Для більш наглядного прикладу, я дослідила нейронну мережу BrainMaker, яку використовувала Microsoft для прямої розсилки.

Microsoft використовувала нейронне мережеве програмне забезпечення BrainMaker, щоб максимізувати прибутки своїх прямих посилань. Щороку компанія відправляла близько 40 мільйонів прямих поштових листів, до 8,5 мільйона зареєстрованих клієнтів. Більшість цих прямих розсилок були спрямовані на те, щоб люди могли оновити програмне забезпечення або придбати супутні товари. До першої поштової розсилки входили усі, хто був у базі даних, але друга розсилка була лише для тих, хто, швидше за все, відповідав.

Таким чином, одним із головних плюсів BrainMaker'а є те, що ця нейронна мережа має більше функцій аналізу, ніж будь-яка інша, як для вихідних даних, так і для вже навчених нейронних мереж.

Але, на мій погляд точність мереж, які ми будуємо і використовуємо (наприклад, той самий - BrainMaker), виявляється незадовільною, або взагалі не дає відповідних результатів чи не може досягти високих позицій в таблицях лідерів. Тому щоб уникнути цього, можна використати деякі способи для підвищення їх ефективності.

Перш за все, для того, щоб поліпшити НМ, я хочу запропонувати використання перевірки на перенавчання. Задля цього, потрібно перевірити нейронну мережу на його існування. Надмірне перенавчання відбувається тоді, коли модель НМ починає запам'ятовувати значення з навчальних даних, замість того, щоб вчитися на їх основі. Коли точність навчання набагато вища, ніж точність тестування, тоді НМ перенавчається. Для того, щоб уникнути цього, потрібно слідкувати за випадковими з'єднаннями між нейронами (Dropouts), паралельно змушуючи мережу знаходити нові шляхи та узагальнювати дані.

Також на мій погляд, можна покращити структуру нейронної мережі, шляхом додавання додаткового прихованого шару нейронів. Це дасть можливість досягти більшої точності, навіть якщо буде використано більше ресурсів. Для визначення помилок в режимі навчання нейромережі і прихованих шарів, зокрема, можна скористатися різними системами візуалізації внутрішнього процесу.

Як висновок, я хочу сказати, що мною було проведено дослідження нейронних мереж, та проаналізовано мережі на прикладі НМ - BrainMaker. Нейронні мережі - це потужний, але при цьому нетривіальний прикладний інструмент. Кращий спосіб навчитися будувати робочі нейромережеві конфігурації - починати з простіших моделей і багато експериментувати та напрацьовувати досвід.

Список використаних джерел

1. What is an artificial neural network? Here's everything you need to know [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/..

2. Neural Network Analysis [Електронний ресурс] – Режим доступу до ресурсу: http://www.ecommerce-digest.com/neural-networks.html.

3. Neural network models (supervised) [Електронний ресурс] – Режим доступу до ресурсу: https://scikit-learn.org/stable/modules/neural_networks_supervised.html.

УДК: 004

ІНТЕРНЕТ РЕЧЕЙ ЯК ПРИЧИНА ВИНИКНЕННЯ НОВИХ КІБЕРЗАГРОЗ

Зубчевська А.О., студ.гр. КБ-161
Петренко Т.А., ст. викладач кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Інтернет речей (Internet of Things – IoT) - одна з найпопулярніших концепцій у науці прогнозування майбутнього, футурології, яка складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані сенсори, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами, за допомогою використання стандартних протоколів зв'язку. Такі мережеві протоколи представляють собою набори правил, і дозволяють здійснювати з'єднання і обмін даними між двома і більше підключеними до мережі пристроями.[1]

Сьогодні поняття «інтернет речей» включає в себе відразу кілька явищ. Це і самі пристрої, які підключені до глобальної мережі і взаємодіють між собою. Це і спосіб підключення - M2M - тобто машина-до-машина, без участі людини. Це і великі об'єми даних, які тепер генерують ці пристрої. [2]

У 2018 році кількість пристроїв, підключених до Інтернету, за даними Statista, перевищила 20 млрд. штук. За прогнозами компанії Cisco до 2020 їх буде вже близько 50 млрд.[3] Інтернет речей - це не тільки розумний холодильник, який сам замовляє їжу для господаря, або чайник, який кип'ятить воду за командою зі смартфона. Це також і розумні датчики на полях, дрони з камерами, завдяки яким можна віддалено моніторити стан ґрунтів, це датчики у громадському транспорті та єдині системи «розумне місто» для моніторингу всіх сфер життя сучасних мегаполісів. Саме тому можна припустити, що вже за декілька років світ навколо нас стане дійсно цифровим, і людство скрізь буде оточувати інтернет речей.

