Скочко П. А., магістрант
Маєвський О.В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОТИДІЇ КІБЕРАТАКАМ НА МЕРЕЖНУ ІНФРАСТРУКТУРУ КОМПАНІЇ

Сучасні компанії стикаються з безпрецедентною кількістю кібератак, які стають дедалі складнішими та більш цілеспрямованими. Традиційні підходи до забезпечення безпеки часто не в змозі ефективно реагувати на такі загрози, що вимагає використання новітніх технологій, таких як штучний інтелект (ШІ). Використання ШІ для виявлення та блокування атак на мережну інфраструктуру компанії відкриває нові горизонти в сфері кібербезпеки, забезпечуючи проактивний та адаптивний підхід до захисту.

Мета дослідження - підвищення ефективності захисту інфраструктури компаній від певних типів кібератак за рахунок впровадження систем штучного інтелекту.

Аналізуються зокрема DDoS-атаки, фішинг, атаки з використанням шкідливого програмного забезпечення, а також можливості виявлення аномалій і загроз у системних журналах, можливості інтеграції ШІ у інші елементи мережного захисту та оцінка ефективністості інтеграції рішень на базі ШІ в єдину систему для забезпечення комплексного захисту мережної інфраструктури компанії.

Результати дослідження буде використано в сфері питань кібербезпеки, шляхом інтеграції рішень на базі ШІ у процес захисту мережевої інфраструктури.

Одним із ключових завдань, які вирішуються завдяки впровадженню ШІ, є автоматичне виявлення підозрілої активності в мережі. Завдяки алгоритмам машинного навчання та глибокого навчання, системи на основі ШІ можуть виявляти аномалії в мережевому трафіку, незвичну поведінку користувачів і аномалії в програмному забезпеченні, що можуть бути ознаками спроби кібератаки. Наприклад, сучасні системи ШІ можуть виявляти навіть незначні зміни в звичайному трафіку, які часто залишаються непоміченими для традиційних засобів безпеки. Враховуючи здатність ШІ швидко обробляти великі обсяги даних, час реакції на загрози значно скорочується, що є критичним для успішного забезпечення безпеки в умовах сучасних кібератак. Окрім виявлення загроз, ШІ має ще одну важливу перевагу: здатність до автоматичного реагування в реальному часі. Системи на основі ШІ можуть автоматично генерувати рішення щодо нейтралізації загроз, що включає блокування зловмисних IP-адрес, припинення підозрілих з'єднань чи ізоляцію скомпрометованих пристроїв. Такі автоматизовані заходи значно зменшують час, який необхідний для реакції на загрози, і мінімізують ймовірність людської помилки. Важливим аспектом використання ШІ є його здатність до постійного самонавчання. Системи безпеки, що базуються на технологіях ШІ, мають унікальну здатність адаптуватися до нових загроз і змін у кіберсередовищі. Алгоритми машинного навчання можуть автоматично коригувати свої стратегії, враховуючи нові інциденти безпеки, що дозволяє системам постійно вдосконалюватися на основі реального досвіду.

Система ШІ, що поєднує всі ці можливості, може стати основою для створення універсальної і адаптивної системи кібербезпеки, яка буде здатна забезпечити захист на всіх етапах — від виявлення загроз до нейтралізації атак і прогнозування майбутніх ризиків. Такі інтегровані системи дозволяють не тільки захистити корпоративну мережу від зовнішніх атак, але й забезпечити внутрішню безпеку, запобігаючи витоку конфіденційної інформації або несанкціонованому доступу зсередини організації.

Перспективи розвитку ШІ в сфері кібербезпеки є надзвичайно широкими. Розвиток машинного навчання та глибокого навчання, зокрема використання більш потужних алгоритмів і більших обсягів даних для навчання моделей, дозволяє створювати ще більш ефективні та точні системи захисту. Завдяки інтеграції ШІ з іншими сучасними технологіями, такими як хмарні обчислення, блокчейн, а також системи для обробки великих даних, можна розробляти більш комплексні рішення для забезпечення кібербезпеки, які можуть працювати в різних сферах та на різних етапах захисту мережі. Це відкриває нові можливості для комплексного захисту мереж, який буде поєднувати не тільки традиційні засоби безпеки, але й новітні інструменти для виявлення та запобігання кіберзагрозам.

Таким чином, впровадження ШІ у процеси забезпечення кібербезпеки є важливим кроком на шляху до створення більш ефективних, адаптивних і надійних систем захисту. Завдяки здатності до постійного навчання, адаптації до нових загроз та інтеграції з іншими технологіями, ШІ стає одним із головних інструментів у боротьбі з кіберзлочинцями. знищення.

Список використаних джерел

1. Russell S. J., Norvig P. Artificial Intelligence: A Modern Approach (2nd Edition). 2nd ed. Prentice Hall, 2002. 1132 p.