© Opirskyy I., Holovchak R., Moysiychuk I. Prospects of development of artificial intelligence in the context of information security // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 2, pp. 108-115.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.26.14757

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Іван Опірський, Романа Головчак, Ірина Мойсійчук

Національний університет «Львівська політехніка»

ОПІРСЬКИЙ Іван Романович, д.т.н., доцент

Рік та місце народження: 1987 рік, м. Сімферополь, АР Крим, Україна.
Освіта: Національний університет «Львівська Політехніка», 2008 рік.
Посада: професор кафедри захисту інформації з 2019 року.
Наукові інтереси: методи і засоби технічного захисту інформації, охорона державної таємниці, проектування комплексних систем захисту інформації, лазерні системи акустичної розвідки, математичні методи та моделі захисту інформації, технічні канали витоку інформації, спецвимірювання .
Публікації: більше 120 наукових публікацій, серед яких наукові статті, монографії, навчальні посібники, тези та матеріали доповідей на конференціях.
E-mail: iopirsky@gmail.com.
Orcid ID: 0000-0002-8461-8996.

ГОЛОВЧАК Романа Василівна

Рік та місце народження: 2001 рік, м. Дрогобич, Львівська область, Україна.
Освіта: студент кафедри захисту інформації Національного університету «Львівська політехніка».
Наукові інтереси: інформаційна безпека держави, правове забезпечення інформаційної безпеки.
E-mail: romana.holovchak.kb.2018@lpnu.ua.
Orcid ID: 0000-0002-2932-3466.

МОЙСІЙЧУК Ірина Русланівна

Рік та місце народження: 2001 рік, с. Тур, Волинська область, Україна.
Освіта: студент кафедри захисту інформації Національного університету «Львівська політехніка».
Наукові інтереси: системи кіберзахисту інформаційних ресурсів, комп'ютерні науки.
E-mail: iryna.moisiichuk.kb.2018@lpnu.ua.
Orcid ID: 0000-0002-7531-5811.

Анотація. *Штучний інтелект – концепція, за якою машини здатні здійснювати деяку інтелектуальну діяльність, що властива людям або тваринам. Іншими словами можна сказати, що це поняття включає в себе будь-який пристрій, який має здатність сприймати його оточення та вживати дій, що збільшують шанс на успішне досягнення цілей. Проте, незважаючи на триваючий прогрес у швидкості комп'ютерної обробки та об'ємі пам'яті, до цих пір немає програм, які могли б зрівнятися з людською гнучкістю в більш широких областях або в завданнях, що вимагають великих повсякденних знань. З іншого боку, деякі програми досягли рівня продуктивності людських експертів і професіоналів у виконанні певних конкретних завдань, так що штучний інтелект в цьому обмеженому сенсі можна знайти в таких різноманітних додатках, як медична діагностика, комп'ютерні пошукові системи і розпізнавання голосу або почерку. Метою даної роботи є, власне, визначення позитивних та негативних аспектів застосування систем штучного інтелекту в галузі безпеки інформації. Визначено, що такі системи мають вагому роль в поточному та подальшому забезпеченні безпеки даних, а також наведено ряд недоліків таких систем для майбутнього їх врахування. У статті було розглянуто те, що штучний інтелект був розроблений шляхом вивчення того, як людський мозок думає,*

навчається і приймає рішення, а потім застосовує ці біологічні механізми до комп'ютерів. На відміну від класичних обчислень, де кодери забезпечують точні входи, виходи і логіку, штучний інтелект заснований на наданні машині вхідних даних і бажаного результату, дозволяючи машині розвивати свій власний шлях для досягнення поставленої мети. Штучний інтелект – це технологія, яка перетворює всі сфери життя. Це широкий інструмент, який дозволяє людям переосмислити, як ми інтегруємо інформацію, аналізуємо дані та використовуємо отримані результати для покращення процесу прийняття рішень. Вони змінюють спосіб, яким ми шукаємо інформацію, як ми спілкуємося один з одним, навіть як ми поводимося. Ця трансформація стосується багатьох областей, включаючи освіту. Основною метою даної статті є огляд вирішення проблем за допомогою штучних технологій. У представленому огляді літератури ми розглянули чотири категорії: індивідуальний освітній контент, інноваційні методи навчання, технологія розширеної оцінки, комунікація між студентом і викладачем. Розглянувши публікації на цю тему, ми представляємо тут можливу картину того, як штучний інтелект змінить ландшафт освіти. Починаючи з короткої історії штучного інтелекту, в даній статті представлений загальний огляд цієї технології.

Ключові слова: *штучний інтелект, машинне навчання, безпека інформації, системи машинного навчання, людина.*

Вступ

Не зважаючи на те, що алгоритми штучного інтелекту з'явилися ще в 60-их роках, інтерес до нього і його розвитку досі не згас. Оскільки сучасні як маленькі компанії, так і великі корпорації почали надавати надзвичайно великого значення інформаційній безпеці та безпосередньому захисту великого потоку даних, питання штучного інтелекту в галузі безпеки постало доволі гостро. Ні для кого не є секретом те, що, так звані, "чорні" хакери вже використовують алгоритми машинного навчання для своїх цілей, при чому доволі успішно. Експерти вже давно визначають необхідність створення "розумної" та автономної системи безпеки. Деякі з них схиляються до думки, що саме штучний інтелект буде запорукою успішності цієї системи. Звичайно, є і інша думка: для забезпечення повного захисту потрібні, власне, люди.

