Андрієнко І. А. курсант факультету № 4 Харківського
національного університету внутрішніх справ
Грищенко Д. О. старший викладач кафедри протидії
кіберзлочинності факультету № 4 Харківського
національного університету внутрішніх справ

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Штучний інтелект (ШІ) – це комп'ютерна система та програма, яка може виконувати завдання, які раніше виконували лише люди. Штучний інтелект може вчитися на даних, розпізнавати зображення та текст, приймати рішення та вирішувати проблеми. Це означає, що програми, що використовують штучний інтелект, можуть самостійно вивчати та аналізувати інформацію та приймати рішення на основі цієї інформації. Штучний інтелект використовується в багатьох галузях, включаючи охорону здоров'я, банківську справу, транспорт, виробництво, бізнес та стартапи [1]. Перші спроби створення штучного інтелекту з'явилися ще в 1950-х роках. Одним з перших, хто спробував створити штучний інтелект, був Джон Маккарті з Массачусетського технологічного інституту (MIT). Він вважається одним з батьків штучного інтелекту та створив термін «штучний інтелект» у 1956 році. Однак, перший повноцінний штучний інтелект був створений не однією особою, а командою дослідників під керівництвом Джона Маккарти, Марвін Мінски та інших вчених в MIT в 1960-х роках. Вони створили програму під назвою «Logic Theorist», яка могла доводити математичні теореми, що було вважалося складним завданням для комп'ютерів того часу. По-перше, давайте розберемося, що таке критична інфраструктура. Критична інфраструктура включає інфраструктурні об'єкти, що забезпечують життєво важливу діяльність населення. Вони впливають на важливі фактори. Це включає в себе електроенергію, електрику, тепло, газ, водопостачання та каналізацію. Це також включає транспортну інфраструктуру, оскільки вона забезпечує доставку продуктів харчування, медикаментів та людей. [2] Штучний інтелект, як і інші технології, може представляти як позитивні, так і негативні аспекти інформаційної безпеки в критичній інфраструктурі. Зловмисники можуть використовувати штучний інтелект для виявлення вразливостей і розробки складних і хитрих кібератак в обхід захисту. Маніпулювання рішеннями штучного інтелекту може призвести до неправильних рішень та неправильного використання систем безпеки. Крім того, проблеми конфіденційності та етики можуть виникнути при використанні штучного інтелекту для збору та аналізу даних. Якщо організація занадто сильно покладається на штучний інтелект для захисту критичної інфраструктури, вона може стати вразливою, якщо їй не довіряють або якщо відбуваються атаки на ці системи. Тому важливо поєднувати штучний інтелект із традиційними методами захисту для розробки стратегії кібербезпеки, яка включає аналіз ризиків та застосування відповідних заходів безпеки. Крім того, штучний інтелект виявив додатки для створення та управління бот□мережі, мережею скомпрометованих пристроїв, контрольованих кіберзлочинцями. Ці мережі можуть використовуватися для різних шкідливих дій, таких як розподілені атаки відмови в обслуговуванні (DDoS), розповсюдження спаму та крадіжка даних. ШІ відіграє 4 ключову роль у спрощенні координації та оптимізації діяльності цих бот-мережей, роблячи їх більш потужними та важкими для розуміння загрозами. Незважаючи на потенційні загрози, пов'язані з використанням штучного інтелекту, він також може мати позитивний вплив на захист критичної інфраструктури. Штучний інтелект може допомогти виявити аномалії мережі та аномальну активність. Це може вказувати на кібератаку. Він також може бути використаний для прогнозування майбутніх загроз та підготовки до можливих атак. Автоматизовані системи, побудовані на основі штучного інтелекту, можуть швидко реагувати на кібератаки, блокувати шкідливі дії та відновлювати системи. Щоб ефективно використовувати штучний інтелект для захисту критичної інфраструктури, необхідно враховувати кілька аспектів. Розробка надійних моделей і алгоритмів, здатних розпізнавати нові типи загроз, є важливим завданням. Також необхідно захистити сам ШІ від атак і маніпуляцій, щоб уникнути помилкових рішень і неправильного використання систем захисту. Також важливо враховувати питання конфіденційності та етики при використанні штучного інтелекту для

збору та обробки даних. Необхідно забезпечити належний рівень захисту та конфіденційності інформації про критично важливу інфраструктуру. Загалом, штучний інтелект може бути потужним інструментом захисту критичної інфраструктури, але його використання вимагає комплексного підходу, ретельної оцінки ризиків та застосування відповідних заходів безпеки для забезпечення надійності та захисту системи.

Література

1. Що потрібно знати про штучний інтелект. bizmag. URL: http://surl.li/nppkr

2. Що таке інфраструктура: чим цивільна відрізняється від критичної. https://fakty.com.ua/ua/ukraine/20221101-shho-take-infrastruktura-chym-czyvilna vidriznyayetsya-vid-krytychnoyi