Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Побудова текстового стеганоконтейнера на основі нейронних мереж

Виконав: студент IV курсу, групи СБс-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Брозь Н.О. (прізвище та ініціали)

Керівник (підпис) Скарга-Бандурова І.С. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль - 2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Брозю Назару Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Побудова текстового стеганоконтейнера на основі нейронних мереж

Керівник роботи Скарга-Бандурова Інна Сергіївна, д.т.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 04 » 04 2023 року № 4/7-349

2. Термін подання студентом завершеної роботи 21.06.2023 р.

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналіз предметної області.
2. Теоретична частина.
3. Практична частина.
4. Безпека життєдіяльності, основи хорони праці

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титулка. 2. Актуальність. 3. Мета, задачі дослідження. 4. Класична схема стеганографічного каналу 5. Порівняння стенографічних методів. 6. Моделі ШНМ. 7 Одна із можлививх варіацій ШНМ. 8. Загальна технологія роботи стегосистеми 9. Аналіз нейромережевих архітектур для генерації стеготекстів. 10, 11. Приклад апробації технології роботи стегосистеми 12. Основні результати проведеного дослідження

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці			

7. Дата видачі завдання 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	04.04 – 06.04	*Виконано*
2.	Підбір джерел про текстові стеганоконтейнери на основі		
	нейромереж	07.04 – 11.04	*Виконано*
3.	Опрацювання джерел про текстові стеганоконтейнери на		
	основі нейромереж	12.04 – 16.04	*Виконано*
4.	Виконання дослідження про текстові стеганоконтейнери		
	на основі нейромереж	17.04 – 23.04	*Виконано*
5	Розроблення програмного коду	24.04 – 29.04	
6.	Оформлення розділу «Аналіз предметної області»	30.04 – 07.05	*Виконано*
7.	Оформлення розділу «Теоретична частина»	08.05 – 15.05	*Виконано*
8.	Оформлення розділу «Практична частина»	16.05 – 21.05	*Виконано*
9.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи охорони праці»	14.05 – 21.05	*Виконано*
10.	Оформлення кваліфікаційної роботи	22.05 – 05.06	*Виконано*
11.	Нормоконтроль	06.06 – 12.06	*Виконано*
12.	Перевірка на плагіат	10.06 – 14.06	*Виконано*
13.	Попередній захист кваліфікаційної роботи	15.06 – 18.06	*Виконано*
14.	Захист кваліфікаційної роботи	22.06	

Студент _____ Брозь Н.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скарга-Бандурова І.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Побудова текстового стеганоконтейнера на основі нейронних мереж // Брозь Назар Олександрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБс–41 // Тернопіль, 2023 // С. – 51, рис. – 24, табл. – 4 , слайдів – 12, бібліогр. – 37.

Ключові слова: СТЕГАНОКОНТЕЙЕР, ЛІНГВІСТИЧНА СТЕГАНОГРАФІЯ, СТЕГАНОГРАМА, БІТОВА ПОСЛІДОВНІСТЬ, RNN, КЛЮЧ-ТАБЛИЦЯ

Кваліфікаційна робота присвячена лінгвістичній стеганографії, а саме створенню ефективного методу текстової стеганографії із застосуванням штучних нейронних мереж.

Проаналізована предметна область дослідження, проведено порівняння сучасних стеганографічних методів. Докладно описано математичний апарат нейромереж, особлива увага приділена рекурентним нейронним мережам, в т.ч мережам довгої короткострокової пам'яті, тимчасовим згортковим мережам та генеративно-змагальним мережам.

Наведено процес навчання нейромережі для задачі мовного моделювання. Розроблено тестовий стенд для зняття атрибутів стеганографічної системи з текстовим стегоконтейнером, створеної на основі нейромереж з різними архітектурами. Продемонстровано працездатність стеганосистеми, котра свідчить, що нейромережні моделі створюють реалістичні повідомлення, приховуючи інформацію. Відображено, що стегосистема поєднує в собі якість текстового стеганоконтейнера (стеготекст виглядає як природній текст) та високу пропускну здатність.

ANNOTATION

Construction of a text steganography container based on neural networks // Broz Nazar // Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2023 // P. - 51, Fig. - 24, Table - 4, Slides - 12, References - 37.

Keywords: STEGANOCONTAINER, LINGUISTIC STEGANOGRAPHY, STEGANOGRAM, BIT SEQUENCE, RNN, KEY-TABLE

Thesis deals with the linguistic steganography, namely the creation of an effective text steganography method using artificial neural networks.

