технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [1].

За даними які опубліковані у звіті з інформаційної безпеки за 2017 рів від компанії Cisco, приблизно в кожному четвертому випадку організація, що піддалася атаці, втрачає бізнес-можливості. Четверо з десяти опитаних повідомляло, що подібні втрати мали велике значення. Кожна п'ята організація втратила замовників внаслідок кібератак [2]. Україну кіберзлочинність не оминула, за 2016 рік було здійснено 247 кібератаки на системи органів державної влади [3]. Згідно даних компанії Trend Micro Incorporated за першу половину 2017 року було зафіксовано більше 82 млн. атак з використання програм-вимагачів, а також 3 тис. спроби здійснення шахрайства з використанням корпоративної пошти (BEC).

В наші дні є три основні типи кібератак, а саме атаки на конфіденційність в мережі, її цілісність та її доступність.

Автори атак, націлені на порушення конфіденційності, хочуть викрасти або виставити у відкритий доступ інформацію, таку як: номера кредитних карток або соціального страхування, отриманих незаконним способом.

Другий тип атак пов’язаний з доступністю мережі – ці атаки біль відомі під назвою «відмова в обслуговувані» (denial-of-service, DoS) або «розподіленої відмови в обслуговувані» (distributed-denial-of-service, DDoS). Атаки данного типу зазвичай направлені на блокування роботи мережі шляхом надісланню їй великої кількості запитів, що приводять до її обвалу. На сьогодні відомі такі DDos атаки як: DDos атаки з використанням ботнетів, DDos атаки з використанням SSL з’єднаня.

Також кібератаки можуть впливати на цілісність мережі. Можна сказати, що такий тип атак частково є «фізичним». Вони націлені на зміну чи знищення комп'ютерних програм, а також на пошкодження устаткування, інфраструктури або інших систем в реальному світі. Після того як комп'ютер або інший пристрій піддається подібній атаці, такий пристрій стає повністю непотрібним.

Дослідники з французького інституту INRIA розробили новий метод атак на системи шифрування, які застосовують 64-бітові блокові шифри 3DES та Blowfish. Цей метод отримав кодове ім’я Sweet32. З його допомогою можна отримати cookie, використовуються для аутентифікації з зашифрованого 3DES HTTPS-трафіку, а також відновлювати імена користувачів і паролі з зашифрованого за допомогою Blowfish трафіку, що передається через VPN [4].

Отже, кібератаки несуть в собі величезну небезпеку не тільки для компаній, а й для держав. Тому держава повинна сприяти приєднанню наукових та навчальних установ, організацій, громадських об’єднань для впровадження певних заходів для усунення кіберзагроз та кібератак.

Список використаних джерел

1. Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VII [Електро- нний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2163-19.

2. Cisco. Річний звіт з інформаційної безпеки, 2017. [Електронний ресурс]. – Режим доступу: http://www.cisco.com/c/dam/m/digital/elqcmcglobal/with/1301152/ReportUKR.pdf.

3. Служба безпеки України [Еклетронний ресурс]. – Режим доступу: https://ssu.gov.ua/ua/news/1/category/2/view/2474#sthash.4E1VYLlG.dN4fEV OL.dpbs.

4. Sweet32: Birthday attacks on 64-bit block ciphers in TLS and open VPN [Електронний ресурс]. – Режим доступу: https://sweet32.info.

5. Інформаційна безпека та комп'ютерні технології: Збірник тез доповідей II Міжнародної науково-практичної конференції, 20-22 квітня 2017 року, м. Кропивницький: ЦНТУ, 2017. – 211 с.

6. Индустрии будущего / Алек Росс ; [пер. с англ. П. Мироно-ва]. – Москва : Издательство АСТ, 2017. – 287с.

Ігнатенко О.П., студент 1 курсу, група МЕКп-171
Науковий керівник - Акименко А.М., к.ф.-м.н., професор
Чернігівський національний технологічний університет

РОЗПІЗНАВАННЯ ТЕКСТУ ТА ЙОГО МЕТОДИ

Тема розпізнавання тексту потрапляє під розділ розпізнавання образів. І для початку коротко про саме розпізнаванні образів.

Розпізнавання тексту або теорія розпізнавання образів це розділ інформатики та суміжних дисциплін, що розвиває основи і методи класифікації та ідентифікації предметів, явищ, процесів, сигналів, ситуацій тощо об'єктів, які характеризуються кінцевим набором деяких властивостей і ознак.

Також вона стверджує, що можна виділити два основних напрямки:

- Вивчення здібностей до розпізнавання, якими володіють живі істоти, пояснення та моделювання їх;
- Розвиток теорії та методів побудови пристроїв, призначених для вирішення окремих завдань в прикладних цілях.

Наблизимося ще ближче до теми розпізнавання тексту. Слід зауважити, що під розпізнаванням тексту зазвичай розуміють три основних способи.

- Порівняння із заздалегідь підготовленим шаблоном;
- Розпізнавання з використанням критеріїв, що розпізнається об'єкта;
- Розпізнавання за допомогою алгоритмів, які самостійно навчаються, в тому числі за допомогою нейронних мереж.

