Навчальна дисципліна:
ШТУЧНИЙ ІНТЕЛЕКТ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ
(КБМ-22-1) (магістри 1 рік)

2 семестр
Лекцій -16 (по 2 год.).
Лабораторних -8 (по 4 год.).

Заняття	**Л-1**	**Л-2**	**Л-3**	**Л-4**	**Л-5**	**Л-6**
Бали	**2**	**2**	**2**	**2**	**2**	**2**
Заняття	**Л-7**	**Л-8**	**Л-9**	**Л-10**	**Л-11**	**Л-12**
Бали	**2**	**2**	**2**	**2**	**2**	**2**
Заняття	**Л-13**	**Л-14**	**Л-15**	**Л-16**	**ЛР-1**	**ЛР-2**
Бали	**2**	**2**	**2**	**2**	**8**	**8**
Заняття	**ЛР-3**	**ЛР-4**	**ЛР-5**	**ЛР-6**	**ЛР-7**	**ЛР-8**
Бали	**8**	**8**	**9**	**9**	**9**	**9**

Бали ЛР = 68, Л = 32

Бали за лекцію нараховуються після відповіді на тест по лекції. Тест проводиться по 4 лекціях. З кожного тесту знімається по 1 балу за лекцію за несвоєчасність здачі.

З ЛР знімаються по 1 балу за кожен тиждень несвоєчасної здачі звіту (Своєчасна здача звітів - 2 тижні з дня проведення ЛР).

Додаткові бали можна отримати за:
Тези доповідей (опубліковані) – 5 б.
Наукова стаття по дисципліні – 10 б.
Індивідуальне завдання (оформлене наукове дослідження) – 10 б.
Участь в олімпіаді чи конкурсі студентських робіт – 10 б. (призове місце - 15 б.)

ЛЕКЦІЯ 1
з навчальної дисципліни «ШТУЧНИЙ ІНТЕЛЕКТ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ»
Тема: Застосування штучного інтелекту в задачах кібербезпеки

Питання лекції

Вступ
1. Історія розвитку штучного інтелекту
2. Напрямки досліджень в галузі штучного інтелекту
3. Напрямки застосування ШІ в кібербезпеці
4. Недоліки і проблеми сучасного штучного інтелекту
Висновки

ЛІТЕРАТУРА

https://safe.cnews.ru/articles/2020-06-01_pochemu_iskusstvennyj_intellekt_vse

https://www.kaspersky.ru/resource-center/definitions/ai-cybersecurity

Вступ

Кількість атак на інформаційні системи зростає щороку двозначними темпами. При цьому атаки стають все витонченішими, потенційних цілей, в число яких тепер входять пристрої інтернету речей і розумні домашні пристрої, - все більше, а збиток від атак - все вище. «Класичні» засоби антивірусної боротьби вже не здатні впоратися з такими епідеміями, і на допомогу приходять рішення на базі штучного інтелекту.

Одночасно з ростом кількості атак і шкоди від них, ростуть і витрати на кібербезпеку. За оцінкою Gartner, витрати на системи інформаційної безпеки (ІБ) і управління ризиками в 2020 році досягали $ 131 млрд, а у 2022-му - збільшаться до $ 174 млрд, з них приблизно $ 50 млрд будуть спрямовані на захист клієнтських систем. Продажі хмарних платформ і додатків для забезпечення безпеки виростуть з $ 636 млн в 2020 р до $ 1,63 млрд в 2023-м, а систем забезпечення безпеки додатків за цей же період - з $ 3,4 млрд до $ 4,5 млрд. Зростає і ринок послуг в області ІБ, за останній рік він збільшився з $ 62 млрд до $ 66,9 млрд.

Однак самі по собі гроші все питання вирішити не можуть. Більшість фахівців з інформаційної безпеки сьогодні перевантажені аналізом журналів, запобіганням спроб злому, розслідуванням можливих випадків шахрайства і т.д. Дефіцит кадрів великий, задачі занадто складні, тому в ІБ-індустрії все з більшою надією дивляться на рішення в області штучного інтелекту.

За оцінкою MarketsandMarkets, 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.

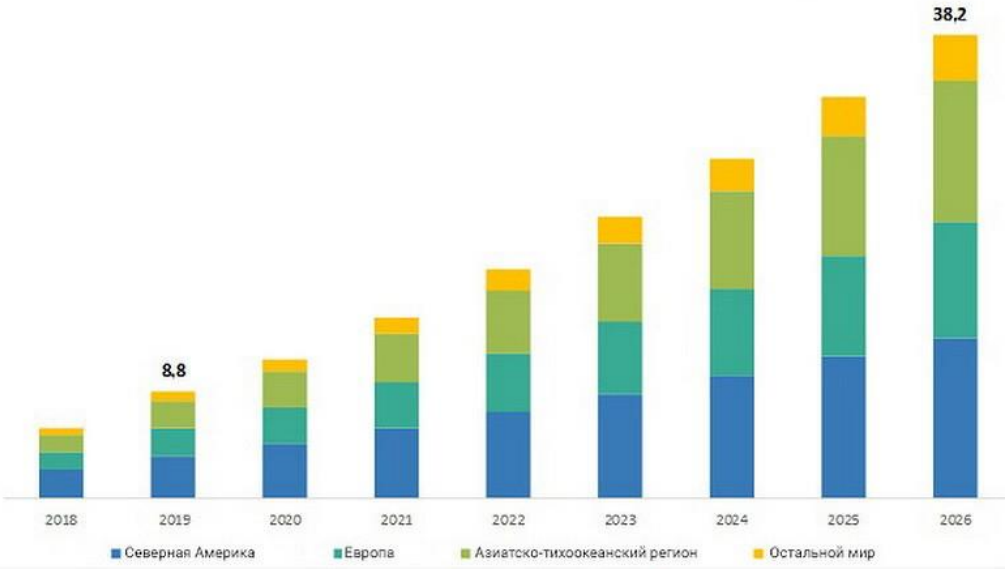


Рис.1. Динаміка ринку засобів ШІ для кібербезпеки по регіонах, $ млрд.
Джерело: MarketsandMarkets, 2019

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.

Передбачається, що штучний інтелект звільнить фахівців від рутинних завдань, взявши на себе більшу частину рутинних процедур. Так, наприклад, ШІ-рішення можуть аналізувати події в сфері безпеки, виявляти відхилення в роботі програм і пристроїв від «норми», і сповіщати про це співробітників служби ІБ.

Інше поле діяльності ШІ - контроль поведінки співробітників, детектування дивацтв в їх поведінці (запит непотрібних по роботі даних, або потрібних - але в незвичайно великих обсягах і т.д.). Особливу увагу правильно навчена система буде приділяти критично важливим корпоративним ресурсам і власникам привілейованих облікових записів - за остаточною оцінкою Forrester Research,

80% порушень в даний час викликані скомпрометованими привілейованими обліковими даними. Так що, як вважають в Gartner, вже в 2021 р засоби PAM (Privileged Access Management, управління доступом привілейованих користувачів) будуть використовувати три чверті великих підприємств (в 2018 р такі кошти застосовували близько половини компаній).