У Австралії вже зараз за допомогою переносних датчиків кожен лікар може відслідкувати стан здоров'я свого пацієнта та реагувати в режимі реального часу. У США мобільний оператор AT&T розробив систему, яка покликана вирішити одну із найнебезпечніших проблем для літніх людей –

несподівані падіння. Суть цього методу полягає у тому, що невеликий пристрій автоматично визначає різку зміну положення тіла власника і одразу ж з'єднується з колл-центром для надання негайної допомоги.

Україна не стоїть осторонь від світових трендів. Великі міста поступово стають «розумними», Київ і Львів є основними флагманами руху. В аграрному сектор, логістиці також використовують рішення для IoT. Хоча в цілому в Україні розвиток відбувається досить повільно, порівняно з іншими розвинутими державами.

Водночас проблема інформаційної безпеки стає однією з головних під час розробки, налагодження та впровадження цих пристроїв. Інтернет Речей на сьогоднішній день – одна з найбільш вразливих технологій з точки зору Інтернет-загроз. Загроза виникає, коли люди купують пристрої і підключають їх до мережі, не змінюючи заводських налаштувань і паролів. Саме це призводить до того, що інші люди можуть віддалено управляти ними. Вже зараз можна наводити приклади, коли зловмисники через Інтернет проникали в інтелектуальну систему управління будинком і, наприклад, підвищували в ньому температуру до +70 градусів. Або підключалися до віддалених систем контролю за дитиною і стежили за ними.

Основні види загроз Інтернету речей:

1. Загроза, що відома під назвою «Диявольський плющ» (Devil's Ivy Problem). Вона не є наслідком дій зловмисників, а викликана недоліками в архітектурі побудови зберігачів інформації. Загрози такого типу є суто технічними і викликають збої у роботі пристроїв або впливають на їх робочий стан;
2. Іншим типом загроз є втрата контролю над пристроями внаслідок збоїв управління на рівні M2M, на рівні конкретного пристрою або ж як прояв цілеспрямованих деструктивних дій. У першу чергу мова йде про пристрої критично важливих інформаційних систем, таких як управління транспортом, зв'язку та енергетики.[4]

Зрозуміло, що пристрої, які постійно перебувають в мережі Інтернет є мішенню для деструктивних дій. У засобах масової інформації є велика кількість фактів хакерських дій в мережах GSM, перехоплення в GPRS та втручання через Bluetooth, WiFi або інфрачервоні порти з різною метою. У такому разі пристрій або захоплюється під управління іншим суб'єктом, або виходить із-під контролю оператора. Якщо говорити про більш прості атаки, то мова йде про ускладнення управління приладом або про технічні збої в його функціях передачі інформації, або підміну даних геолокації пристрою. Унаслідок різноманітності пристроїв Інтернету речей зазначені вище небезпеки є надзвичайно серйозними.

Для того, аби забезпечити безпеку в сфері IoT , необхідно визначити систему стратегічних принципів, розробити відповідні стандарти, в тому числі методи реагування на загрози безпеки інтернету речей, які будуть розповсюджені на виробників, розробників, постачальників послуг, а також державних і комерційних споживачів, та визначені наступним чином:

- упровадження вимог безпеки на етапі розробки приладу;
- забезпечення своєчасного оновлення засобів безпеки та управління уразливостями;
- надання пріоритету вимогам безпеки відповідно до потенційного впливу;
- забезпечення поінформованості стосовно приладів у сфері Інтернету речей;
- обережне та обдумане під'єднання до мережі.

Із урахування вже існуючої моделі, забезпечення кібербезпеки в Україні, на мою думку, скоріш за все належить до компетенції Національного координаційного центру з питань кібербезпеки. Окрім цього, вітчизняні законодавчі та нормативно-правові новації у цій сфері мають ґрунтуватись на відповідних рекомендаціях, що мають бути підготовлені фахівцями і враховувати кращі зразки світової практики.

Здійснений аналіз дає змогу дійти висновку, що на сьогодні інтернет речей вже серйозно вплинув на рівень кібербезпеки в сучасному суспільстві. Причиною цьому є постійно зростаюча кількість процесів що проходять без контролю людини. На сьогоднішній день існує не так багато досліджень на тему проблем безпеки у сфері IoT, тому ми вважаємо за необхідне в подальшому це питання розглядати більш ґрунтовно.

Список використаних джерел

1. Інтернет Речей: концепція IoT[Електронний ресурс]-2018,- Режим доступу:https://futurum.today/internet-rechei-kontseptsiia-iot-shcho-chekaty-vid-maibutnoho/

2. Інтернет Речей [Електронний ресурс]-2018,- Режим доступу: https://apptractor.ru/internet-veshhey

3.Технологія інтернету речей [Електронний ресурс]-2018,- Режим доступу: https://www.cisco.com/c/ru_ua/about/press/2015/04-04032015e.html3.

4.Основні інтернет-загрози [Електронний ресурс]-2018,- Режим доступу: http://safe-city.com.ua/osnovni-internet-zagrozy/