Методи розпізнавання образів:

- Для оптичного розпізнавання образів можна застосувати метод перебору вигляду об'єкта під різними кутами, масштабами, зсувами й т. д. Для букв потрібно перебирати шрифт, властивості шрифту й т. д.
- Другий підхід — знайти контур об'єкта й досліджувати його властивості (зв'язність, наявність кутів і т. д.)
- Ще один підхід — використовувати штучні нейронні мережі. Цей метод вимагає або великої кількості прикладів задачі розпізнавання (із правильними відповідями), або спеціальної структури нейронної мережі, що враховує специфіку даної задачі.

Технологія розпізнавання:

Складність машинного розпізнавання текстів полягає в тому, що його неможливо побудувати за чітким алгоритмом хоча б тому, що для написання однієї і тієї ж букви існує безліч варіантів написання (шрифт, накреслення). Для того, щоб отримати коректний результат система повинна їх «осмислити». Іншими словами, для розпізнавання тексту потрібно моделювання міркувань людини в подібній ситуації, а це прийнято позначати терміном «штучний інтелект». Виходячи з принципу цілісності распознаваемое зображення розглядається як єдиний об'єкт, що складається з частин, пов'язаних між собою просторовими співвідношеннями. За принципом цілеспрямованості розпізнавання будується як процес висування і цілеспрямованої перевірки гіпотез про об'єкт, а принцип адаптивності передбачає здатність системи до самонавчання. Для висунення гіпотез про те, що може являти собою зображення, застосовуються так звані прізнаковие класифікатори. Вони використовують ряд ознак, на основі яких програма обчислює ступінь близькості розпізнається зображення і відомих їй класів зображень, після чого видає список відповідних класів. Крім того, прізнакові класифікатори застосовуються також і для підвищення точності розпізнавання зображень з дефектами. Отриманий набір класів послідовно перевіряється структурним класифікатором, які аналізують кожен символ. Скажімо, якщо FineReader вважає, що на сторінці зображена буква «Ф», він спеціально перевіряє ті ознаки, які повинні бути саме у літери «Ф», а не у будь-якої іншої, порівнюючи цей символ зі структурним еталоном. Структурний стандарт визначає символ як комбінацію структурних елементів (відрізок, дуга, кільце, точка), що знаходяться в певних відносинах між собою. Процес розпізнавання ділиться на етапи виділення структурних елементів в зображенні і зіставлення їх з еталоном. Із завершенням роботи диференціального класифікатора закінчується розпізнавання і починається етап перевірки підсумкового списку гіпотез. Остаточна стадія розпізнавання здійснюється системою контексту - при наявності певної кількості розпізнаних літер з слова програма, використовуючи словник, може «здогадатися», що це за слово. Базові принципи цілісності, цілеспрямованості і адаптації залишаються незмінними від версії до версії програми FineReader, адже саме вони дозволяють комп'ютеру наблизитися до логіки мислення людини. Крім описаної вище програми існують і інші програми.

Розпізнавання широко використовується для конвертації книг і документів в електронний вигляд, для автоматизації систем обліку в бізнесі, економіці або для публікації тексту на веб-сторінці. Оптичне розпізнавання тексту дозволяє редагувати текст, здійснювати пошук слів чи фраз, зберігати його в більш компактній формі, демонструвати або роздруковувати матеріал, не втрачаючи якості, аналізувати інформацію.

Список використаних джерел

1. Гранічін О.Н., Шалим Д.С. Рішення завдання автоматичного розпізнавання окремих слів мови за допомогою рандомізованого алгоритму стохастичною апроксимації // Нейрокомп'ютери: розробка, застосування, 2009, № 3, с. 58-64.

2. Горбань А., Россиев Д. Нейронные сети на персональном компьютере. //Новосибирск, Наука, 1996. - С 114 - 119.

3. Шалим Д.С. Рандомізований алгоритм стохастичною апроксимації в задачі розпізнавання друкованих текстів арабської мови // Праці VIII Міжнародної конференції «Ідентифікація систем та завдання управління» SICPRO '09. Москва, 2009 г.

Клецкіна Т.В., студентка 1 курсу, група МЕК-171, факультет економіки
Науковий керівник - Акименко А.М., к.ф.-м.н., професор
Чернігівський національний технологічний університет

АВТОМАТИЗОВАНІ СИСТЕМИ ОБРОБКИ ІНФОРМАЦІЇ

Останнім часом все більшою популярністю користуються багатофункціональні мобільні пристрої. Сьогодні багато людей довіряють своєму телефону зберігання і обробку різної інформації - від повідомлень електронної пошти до щоденника і даних платіжних систем. Одна з виникаючих при цьому проблем - це введення даних. Залежно від завдання як джерело даних можуть виступати, наприклад, інші електронні пристрої, інформація, одержувана з інтренет, або реальні документи. Для отримання даних з останніх потрібно механізм