Ступінь зацікавленості служб ІБ в штучному інтелекті змінюється від країни до країни, а також залежить від галузі. На початку року консалтингова компанія Capgemini опублікувала результати дослідження про стан в області кібербезпеки. Компанією було опитано 850 керівників вищої ланки з 10 країн (Австралії, Великобританії, Німеччини, Індії, Італії, Іспанії, Нідерландів, США, Франції, Швеції), 20% респондентів займали пост IT-директора, 10% - керівника служби IT-безпеки. Компанії представляли сім сфер діяльності - виробництво споживчих товарів, ритейл, банківський сектор, страхування, автомобілебудування, ЖКГ та телеком.

Картина виявилася невеселою. Більше половини (56%) відзначили, що їх ІБ-аналітики перевантажені, тому в майже чверті (23%) компаній розслідуються не всі виявлені інциденти, а, значить, не вживаються заходи для запобігання аналогічних атак в майбутньому. 42% відзначили зростання кількості атак на «чутливі до часу» додатка, до таких належать, наприклад, ПЗ для управління транспортом, зростання такого роду інцидентів склало 16%.

Не дивно, що 69% опитаних вважають, що для ефективного реагування на кібератаки *необхідні засоби штучного інтелекту*. Ця цифра - середня по всіх галузях, скажімо серед керівників телекомунікаційних компаній такої думки дотримуються 80%, а в ЖКГ вона менше 60%.

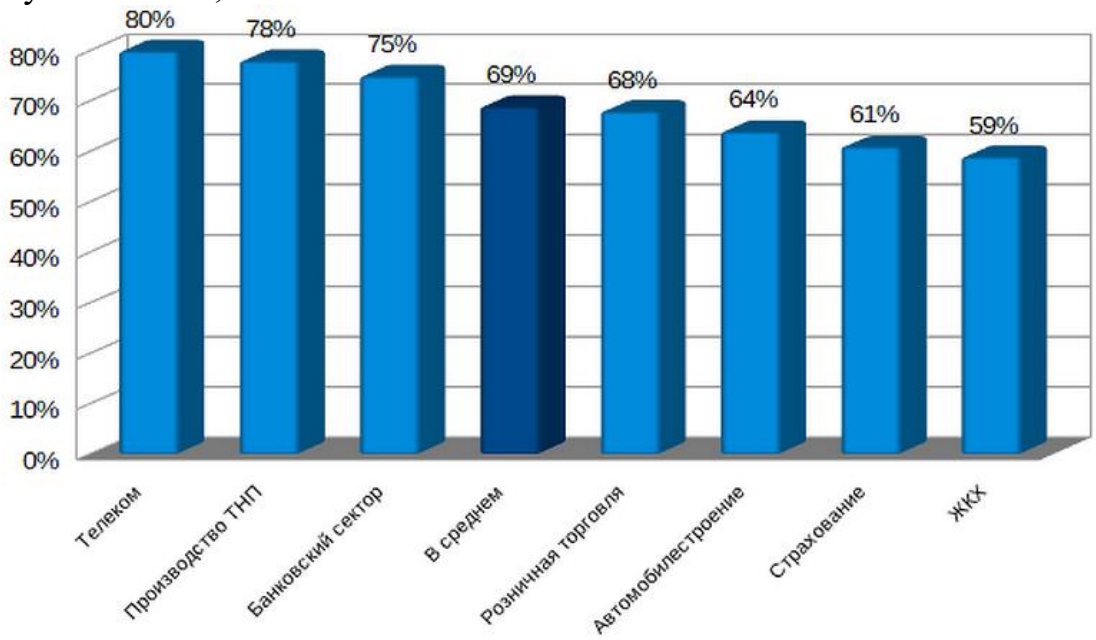
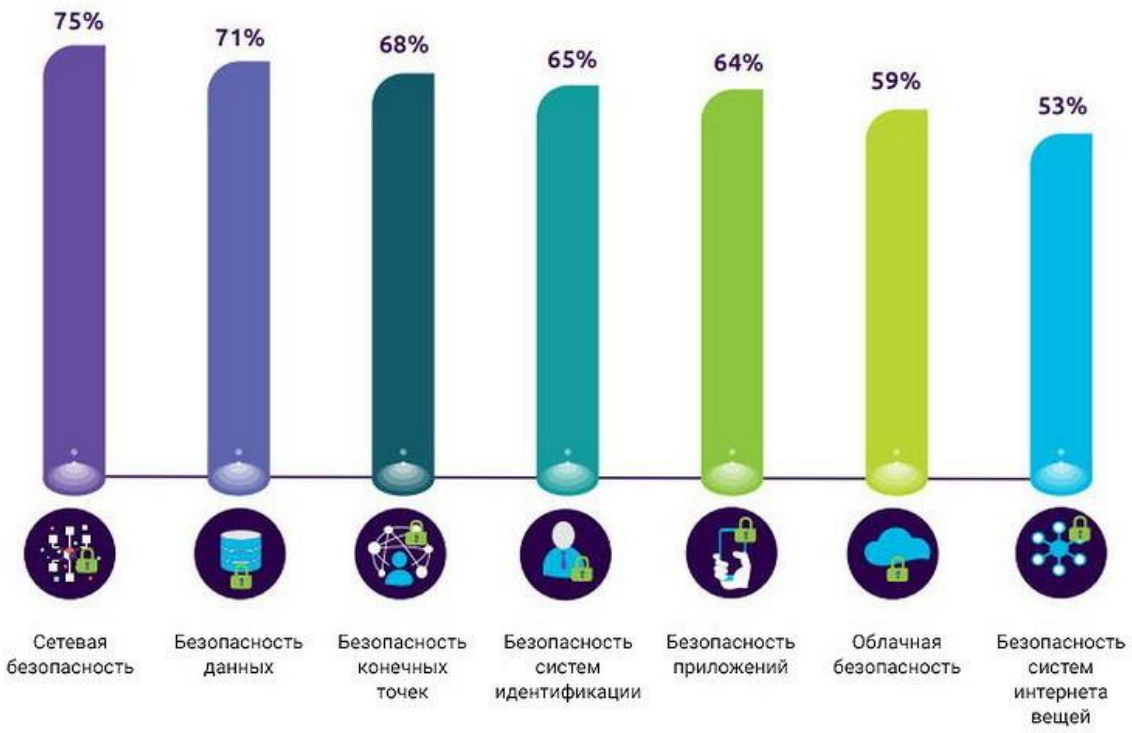


Рис. 2. Частка організацій, які вважають, що без коштів ШІ вони не зможуть боротися з кібератаками, по галузях. Джерело: Capgemini, 2020

За оцінкою Capgemini, якщо до 2019 г. майже кожна п'ята організація використовувала штучний інтелект для поліпшення кібербезпеки, то з 2020 року таких організацій вже понад 60%. Майже половина опитаних (48%) заявила, що бюджети на ШІ-рішення в області кібербезпеки збільшаться з 2020 фінансового року в середньому на 29%.

Втім, обсяги вкладень будуть досить сильно змінюватися від країни до країни. Якщо в США 83% респондентів вважають, що вони не впораються з кібератаками без залучення коштів ШІ, то в Швеції - всього лише 54%.



Рівень використання коштів ШІ для захисту IT-інфраструктури. Джерело: Capgemini, 2020

Пріоритетні варіанти використання ШІ для підвищення рівня кібербезпеки - забезпечення безпеки мережі і захист даних. Рішення інтернету речей поки відстають, але і з'явилися вони лише в останні роки.