Поточний стан розвитку штучного інтелекту

Автоматизація з кожним роком набирає все більших обертів, а компанії все більше інвестують в її розвиток з метою замінити людську робочу силу, заявляє Forbes. Роботам не потрібно відпочивати, їм не потрібен час на обід чи на сон. Великі корпорації з колосальними кількостями найманих працівників однозначно будуть у виграшній ситуації від розвитку систем Штучного Інтелекту (ШІ). В свою чергу Білл Гейтс в своєму інтерв'ю для Time заявив, що серед усіх сучасних розробок, саме ШІ має найбільший потенціал змінити наші життя: зробити їх «продуктивнішими, ефективнішими, а загалом легшими».

Натан Бенайч та Ян Хогарт, які є серійними інвесторами галузі штучного інтелекту, заявляють, що штучний інтелект стане рушійною силою технічного прогресу в нашому все більш цифровому світі, керованому даними. Причиною цього вони визначають у тому, що нас оточують продукти людського інтелекту, незалежно чи культура це чи споживчі продукти. Ще у 2018 році ШІ досяг великого прогресу в сфері комп'ютерних ігор (зокрема StarCraft II, Quake III Arena (Capture the Flag), Dota2). Чому вибір середовища навчання для ШІ зупинився саме на іграх? Відповідь надзвичайно проста: саме там легко здійснити моніторинг процесу пристосування до мінливого середовища та варіації великої кількості змінних. Йдеться про системи ШІ, засновані на технології reinforcement learning. Автори звертають увагу на те, що виграш над реальним гравцем є менш важливим результатом, ніж вивченням методів досягнення цього результату. Системи ШІ можна порівняти з дітьми, які шляхом застосування комп'ютерних ігор здобувають нові навички, засвоюють невідомі раніше моделі поведінки без реальної загрози в житті. Мабуть, саме через вище вказану причину тестування систем машинного навчання є цілком доцільним в цьому середовищі (рис. 1).

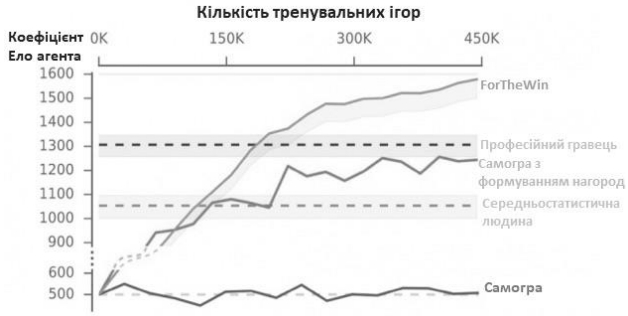

Рис. 1. Розробники компанії Deep Mind створили ШІ FTW (ForTheWin), який навчається під час гри і перемагає професійних кіберспортсменів

На діаграмі, поданій вище, неозброєним оком видно вражаючу стрімкість динаміки навчання ШІ. Авжеж, такий успіх в розвитку в комп'ютерних іграх зовсім не гарантує ідентичний результат при застосуванні в реальному житті, але можемо сказати, що це чудове місце для початку, проте однозначно не кінцева мета розвитку систем машинного навчання.

Зараз ШІ здатен навіть написати музику, відповідно до вподобань людини. Одним з перших творінь була колискова, яка за висновками медиків має заспокійливо-лікувальний ефект на людський мозок. Також, системи ШІ змогли написати цілий альбом в стилі black metal «Coditany of Timeness». Проаналізувавши інші композиції цього жанру, система змогла самостійно створити свій альбом з 5 творів.

Відповідно до результатів досліджень McKinsey & Company ШІ виявив здатність виявляти каталізатори виникнення емоцій та почуттів у людини. Це може свідчити про те, що з часом впливати на точки зору, принципи людини стане в рази легше. Таким чином недобродушні розробники нейронних мереж зможуть досягати своєї вигоди, незважаючи на думки простих людей.

Проблеми, які могли бути вирішеними за допомогою систем ШІ

Насправді, дуже важко сказати, як би закінчилась та чи інша історія, якби щось змінити, неможливо точно змоделювати ситуацію. Проте, зробити припущення ми в силі. Системи машинного навчання могли б змінити перебіг дуже багатьох значущих подій в історії як України, так і світу взагалі. Йдеться не лише про різноманітні кібератаки, які здійснюються щоденно(не беремо до уваги їх розмір та значущість нанесених збитків), а й про глобальні катастрофи, так як вибух на Чорнобильській Атомній Електростанції 1986 року, вибух на хімзаводі Phillips Petroleum Company 1989 року тощо.

