**Література**

1. ШТУЧНИЙ ІНТЕЛЕКТ (ШІ) – це що таке та як працює, види і приклади.
2. Застосування штучного інтелекту: 13 прикладів ШІ.
3. Як штучний інтелект використовують у різних галузях – Блог на Brainberry.ua.
4. Сфери застосування технологій штучного інтелекту в Україні: концепція ...
5. Види штучного інтелекту, його складові та історія виникнення.
6. Як діє штучний інтелект і перспективи його використання.
7. Штучний інтелект: сьогодення та майбутнє.

## ХМАРНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА

***Насатов О.І.,*** студент МК-51-24
Науковий керівник – ***Плєхова Г.А.,*** доц., к.т.н.
*Харківський національний автомобільно-дорожній університет*

**Вступ**

У сучасному цифровому середовищі хмарні технології стали важливою частиною інформаційної інфраструктури, дозволяючи користувачам і компаніям зберігати, обробляти та передавати дані через Інтернет за допомогою віртуальних ресурсів. Популярність хмарних сервісів зростає через їхні переваги, такі як гнучкість, масштабованість та зменшення витрат. Однак, з активним використанням хмарних рішень зростають і ризики порушення кібербезпеки. У цій статті розглянемо основні загрози, що виникають у хмарних середовищах, та ефективні стратегії захисту від них.

Хмарні технології стали невід'ємною частиною сучасної IT-інфраструктури, забезпечуючи користувачам миттєвий доступ до потужних обчислювальних ресурсів і сервісів за потреби. Замість використання власних серверів та апаратного забезпечення, компанії можуть оперативно користуватися хмарними ресурсами для зберігання даних, запуску програмного забезпечення або виконання обчислень в реальному часі. Це дозволяє зберігати високу гнучкість і масштабованість незалежно від обсягів роботи та потреб користувачів.

Кібербезпекові загрози в хмарних середовищах.

Разом із популяризацією хмарних технологій зростає й кількість загроз кібербезпеки. Серед найбільш поширених – несанкціонований доступ до даних, атаки на відмову в обслуговуванні (DoS та DDoS), маніпулювання даними та вразливості віртуалізації. Недостатній захист даних може призвести до серйозних наслідків: втрати конфіденційної інформації, порушення приватності користувачів і значних фінансових втрат.

Стратегії захисту в хмарних середовищах

Для забезпечення надійної кібербезпеки у хмарних технологіях потрібен всебічний підхід і ретельне управління ризиками. Ось кілька стратегій, які допоможуть ефективно контролювати загрози:

- Шифрування даних: Використання надійних методів шифрування для захисту конфіденційної інформації, зокрема алгоритмів шифрування з ключами великої довжини, таких як AES-256, а також регулярне оновлення цих ключів.
- Постійний моніторинг безпеки: Регулярний контроль активності та виявлення потенційних загроз для швидкого реагування. Це може включати системи моніторингу, які аналізують великі обсяги даних для виявлення аномальної активності та надсилають сповіщення про можливі загрози.
- Двофакторна аутентифікація: Використання додаткового рівня антентифікації для захисту від несанкціонованого доступу. Наприклад, разом із паролем користувач може вводити одноразовий пароль (OTP) або використовувати біометричні дані.
- Регулярні оновлення та патчі: Своєчасне оновлення програмного забезпечення та встановлення патчів для виправлення вразливостей системи.
- Захист мережі: Встановлення та підтримання мережевих заходів безпеки, таких як брандмауери та засоби моніторингу, що забезпечують фільтрацію пакетів та блокування небезпечного трафіку.
- Навчання та підвищення обізнаності користувачів: Організації повинні проводити тренінги та семінари для підвищення рівня обізнаності користувачів щодо загроз кібербезпеки, а також надавати доступ до навчальних матеріалів і онлайн-ресурсів.

Хмарні технології пропонують чимало переваг, проте вони також вимагають відповідального підходу до забезпечення безпеки. Ефективна реалізація зазначених стратегій допоможе захистити дані та зменшити ризики порушення безпеки у хмарних середовищах.

Приклад ефективності

Регулярні оновлення та патчі є однією з найважливіших стратегій захисту в хмарних середовищах. Цей підхід допомагає уникнути багатьох загроз, забезпечуючи актуальність і безпеку систем та інформації.

Приклад успішного застосування стратегії регулярних оновлень можна побачити на прикладі компанії X, яка використовує хмарні сервіси для зберігання і обробки конфіденційних даних клієнтів. Компанія X регулярно оновлює своє програмне забезпечення та встановлює патчі, які надають розробники. У лютому цього року було виявлено вразливість в одному з додатків, які використовувалися для обробки даних. Завдяки системі регулярних оновлень, компанія X одразу отримала повідомлення від постачальника хмарних послуг про випуск патча для виправлення вразливості. Компанія негайно встановила патч і вжила заходів для мінімізації ризиків. Завдяки швидким діям та своєчасному встановленню патчів, компанія уникнула потенційних наслідків вразливості, таких як втрата клієнтських даних або порушення конфіденційності. Цей

випадок підтверджує ефективність стратегії регулярних оновлень та патчів для забезпечення безпеки в хмарних середовищах.

Ще одним прикладом ефективності цієї стратегії є кібератака WannaCry у 2017 році. Вразливість, яку використала ця атака, була відома як "EternalBlue" і стосувалася операційних систем Windows.

Microsoft випустила патч для цієї вразливості за місяць до атаки, але багато організацій не встигли вчасно його встановити. Ті компанії, які оновили свої системи, були захищені від вірусу, тоді як інші стали жертвами WannaCry.

**Висновок**

Забезпечення кібербезпеки в хмарних технологіях є складним, але надзвичайно важливим завданням у сучасному цифровому світі. Недостатня увага до безпеки може призвести до серйозних наслідків, таких як втрата даних, порушення приватності або фінансові збитки.

Тому організаціям необхідно приділяти особливу увагу кібербезпеці та вживати всіх можливих заходів для захисту своєї інфраструктури та даних. Поєднання стратегій, розглянутих у цій статті, допоможе ефективно захищати дані та інфраструктуру в хмарних середовищах, забезпечуючи їхню безпеку у цифрову епоху.

## ІГРОЇЗАЦІЯ НАВЧАННЯ ШКОЛЯРІВ ЗА ДОПОМОГОЮ ДОДАТКІВ

***Кіс І.С.,*** студент МК-51-24
Науковий керівник – ***Плєхова Г.А.,*** доц., к.т.н.
*Харківський національний автомобільно-дорожній університет*

**Вступ**

У сучасному технологічному світі навчання програмуванню зіштовхується з новими викликами, але й відкриває численні можливості. Щоб зацікавити молоде покоління цією важливою галуззю, розробники створюють ігрові платформи для навчання програмуванню.

Такий підхід не тільки приносить задоволення, але й допомагає розвивати творчі й логічні здібності, а також стимулює інтерес до науки й технологій. У цій статті ми проаналізуємо три популярні ігрові платформи для навчання програмуванню: Roblox Studio, Minecraft Education та Scratch. Кожна з них орієнтована на різні вікові групи та надає унікальні можливості для навчання й розвитку творчих здібностей.