Зрозуміло, можливості штучного інтелекту використовують або готуються використовувати не тільки співробітники служб інформаційної безпеки, але і їхні опоненти - зловмисники з хакерських структур.

ШІ в руках хакерів, так само, як і на службі відділів ІБ, може взяти на себе різноманітну «рутину», наприклад - розсилку фішингових листів, аналіз захисних механізмів корпоративних систем і пошук їх слабких місць. За рахунок можливостей ШІ-систем до навчання вони можуть бути ефективно використані також для здійснення цільових атак на конкретних людей, зазвичай - високопоставлених (цей вид фішингу називається whaling (полювання на китів).

Наприклад, в IBM Research створили хакерський інструмент DeePLocker, в якому за допомогою ШІ «сховали» вірус-шифрувальник WannaCry всередині

програми відеоконференцзв'язку. Програма працює нормально, поки не потрапляє на комп'ютер до наміченої жертви, яку ідентифікує за допомогою засобів розпізнавання особи, голосу, деяких інших додаткових чинників. Після чого запускається вірус, який доти нічим себе не виявляв, і тому не піддавався упізнання антивірусними засобами.

А дослідники Нью-Йоркського університету створили нейромережу DeepMasterPrints, здатну підробляти відбитки пальців - в ході тестування спрацювали 23% створених нею відбитків.

Споконвічне змагання «щита і меча» в плані використання штучного інтелекту для захисту від кібератак і для посилення їх потужності, вже йде і його інтенсивність буде швидко наростати. Від того, хто більше досягне успіху в цій гонці, багато в чому залежить безпека IT-систем вже в найближчі роки.

Таким чином, рішення ШІ вже застосовуються в кібербезпеці, а в подальшому будуть застосовуватись ще більше!

Спробуємо розібратися що ж таке ШІ.

Загалом поняття "штучний інтелект" є *досить розмитим*. Практично вся сучасна техніка обладнується мікрочіпами, а виробники переконують споживачів про наявність ШІ в їх виробах. Але, в більшості це є просте копіювання людиноподібної лінії поведінки на штучно створеному об'єкті для зменшення витрат і часу людини.

Базові поняття штучного інтелекту

Термін **інтелект** (*Intelligence*) походить від латинського поняття intellectus - розум, розум, розум.

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.

Діяльність мозку - це **мислення**. Інтелект і мислення пов'язані багатьма цілями і завданнями: розпізнавання ситуацій, логічний аналіз, планування поведінки. Характерними особливостями інтелекту є здатність до ***навчання, узагальнення, накопичення досвіду, адаптація до умов, що змінюються в процесі вирішення завдань***.

Виходячи з самого визначення ШІ випливає **основна проблема** у створенні інтелекту: ***можливість або неможливість моделювання мислення дорослої людини або дитини***.

1. Історія розвитку штучного інтелекту

Перші серйозні дослідження щодо створення ШІ були зроблені практично відразу після появи перших ЕОМ.

Народження науки про штучний інтелект. 1943 - 1956

Протягом цього періоду група вчених з широкого спектру областей науки почали обговорювати можливість створення штучного мозку.

Дослідження в нейрології показали, що мозок являє собою мережу з нейронів, які обмінюються між собою електричними сигналами за принципом «все або нічого», 0 або 1.

Кібернетика Норберта Вінера описала основи управління і стабільності в електричних мережах.

Теорія інформації Клода Шеннона описала цифрові сигнали.

Теорія обчислення Алана Т'юринга показала, що будь-які обчислення можуть бути виконані за допомогою цифрових операцій.

Уолтер Піттс і Уоррен Маккаллок проаналізували мережі, які складалися з ідеалізованих штучних нейронів і показали, як вони можуть виконувати найпростіші логічні функції. Вони були першими, хто описав те, що дослідники згодом назвуть нейронною мережею.

Одним із студентів, натхнених їх ідеями був Марвін Мінський, якому тоді було 24 роки. Згодом він став одним з найбільш помітних лідерів та інноваторів в області ШІ на наступні 50 років.

У 1951 було написано програми для гри в шашки і шахи, що стало віхою прогресу в ШІ на довгі роки.

Дартмутська конференція 1956

Дартмутський семінар - конференція з питань штучного інтелекту відбулася влітку 1956 року в Дартмутському коледжі протягом 2 місяців. Конференція мала важливе значення для науки: вона познайомила між собою людей, що цікавилися питаннями моделювання людського розуму, затвердила появу нової галузі науки і дала їй назву - «Artificial Intelligence» - «Штучний інтелект».

План конференції складено відповідно до тези, що «кожен аспект навчання або будь-якої іншої властивості інтелекту можна описати настільки детально, що може бути змодельований на комп'ютері».

Організаторами семінару були Джон Маккарті, Марвін Мінскі, Клод Шеннон і Натаніель Рочестер. Вони запросили всіх відомих американських дослідників, так чи інакше пов'язаних з питаннями теорії управління, теорії автоматів, нейронних мереж, теорії ігор і дослідженням інтелекту.

На семінарі були присутні 10 осіб:

Джон Маккарті, Дартмутський коледж
Марвін Мінскі, Гарвардський університет
Клод Шеннон, Bell Laboratories
Натаніель Рочестер, IBM

Артур Самюель, IBM
Аллен Ньюелл, Університет Карнегі - Меллон
Герберт Саймон, Університет Карнегі - Меллон
Тренчард Мур, Прінстонський університет
Рей Соломонів, Массачусетський технологічний інститут
Олівер Селфрідж, Массачусетський технологічний інститут

Метою конференції був розгляд питання: чи можна моделювати інтелектуальні процеси мислення і творчості за допомогою обчислювальних машин. Як ключові питання учасники виділили: розуміння мови, самонавчання і самовдосконалення комп'ютерів.

Десять вчених абсолютно серйозно припускали, що зможуть досягти істотних результатів з даних питань, якщо працюватимуть разом протягом двох місяців.

Золоті роки : 1956-1974

Роки після 1956 були ерою відкриттів, спринту по новій галузі. Програми, розроблені в цей час, для більшості людей здавалися просто приголомшливими, подібна «інтелектуальна» поведінка машин здавалася неймовірною. Дослідники проявляли небувалий оптимізм як в особистому спілкуванні, так і в публікаціях, пророкуючи, що повноцінна інтелектуальна машина буде створена менш ніж за 20 років. Урядові агентства, напр., ARPA (Advanced Research Projects Agency), вкладали значні кошти в розвиток цієї нової області.

Багато програм, створених в ті роки, використовували лабіринтний алгоритм. Для досягнення певної мети (виграш в грі або доказ теореми), вони рухалися до мети подібно до руху в лабіринті, повертаючись до точки розгалуження і вибираючи інший шлях, якщо цей виявився тупиковим.