Напевно доцільно буде розглядати аварію на ЧАЕС, оскільки саме ця подія стала світовим символом техногенної катастрофи. Уявіть собі, випробування реактора проводить не група людей, а ШІ, який попередньо пройшов навчання. Чи почала б така система випробування в умовах такого фізичного та техногідравлічного стану стабільності, який можна було порушити навіть незначними коливаннями? Важко сказати, проте скоріш за все, ні. Цей стан реактора і сам був викликаний некомпетентними діями персоналу, проте на цьому етапі цілком реально було запобігти катастрофі. Групі, котра проводила дану операцію, попросту не були доступні усі необхідні дані для визначення готовності реактора до випробування. Власне йде мова про вирішальний замір - оперативний запас реактивності. Чи помітила б система ШІ невідповідність значень змінних перед запуском випробування? Ми не можемо знати напевне, але маємо сміливість припустити, що так. Безпосереднім імпульсом для виникнення такої масштабної катастрофи стало введення в дії системи аварійної зупинки реактора, котра містила фатальну помилку в своїй конструкції і призвела до старту розгону потужності реактора. Ще в першій частині статті було зазначено: роботам не потрібен відпочинок, сон чи їжа. О 2 години ночі робот буде абсолютно такий же уважний та прискіпливий як і о 15 дня. Веду до того, що люди, які прийшли на зміну, цілком ймовірно приймали б зовсім інші рішення в екстремальній ситуації. Людей переповнювало почуття невідомості та страху, чого точно не може відчувати нейронна мережа. Не можна сказати точно, що за наявності такої мережі в роботі реактора в ту ніч, аварія б не відбулась чи наслідки могли б бути не настільки масштабними, але хочеться вірити в те, що дякуючи саме системам ШІ людство більше не зустрінеться з такою глобальною катастрофою.

Якщо говорити лише про забезпечення інформаційної безпеки засобами нейронних мереж, то можна згадати доволі багато різноманітних атак, яким можливо б дала відбій система ШІ. Наприклад злом Home Depot(2014), злом eBay(2014), атака на Ashley Madison(2015) тощо.

Для прикладу розглянемо злам Home Depot. Як повідомляє керівництво платформи, зловмисники ввійшли в мережу під обліковим записом так званого «продавця». Вже звідти хакери отримали доступ до «особливих» прав, що надало їм можливість завантажувати свій унікальний код в систему, який забезпечував саморозгортання на платформах самообслуговування сайту. Оскільки шкідливе програмне забезпечення ніколи не використовувалось раніше, воно доволі довгий проміжок часу не було виявленим. Як наслідок, було викрадено близько 56 мільйонів платіжних даних та 54 мільйонів електронних адрес з баз даних сервісу. Як відомо, атака сталася через вразливість операційної системи Windows(згодом був випущений «патч», який закривав прогалину в безпеці, проте було вже пізно). Неможливо точно підрахувати збиток нанесений цією вразливістю, але важливий факт - це одна з наймасовіших крадіжок даних користувача в історії. Чи могли системи ШІ не допустити цього? Навряд, проте однозначно могли зменшити розмір нанесених збитків, як мінімум завдяки більш своєчасному виявленню атаки.

Переваги ШІ над людською роботою очевидні. Така система однозначно є в рази уважнішою та прискіпливішою до процесів, які відбуваються. Враховуючи швидкість «самонавчання» нейронних мереж, можна сказати, що у вчасному виявленні загроз (за умови коректного формування завдань мережі), їм не буде рівних. Можливо, на даній стадії розвитку ШІ не може забезпечити необхідну реакцію на негативні процеси, проте однозначно зможе.

Аналіз заяв авторитетних компаній, фахівців та їх аргументів щодо подальшого використання штучного інтелекту в області безпеки

Замість того щоб служити заміною людському інтелекту і винахідливості, штучний інтелект зазвичай розглядається як допоміжний інструмент. Хоча штучний інтелект в даний час насилу справляється з завданнями здорового глузду в реальному світі, він вміє обробляти і аналізувати величезні масиви даних набагато швидше, ніж це може зробити людський мозок. Програмне забезпечення штучного інтелекту може потім повернутися з синтезованими курсами дій і представити їх користувачеві-людині. Таким чином, люди можуть використовувати штучний інтелект, щоб допомогти згладити можливі наслідки кожної дії та спростити процес прийняття рішень.

За словами Аміра Хусейна, засновника і генерального директора компанії машинного навчання SparkCognition., штучний інтелект - це свого роду друге пришестя програмного забезпечення. Це така форма програмного забезпечення, яка сама приймає рішення і здатна діяти навіть у ситуаціях, не передбачених програмістами. Штучний інтелект володіє більш широкими можливостями прийняття рішень на відміну від традиційного програмного забезпечення.

Ці риси роблять штучний інтелект дуже цінним у багатьох галузях промисловості, будь то просто допомога відвідувачам і співробітникам ефективно пересуватися по корпоративному корпусу або виконання такого складного завдання, як моніторинг вітряної турбіни, щоб передбачити, коли вона буде потребувати ремонту.

Машинне навчання часто використовується в системах, які захоплюють величезні обсяги даних. Наприклад, інтелектуальні системи управління енергією збирають дані з датчиків, прикріплених до різ-

них активів. Потім масиви даних контекстуалізуються алгоритмами машинного навчання і передаються особам, які приймають рішення, щоб краще зрозуміти вимоги до використання енергії та технічного обслуговування.