The subject area of the research was analyzed, and a comparison of modern steganographic methods was carried out. The mathematical apparatus of neural networks is described in detail, special attention is paid to recurrent neural networks, including long-short-term memory networks, temporal convolutional networks, and generative-competitive networks.

The process of training a neural network for the problem of language modeling is presented. A test bench has been developed for removing the attributes of a steganographic system with a text stegocontainer, created on the basis of neural networks with different architectures. The operability of the steganosystem is demonstrated, which indicates that neural network models create realistic messages while hiding information. It is shown that the stegosystem combines the quality of a text steganocontainer (stegotext looks like natural text) and high throughput.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

bpc (bits-per-character) – біт-на-символ.

bpw (bits-per-word) – біт-на-слово.

GAN (Generative Adversarial Nets) – генеративно-змагальні мережі.

GRU (Gated Recurrent Units) – керовані рекурентні блоки.

LSTM (Long Short-Term Memory) – мережа довгої короткострокової пам'яті.

RNN (Recurrent Neural Networks) – рекурентні нейронні мережі.

SVM (Support Vector Machine) – метод опорних векторів.

tanh – гіперболічний тангенс.

TCN (Temporal Convolutional Networks) - тимчасові згорткові мережі.

БП – багатошаровий перцептрон (MultiLayer Perceptron, MLP).

ЗЗ – зворотній зв’язок.

МЗПП (Метод Зворотного Поширення Помилки - Backpropagation, Backprop) – алгоритм навчання багатошарових перцептронів, заснований на обчисленні градієнта функції та помилок.

МН – машинне навчання.

Перплексія (perplexity) – міра того, наскільки добре розподіл ймовірностей або ймовірнісна модель прогнозує вибірку.

СК – стан комірки.

СМ – стеганографічні методи.

СШ – сигмоїдальний шар.

ФА – функція активації.

ШНМ – штучна нейронна мережа.

ЗМІСТ

ВСТУП

Упродовж останніх років через збільшення потреби у захисті конфіденційних даних підвищується інтерес до СМ захисту інформації. На відміну від криптографічних методів, в яких приватність даних убезпечується при допомозі їх перетворення, у стеганографії приховується власне факт існування таких даних під час її передачі, обробки чи зберігання. СМ вбудовують приховане повідомлення у цифровий об'єкт даних, який зазвичай називається контейнер. Як контейнер виступають файли зображень, відео-і аудіофайли, текстові та виконувані файли. При цьому СМ дають змогу розв’язувати, в тому числі, завдання захисту від несанкціонованого копіювання, відслідковування поширення даних.

МН є однією з найперспективніших галузей комп'ютерних наук на даний момент. Воно використовується в різноманітних сферах, в т.ч. прогнозоване обслуговування, оптимізація ланцюга постачання, розпізнавання об'єктів на зображеннях та відео, розпізнавання шахрайства, синтезу та розпізнавання мови, персоналізація охорони здоров'я, скорочення дорожнього трафіку, раціональне планування розкладу польотів та багато інших. Часто МН використовується для обробки текстових даних [1].

МН дедалі частіше стало застосовуватися у сфері комп'ютерної безпеки. Наприклад, у детектуванні різних атак, аналізі мережного трафіку, в атаках на додатки, у розпізнаванні спаму. Останнім часом МН застосовується також і у стеганографії [2,3].

Одним із актуальних напрямів у галузі комп'ютерної безпеки є питання розробки прихованих каналів на основі СМ. В даний час отримують "друге народження" дослідження в галузі методів текстової стеганографії, коли секретне повідомлення вбудовується в текстові дані.

Ця робота присвячена лінгвістичній стеганографії [4], коли секретна інформація вбудовується в текст, який у результаті виглядає як текст природною мовою. З 2010-х років мовні моделі, що використовують різні архітектури ШНМ, досягли проривних результатів, продемонструвавши в експерименті кращі

показники перплексії, ніж статистичні методи моделювання мови. Сьогодні найбільш перспективними методами моделювання мови є методи, котрі базуються на ШНМ. В роботі досліджуватиметься стегосистема, в якій для генерації тексту властиво природною мовою використовується нейромережа. Демонструється, що стегосистема поєднує в собі якість текстового стеганоконтейнера (стеготекст виглядає як текст природною мовою) з високою пропускною здатністю (кількість bpw стеготексту).

Метою роботи є розробка ефективного методу текстової стеганографії з урахуванням апарату нейронних мереж.