Оптимізм

Перше покоління дослідників у галузі ШІ робило такі передбачення про свою роботу:

1958 - H. Simon, A. Newell : «протягом десяти років цифровий комп'ютер буде чемпіоном світу з шахів» і «протягом десяти років комп'ютер відкриє і доведе нову важливу математичну теорему»

1965 - H. Simon : «протягом 20 років машини будуть здатні виконувати будь-яку роботу, на яку здатна людина»

1967 - M. Мінскі : «протягом покоління проблема створення штучного інтелекту буде практично повністю вирішена»

1970 - M. Мінскі : «в інтервалі від 3 до 8 років ми будемо мати машину з інтелектом, порівнянним із середнім людським рівнем»

Фінансування

У 1963 MIT (Массачусетський Технологічний Університет), «AI Group», Minsky & McCarthy, отримали грант на $ 2.2 млн. від ARPA, яке продовжувало фінансування в розмірі $ 3 млн. в рік до 70-х. Такого ж масштабу фінансування задіяно стосовно «Stanford AI Project», John McCarthy та програми Newell та

Simon, Carnegie Mellon University. Ще одна лабораторія з дослідження ШІ була заснована в Единбурзькому Університеті в 1956. Ці чотири інститути стали основними центрами розробки і досліджень в області ШІ на довгі роки.

Перцептрони

Перцептроном було названо різновид нейронної мережі, що запропонована Френком Розенблатом в 1958 р. Як і більшість дослідників ШІ, він був оптимістично налаштований щодо потенційних можливостей перцептронів, пророкуючи, що «перцептрон може виявитися здатним навчатися, приймати рішення, перекладати з однієї мови на іншу».

Активна дослідницька програма в цій області була розпочата в 60-х роках, але вона була раптово перервана незабаром після публікації Мінські та Паперт в 1969 році книги «Перцептрони». В ній стверджувалося, що існують значні обмеження на можливості перцептронів, і що передбачення Розенблата були надмірним перебільшенням. Ефект від цієї книги був руйнівним - більш ніж на 10 років дослідження в цій області були практично повністю припинені.

Перша «зима» штучного інтелекту, 1974 - 1980 (The first AI Winter)

За проханням Британської ради з наукових досліджень відомий математик Сер Джеймс Лайтхіл підготував доповідь «Штучний інтелект: Загальний огляд», що опублікована в збірнику праць Симпозіуму з штучного інтелекту в 1973 році. Лайтхіл описав стан розробок у галузі штучного інтелекту і дав дуже песимістичні прогнози для основних напрямків цієї науки. В його доповіді рівень досягнень в галузі ШІ був визначений як розчаровуючий, а загальна оцінка була негативною з позицій практичної значущості.

У 70-х роках ШІ став предметом критики і зменшення фінансування. Дослідники ШІ не змогли адекватно оцінити складність проблем, з якими вони зіткнулися. Їх надмірний оптимізм породив неймовірно високий рівень надій і очікувань, і коли обіцяні результати не змогли матеріалізуватися, фінансування ШІ припинилося.

Водночас, напрям ШІ, що торкався нейронних мереж було повністю закрито на 10 років в результаті руйнівної критики перцептрона Марвіном Мінскі.

Незважаючи на труднощі (обмежена обчислювальна потужність, ефект «комбінаторного вибуху» в більшості алгоритмів, величезні обсяги даних, необхідних для обробки в задачах, пов'язаних з розпізнаванням мови і образів), з якими зіткнулися в 70-ті роки, було висловлено нові ідеї в областях логічного програмування, міркувань на основі «здорового глузду» і багато іншого.

Бум 1980 - 1987

У 80-х роках різновид ШІ - програм, що названі «експертні системи» було використано низкою великих корпорацій і стала мейнстримом в ШІ - дослідженнях. У 1980 експертна система XCON була закінчена в CMU для Digital

Equipment Corporation. Вона приносила компанії $ 40 мільярдів на рік до 1986 р. До 1985 вони виділяли мільярд $ в рік на дослідження ШІ.

Тоді ж японський уряд почав «агресивне» фінансування проекту по створенню ШІ на основі комп'ютера п'ятого покоління (див. Комп’ютер 5 покоління). Нажаль, проект не виправдав покладені на нього надії.

Іншою важливою подією стало відродження нейронних мереж в роботах Джона Хопфилда (мережі Хопфілда) і Девіда Румельхарта (Back Propagation - алгоритм зворотного поширення похибки).

Друга «зима» ШІ, 1987 - 1993 (The second AI winter)

Інтерес і участь бізнес-спільноти в дослідженнях ШІ (їх спонсоруванні) зазнала сплеск і спад згідно з класичною схемою економічного міхура. Ринок спеціалізованого «заліза» для ШІ в 1987 почав занепадати. Персональні комп'ютери від Apple і IBM неухильно нарощували швидкість і потужність і в 1987 стали більш продуктивними в порівнянні з більш спеціалізованими і дорогими комп'ютерами.

1993 - наші дні

Область дослідження, що пов'язана з ШІ, нарешті досягла деяких з своїх початкових цілей. Певні розробки зайняли свою нішу в технологічній індустрії. Частково успіх було досягнуто завдяки збільшеній обчислювальної потужності, частково завдяки фокусуванню на специфічних проблемах.

Але, мрія про інтелект, рівний людському, не здійснилася, тому, дослідники ШІ стали набагато більш обачними та обережними у своїх прогнозах і судженнях.

Сьогодні розробка систем ШІ відбувається інтенсивними темпами і над цією проблемою працюють найбільші світові інститути.

2. Напрямки досліджень в галузі штучного інтелекту

В дослідженнях у галузі штучного інтелекту склалося два головних напрямки: *біонічний і прагматичний*.

Біонічний напрямок досліджень в галузі штучного інтелекту засновано на припущенні про те, що якщо в штучній системі відтворити структури і процеси людського мозку, то й результати вирішення завдань такою системою будуть подібні до результатів, що отримує людина. В цьому напрямку досліджень виділяються:

Машинне навчання - це спрощена версія процесу навчання, яке відбувається з людиною. Як правило, в машинному навчанні наявний певний набір прикладів, спостережень, реакцій до цих спостережень. Задача полягає у тому, щоб сконструювати такі моделі, які будуть максимально ефективно описувати наявні дані і робити достовірні прогнози.

Нейромережні алгоритми. В його основі лежать системи елементів, які подібно до нейронів головного мозку здатні відтворювати деякі інтелектуальні функції. Прикладні системи, розроблені на основі цього підходу, називаються нейронними мережами.

Структурно-евристичний підхід. В його основі лежать знання про поведінку спостережуваного об'єкта або групи об'єктів і міркування про ті структури, які могли б забезпечити реалізацію спостережуваних форм поведінки. Прикладом подібних систем служать *мультиагентні системи*.

Еволюційні алгоритми. В цьому випадку можна вирішити завдання, що формулюється в термінах еволюціонуючої популяції організмів - сукупності підсистем, що протидіють і співпрацюють, в результаті функціонування яких забезпечується необхідна рівновага (стійкість) всієї системи в умовах постійно змінних впливів середовища. Такого роду підхід реалізовано в прикладних системах на основі *генетичних алгоритмів*.

Нечітка логіка. Найбільш вражаючим в людському інтелекті є здатність приймати правильні рішення в умовах неповної та нечіткої інформації. Побудова моделей наближених роздумів людини і використання їх в комп'ютерних системах представляє сьогодні одну з найважливіших проблем науки. "Штучний інтелект", який легко вирішує завдання управління складними технічними комплексами, часто є безпорадним в простих ситуаціях повсякденного життя. Для створення інтелектуальних систем, здатних адекватно взаємодіяти з людиною, потрібно застосовувати новий математичний апарат, який переводить неоднозначні життєві твердження в мову чітких і формальних математичних формул.