Хусейн вважає, що штучний інтелект є незамінним союзником, коли мова заходить про пошук дірок в захисті комп'ютерних мереж. Ми дійсно не можете мати достатньо експертів з кібербезпеки, щоб розглянути ці проблеми, через масштаб і зростаючу складність.

Штучний інтелект також змінює системи управління взаємовідносинами з клієнтами (CRM). Програмне забезпечення, таке як Salesforce або Zoho, вимагає інтенсивного втручання людини, щоб залишатися актуальним і точним. Але коли ми застосовуємо штучний інтелект до цих платформ, звичайна CRM-система перетворюється на автокорегуючу систему, яка залишається на вершині нашого управління відносинами.

Ще один приклад універсальності штучного інтелекту - це фінансовий сектор. Доктор Хосейн Рахнама, засновник і генеральний директор консьєрж-компанії штучного інтелекту Flybits і запрошений професор Масачусецького технологічного інституту, працював з TD Bank над інтеграцією штучного інтелекту в звичайні банківські операції, такі як іпотечні кредити.

У Salesforce вважають, що штучний інтелект має величезний потенціал для поліпшення роботи організації. Ця наступна хвиля штучного інтелекту дозволить компаніям постійно адаптувати процеси, засновані на минулому досвіді, що призведе, наприклад, до значного поліпшення таргетингу клієнтів, оскільки алгоритми глибокого навчання зможуть виявляти патерни поведінки, які з більшою ймовірністю приведуть до продажів. У ланцюжках поставок і виробництві потенційні вигоди включатимуть прогнозоване технічне обслуговування обладнання, а також оптимізацію прибутковості і запасів.

Експерти в галузі штучного інтелекту розглядають охорону здоров'я, юриспруденцію, освіту і навіть дослідження в області штучного інтелекту як кращі ранні можливості для помічників на робочому місці. На думку керівник досліджень IBM Cognitive Solutions Костаса Бекаса, якщо ми можемо використовувати штучний інтелект для автоматичного читання 400 000 наукових робіт, систематизувати знання, а потім об'єднати свою інтуїцію з машинним навчанням, ми зможемо загострити область досліджень. Це те, що, на нашу думку, дійсно змінить світ для досліджень в майбутньому.

Здатність людей ефективно взаємодіяти з системами штучного інтелекту за допомогою вербального, контекстуального спілкування дозволить вченим впровадити технологію в об'єкти навколо нас, незалежно від того, чи є у них екран чи ні.

Головний вчений IBM Watson Грейді Буч уявляв штучний інтелект і когнітивну силу в аватарці, об'єкті у вашій руці, роботі або навіть в стінах операційної, конференц-залу або космічного корабля. Якби ми були психологами і хотіли визначити, хто знаходиться в кімнаті, хто дивиться на кого, хто знаходиться в клітці один з одним або розмовляє один з одним, у нас був би в стінах когнітивний асистент.

Кемпбелл з IBM погоджувався, що системи штучного інтелекту, які розробляються, матимуть сильні та слабкі сторони. І у людей є сильні і слабкі сторони. Таким чином, потрібно способувати змусити людей і комп'ютери добре працювати разом.

Аналіз штучного інтелекту як гаранта повної безпеки даних в майбутньому

У все більш оцифрованому світі кібератаки зростають в обсязі, стаючи все більш складними. Оскільки все більше компаній використовують Інтернет для власних цілей, кіберзлочинці шукають способи проникнути у ваші захисні системи. Завдяки ШІ, машинному навчанню та розвідуванню кіберзагроз, підприємства можуть реагувати на загрози з підвищеною впевненістю та більшою швидкістю. Використання штучного інтелекту може допомогти розширити горизонти існуючих рішень в області кібербезпеки і прокласти шлях до створення нових. У міру того як мережі стають все більші і складніші, штучний інтелект може стати величезним благом для кіберзахисту організацій. Простіше кажучи, зростаюча складність мереж виходить за рамки того, з чим люди здатні впоратися самостійно.

Також штучний інтелект може вчитися і адаптуватися через досвід. В даний час Машинне навчання дозволяє машинам навчати самих себе. Це означає, що вони можуть створювати моделі для розпізнавання образів, а не покладатися на людей, щоб побудувати їх.

Штучний інтелект навчений споживати велику кількість даних, як блоги і новинні сюжети, що дає зрозуміти – він краще розуміє загрози кібербезпеки. Звідси, штучний інтелект в кібербезпеці використовує дані для виявлення загроз (дивні файли, підозрілі адреси тощо), перш ніж почати відповідь на законну загрозу.

Як уже згадувалося раніше, штучний інтелект і машинне навчання знижують ризик людської помилки. Люди можуть втомлюватися і відчувати нудьгу при виконанні монотонного завдання. Команди кібербезпеки намагаються працювати під вагою всіх даних, необхідних для оцінки ризиків, але ШІ може швидко розпізнати всі загрозливі фактори. Однак штучний інтелект і людський інтелект повинні працювати разом. Крім того, людські експерти забезпечують здоровий глузд, якого немає у машин, і все ж краще справляються з рішенням, які дії зробити.