В процесі виконання роботи потрібно вирішити наступні завдання:

– провести порівняння сучасних СМ;

– вивчити математичний апарат нейронних мереж;

– розробити тестовий стенд для зняття характеристик стеганографічної системи з текстовим стегоконтейнером, побудованої на базі нейромереж з різними архітектурами.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Основні поняття

Як термін стеганографія утворюється в середні віки, проте її методи вже застосовувалися і до нашої ери. У більшості випадків повідомлення приховували фізичним способом (воскові глиняні дощечки, татуювання на рабах, невидимі чорнила та інші методи). З ранніх СМ з використанням тексту як контейнер відомий книжковий “шифр” Енея Тактика. Інформація передавалася за допомогою непримітних текстових позначень, наприклад, дірок від голки, котрі проставлені поруч із символами, які у сумі формують вихідний текст секретного повідомлення.

В сучасних термінах, стеганографія - це спосіб передавання інформації, при якому ховається сам факт зберігання або передачі в деякому контейнері, причому факт власне передачі може бути розкритий тільки одержувачем, який знає алгоритм приховування інформації [5]. На рис. 1.1 представлена класична схема каналу стеганографії.

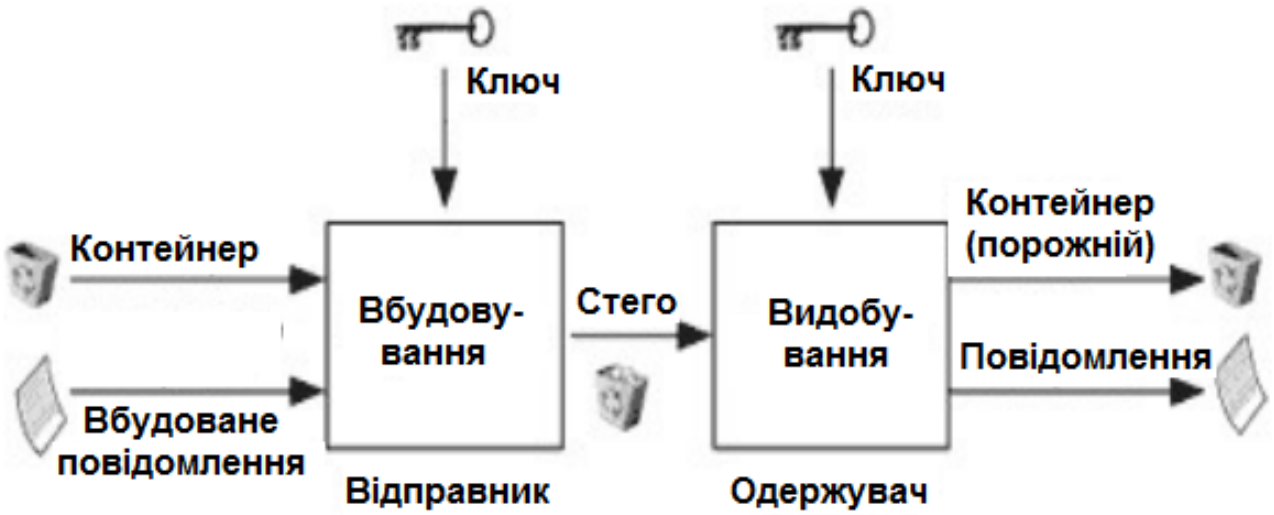


Рисунок 1.1 – Класична схема стеганографічного каналу

Основні елементи каналу стеганографії:

– вбудовуване повідомлення - вихідний текст, що використовується для створення стегоконтейнера, що передається;

– контейнер - сигнал, потік чи файл, що містить у собі приховане повідомлення;

– вбудовування - приховування повідомлення у контейнері;

– стегоконтейнер (обкладинка, стего) – результат вбудовування;

– вилучення - отримання прихованого повідомлення із контейнера;

– ключ (стегоключ) - дані, які застосовуються для вбудовування/вилучення, може бути відсутнім.

Для покращення рівня безпеки секретне повідомлення може бути зашифроване до приховування в контейнері, завдяки цьому підвищується ймовірність не тільки того, що повідомлення не буде виявлено та/або розкрито, але й факту виявлення передачі, навіть якщо контейнер разом із прихованим зашифрованим повідомленням потрапив до третьої сторони .

Узагальнена модель стеганосистеми показана на рис. 1.2.

Рисунок 1.2 – Загальна схема стеганосистеми

1.2 Характеристики стеганографічних методів захисту інформації

Головні характеристики СМ:

– прихованість;

– пропускна здатність;

– стійкість.

Безпека стегосистеми виходить з цих трьох характеристик.

Прихованість – неможливість виявлення вбудованих даних без додаткової інформації про параметри вбудовування. Можна охарактеризувати через стійкість до різних методів стегоаналізу (загальних, спеціалізованих, статистичних, нейромережевих).

