найкраща комбінація

Роль **AI** у кібербезпеці

Аналітика- Прийняття рішень - Прогнозування

Дякую за увагу :)