Ми можемо подолати багато ризикованих ситуацій, розробивши робота з штучним інтелектом, який, у свою чергу, може робити ризиковані речі для нас. Нехай він відправляється на Марс, знешкоджує бомбу, досліджує найглибші частини океанів, видобуває вугілля і нафту, його можна ефективно використовувати в будь-яких природних або техногенних катастрофах.

Переваги, описані вище, є лише малою частиною потенціалу ШІ в наданні допомоги кібербезпеки, але є і обмеження, які заважають машині стати основним інструментом, використовуваним в цій галузі. Для того, щоб побудувати і підтримувати систему

штучного інтелекту, компаніям буде потрібно величезна кількість ресурсів, включаючи пам'ять, дані і обчислювальну потужність. Крім того, оскільки системи штучного інтелекту навчаються за допомогою навчальних наборів даних, фірмам з кібербезпеки необхідно отримати в свої руки безліч різних наборів даних про шкідливі коди, нешкідливі коди і аномаліях. Отримання всіх цих точних наборів даних може зайняти дуже багато часу та ресурсів, які деякі компанії не можуть собі дозволити.

Штучний інтелект надає дивовижні можливості для задоволення самих спеціалізованих потреб клієнтів і створення абсолютно нових бізнес-моделей. Вона має здатність вирішувати деякі з найбільш гострих соціальних проблем. Але, оскільки рішення на основі штучного інтелекту починають мати все більший вплив на людське життя, виникають етичні питання про те, як технологія впливає на суспільство. Як ми можемо гарантувати, що ШІ ставиться до всіх справедливо, і в якій мірі організація несе відповідальність за захист конфіденційності?

Однак системи штучного інтелекту розроблені людьми і вони будуть ідеальними настільки, наскільки в них надходять дані. Навіть коли один алгоритм створює інший, початковий алгоритм був створений людьми і тому схильний до людських упереджень. Інсайт або передбачення не є більш чесним просто тому, що його згенерував бот.

На думку Тімніта Гебру, наукового співробітника команди етичного штучного інтелекту в Google, нам ще багато чого належить зробити, щоб навчити моделей міркувати розсудливо. Їх можна навчити тільки знаходити закономірності в історичних даних. Проблема полягає в тому, що ці навчальні дані не є нейтральними — вони можуть легко відображати упередження людей, які їх зібрали. Це означає, що він може кодувати тенденції та моделі, які відображають і увічнюють забобони та шкідливі стереотипи.

Оскільки вище ми описували в основному переваги систем ШІ, хочемо окремо виділити їх конкретні недоліки:

1.Моделі машинного навчання часто навчаються за даними з потенційно недостовірних джерел, включаючи інформацію про натовп, дані соціальних медіа та створені користувачем дані, такі як рейтинг задоволеності клієнтів, історія покупок або веб-трафік. Супротивники можуть впроваджувати на задньому плані або «троянців» у моделі машинного навчання шляхом отруєння навчальними наборами зі шкідливими зразками.

2.У традиційній системі компрометація впровадження бекдор означає створення секретного способу доступу до системи, не будучи авторизованим користувачем. Зазвичай це проявляється у формі програміста, який вручну кодує бекдор в систему, яку вони будують, або хакера, що впроваджує фрагмент коду, який відкриває систему для доступу з іншого засобу. Може бути дивним дізнатися, що такі чорні ходи можуть бути імплантовані в глибокі нейронні мережі для досягнення бажаних результатів від небажаних або спеціальних вхідних даних.

3.Можливість атак, які не потребують зміни моделі чи тренувальних даних, що дозволяє зовнішнім зловмисникам використовувати цей підхід. Це суперечлива атака. Візьміть два зображення нижче, візуально для людського ока вони виглядають як однакові зображення червоної лисиці. Перше зображення дійсно є незмінним зображенням червоної лисиці, однак друге зображення було змінено нейронною мережею атакуючих нападів таким чином, що класифікуюча нейронна мережа здатна класифікувати це зображення майже досконалою мірою точності, як Дональд Трамп. Природно, це створює проблему для Дональда Трампа (і перевага для спільноти лисиць), якщо системи безпеки Білого дому для розпізнавання обличчя покладаються на DCNN (рис. 2), (рис. 3).

Рис. 2. Оригінальне зображення лисиці, проаналізоване ШІ

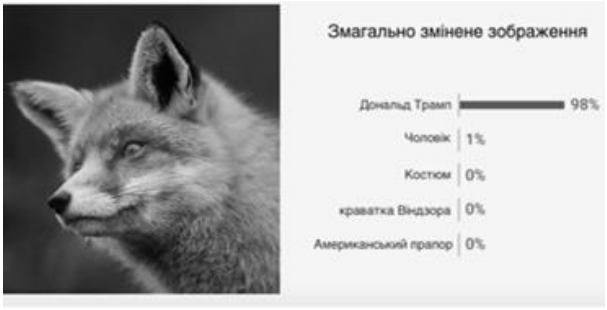

Рис. 3. Змінене зображення лисиці, проаналізоване ШІ

4.Навіть якщо припустити, що набір даних без спотворень і високоточна модель, цей успіх супроводжується дуже важливим застереженням: моделі, «засвоєні» сучасними моделями машинного навчання, є відносно крихкими. В результаті модель працює тільки з даними, які за своєю природою є такими самими, використовуваним в процесі навчання. Якщо використовувати дані, які навіть трохи відрізняються за своїм характером від типів змін, які він бачив у вихідному наборі даних, модель може повністю потерпіти невдачу. Це серйозне обмеження, яке можуть використовувати зловмисники: вводячи штучні зміни, такі як шматочок стрічки або інші відхиляються шаблони, зловмисник може порушити модель і контролювати її поведінку на основі введеного штучного шаблону.

