УДК 004.056

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Товстик Вадим Олександрович
Чукалов Кирило Едуардович
Жмуровська Катерина Романівна
Стецик Роман Мирославович
курсанти факультету № 4
Харківського національного університету внутрішніх справ
Онищенко Юрій Миколайович
заступник декана з навчально-методичної роботи факультету № 4
Харківського національного університету внутрішніх справ
кандидат наук з державного управління, доцент

У зв'язку зі стрімким та потужним розвитком технологій штучного інтелекту (далі – ШІ) стало можливим використовувати їх для ефективної розробки алгоритмів та заходів щодо захисту об’єктів критичної інфраструктури. ШІ може стати дієвим інструментом у виявленні та протидії кібератакам, що робить цю тему важливою для подальших досліджень та розробок. Кіберзахист об’єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації таких об’єктів. Заходи із захисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інфраструктури [1].

Алгоритми машинного навчання можуть аналізувати мережевий трафік і розпізнавати аномальну поведінку, яка є індикатором потенційних кібератак. Крім того ШІ використовується для аналізу поведінки користувачів і виявлення будь-якої аномальної поведінки, яка може вказувати на загрозу. Іншим прикладом є створення систем виявлення вторгнень, які використовують створені ШІ алгоритми для розпізнавання небезпечних тенденцій, процес ідентифікації фішингових атак стає більш ефективним завдяки використанню моделей машинного навчання для ідентифікації та запобігання спробам

викрадення даних. Сучасні системи ШІ ґрунтуються на методах, які вразливі для руйнівних кібератак, дуже небезпечних для функціонування інформаційних систем, завдяки чому зловмисники можуть здобути контроль над ними і маніпулювати для безпосереднього впливу на безпеку користувачів. Тому доцільно розробити надійні та ефективні заходи із забезпечення цифрової безпеки. При цьому експерти виділяють як звичайні вразливості програмного забезпечення, так і специфічні вектори кібератак на ШІ (відмова в обслуговуванні, витік даних, модифікація даних, троянські програми, кібератаки тощо), які характеризуються різним рівнем ймовірності, тяжкості та впливу на безпеку систем ШІ в цілому [2].

Захист об’єктів критичної інфраструктури, таких як електростанції, транспортні системи та урядові установи, має першорядне значення для забезпечення безпеки та добробуту людей і суспільства в цілому. Традиційні системи відеоспостереження існують десятиліттями, забезпечуючи моніторинг та запис діяльності персоналу в цих чутливих зонах. Однак вони часто страждають від таких обмежень, як людські помилки, повільний час відгуку і нездатність ефективно обробляти і аналізувати великі обсяги даних. Саме тут у гру вступає відеоспостереження зі ШІ, що використовує передові технології для подолання цих проблем і забезпечення підвищеної інформативності про події.

Відеоспостереження з інтегрованим ШІ може аналізувати великі обсяги відеоінформації в режимі реального часу. Алгоритми машинного навчання полегшують виявлення небезпечних ситуацій, таких як незаконний доступ або незвичайна діяльність. Коли небезпека розпізнається, система відеофіксації може автоматично інформувати операторів та ініціювати процедури безпеки, призначені для запобігання кібератакам або іншим небезпечним ситуаціям [3].

Проведення експериментів, які оцінюють ефективність застосування ШІ в конкретних ситуаціях кібернетичних загроз, дозволяє провести спеціальний аналіз і оцінку продуктивності алгоритмів і моделей у реальних ситуаціях. Ці експерименти можуть включати експерименти з кібератаками, тестування робочих навантажень або використання реальних даних для оцінки

ефективності ШІ в боротьбі із загрозами. Отримані результати можуть служити основою для подальшого вдосконалення та оптимізації алгоритмів, що допомагають підняти рівень захисту в реальних умовах. Такий підхід сприяє розробці більш ефективних та адаптованих стратегій захисту від непередбачуваних кібернетичних загроз. Результати експериментів допомагають уточнити та підвищити ефективність ШІ, а також розробити ефективніші методи протекції в конкретних ситуаціях.

Основна загроза поширення відкритих інструментів генеративного ШІ полягає у тому, що ці технології будуть доступні не тільки для забезпечення кібербезпеки, але і для кібернападів. Хоча поточна інфраструктура на рівні ChatGPT, Gemini(Bard) не дозволяє хакерам створювати нові віруси чи модифікувати поточні, вони можуть використовувати її у режимі co-pilot. А значить – витрачати набагато менше часу на підготовку атак. Наприклад, нещодавно з’явився автоматизований алгоритм WormGPT. Він допомагає шахраям генерувати переконливі спам-листи, що обходять систему спам-фільтрів. Для цього система використовує датасет бізнес-листів зі зламаних корпоративних поштових скриньок. Як наслідок, протягом останнього року збільшилася кількість інцидентів з фішингом, вірусами-вимагачами тощо.