Пропускна здатність. Є критерієм оцінки кількості інформацію, яку можна надіслати за допомогою стегоконтейнера. Вона вимірюється в кількості інформації, яка може бути вкладена в один елемент контейнера або в одне слово (bpw / bpc).

Стійкість. Стійкість до модифікації контейнера з метою спотворення, навмисного введення хибних повідомлень або руйнування поміщеної інформації у контейнер. Також означає здатність методу вбудовування та вилучення не допускати, протистояти змінам третім особам за допомогою будь-яких методів обробки. У цьому випадку стеганографії, якщо стегофайли не піддаються впливу і не змінюються під час відправлення, це не вважається атакою, і одержувач отримує стегофайл таким, яким він був відправлений. В іншому випадку такі атаки, як стиснення, перетворення формату файлу та перетворення між цифровим та аналоговим форматом можуть відбуватися під час процесу комунікації.

Термін «безпека» у стеганографії відноситься до «невиявлення». Отже, стеганографічний підхід є безпечним, коли дані, що він приховує, неможливо знайти із застосуванням статистичних методів будь-якою третьою стороною. Безпека – головна вимога для запобігання доступу третіми особами або комп'ютерами під час спілкування з використанням незахищеного каналу, таким чином гарантується, що дані залишаються незмінними.

1.3 Особливості стеганографічних методів

Відповідно до [6] серед методів текстової стеганографії можна виділити:

– синтаксичні, наприклад використання додаткових прогалин між словами, коли дин пробіл відповідає нулю, а два - одиниці;

– методи, що генерують текст, подібний до природного, наприклад на основі контекстно-вільних граматик;

– семантичні методи, наприклад, метод Tyrannosaurus Lex (T-lex), що використовує заміну слів у реченні на їх синоніми або метод перефразування.

На стеганографічні системи з контейнером у текстовому форматі існують такі види атак:

– візуальні атаки. Такі атаки чи маніпуляції з боку читачів належать до людського чинника. Часто третя сторона може візуально спостерігати зміни об'єкта стегофайлу. Ці модифікації можуть складатися з синтаксичних, семантичних, парафразуючих, лексичних, риторичних змін тощо. Припустимо, що зловмисник повністю отримав доступ до обкладинки, і якщо він підозрює, що в обкладинки існують якісь модифікації, він може маніпулювати нею (тобто це може бути навмисне видалення, вставка або зміна порядку слів/символів);

– структурні атаки. Цей вид включає зміну макету обкладинки. У деяких випадках зловмисники можуть змінити форматування або кодування, що може призвести до руйнування прихованого повідомлення;

– статистичні атаки. Працюють на основі ймовірності вгадати правильний стего, враховуючи кількість слів, прогалин тощо. По суті, ця атака використовує знання про існуючі підходи для декодування/вгадування оригінального стего з використанням функцій розподілу ймовірностей.

На основі викладеного вище проведемо порівняльний аналіз основних СМ із контейнером у вигляді тексту за основними характеристиками.

Метод гомогліфічної заміни. Відноситься до синтаксичних. Гомогліф — один із двох або більше символів, які здаються ідентичними. Приховування інформації відбувається побітово шляхом заміни символів словами контейнера такими символами.

Метод заміни пробілів табуляцій. Відноситься до синтаксичних. Приховування відбувається аналогічно до попереднього методу, але відрізняється заміною пробілу після слова на два або кілька пробілів для приховування секретного повідомлення.

Метод, заснований на друкарських помилках. Відноситься до синтаксичних. Приховування інформації відбувається побітово шляхом заміни букв у словах контейнера, створюючи друкарську помилку.

На основі Марківського ланцюга. Цей метод відноситься до генеруючих. Суть методу – генерація тексту (стеганографічного контейнера) на основі ланцюга Маркова та прихованого послання. Ланцюг Маркова будується заздалегідь з використанням текстового шаблону.

Спосіб позицій букв. Цей метод відноситься до синтаксичних. Стегоконтейнер генерується по ї-тій позиції вбудованого повідомлення. Акровірш є окремим випадком цього методу, це коли, для прикладу, перші літери слів у кожній стрічці формують повідомлення.

Метод кодування довжин серій синонімів. Відноситься до семантичних. Приховування інформації відбувається побітово шляхом заміни слів на синоніми у контейнері.

ШНМ. Методи на їх основі можуть належати до трьох перелічених вище категорій. Стегоконтейнер генерується на основі навчання за ключовими даними, для прикладу як в [7 – 9].

В результаті в табл. 1.1 проаналізовано СМ з контейнером в текстовому форматі за основними характеристиками.