Прагматичний напрямок ґрунтується на припущенні про те, що розумова діяльність людини є «чорним ящиком». Але, якщо результат функціонування штучної системи збігається із результатом діяльності експерта, то таку систему можна визнати інтелектуальною незалежно від способів отримання цього результату. При такому підході не ставиться питання про адекватність використаних в комп'ютері структур і методів до тих структур чи методів, якими користується в аналогічних ситуаціях людина, а *розглядається лише кінцевий результат вирішення конкретних завдань*.

З точки зору кінцевого результату в прагматичному напрямку можна виділити три цільові області:

Розробка методів подання й обробки знань - є однією з основ сучасного періоду розвитку штучного інтелекту;

Інтелектуальне програмування - розбивається на кілька груп. До них відносять ігрові програми, природно-мовні програми (системи машинного

перекладу, автоматичного реферування, генерації текстів), розпізнавальні програми, програми створення творів живопису та графіки.

Створення інструментарію. Інструментарій - мови для систем штучного інтелекту; дедуктивні та індуктивні методи автоматичного синтезу програм; лінгвістичні процесори; системи аналізу та синтезу мови; бази знань; оболонки, прототипи систем; системи когнітивної графіки;

Спільним для перелічених програм є широке використання пошукових процедур і методів вирішення переборних завдань, пов'язаних з пошуком і переглядом великого числа варіантів. Ці методи застосовуються при машинному рішенні ігрових завдань, в задачах вибору рішень, при плануванні доцільної діяльності в інтелектуальних системах.

Суть реалізації ШІ в теорії і на практиці

Суть реалізації мислення досі до кінця не з'ясована і залишається таємницею для науки. Сьогодні комп'ютери переробляють здебільшого не саму інформацію, а лише вміст комірок пам'яті, які можна заповнити чим завгодно. Отже, комп'ютери не "*осмислюють*" зміст інформації на відміну від людей, для яких характерним є виключно осмислені поняття. Образно можна сказати, що в людей процес мислення відбувається в душі, в той час як для машин її не існує.

З яких компонентів зазвичай будується система штучного інтелекту, та й будь-якого інтелекту взагалі?

У першу чергу ШІ - це сукупність "*заліза*" та відповідного *програмного забезпечення*. В якості першого зазвичай виступає комп'ютер певної конфігурації і обслуговуючі механізми (маніпулятори, відеокамери, звукові та інші датчики). Більшою мірою на "*інтелектуальність*" машини в цілому впливає програмна начинка, яка визначає ступінь "просунутості" даного ШІ.

В електронній начинці ШІ **в першу чергу** присутня величезна кількість пам'яті, на основі якої і будуються всі міркування та висновки. Зрозуміло, що всі знання з різних областей в пам'ять ШІ закласти неможливо, але зробити інтелектуальну систему в певній галузі пізнання цілком можливо. Зазвичай, людина спочатку закладає в систему мінімальні пізнання про світ. Далі ці пізнання розширюються в процесі накопичення досвіду і вкладення його людиною (пасивний шлях) або самою системою (активний шлях) в результаті її адаптації до умов навколишнього середовища. Однак комп'ютерна пам'ять являє собою лише просту сукупність файлів і папок.

Пам'ять людини влаштовано набагато складніше - вона оперує не файлами, що є клаптиками інформації. **Людська пам'ять - це пам'ять образів.** Людську пам'ять можна порівняти з *кометою*: позаду - довгий "хвіст" життєвого досвіду, який з часом автоматично забувається і затирається новим; сама комета - це шар

реальної щосекундної пам'яті; тонкий передній шар - це туманні міркування (передбачення) людського майбутнього. І поки що пам'ять систем ШІ в корені відрізняється від людської.

В другу чергу сам логічний процес обчислення ситуації відбувається в пристрої обробки інформації. Найчастіше це певне програмне забезпечення та центральний процесор комп'ютера. Від можливостей цього центру обробки інформації безпосередньо залежить продуктивність і активність ШІ.

Найголовнішою відмінністю програмного забезпечення справжнього штучного інтелекту від простих додатків є в *можливість "мислити" образами.* За допомогою образного мислення сьогодні стали доступними такі технології, як стиснення і кодування інформації, обробка біометричних образів, оптимізація гами передачі кольору, подібний пошук, аналіз сенсу зображень, автоматична каталогізація інформації, алгоритми розпізнавання та класифікації образів.

Для людини прикладами образів можуть бути небо, хмари, музика, море, вірші тощо. Здатність сприйняття зовнішнього світу у формі образів дозволяє людям дізнаватися нескінченно велику кількість об'єктів і розуміти один одного незалежно від національної приналежності.

Процес сприйняття об'єкта як образа для машини має деякі особливості. Зазвичай, перед виділенням образу (наприклад, графічного) заздалегідь вважається відомим лише те, що потрібно розділити множину точок деякого простору на дві або більше областей, і що після поділу всі точки будуть належати до цих двох (або більше) областей. При цьому, заздалегідь відомо лише розташування точок вихідної області (їх приблизні координати). Далі, відбувається сам процес поділу точок на області (образи) за певними критеріями (для зображення це буде зміна кольорів і контрастів). Іноді потрібно обробити зображення так, щоб точки були більш явними для розділення (наприклад, перевести кольорове зображення в чорно-біле) - це зробить чутливість поділу вищою (так працює більшість програм для розпізнавання тексту).

Якщо система зможе самостійно класифікувати і фільтрувати не лише раніше відомі об'єкти, але і невідомі (не знаючи їх властивостей, за зовнішнім виглядом), то цей процес буде називатися самонавчанням. Сьогодні системи ШІ можуть розрізняти тільки нечисленні образи в невеликих заданих просторах.

Важливою особливістю ШІ має стати його **навчання** і над цією проблемою працюють численні вчені в усьому світі. Навчання, зазвичай, визначається як процес, в результаті якого система поступово набуває здатність відповідати потрібними реакціями на певні зовнішні впливи. Сьогодні існують прототипи обладнання, що здатні навчатися найпростішим механічним операціями (обробка деталей на верстаті, копіювання людської ходи). Дуже часто методи машинного навчання застосовують для рішень задач кібербезпеки.

Для вирішення тієї чи іншої задачі ШІ сьогодні необхідний алгоритм рішення (втім, як і будь-якій людині). **Алгоритм** - це точне розпорядження про виконання в певному порядку операцій для вирішення певної задачі. Знаходження алгоритму

для людини або машини пов'язано з тонкими і складними міркуваннями. Ці міркування часто вимагають винахідливості і творчого підходу, тому, машина постійно потребує взаємодії з людиною через брак вищевказаних якостей. Машині не властивий "метод тику" - вона лише шукає варіанти вирішення проблеми за допомогою прописаних в базі даних.