5.Іншим викликом є той факт, що роботу деяких систем ШІ неможливо пояснити повністю. Припускають, що ця відсутність пояснень може підвищити сприйняття ризику та обмежити використання ШІ для деяких застосувань, наприклад, у критично важливих для безпеки умовах та з високою регламентацією.

Такі деякі переваги і недоліки штучного інтелекту. Кожен новий винахід або прорив буде мати і те, і інше, але ми, люди, повинні піклуватися про це і використовувати позитивні сторони винаходу для створення кращого світу. Штучний інтелект володіє

величезними потенційними перевагами. Ключ для людей буде гарантувати, що" повстання роботів " не вийде з-під контролю. Деякі люди також кажуть, що штучний інтелект може знищити людську цивілізацію, якщо він потрапить в чужі руки. Але все ж жодне з додатків штучного інтелекту, створених в такому масштабі, не може знищити або поневолити людство.

Що ж, давайте порівняємо людину і штучний інтелект, коли справа доходить до обробки інформації. Один повний аналіз безпеки, який читає машина, в середньому становить лише 10 слів, прочитаних людиною (рис. 4).

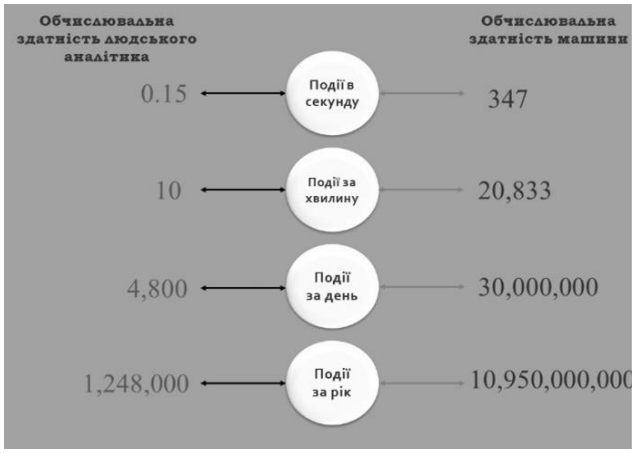

Рис. 4. Обробка даних людини та машини

Навіть найменша затримка може означати різницю між атакою і дією (рис. 5).

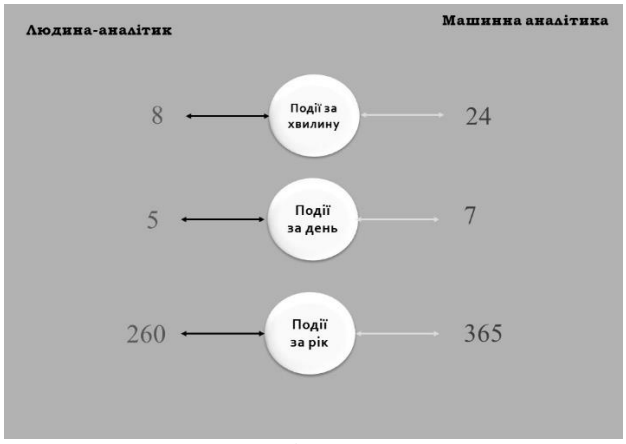

Рис. 5. Атака і дія

Бути аналітиком з кібербезпеки у великій компанії сьогодні - все одно що шукати голку в стозі сіна, якби цей стіг мчав до вас зі швидкістю оптоволокна. У кібербезпеки недостатньо часу; це не може зайняти години або навіть дні, щоб зрозуміти, чому відбувається атака. Ось чому отримання аналітиком можливості створювати і налаштовувати моделі машинного навчання є найбільш важливим аспектом системи. Розмах і масштаб сьогоднішніх загроз кібербезпеки-це нова норма. На щастя, наявні в даний час інструменти, такі як штучний інтелект і машинне навчання, все більшою мірою здатні впоратися з цим завданням. Щоб успішно використовувати нові, передові технології для боротьби з сьогоднішнім постійно мінливим ландшафтом загроз, взаємодія людини і машини-це те, над чим ми повинні працювати.

Висновок

Штучний інтелект дозволяє машинам вчитися на досвіді, пристосовуватися до нових вхідних даних і виконувати людські завдання. Більшість прикладів штучного інтелекту, про які ви чуєте сьогодні – від комп'ютерів, що грають в шахи, до самокерованих автомобілів - значною мірою залежать від глибокого навчання та обробки мови. Використовуючи ці технології, комп'ютери можуть бути навчені виконувати певні завдання, обробляючи великі обсяги даних і розпізнаючи закономірності в даних. Штучний інтелект збирається змінити кожну галузь, але ми повинні зрозуміти його межі. Принципове обмеження ШІ полягає в тому, що він навчається на основі отриманих даних. Немає іншого способу, за допомогою якого можна було б інкорпорувати знання. Це означає, що будь-які неточності в даних будуть відображені в результатах. І будь-які додаткові шари прогнозу або аналізу повинні бути додані окремо.