Як параметр оцінки ефективності методів стегоаналізу використовують ймовірність виявлення секретного повідомлення в контейнері. При цьому існує два роду помилки: помилка 1-го роду - порожній контейнер (без секретного повідомлення) приймається за заповнений (з секретним повідомленням); помилка 2-го роду – заповнений контейнер приймається за порожній.

Таблиця 1.1 – Порівняння СМ

Властивості/ метод	Гомогліфічна заміна	Заміна пробілів/ табів	Помилки	На основі Марківського ланцюга	Метод позицій букв	Метод кодування довжин серій синонімів	ШНМ
Прихованість	Висока	Висока, але менша за попередню	Висока, але менша за попередню	Нижче за перші тр	Висока	Нижче за перші три	Висока
Пропускна здатність	>1 bpw	>1 bpw	>1 bpw	0,03 – 10% від обкладинки	>7 bpw	>1 bpw	>1 bpw
Стійкість	Нестійка, повідомлення втрачаєтьс я при обмеженні до юнікоду	Нестійка, повідомлення втрачається при обмеженні до табуляцій, кількості пропусків	Нестійка, але стійкіша за попередні, повідомлення може загубитися при автовиправленні помилок, нестійкий до частотного аналізу	Стійка	Стійка	Стійка	Стійка
Особливості	Простота реалізації	Простота реалізації	Простота реалізації	Контейнери виходять досить довгими - до 10000 слів	Простота реалізації		

Синтаксичні методи можна виявити за допомогою простого аналізу, наприклад, факт присутності значного числа помилок в орфографії тексту буде говорити про можливість використання стеганографії. Методи, що генерують текст, є більш складними. Отриманий стеготекст завжди задовольнятиме правила граматики мови. У цьому випадку можна використовувати частоту слів і її дисперсію в аналізованому тексті і далі за допомогою SVM класифікатора

визначається факт наявності стеготексту.

Одним з очевидних недоліків методів, що генерують текст, подібний до природного, - безглуздий підсумковий текст. Проте завдання визначення свідомості тексту вимагає участі людини, що не завжди можливо. Тому для цих методів актуальним є побудова таких засобів аналізу, котрі працюють без участі людини.

2 ТЕОРЕТИЧНА ЧАСТИНА

У цьому розділі розглядаються такі моделі ШНМ:

– одно- та багатошарові перцептрони;
– RNN;
– LSTM;
– GRU;
– TCN
– GAN.

2.1 Перцептрон

Одношаровий перцептрон (інша назва - перцептрон Розенблатта) - ШНМ, всі нейрони котрої володіють жорсткою пороговою ФА. Є однією із найбільш простих моделей ШНМ з простим алгоритмом навчання і здатністю розв’язувати тільки самі прості задачі. В ранніх 60-х роках XX ст. ця модель спричинила значну цікавість і викликала поштовх до розвитку ШНМ. Стандартний варіант такої ШНМ – одношаровий тринейронний перцептрон – представлений на рис. 2.1.

Мережа, показана на рисунку, містить n входів, на котрі поступають сигнали, котрі проходять за синапсами на 3 нейрони. Ці три нейрони формують один шар ШНМ і випускають три вихідні сигнали властиво.