Важливу роль у функціонуванні ШІ виконують функції аналізу інформації та накопичення *життєвого досвіду*. Спостерігаючи за дітьми, ми переконуємося, що більшу частину знань вони отримують шляхом навчання і спілкування з навколишнім світом, а не ті, що закладені в них заздалегідь. Винахід *ефективного механізму самоаналізу* та самостійного накопичення життєвого досвіду поставить ШІ на значно вищий рівень порівняно з сучасним.

3. Напрямки застосування ШІ в кібербезпеці

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.

При пошуку нових способів застосування машинного навчання і штучного інтелекту в області кібербезпеки важливо окреслити *коло сучасних проблем в цій сфері*. Технології штучного інтелекту 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. Наприклад, навіть при наявності великої команди IT-фахівців правильне 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 усунення проблем, що виникають при заміні, модифікації і оновлення мережевих систем.

Уявімо, що поверх старого локального середовища необхідно встановити нову інтернет-інфраструктуру, наприклад систему хмарних обчислень. З метою безпеки корпоративних систем команді IT-фахівців необхідно забезпечити їх сумісність. Оцінка надійності конфігурації вручну може стати дуже трудомістким процесом, так як працівникам IT-служби доведеться поєднувати роботу з нескінченними оновленнями і повсякденні завдання. При наявності інтелектуальних адаптивних засобів автоматизації фахівці можуть оперативно отримувати поради щодо вирішення виявлених проблем. На основі таких засобів

можна навіть створити систему для автоматичної настройки необхідних параметрів.

Ефективність ручної праці при відтворенні повторюваних дій

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. Після початкової підготовки пристроїв IT-фахівцям часто доводиться знову повертатися до них, щоб виправити конфігурацію або оновити налаштування, які можна змінити віддалено.

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

Втома від сповіщень про загрози може стати ще однією проблемою для організацій, які не приймають заходи боротьби з нею. Чим складнішою стає багаторівнева побудова систем безпеки, тим більшою стає і поверхня атаки. Багато системи безпеки реагують на відомі проблеми потоком автоматичних повідомлень. В результаті для того, щоб знайти рішення і вжити заходів, IT-фахівцям доводиться аналізувати їх окремо.

Але через велику кількість вхідних сигналів цей процес стає дуже трудомістким. В результаті втома від прийняття рішень стає повсякденною проблемою для співробітників служб кібербезпеки. Ухвалення проактивних заходів щодо нейтралізації відомих загроз і вразливостей є оптимальним варіантом, однак багатьом командам не вистачає часу і співробітників, щоб тримати оборону на всіх напрямках.

Іноді командам доводиться зосередитися на найбільш гострій проблемі, а другорядні завдання відсунути на другий план. Використання ШІ для забезпечення кібербезпеки може допомогти IT-фахівцям ефективно справлятися з великою кількістю загроз. Протидію кожній з них можна значно спростити, якщо об'єднувати однотипні загрози разом за допомогою автоматичного маркування. Крім того, деякі проблеми може усунути сам алгоритм машинного навчання.

Час реагування на загрозу

Час реагування на загрозу - один з найважливіших показників ефективності служби кібербезпеки. Відомо, що атаки дуже швидко переходять від експлуатації уразливості до розгортання. Раніше, перш ніж почати атаку, зловмисникам доводилося вручну перевіряти всі вразливі місця і обхідними шляхами виводити з ладу системи безпеки - іноді цей процес міг займати тижні.

На жаль, технологічні інновації існують не тільки в області кіберзахисту. Зараз автоматизація кібератак стає все більш поширеним явищем. Такі загрози, як шифрувальники LockBit, що недавно з'явилися, значно скоротили час, необхідний для шкідливого вторгнення. Сьогодні деякі атаки успішно проводяться лише за півгодини.

Реакція людини може бути недостатньо швидкою, навіть якщо тип атаки добре відомий. Саме тому багато команд фахівців з безпеки частіше займаються усуненням наслідків успішних атак, ніж запобігають їх. Окрему небезпеку становлять невиявлені атаки.

Технології машинного навчання здатні витягувати дані про атаки, групувати їх і готувати для аналізу. Вони можуть надавати фахівцям з кібербезпеки звіти, щоб спростити обробку даних і прийняття рішень. Крім звітів, такий тип системи безпеки може також запропонувати рекомендовані дії для обмеження подальшого збитку і запобігання подальших атак.

Виявлення і прогнозування нових загроз

Виявлення і прогнозування нових загроз - це ще один фактор, що впливає на час реагування на кібератаки. Як зазначалося вище, затримка при реагуванні виникає навіть при загрозах відомих типів. Нові види атак, моделі поведінки та інструменти можуть збити фахівців з пантелику, в результаті чого вони будуть реагувати ще повільніше. Гірше того, такі менш помітні загрози, як крадіжка даних, іноді можуть залишитися і зовсім невиявленими. Опитування, проведене компанією Fugue в квітні 2020 року, показало, що приблизно 84% IT-фахівців стурбовані тим, що можуть не знати про вже скоєний злом їх хмарних систем.

Постійний розвиток технологій, що стоять на озброєнні зловмисників, і поява атак нульового дня - це фактори, які доводиться завжди враховувати, будуючи захист мереж. На щастя, методи кібератак зазвичай не винаходяться з нуля. Оскільки основою для них часто служать тактики, платформи і вихідні коди минулих атак, технологій машинного навчання є на чому базуватися при накопиченні знань.

Програма на основі машинного навчання допоможе розпізнати атаку, виявивши спільні риси у новій загрози і виявлених раніше. Машина, на відміну від людини, проведе таке порівняння швидко - що ще раз підкреслює необхідність застосування адаптивних моделей безпеки. Машинне навчання може полегшити прогнозування нових загроз і скоротити час реагування за рахунок більш ефективної роботи з базою існуючих загроз.

Кадровий потенціал

Проблема кадрового потенціалу належить до систематичних. З нею стикаються відділи IT та кібербезпеки безлічі компаній у всьому світі. Іноді знайти кваліфікованих фахівців з необхідними навичками може бути складно.

Однак набагато частіше проблема полягає в тому, що наймання співробітників вимагає виділення чималих коштів з бюджету організації. Зміст персоналу вимагає не тільки оплати повсякденної праці, а й задоволення

поточних потреб в навчанні та підтвердження кваліфікації. Професіонал в області кібербезпеки зобов'язаний йти в ногу з часом і бути в курсі постійних інновацій, про які ми згадували вище.

Наявність інструментів на основі ШІ дозволить скоротити штат фахівців. Хоча їм буде необхідно, постійно підвищуючи кваліфікацію, освоювати передові досягнення в області штучного інтелекту і машинного навчання, компанія зможе заощадити час і гроші завдяки меншій чисельності цих співробітників.

Адаптованість

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.

Якщо співробітники не знайомі з певними методами роботи, інструментами та системами, ефективність всієї команди може виявитися невисокою. Навіть така, здавалося б, проста процедура, як прийняття командою нових політик безпеки, може затягнутися. Така природа людини, ми не можемо миттєво освоїти нові види діяльності. На це потрібен час. Однак за допомогою правильних наборів даних можна перетворити добре навчені алгоритми в рішення, відповідні необхідним вимогам.

Роль ШІ в кібербезпеки

У сфері кібербезпеки штучний інтелект включає в себе дисципліни машинного і глибокого навчання, однак у нього є і своя власна роль.

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*.

