Надалі штучний інтелект буде допомагати компаніям визначатися, в які нові технології безпеки слід вкладатися.

Є великий простір для розвитку. Сьогодні AI використовується в безпеки дуже обмежено. Можна говорити про відставання від інших галузей, і навіть разюче, що самоврядні автомобілі з'являються раніше, ніж мережі, що захищають самі себе. Нинішні платформи AI ще по суті не "розуміють" навколишній світ. Ці технології добре справляються з класифікацією даних, які схожі на зрізи і які використовувалися для навчання. Але штучний інтелект не є по-справжньому розумним - він не може зрозуміти ідею, що лежить в основі тієї чи іншої атаки. Тому людина, як і раніше, є ключовим елементом будь-якого рішення в області кіберзахисту.

І все ж прогрес в боротьбі з кіберзагрозами є. Існує такий напрямок досліджень, як генеративні змагальні мережі, - коли одночасно працюють дві моделі машинного навчання з протилежними цілями. Наприклад, одна намагається щось знайти, а інша - приховати те ж саме від виявлення. Цим принципом можна користуватися при створенні команд умовного противника, щоб з'ясовувати, якими можуть бути нові загрози.

Майбутнє інформаційної безпеки - за інтелектуальними системами, здатними забезпечити глибоку аналітику, прогнозування всього спектру ризиків і загроз. Впровадження таких систем створить необхідність перебудови бізнес-процесів підприємств з урахуванням використання сучасних інформаційних технологій.

Список використаних джерел

1. https://www.osp.ru/cio/2017/10/13053560/
2. https://www.osp.ru/cio/2017/10/13053565/
3. https://ayehu.com/role-artificial-intelligence-cybersecurity/
4. https://www.esecurityplanet.com/network-security/how-ai-is-redefining-cybersecurity.html
5. https://www.cio.ru/articles/181217-Gonka-vooruzheniy-iskusstvennyy-intellekt-i-kiberbezopasnost
6. https://www.cio.ru/articles/071217-Iskusstvennyy-intellekt-na-strazhe-kiberbezopasnosti

---

УДК 004.056.5

НЕЙРОМЕРЕЖА NVIDIA GAUGAN

Полевод О. М., Трощилов М. О., студ. гр. КБ-171

Науковий керівник: **Петренко Т. А.,** ст. викладач кафедри кібербезпеки та математичного моделювання

Національний університет «Чернігівська політехніка»

У 2019 році компанія Nvidia представила розробку нейромережі яка здатна із найпростіших замальовок (лінії та окружності) згенерувати детальні пейзажі природи. GauGAN дозволяє створювати віртуальні світи - і не тільки для розваги, але і для роботи. Так, архітектори, фахівці з ландшафтного дизайну, розробники ігор - всі вони можуть почерпнути щось корисне. Штучний інтелект відразу «розуміє», чого хоче людина і доповнює початкову ідею величезною кількістю деталей. Користувачі цього інструменту можуть змінювати початкову задумку, модифікувати пейзаж або інше зображення, додавати небо, піски, море і т.п., причому додавання відбувається всього за пару секунд. У цій роботі ми хочемо дослідити як саме працює дана технологія і що лежить в її основі.

Генерація зображень

Інструмент побудовано на технології генеративно-конкуруючих мереж (GAN), в основі яких лежить глибинне навчання. У більшості сучасних додатків глибинного навчання використовується нейронний дискримінантний тип (дискримінатор), а SPADE - це генеративна нейронна мережа (генератор).

Дискримінатор займається класифікацією даних, що вводяться. Наприклад, класифікатор зображення - це дискримінатор, який бере зображення і вибирає одну підходящу мітку класу, наприклад, визначає зображення як «собаку», «автомобіль» або «світлофор», тобто вибирає мітку, яка цілком описує зображення. Оскільки зв'язок між зображенням і його

класом дуже складний, нейронні мережі пропускають його через стек з безлічі шарів, кожен з яких «трохи» обробляє його і передає свій висновок на наступний рівень інтерпретації.

