УДК 004.056.223

Ілля Сергійович Казмірчук,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Володимир Анатолійович Євтушок,
старший викладач кафедри тактико-спеціальної
та фізичної підготовки факультету № 2
Харківського національного університету внутрішніх справ

Штучні нейронні мережі, їх використання у кіберзлочинності та боротьбі з нею

Останні роки ознаменувалися значним ривком у розвитку штучних нейронних мереж. І хоча перші спроби створити штучну нейронну мережу були ще у 40-х роках 20 ст., але саме останні події, пов'язані із ними, змусили суспільство широко говорити про них.

Для початку з'ясуємо, що ж таке нейронна мережа. Це математична програмна модель, побудована за принципом функціонування біологічних нейронних мереж – мереж нервових клітин живого організму. Головною особливістю таких мереж є те, що вони не програмуються в звичайному сенсі цього слова, а «навчаються» подібно до людського мозку. В процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними й вихідними, а також здійснювати узагальнення.

Нейронна мережа під назвою Deepfake показує можливості даної технології та як саме їх можуть використовувати у кіберзлочинності. Наприклад, відео 2018 року, де показується екс-президент США Барак Обама та його слова змінені на ті що він ніколи не говорив, наприклад різко негативне звертання на адресу чинного президента США Дональда Трампа. При цьому мова та міміка людини відтворена нейронною мережею є надзвичайно правдоподібною та майже неможливо помітити підміну неозброєним оком. Таким чином, будь-яка людина коли-небудь знята на відео може стати ціллю злочинців, особливо політики, слова яких можуть викликати надзвичайно різку реакцію у суспільстві.

Так, зімітувавши лише голос людини, зловмиснику вдалося за допомогою нейронної мережі викрасти майже чверть мільйона доларів. Злочинець скопіював голос керівника потерпілої особи та вона, не запідозривши підміни, зробила переказ грошей. Це лише один з подібних випадків використання технології для злочинних дій, проте уже зараз можна сказати що вона ставить під сумнів доцільність використання технологій верифікації та ідентифікації за допомогою голосу особи.

Також нейронні мережі можуть значно спростити та прискорити роботу правоохоронних органів. Так звані Face detectors мережі здатні майже із сто відсотковою вірогідністю знайти людину за її фото у базі даних. При чому алгоритм дуже стійкий до змін – людині необов'язково дивитися в камеру, навіть можуть бути присутні деякі загороджуючі предмети: окуляри, борода або медична маска. Так вже у 2015 році китайська влада запустили проект по створенню національної бази даних на основі системи розпізнавання осіб. У країні будують мережу камер відеоспостереження, яку у Китаї називають найбільшою в світі: 176 мільйонів камер вже встановлені, та ще близько 450 мільйонів планується встановити до 2020 року. За задумом влади, до 2020 року штучний інтелект зможе за три секунди дізнатися в обличчя кожного з майже 1,4 мільярда жителів країни.

Отже, зважаючи на значний розвиток нейронних мереж, можна сказати що вони внесли свій вплив як на повсякденне життя людей, так і на розвиток кіберзлочинності й боротьби із нею. На мою думку правоохоронним органам України потрібно використати китайський досвід, та використовуючи такі мережі значно полегшити виконання деяких завдань, таких як пошук зниклих осіб, або ідентифікація особи у натовпі.

Одержано 28.10.2019