Щоб краще зрозуміти суть питання, розглянемо сучасні методи використання ШІ і лежать в його основі дисциплін. Автономні системи не мають широкого поширення, особливо в області кібербезпеки. Їх робота не вимагає втручання з боку, і багато людей зазвичай асоціюють їх з ШІ. Однак системи на базі ШІ, що служать додатковим інструментом для забезпечення захисту, доступні і практичні.

В ідеальному варіанті роль ШІ в сфері кібербезпеки зводиться до інтерпретації закономірностей, виявлених алгоритмами машинного навчання. Звичайно, сучасний ШІ поки не здатний інтерпретувати результати так само добре, як людина. Ця область активно розвивається, ведеться пошук алгоритмів, схожих з людським мисленням. Але до створення справжнього ШІ ще далеко. Машинам ще тільки належить навчитися переосмислювати ситуації, оперуючи абстрактними поняттями. Їх творчі можливості і здатність до критичного мислення поки далекі від популярного образу ідеального ШІ.

Роль машинного навчання в кібербезпеці

Рішення для забезпечення безпеки із застосуванням технологій машинного навчання відрізняються від поширеного уявлення про штучний інтелект. Однак на сьогоднішній день у сфері кібербезпеки вони являють собою найбільш потужні інструменти на базі ШІ. В рамках цієї технології для визначення ймовірності того чи іншого події використовуються шаблони даних.

У певному сенсі машинне навчання можна протиставити «істинному» ШІ. Машинне навчання в першу чергу орієнтовано на точність, а не на результат. Це означає, що алгоритм діє, навчаючись на основі набору даних, орієнтованого на конкретну задачу. Його робота зводиться до пошуку оптимального способу виконання даного завдання. Він буде прагнути знайти рішення, єдино можливе на основі наявних даних, навіть якщо воно не буде ідеальним. Технологія машинного навчання не осмислює дані, а це означає, що дана задача як і раніше лягає на плечі фахівців.

Технології машинного навчання відмінно справляються з одноманітними завданнями, наприклад ідентифікацією закономірностей в даних і перевіркою їх на відповідність шаблонами. Подібна монотонна діяльність стомлює співробітників, знижуючи їх працездатність. Таким чином, людина досі відповідає за інтерпретацію даних, в той час як машинне навчання допомагає привести дані в легку для читання і готову до аналізу форму. У сфері кібербезпеки можливості машинного навчання можуть використовуватися для різних цілей:

Класифікація даних

При класифікації даних точкам даних присвоюються певні категорії за встановленим правилам. Даний процес маркування є важливою частиною таких аспектів проактивних заходів безпеки, як побудова профілів атак і вразливостей.

Кластеризація даних

При кластеризації даних відсіяні в ході класифікації значення об'єднуються в кластери з загальними або нетиповими характеристиками. Її можна використовувати при аналізі даних по атакам, до яких система ще не підготовлена. Кластери допоможуть визначити, яким чином проводилася атака, які уразливості використовувалися і до яких даними був отриманий доступ.

Рекомендації щодо подальших дій

Рекомендації щодо подальших дій підвищують ефективність проактивних заходів системи безпеки на базі машинного навчання. Вони виводяться на основі моделей поведінки і раніше прийнятих рішень і пропонують найбільш раціональний порядок дій. Тут важливо повторити, що рекомендації не є усвідомленим рішенням, як у випадку справжнього автономного ШІ. Швидше, це адаптивна система, здатна вибудовувати логічні взаємозв'язки на основі наявних

точок даних. Такий тип інструментів може надати істотну допомогу при реагуванні на загрози і управлінні ризиками.

Синтез можливостей

Синтез можливостей дозволяє отримувати абсолютно нові результати на основі історичних і нових наборів даних. Тут, на відміну від рекомендацій, більше уваги приділяється визначенню ймовірності повторення минулих станів системи. Наприклад, синтез можна використовувати для попереднього дослідження вразливостей в системах організації.

Прогнозування

Прогнозування - це найбільш просунутий з процесів, заснованих на машинному навчанні. Визначення можливих результатів досягається шляхом оцінки існуючих наборів даних. В першу чергу прогнозування можна використовувати для побудови моделей загроз, запобігання шахрайства, а також для захисту від витоку даних. Воно є основою багатьох Інтелектуальних рішень для кінцевих точок.

Приклади використання машинного навчання в кібербезпеці

Ось кілька прикладів, що 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.

Профілі безпеки на основі даних про роботу системи

Крім поведінки користувача, основою для створення профілю безпеки може також служити аналіз роботи окремо взятого справного комп'ютера. Наприклад, завантаження процесора і пам'яті поряд з такими ознаками, як інтенсивне використання інтернет-каналу, може вказувати на шкідливу активність. Проте деякі користувачі можуть регулярно використовувати великі обсяги даних - проводячи відеоконференції або часто завантажуючи великі файли мультимедіа. Вивчивши звичайну завантаженість системи, алгоритм може визначити відхилення, як у випадку з поведінкою користувача.

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.

4. Недоліки і проблеми сучасного штучного інтелекту

Сьогодні ми маємо можливість спостерігати постійне зростання обчислювальної потужності комп'ютерів, але це не означає появи в них ШІ. На жаль, навіть принципи роботи людської психіки сьогодні залишаються неясними. А оскільки ШІ спочатку замислювався як прообраз людини, то його створення пов'язане з невідомістю. Однак зростання продуктивності комп’ютерів у поєднанні з підвищенням якості алгоритмів обробки робить можливим застосування різних наукових методів на практиці в різних сторонах життя людства.

Розглянемо основні проблеми, пов'язані з розробкою ШІ на практиці.

Більшість сучасних розробок ШІ використовують кілька типів понять: ТАК (добре) і НІ (погано). В математиці і електроніці це нормально, але в житті точні поняття використовують рідко. Оскільки спочатку ШІ замислювався як людиноподібний інтелект, що слугує доповненням до людини, то догодити цьому самій людині буде дуже нелегко. Як, наприклад, машині зрозуміти депресивний

стан або ейфорію людини? Поняття "веселий" і "сумний" для машини тут ніяк не підходять.

Проблеми в розробці ШІ простежуються і на рівні формування образів і образної пам'яті. Оскільки образи в мисленні людини взаємопроникають один в одного, то формування образних ланцюжків у людей не представляє складності - воно асоціативно. Файли ж, на противагу до образів, є відокремленими пакетами машинної пам'яті. В пам'яті людини пошук даних ведеться не за вмістом пам'яті, а вздовж готових ланцюжків асоціативних зв'язків. Комп'ютер же шукає тільки конкретні файли.

Приклад: для людини не буде проблемою впізнати обличчя друга на фотографії, навіть якщо він схудне або видужає, і це є яскравим прикладом асоціативної пам'яті. Для машини це практично неможливо. Вона не зможе відрізнити головне від другорядного. Для отримання результату ШІ використовує тільки певну базу відомих даних. Йому невластивий експеримент.

Проблема перекладу з однієї мови на іншу, а також навчання машини мові. Якщо ви запропонуєте сучасним програмам-перекладачам (наприклад, Promt) перевести будь абзац з книги на іншу мову, то зрозумієте, що якістю тут і не пахне. В результаті ви отримаєте простий набір слів. Чому? Тому, що для перекладу цілих речень необхідно розуміти сенс речення, а не просто перекладати слова. Сучасні ШІ - програми не можуть поки виділяти сенс у тексті (ймовірно, тому, що посередником для перекладу, скажімо, з англійської на українську, є бездушна машинна мова - мова одиниць і нулів).