Водночас злочинців суттєво не побільшало – просто тепер одна людина може розширити охоплення своєї діяльності. Існує ризик того, що генеративний ШІ буде використано для створення та поширення неправдивої інформації та чуток. За допомогою цих технологій можна автоматично створювати контент, який має на меті переконати користувачів і вплинути на їхні думки чи дії. Наприклад, генеративний ШІ можна використовувати для створення фейкових новин, відео або персонажів, які мають високу популярність у соціальних мережах. Це може сприяти передачі неточної інформації та призвести до значної втрати довіри громадськості до інтернет-джерел [4].

Важливим фактором протидії цьому є залучення громадськості до спільних зусиль щодо вирішення проблеми зловживання генеративним ШІ та

розробки протоколів безпеки для його використання. Загалом, для компаній, які хочуть підвищити ефективність, безпеку, продуктивність, інновації та інші важливі бізнес-результати, ШІ стає найпопулярнішим вибором. Проте бізнес-спільнота повинна усвідомлювати необхідність забезпечення безпеки, керування та підтримки відповідності цій революційній технології, щоб забезпечити безпеку своїх операцій у кіберпросторі. У результаті, щоб скористатися численними перевагами ШІ необхідно спочатку зрозуміти весь ландшафт власної технології та те, як її можна безпечно використовувати для впровадження ШІ. Від інфраструктури хмар і кіберпростору до даних і керування додатками, є кілька сфер, якими компаніям слід зайнятися, щоб підвищити свою готовність до впровадження ШІ у своїй діяльності [5].

Для успішного впровадження рекомендується розробити чітку стратегію, яка визначатиме цілі, завдання та етапи впровадження ШІ. Важливо також подбати про підготовку кваліфікованих фахівців, які розуміють принципи роботи ШІ та можуть ефективно їх використовувати. Необхідно збирати, очищати та сортувати дані з різних джерел для забезпечення ефективної роботи алгоритмів ШІ. Системи ШІ повинні безперебійно працювати з існуючими системами кіберзахисту, а також бути захищеними від кібератак та маніпуляцій. Важливо впровадити систему моніторингу та оцінки ефективності роботи систем ШІ, а також співпрацювати з міжнародними організаціями та партнерами в галузі забезпечення приватності та безпеки. Впровадження ШІ в захисті об'єктів критичної інфраструктури – це складний, але важливий процес, який потребує комплексного та системного підходу, ґрунтованого на кращих практиках. Слід також враховувати етичні та правові аспекти використання ШІ, щоб мінімізувати ризики та не допустити зловживань.

Використання ШІ в системі безпеки об'єктів критичної інфраструктури має значний потенціал для підвищення рівня захисту. Інтеграція інтелектуальних систем дозволяє автоматизувати виявлення та протидію кіберзагрозам, а використання алгоритмів машинного навчання покращує ефективність комплексних заходів. Підкреслюється необхідність постійного

вдосконалення технологій та врахування етичних аспектів для успішного впровадження ШІ у сфері функціонування об'єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п#Text (дата звернення: 24.03.2024).
2. SIDCON, International Consulting Company. Забезпечення кібербезпеки впровадження штучного інтелекту: аналіз вразливостей, загроз та засобів захисту. LinkedIn. URL: http://surl.li/rwppx (дата звернення: 24.03.2024).
3. Покращення захисту критично важливої інфраструктури за допомогою відеоспостереження зі штучним інтелектом – TVT Digital | Офіційний сайт – Системи відеоспостереження та IP-домофонія. TVT Digital | Офіційний сайт. URL: http://surl.li/rwpqm (дата звернення: 24.03.2024).
4. Валентина Шимкович. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. Robot_dreams – онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс. URL: http://surl.li/ncufj (дата звернення: 24.03.2024).
5. Модернізація господарського законодавства – Впровадження технологій штучного інтелекту у забезпечення національної безпеки та обороноздатності України: проблеми та перспективи повоєнного періоду. Координата – Платформа стратегічної та законотворчої аналітики. URL: http://surl.li/gunlw (дата звернення: 24.03.2024).