Генеративні мережі на зразок SPADE отримують набір даних і прагнуть створювати нові оригінальні дані, які виглядають так, ніби вони належать цьому класу даних. У загальному випадку введення даних в таку мережу полягає у введенні просто вектора випадкових чисел, причому кожен з можливих наборів даних, що вводяться створює своє зображення. Система керується своєрідним кресленням, який називається «картою сегментації». Остання вказує, що і де розміщувати. SPADE проводить процес, зворотний семантичної сегментації, згаданої нами вище. В цілому, дискримінаційна задача, яка переводить один тип даних в інший, має аналогічне завдання, але йде іншим, незвичним шляхом.

Між класифікатором і генератором зображення є одна важлива відмінність, і полягає вона в тому, як саме вони змінюють розмір зображення в ході його обробки. Класифікатор зображення повинен зменшувати його доти, поки зображення не втратить всю просторову інформацію і не залишаться тільки класи. Це може бути досягнуто об'єднанням шарів, або через використання «згортувальних» мереж, через які пропускають окремі пікселі. А генератор створює зображення за допомогою процесу оберненого до «згортування».

Для тренування мережі потрібно проводити порівняння з класифікаторами зображень, де кожне з них має правильну мітку класу. Знаючи вектор передбачення мережі і правильний клас, ми можемо використовувати алгоритм зворотного поширення (backpropagation algorithm), щоб визначити параметри оновлення мережі. Це потрібно, щоб підвищити її точність у визначенні потрібного класу і зменшити вплив інших класів. Але на даному етапі з‘являється проблема, яка полягає в тому, що коли генератор створює зображення, для кожного пікселя немає «правильних» значень (ми не можемо порівняти результат, як у випадку класифікатора по заздалегідь підготовленій базі). Теоретично, будь-яке зображення, яке виглядає правдоподібно і схоже на цільові дані, є дійсним, навіть якщо його значення пікселів сильно відрізняються від реальних зображень.

Рішення полягає в тому, щоб генерувати зображення, використовуючи дві нейронні мережі замість однієї: одна мережа - генератор, друга - класифікатор зображень (дискримінатор). Завдання дискримінатора полягає в тому, щоб відрізняти вихідні зображення генератора від реальних зображень з первинного набору (класи цих зображень позначені як «підроблені» і «реальні»). Робота ж генератора полягає в тому, щоб «обдурити» дискримінатор, створюючи зображення, максимально схожі на зображення в наборі даних. Можна сказати, що генератор і дискримінатор є конкурентами в цьому процесі. Звідси і назва: генеративно-конкурентна мережа.

Генерація зображень із випадкових наборів даних

SPADE не просто використовує випадкові дані. Ця мережа використовує зображення, яке називається картою сегментації: вона призначає кожному пікселю клас матеріалу (наприклад, трава, дерево, вода, камінь, небо). З цього зображення-карти SPADE і генерує те, що виглядає як фотографія. Для того щоб генератор вивчив цей підхід, йому потрібен набір карт сегментації і відповідні фотографії. Розробники модифікують архітектуру GAN так, щоб і генератор, і дискримінатор отримали карти сегментації. Генератору, звичайно, потрібна карта, щоб знати, де будуть розташовані ті чи інші об’єкти. Дискримінатору вона також необхідна, щоб переконатися, що генератор розміщує правильні речі в правильних місцях.

В ході навчання генератор вчиться не ставити траву там, де на карті сегментації вказано «небо», оскільки в іншому випадку дискримінатор легко визначить неправильне зображення, і так далі.

Висновок

Отже, нейромережі вже давно вчать брати участь в творчому процесі. Наприклад, в минулому році, деякі з них могли створювати 3D моделі. Крім того, розробники з навчили мережу відновлювати тривимірні простори і об'єкти за малюнками, фотографіями, ескізами. Для того, щоб відтворити просту фігуру, нейромережі вистачає однієї картинки, для створення більш складних об'єктів потрібно п'ять картинок для «тренування».