Сучасні системи штучного інтелекту навчені виконувати чітко визначені завдання. Система, яка грає в покер, не може грати в пасьянс або шахи. Система, яка виявляє шахрайство, не може керувати автомобілем або давати вам юридичні консультації. Насправді, система штучного інтелекту, яка виявляє шахрайство в сфері охорони здоров'я, не може точно виявити податкове шахрайство. Іншими словами, ці системи дуже і дуже спеціалізовані. Вони зосереджені на одному завданні і поводяться далеко не так, як люди. Аналогічним чином, самонавчальні системи не є автономними системами. Уявні технології штучного інтелекту, які ми бачимо в кіно і телебаченні, все ще є науковою фантастикою. Але комп'ютери, які можуть досліджувати складні дані для вивчення та вдосконалення конкретних завдань, стають досить поширеними.

Література

[1]. *Сучасний стан та перспективи розвитку робототехніки в Україні*. [Електронний ресурс]. Режим доступу: http://oldconf.neasmo.org.ua/node/2298.

[2]. *Як прогресує штучний інтелект: звіт про останні досягнення*. [Електронний ресурс]. Режим доступу: https://www.epravda.com.ua/publications/2019/07/15/649648/.

[3]. *10 прикладів, як штучний інтелект може змінити ваш спосіб життя*. [Електронний ресурс]. Режим доступу: https://www.radiosvoboda.org/a/29015231.html.

[4]. *Найбільші кібератаки проти України з 2014 року. Інфографіка*. [Електронний ресурс]. Режим доступу: https:// nv. ua/ ukr/ ukraine/ events/ najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

[5]. *Апокаліпсис у мережі. 7 найбільших хакерських атак в історії.* [Електронний ресурс]. Режим доступу: https://nv.ua/ukr/techno/gadgets/apokalipsis-v-merezhi-7-najbilshih-hakerskih-atak-v-istoriji-1393066.html.

[6]. *Десять найстрашніших техногенних катастроф, які увійшли в історію людства*. [Електронний ресурс]. Режим доступу: https://khm.depo.ua/ukr/khm/ desyat – naystrashnishih – tehnogennih - katastrof-v-istoriyi-lyudstva-10022016200100.

[7]. *Чорнобильська атомна електростанція*. [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/Чернобыльская_АЭС.

[8]. *Home Depot: Вследствие взлома в сентябре были похищены 53 миллиона адресов электронной почты*. [Електронний ресурс]. Режим доступу: https://www.securitylab.ru/news/461601.php.

[9]. *Причини та масштаби аварії.* [Електронний ресурс]. Режим доступу: https://chnpp.gov.ua/ua/uk/component/content/article/42-about/accident-of-1986/175-2012-02-01-08-01-38529.

[10]. *A look at the positive side of AI and drones*. [Електронний ресурс]. Режим доступу: https://borgenproject.org/a-look-at-the-positive-side-of-ai-and-drones/.

[11]. *Positive & Negative Effects of Artificial Intelligence*. [Електронний ресурс]. Режим доступу: https:// www.koganpage.com/ article/ positive-negative-effects-of-artificial-intelligence.

[12]. *Advantages of Artificial Intelligence*. [Електронний ресурс]. Режим доступу: https://www.educba.com/advantages-of-artificial-intelligence/.

[13]. *Benefits & risks of artificial intelligence*. [Електронний ресурс]. Режим доступу: https://futureoflife.org/ background/benefits-risks-of-artificial-intelligence/.

[14]. *What is the future of artificial intelligence?* [Електронний ресурс]. Режим доступу: https://www.quora.com/What-is-the-future-of-artificial-intelligence-1.

[15]. *Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop.* [Електронний ресурс]. Режим доступу: https://www.nap.edu/read/25488/chapter/6.

[16]. *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It*. [Електронний ресурс]. Режим доступу: https://www.belfercenter.org/publication/AttackingAI.

[17]. I. Nicolae, M. Sinn, *The Adversarial Robustness Toolbox v0.3.0: Closing the Backdoor in AI Security*. [Електронний ресурс]. Режим доступу: https://www.ibm.com/blogs/research/2018/08/art-v030-backdoor/.

[18]. J. Aungiers, *AI security neural network backdoors.* [Електронний ресурс]. Режим доступу: https://www.altumintelligence.com / articles / a / AI-Security-Neural-Network-Backdoors.