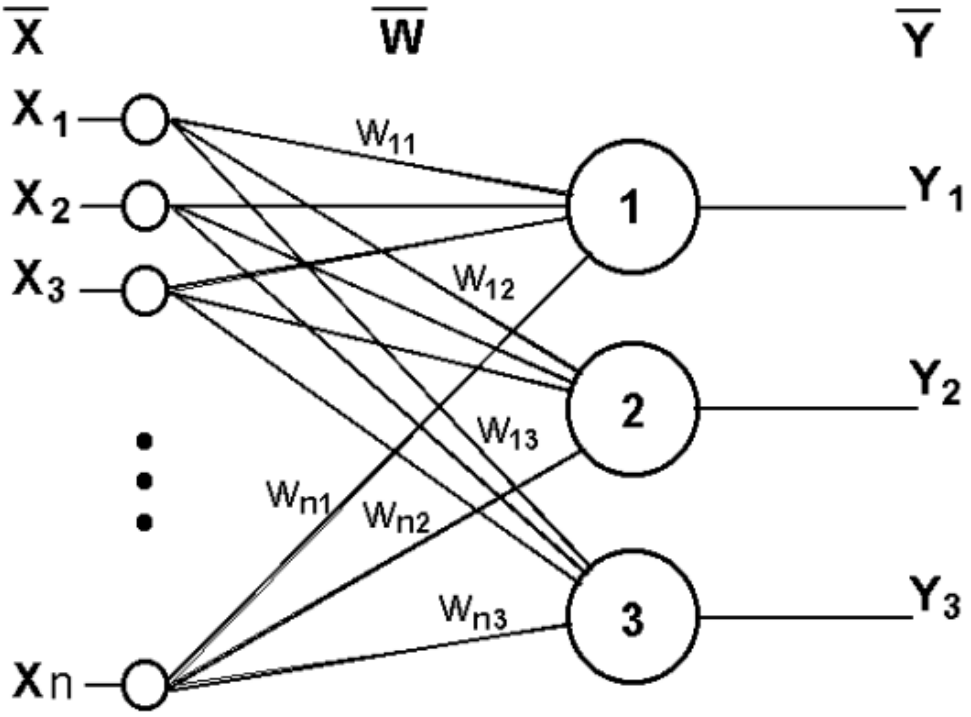


Рисунок 2.1 – Одношаровий тринейронний персептрон

MLP – ШНМ прямого розповсюдження сигналу (відсутній ЗЗ), в котрій вхідний сигнал трансформується у вихідний, прямуючи через декілька шарів послідовно.

Вхідним називається перший шар, вихідним – відповідно останній. Всі шари мають «вироджені нейрони» , часом, число шарів не береться до уваги. У багатошаровому перцептроні, окрім шарів вхідного та вихідного, існує як мінімум один проміжний. Він носить назву прихованого. Існування більше, ніж одного такого шару необхідне тільки при застосуванні нелінійних ФА.

Варіант двошарового перцептрона показано на рис. 2.2.

ШНМ на рис. 2.2, володіє *n* входами. Туди приходять сигнали, котрі слідують далі синапсами на 3 нейрони, які формують найперший шар. Вподальшому сигнали з виходів цього шару транслюються обом нейронам другого шару, котрі зі свого боку, надсилають два властиво вихідні сигнали.

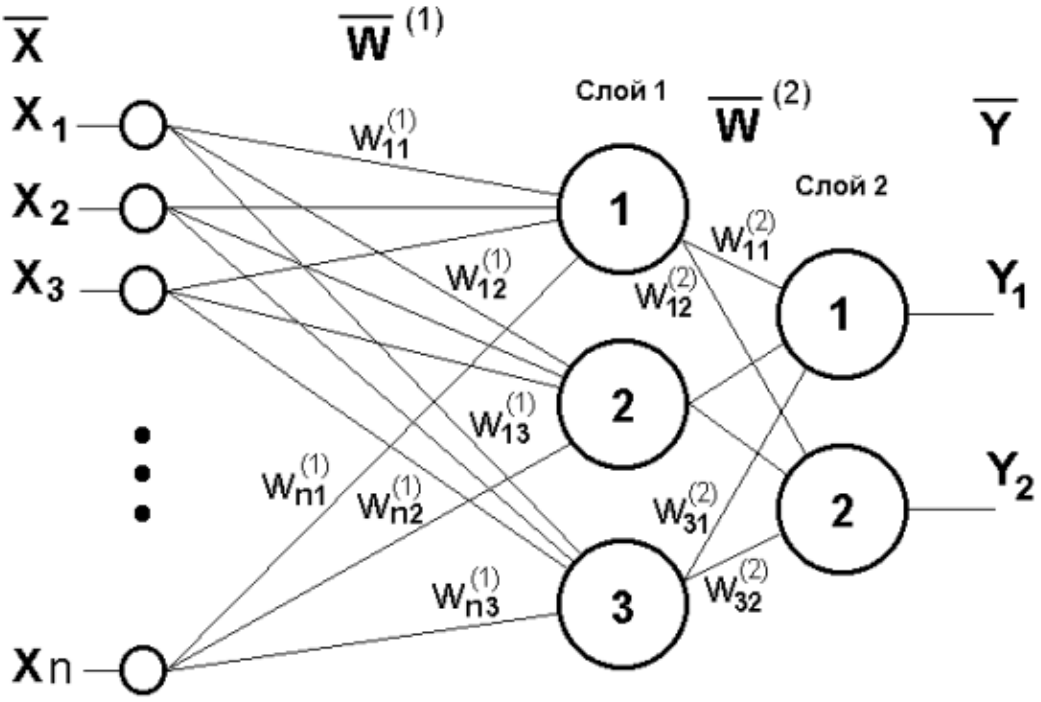


Рисунок 2.2 – Двошаровий перцептрон

Під час навчання при використанні МЗПП [11] ваги нейронів всякого шару нейромережі коригуються, зважаючи на сигнали, що надійшли з первинного шару, і нев'язку кожного шару, котра розраховується рекурсивно у зворотному напрямку від фінального шару до найпершого.

