УДК 004.81

Устименко.В.О., студентка гр.125-22-2
Науковий керівник:Олішевський І.Г., асистент кафедри БІТ
(Національний технічний університет "Дніпровська політехніка", м.Дніпро, Україна)

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ КІБЕРБЕЗПЕКИ

В останні роки штучний інтелект (ШІ) став найважливішим інструментом посилення роботи людських команд з інформаційної безпеки. ШІ забезпечує настільки необхідний аналіз та виявлення загроз, які фахівці з кібербезпеки можуть використовувати для зниження ризику злому та підвищення рівня безпеки, оскільки люди вже не можуть адекватно захистити динамічну корпоративну поверхню атаки. Передбачається, що у сфері кібербезпеки системи на основі штучного інтелекту зможуть захистити організації від Інтернет - загроз, визначати типи шкідливих програм, забезпечувати дотримування стандартів безпеки та допоможуть створити кращі стратегії запобігання атакам та відновлення після атак. За оцінкою Marketsand Markets, в 2019-2026 рр. зростання ринку засобів ШІ для забезпечення кібербезпеки буде рости в середньому на 23,3% в рік, з $ 8,8 млрд до $ 38,2 млрд (рис. 1)

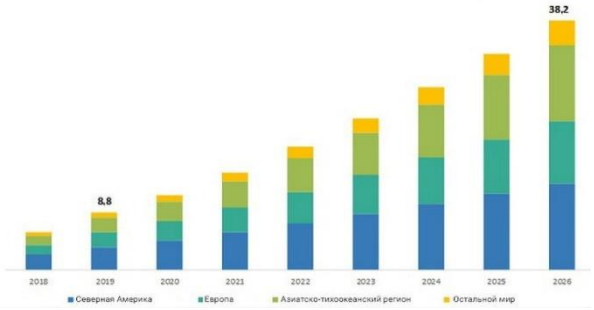

Рис.1. Динаміка ринку засобів ШІ для кібербезпеки по регіонах, $ млрд.
Джерело: MarketsandMarkets, 2019

З огляду на гостру нестачу досвідчених фахівців щодо забезпечення безпеки і величезні обсяги даних, з якими доводиться працювати організаціям, багато компаній вже використовують можливості штучного інтелекту (ШІ) для забезпечення кібербезпеки або планують зробити це.

Спробуємо розібратися що ж таке ШІ.

Штучний інтелект (*Artificial Intelligence* - AI) розуміється як здатність автоматичних систем брати на себе функції людини, вибирати і приймати оптимальні рішення на основі раніше отриманого життєвого досвіду і аналізу зовнішніх впливів. Будь-який інтелект спирається на діяльність. Багато хто вважає, що впровадження штучного інтелекту в технології кібербезпеки стане свого роду революцією і станеться це набагато раніше, ніж можна було б припустити. Насправді ж в майбутньому нас, швидше за все, чекають лише поступові поліпшення в цій галузі. Але навіть ці кроки на шляху до абсолютної автономності все ж далеко виходять за рамки наших можливостей в минулому. Незабаром штучний інтелект на основі машинного навчання стане потужним інструментом забезпечення кібербезпеки. У цій сфері, як і інших галузях, участь людини давно вважається важливим, незамінним елементом. І хоча в даний час кібербезпека, як і раніше, багато в чому залежить від роботи фахівців, у вирішенні певних завдань машини поступово починають нас випереджати.

Наведемо кілька прикладів, які підкреслюють цінність машинного навчання в сфері кібербезпеки:

Класифікація даних по конфіденційності для дотримання нормативів по їх обробці

Останнім часом захист від порушення законів про конфіденційність даних став одним з головних пріоритетів для організацій. З прийняттям Загального регламенту ЄС щодо захисту даних (GDPR) з'явилися і інші правові заходи, наприклад Каліфорнійський закон про захист прав споживачів (CCPA). Обробка даних клієнтів і користувачів повинна здійснюватися відповідно до цих актів. Зазвичай це означає, що необхідно передбачати можливість видалення даних за запитом. Недотримання цих законів тягне за собою великі штрафи і збитки репутації. Класифікація даних допоможе відокремити дані, що ідентифікують користувача, від анонімізуючих і неідентіфікуючих. Вона позбавить від необхідності вручну аналізувати величезні масиви старих і нових даних, особливо в великих організаціях і компаніях з довгою історією.

Профілі безпеки на основі поведінки користувачів

Створення індивідуальних профілів співробітників на основі їх користувальницької поведінки дозволяє адаптувати систему безпеки до структури конкретної організації. Ця модель може виявити неавторизованого користувача, проаналізувавши відхилення в його поведінці. Такі незначні нюанси, як особливості натискання клавіш на клавіатурі, можуть послужити основою для предиктивної моделі загрози. Позначивши можливі результати потенційних несанкціонованих дій, система безпеки на основі машинного навчання може запропонувати способи для зменшення потенційної поверхні атаки.

Блокування ботів на основі поведінки

Дії ботів можуть заважати роботі веб-сайтів, перевантажуючи їх запитами. Ця проблема особливо актуальна для організацій, бізнес яких залежить від інтернет-трафіку. Наприклад, для онлайн-магазинів, у яких немає фізичних торгових точок. Звичайні відвідувачі можуть зіткнутися з повільною роботою сайту, що призведе до втрати трафіку і потенційних клієнтів. Технології на основі машинного навчання можуть ідентифікувати активність ботів і блокувати її навіть при використанні коштів анонімізації, наприклад віртуальних приватних мереж. На основі даних про поведінку зловмисників алгоритм формує прогнозні моделі і превентивно блокує нові веб-адреси з такою ж активністю.

Роблячи висновок з всього сказаного, можна сказати, що високоінтелектуальне мислення - це властивість не високоорганізованої матерії, а властивість високоорганізованої душі. Тварини і людина здатні ставити і вирішувати завдання. Комп'ютери - пристрої неживі, сьогодні їх олюднюють програмісти, а машини лише слідують їх вказівками. На жаль, якою б не була складною сучасна програма, які б складні алгоритми не було в неї закладено, в кінцевому підсумку вона не зможе зробити нічого крім того, що не передбачено її автором. Можливо, в майбутньому щось і зміниться, але не сьогодні…

Ось кілька кроків, які ми можете зробити, щоб наблизити майбутнє кібербезпеки:

1. Інвестуйте в технології майбутнього. У міру того як загрози стають все складніше, зростає збиток від експлуатації вразливостей, що виникають через використання застарілих технологій або ручних процесів, які можна автоматизувати. Щоб знизити ризики, вам потрібно йти в ногу з часом. Використовуйте передові технології для комплексного захисту робочих місць, - з ними ви будете краще підготовлені до будь-яких змін.
2. Галузі потрібно більше експертів щодо забезпечення кібербезпеки на основі штучного інтелекту і машинного навчання. Ефективність засобів мережевої безпеки, заснованих на технологіях машинного навчання, значно підвищиться при наявності співробітників, здатних обслуговувати і налаштовувати їх у міру необхідності. Однак пропозиція кваліфікованих фахівців на світовому ринку набагато менше попиту на них.

3. Команди фахівців залишаться невід'ємною частиною відділів кібербезпеки. Життєво важливе значення для прийняття рішень як і раніше будуть мати критичне мислення і творчий підхід. Як уже згадувалося вище, ні технології машинного навчання, ні ШІ поки не володіють цими якостями. Тому вони повинні бути інструментом в руках вашої команди фахівців з кібербезпеки.

Перелік літератури

1. Основні напрями застосування технологій штучного інтелекту у кібербезпеці/Савченко В.А [Доповідь] -2020-5с.