УДК 004.89

[1]Пулеко К. І., студент, гр. ЗКБ-18,
[2]Поліщук Ю. Я., аспірант
Науковий керівник: [1]Пулеко І. В., канд. тех. наук,
доцент, доцент кафедри КІ та КБ
1-Державний університет «Житомирська політехніка»;
2-Національний авіаційний університет

АНАЛІЗ НАПРЯМКІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ

На сьогоднішній день кількість атак на інформаційні системи щороку зростає двозначними темпами. При цьому атаки стають все ви-тонченішими, потенційних цілей стає все більше, а збиток від атак – все вище. «Класичні» засоби протистояння кіберзагрозам вже не здатні впоратися з такими епідеміями, і на допомогу приходять рішення на базі штучного інтелекту (ШІ).

За своєю суттю ШІ сконцентрований на досягненні результату, при цьому точність не так вже й важлива. Його кінцева мета – це природна реакція при вирішенні складних завдань. Істинний ШІ здатний діяти самостійно. Він повинен знаходити ідеальне рішення в конкретній ситуації, а не просто робити висновки на основі набору даних і запрограмованої логіки. В ідеальному варіанті роль ШІ в сфері кібербезпеки зводиться до інтерпретації закономірностей, виявлених алгоритмами ШІ. Звичайно, сучасний ШІ поки не здатний інтерпретувати результати так само добре, як людина. Ця область активно розвивається, ведеться пошук алгоритмів, схожих з людським мисленням.

При пошуку нових способів застосування машинного навчання і штучного інтелекту в області кібербезпеки важливо окреслити коло сучасних проблем в цій сфері. Технології ШІ можуть бути корисні для поліпшення багатьох процесів і аспектів, які ми вже давно приймаємо за даність.

Помилки конфігурації, викликані людським фактором. З людським фактором пов'язана значна частина слабких місць кібербезпеки. Нап-риклад, навіть при наявності великої команди IT-фахівців правильна конфігурація системи може бути неймовірно важким завданням. Комп'ютерна безпека постійно вдосконалюється, і, на сьогоднішній день, ця область стала більш складною, ніж будь-коли. Інтелектуальні інструменти можуть допомогти в пошуку і усуненні проблем, що виникають при заміні, модифікації і оновлення мережевих систем.

Ефективність ручної праці – ще одна проблема кібербезпеки. Процес, що виконується вручну, неможливо кожного разу відтворювати в точності однаково, особливо в такому динамічному середовищі, яким є сучасний ландшафт кібербезпеки. Настроювання безлічі корпоративних кінцевих пристроїв – одне з найбільш трудомістких завдань. Не варто також забувати, що характер загроз постійно змінюється. Якщо за реагування на них відповідають люди, швидкість їх дій може бути знижена при зіткненні з несподіваними проблемами. Система, заснована на ШІ і технологіях машинного навчання, може працювати в тих же умовах з мінімальною затримкою.

Втома від сповіщень про загрози може стати ще однією проблемою для організацій, які не приймають заходи боротьби з нею. Через велику кількість вхідних сигналів процес аналізу технічних повідомлень стає дуже трудомістким. В результаті втома від прийняття рішень стає повсякденною проблемою для співробітників служб кібербезпеки.

Час реагування на загрозу – один з найважливіших показників ефективності служби кібербезпеки. Відомо, що атаки дуже швидко переходять від експлуатації уразливості до розгортання. Технології машинного навчання здатні витягувати дані про атаки, групувати їх і готувати для аналізу. Вони можуть надавати фахівцям з кібербезпеки звіти, пропонувати рекомендаційні дії, щоб спростити обробку даних і прийняття рішень.

Виявлення і прогнозування нових загроз – це ще один фактор, що впливає на час реагування на кібератаки. Нові види атак, моделі поведінки та інструменти можуть збити фахівців з пантелику, в результаті чого вони будуть реагувати ще повільніше. Машинне навчання може полегшити прогнозування нових загроз і скоротити час реагування за рахунок більш ефективної роботи з базою існуючих загроз.

Проблема кадрового потенціалу. Іноді знайти кваліфікованих фахівців з необхідними навичками в області кібербезпеки може бути складно. Наявність інструментів на основі ШІ дозволить скоротити штат фахівців, однак їм буде необхідно буде, постійно підвищуючи кваліфікацію в області ШІ і машинного навчання.

Адаптованість персоналу. На відміну від інших аспектів проблема адаптованості не так очевидна, проте може різко позначитися на можливостях служби безпеки. Фахівцям може бути складно привести свої навички у відповідність з конкретними вимогами компаній. Однак за допомогою правильних наборів даних можна перетворити добре нав-чені алгоритми в рішення, відповідні необхідним вимогам.