УДК 654.071

Опирский И.Р., Головчак Р.В., Мойсийчук И.Р. Перспективы развития искусственного интеллекта в контексте информационной безопасности

Аннотация. *Искусственный интеллект - концепция, согласно которой машины способны осуществлять некоторую интеллектуальную деятельность, которая присуща людям или животным. Другими словами, можно сказать, что это понятие включает в себя любое устройство, обладающий способностью воспринимать его окружения и предпринимать действия, увеличивающие шанс на успешное достижение целей. Однако, несмотря на продолжающийся прогресс в скорости компьютерной обработки и объеме памяти, до сих пор нет программ, которые могли бы сравниться с человеческой гибкостью в более широких областях или в задачах, требующих больших повседневных знаний. С другой стороны, некоторые программы достигли уровня производительности человеческих экспертов и профессионалов в выполнении определенных конкретных задач, так что искусственный интеллект в этом ограниченном смысле можно найти в таких разнообразных приложениях, как медицинская диагностика, компьютерные поисковые системы и распознавания голоса или почерка. Целью данной работы является, собственно, определение положительных и отрицательных аспектов применения систем искусственного интеллекта в области безопасности информации. Определено, что такие системы имеют весомую роль в текущем и последующем обеспечении безопасности данных, а также приведен ряд недостатков таких систем для будущего их учета. В статье были рассмотрены то, что искусственный интеллект был разработан путем изучения того, как человеческий мозг думает, учится и принимает решение, а затем применяет эти биологические механизмы к компьютерам. В отличие от классических вычислений, где кодеры обеспечивают точные входы, выходы и логику, искусственный интеллект основан на предоставлении машине входных данных и желаемого результата, позволяя машине развивать свой собственный путь для достижения поставленной цели. Искусственный интеллект - это технология, которая превращает все сферы жизни. Это широкий инструмент, который позволяет людям переосмыслить, как мы интегрируем информацию, анализируем данные и используем полученные результаты для улучшения процесса принятия решений. Они меняют способ, которым мы ищем информацию, как мы общаемся друг с другом, даже если мы ведем себя. Эта трансформация касается многих областей, включая образование. Основной целью данной статьи является обзор решения проблем с помощью искусственных технологий. В представленном обзоре литературы мы рассмотрели четыре категории: индивидуальный образовательный контент, инновационные методы обучения, технология расширенной оценки, коммуникация между студентом и преподавателем. Рассмотрев публикации на эту тему, мы представляем здесь возможную картину того, как искусственный интеллект изменит ландшафт образования. Начиная с краткой истории искусственного интеллекта, в данной статье представлен общий обзор этой технологии.*

Ключевые слова: *искусственный интеллект, машинное обучение, безопасность информации, системы машинного обучения, человек.*

Opirskyy I., Holovchak R., Moysiychuk I. Prospects of development of artificial intelligence in the context of information security

Abstract. *Artificial intelligence is a concept in which machines are capable of performing some intellectual activity that is inherent in humans or animals. In other words, this concept includes any device that has the ability to perceive its environment and take actions that increase the chance of successfully achieving goals. However, despite ongoing progress in computer processing speed and memory, there are still no programs that can match human flexibility in broader areas or in tasks that require extensive daily knowledge. On the other hand, some programs have reached the level of productivity of human experts and professionals in performing certain specific tasks, so that artificial intelligence in this limited sense can be found in such*

diverse applications as medical diagnostics, computer search engines and voice or handwriting recognition. The purpose of this work is, in fact, to determine the positive and negative aspects of the use of artificial intelligence systems in the field of information security. It is determined that such systems have an important role in the current and future data security, as well as a number of shortcomings of such systems for their future consideration. The paper discusses that artificial intelligence was developed by studying how the human brain thinks, learns, and makes decisions, and then applies these biological mechanisms to computers. Unlike classical computing, where encoders provide accurate inputs, outputs, and logic, artificial intelligence is based on giving the machine input and the desired result, allowing the machine to develop its own path to achieve its goal. Artificial intelligence is a technology that transforms all spheres of life. It is a broad tool that allows people to rethink how we integrate information, analyze data, and use the results to improve decision-making. They change the way we look for information, how we communicate with each other, even how we behave. This transformation affects many areas, including education. The main purpose of this article is to review the solution of problems using artificial technologies. In the presented literature review, we considered four categories: individual educational content, innovative teaching methods, advanced assessment technology, communication between student and teacher. Having considered publications on this topic, we present here a possible picture of how artificial intelligence will change the landscape of education. Starting with a brief history of artificial intelligence, this article provides an overview of this technology.
Keywords: *artificial intelligence, machine learning, information security, machine learning systems, humans.*

Опірський Іван Романович, д.т.н., доц., професор кафедри захисту інформації Національного університету «Львівська політехніка».
Опирский Иван Романович, д.т.н., доц., профессор кафедры защиты информации Национального университета «Львовская политехника».
Opirskyy Ivan, Doctor of Technical Sciences, Associate Professor, Professor of the Department of Information Protection of the National University "Lviv Polytechnic".

Головчак Романа Василівна, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Головчак Романа Васильевна, студент кафедры защиты информации Национального университета «Львовская политехника».
Holovchak Romana, student of the Department of Information Protection of the National University "Lviv Polytechnic".

Мойсійчук Ірина Русланівна, студент кафедри захисту інформації Національного університету «Львівська політехніка».
Мойсийчук Ирина Руслановна, студент кафедры защиты информации Национального университета «Львовская политехника».
Moysiychuk Iryna, student of the Department of Information Protection of the National University "Lviv Polytechnic".

Отримано *13 червня 2020 року*, затверджено редколегією *11 липня 2020 року*