Простота математичних обчислень. Останнім часом багатьма провідними фахівцями в галузі ШІ внесено пропозицію щодо виключення зі списку високоінтелектуальних завдань простого алгебраїчного рішення рівнянь, оскільки для цього сьогодні є стандартні послідовні алгоритми обчислень. Це не вимагає складних, багатоетапних і часто непослідовних інтелектуальних здібностей. Розпізнавання тексту, гра в шахи та шашки, розпізнавання звуків на сьогодні успішно застосовуються на практиці, але їх хочуть прибрати з проблем ШІ.

Сучасні розробки, пов'язані зі штучним інтелектом, нездатні до самокопіювання (розмноження). На сучасному етапі розвитку кібернетики та електроніки абсолютно самостійне самокопіювання роботів є неможливим, необхідно хоча б часткове (часто значне) втручання людини. Однак для програм цей процес є простим, наприклад, можливості утиліт самостійно копіюватися в іншу директорію. Яскравим прикладом є комп'ютерні та мобільні віруси, які здатні до безконтрольного розмноження і виконання руйнівних дій.

Ще одна проблема на шляху до створення ШІ - відсутність в нього всякого прояву волі. Як це не дивно звучить, але в сучасних комп’ютерів є колосальні можливості до складних розрахунків, але абсолютно відсутні будь бажання. Навіть якщо комп’ютер забезпечити мікрофоном і акустикою, це не

означає, що він почне самостійно писати музику або мимовільно запускати будь-які додатки. Він не ледачий - просто у нього немає бажань. Комп'ютеру все одно, хто з ним працює, навіщо і з якою метою.

В сучасних прототипах ШІ відсутні стимули до подальшого вдосконалення. В природі на будь-який живий організм діє фактор природного відбору, який породжує постійне пристосування до умов навколишнього середовища. Голод, прагнення вижити і дати потомство - це фактори, що постійно діють на живий організм, як стимул до подальшого вдосконалення.

Мотивація більшості сучасних ШІ є дуже примітивною: людина задала задачу - машина її виконує без варіантів і емоцій. Теоретично на мотивацію і вдосконалення може вплинути введення зворотних зв'язків комп'ютер -> людина і створення покращеної системи самонавчання машини. Правда, це тільки теорія - на практиці ж все виявляється набагато складніше. Однак подібна робота вже проводиться. Як стимул вибрано елементарне почуття голоду - провісник швидкого закінчення енергетичних ресурсів і, відповідно, існування машини. Американець С. Вілкінсон створив "гастроробота" на ім'я "Жуй - жуй". Машина харчується цукром, і основою її поведінки є дослідження навколишнього світу в пошуках їстівного. Тіло "Жуй - жую" складається з трьох візків, а відчуття голоду є його постійним супутником, оскільки акумулятори постійно вимагають перезарядки. Проблемою є часті помилки машини у виборі продуктів харчування.

Деяка примітивність штучних нейронних мереж. Штучні нейронні мережі демонструють сьогодні дивовижні переваги, що властиві людському мозку. Вони навчаються на основі особистого досвіду, узагальнюють інформацію, самоконфігуріруются, витягують головне з інформації з зайвими даними. Однак навіть найрозвиненіші штучні мережі не можуть дублювати функції людського мозку. Реальний інтелект, що демонструється сьогодні складно влаштованими нейронними мережами, знаходиться нижче рівня розвитку інтелекту дощового хробака.

Неефективність штучного інтелекту у військових цілях. Останнім часом у ЗМІ досить часто з'являються новини про створення ШІ у військових цілях. Проте в реальності перед розробниками подібних машин-роботів стоять дуже складні і часто нерозв'язні завдання. Перш за все це недоліки систем автоматичного розпізнавання, нездатних самонавчатися і адекватно аналізувати інформацію в режимі реального часу (приймати потрібні рішення в потрібну хвилину). Такий бойовій машині дуже важко, а швидше за все - практично неможливо, буде відрізнити на полі бою своїх від чужих.

Також поки не розроблено алгоритмів роботи подібних пристроїв в умовах незнайомої місцевості. Подібні бойові одиниці здатні сьогодні максимум до простого дистанційного керування. Більш видатні результати досягнуто військовими в прикладних напрямках: точне розпізнавання мови і тембру голосу, різноманітні "детектори брехні", створення консультаційних систем (зниження

однотипних дій і навантаження на пілотів в режимі реального польоту), системи низкорівневого аналізу зображення, отриманого від відеокамери, і т. д.

Крім цього, сьогодні створено досить велику кількість приладів з подобою ШІ, покликаних вдосконалити роботу збройних сил: різноманітні інтелектуальні сонари і радари для виявлення цілей, супутникова система позиціонування для точного координування локалізації військ та їх пересування, різноманітні системи навігації в судноплавстві.

Майбутнє кібербезпеки

Незважаючи на бурхливі обговорення майбутнього цієї сфери безпеки, все ж існують обмеження, про які слід згадати.

Для машинного навчання необхідні набори даних, проте в деяких випадках їх збір і використання можуть протиріччьзаконам про конфіденційність даних. Програмних систем, навчальним алгоритми, потрібно безліч точок даних для побудови точних моделей, що погано поєднується з «правом на забуття». Наявність ідентифікує людини інформації в деяких даних може бути порушенням, тому необхідно передбачити можливі рішення цієї проблеми. Одне з них - системи, які роблять доступ до вихідних даних після навчання практично неможливим. Анонімізація точок даних також розглядається як можливий вихід, але цей метод необхідно вивчити глибше, щоб уникнути спотворення логіки програм.

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.

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.

Висновки

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...

Вчені намагаються відкрити завісу віддаленого майбутнього. Чи можливе створення штучного інтелекту? Чи можна створити такі людиноподібні системи, які зможуть мислити абстрактними образами, будуть саморозмножуватися, самонавчатися, коректно реагувати на зміни навколишнього середовища, володіти почуттями, волею, бажаннями? Чи можна створити відповідні алгоритми? Чи зможе людство контролювати такі об'єкти? На жаль, відповідей на ці питання поки немає. Залишається сподіватися на те, що, якщо штучний інтелект можна створити в принципі, то рано чи пізно він буде створений.

Три поради на шляху до майбутнього кібербезпеки

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

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.

Інструменти на базі ШІ і машинного навчання повинні допомагати вашим фахівцям, а не заміняти їх. Уразливості як і раніше будуть існувати. Сьогодні жодна система на ринку не є абсолютно надійною. Оскільки навіть адаптивні системи на базі ШІ можуть бути обмануті за допомогою витончених методів атаки, переконайтеся, що ваша ІТ-команда навчилася працювати з цією інфраструктурою і підтримувати її.

Регулярно оновлюйте свої політики в області обробки даних відповідно до змін в законодавстві. Конфіденційність даних стала об'єктом уваги керівних органів у всьому світі. У доступному для огляду майбутньому для більшості підприємств і організацій вона залишиться одним з основних питань на порядку денному.