2.2 RNN

У звичайних ШНМ відсутня властивість запам'ятовувати попередній СК, і в цьому їх головний недолік. Вирішити цю проблему допомагають RNN. Вони мають ЗЗ і дають змогу утримувати дані [12]. На рис. 2.3 представлений блок простої RNN.

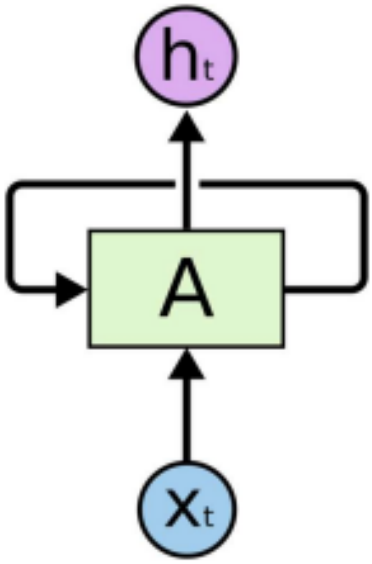


Рисунок 2.3 – Проста RNN

RNN володіють ЗЗ. На рис. 2.3 частина ШНМ набуває вхідного значення і повертає його. Існування ЗЗ дає змогу надсилати дані покроково.

RNN можна розглядати як декілька реплік однієї мережі, в якій кожна надсилає дані наступній репліці. Якщо розгорнути ЗЗ, утвориться конструкція, наведена на рис. 2.4:

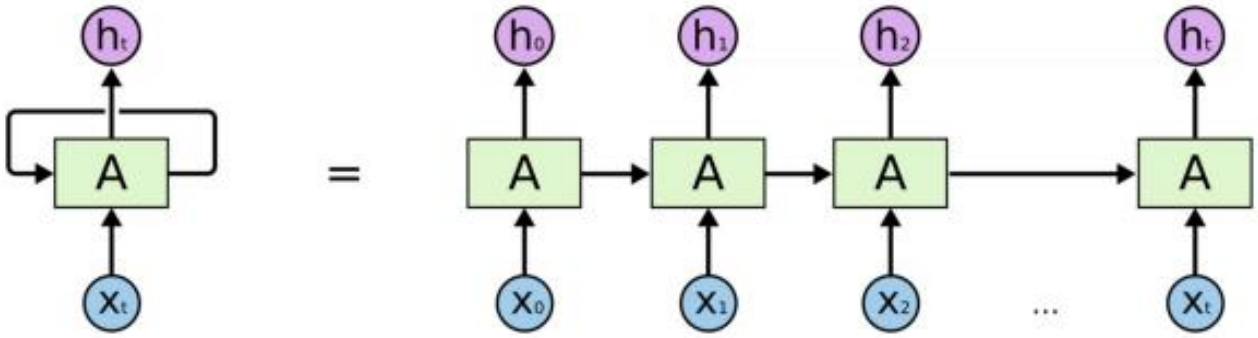


Рисунок 2.4 – RNN у розгорненні

Власне той факт, що RNN схожі на ланцюжок, говорить, що вони перебувають у тісному зв’язку із послідовностями та списками. Таким чином, RNN – найприродніша архітектура ШНМ для опрацювання таких данимх.

Упродовж останнього часу RNN успішно використовували до цілої множини завдань різного роду:

– розпізнавання мови [13];
– мовне моделювання [14];
– переклад [15];
– розпізнавання зображень [16].

Значна частина цих успіхів стосується LSTM [17] – модифікації RNN, яка у багатьох завданнях значно перевищує основну архітектуру. Фактично всі значні результати RNN досягнуто саме при застосуванні LSTM.

Що приваблює в RNN? Це те, що вони допустимо здатні зв'язувати попередні дані з біжучею задачею, для прикладу, інформація про попередній кадр відео могла б посприяти в ідеї біжучого кадру. Коли б RNN мали таку здатність, вони були б напрочуд корисні.

Іноді для реалізації біжучої задачі нам потрібна лише нещодавня інформація. Розберемо, як варіант, мовну модель, котра спробує визначити чергове слово виходячи з попередніх. Якщо стоїть завдання визначення фінального слова у реченні "човен пливе рікою", нам не потрібен ширший контекст; у разі досить явно, що ним буде "рікою". Тут, якщо відстань між актуальними даними та місцем, в котрому вона потрібна мала, RNN уміють навчитися застосуванню даних з минулого СК, рис. 2.5.