Що стосується GauGAN, то цей інструмент явно знайде гідне комерційне застосування - у багатьох напрямках бізнесу та науки є необхідність в подібних сервісах.

Список використаних джерел

1. Генеративна змагальна мережа [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%93%D0%B5%D0.
2. Как именно работает нейросеть NVIDIA GauGAN [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/company/itsumma/blog/447896/.
3. Nvidia [Електронний ресурс] – Режим доступу до ресурсу: https://www.nvidia.com/ru-ru/.

УДК 004.056.5

SYMANTEC DATA LOSS PREVENTION: РОЗРОБКА НАЙОПТИМАЛЬНІШОГО ВАРІАНТУ РЕАЛІЗАЦІЇ

Лисиця Т. А., студ. гр КБ-171,
Ткач Ю. М., д.пед.н., доцент
Національний університет «Чернігівська політехніка»

На сьогоднішній день інформація становить досить високу цінність. Тому цілком закономірно, що одним із найбільш вагомих завдань для безлічі компаній, незалежно від галузі виробництва чи сфери надання послуг, є обмеження несанкціонованого доступу до конфіденційної інформації. Застосування типових заходів безпеки, зокрема таких як антивіруси і фаєрволи, може допомогти у забезпеченні захисту організації від зовнішніх небезпек, але ніяк не від внутрішніх (наприклад: проникнення на територію організації зловмисника, халатність співробітників). Вдалим рішенням стане використання системи запобігання витоку інформації або DLP-системи.

В результаті дослідження та аналізу статистики використання систем захисту інформації було виявлено, що протягом тривалого часу в розробці і впровадженні DLP систем компанія Symantec займає передові позиції на українському ринку. Проте використання всього програмного комплексу Symantec Data Loss Prevention часто є недоступним для середніх та малих компаній і вдалим рішенням стане вдало підібране поєднання окремих програмних компонентів, розбір яких і буде в подальшому здійснено в даній статті.

Для аналізу поставленої проблеми було використано метод експертних оцінок та метод інверсії. Для перетворення даних критеріїв у ранжування було використано метод рядкових сум та порівняно утворені ранги. Після подальшого перегляду та аналізу було застосувати метод ключових питань та метод суду. Сформульовані критерії вибору представлені в табл.1.

Таблиця 1 – Загальні критерії вибору для всіх варіантів реалізації

<table>
<tr><td colspan="8">Варіанти реалізації</td></tr>
<tr><td>Призначення</td><td>Бази даних</td><td>Локальні ПК та ноутбуки</td><td>Локальна мережа</td><td>Корпоративні сховища</td><td>Дані з мобільних</td><td colspan="2">Глобальна мережа</td></tr>
<tr><td>Метод виявлення контенту</td><td colspan="2">Described Content Matching (DCM)</td><td colspan="2">Exact Data Matching (EDM)</td><td>Indexed Document Matching (IDM)</td><td colspan="2">Vector Machine Learning (VML)</td></tr>
<tr><td>Мережеві протоколи</td><td colspan="2">IRC-орієнтовані</td><td colspan="2">IM-орієнтовані</td><td>Web-орієнтовані</td><td colspan="2">Інші (TCP, ICMP, UDP)</td></tr>
<tr><td>Захист інформації</td><td colspan="4">Всередині</td><td colspan="3">Зовні</td></tr>
<tr><td>Підтримка ОС</td><td colspan="2">Linux</td><td>Windows</td><td>Solaris</td><td>MAC OS</td><td colspan="2">AIX</td></tr>
<tr><td>Контроль переміщення даних</td><td colspan="3">Активний</td><td colspan="4">Пасивний</td></tr>
<tr><td>Режим роботи</td><td colspan="3">Реальний час</td><td colspan="4">По збереженому трафіку</td></tr>
</table>