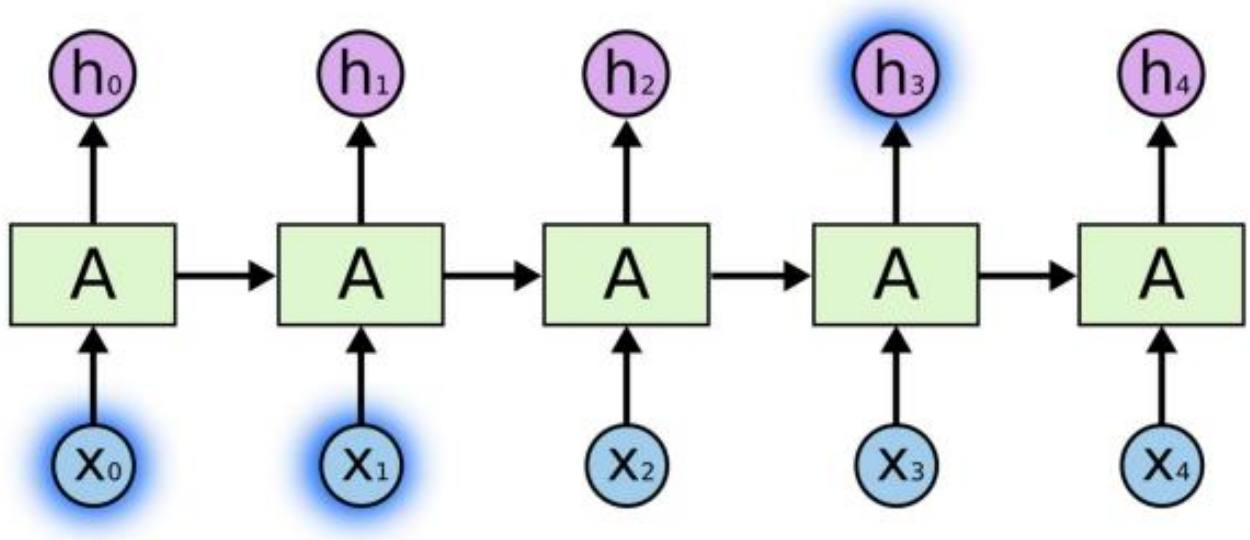


Рисунок 2.5 – Використання інформації з минулого СК

Проте можливі варіанти, коли нам потрібно більше контексту. Уявімо, що

потрібно припустити фінальне слово у такому тексті “Я зростав у Португалії... Я швидко розмовляю португальською”. Найближчий зміст припускає, що фінальним словом будитиме назва мови, проте щоб визначити котра саме, треба контекст Португалії з віддаленішого минулого СК. Тобто, невідповідність між нагальною інформацією та точкою її прикладання може бути значною.

Шкода, але з ходом збільшення цієї відстані, RNN позбуваються здібності пов'язувати інформацію, рис. 2.6.

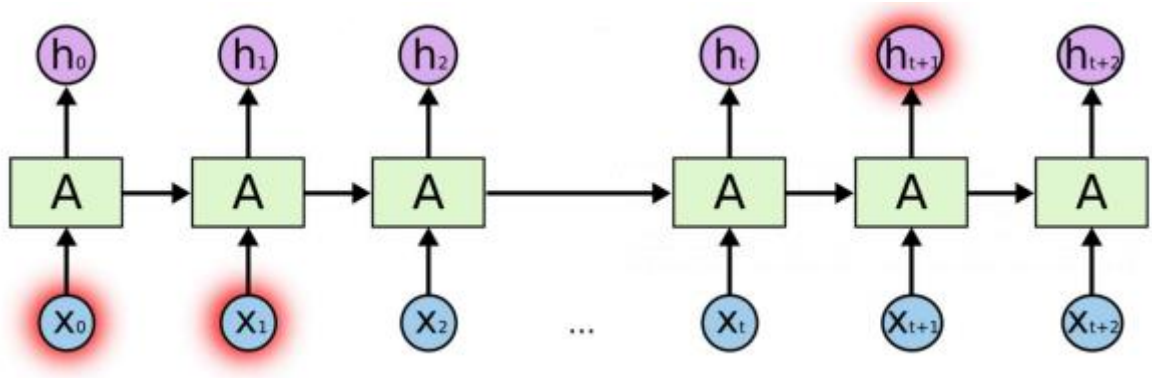


Рисунок 2.6 – Втрата здатності зв'язувати інформацію

Теоретично проблеми з опрацюванням довгострокових залежностей у RNN не мало би бути. Користувач може відповідально встановлювати атрибути ШНМ для розв’язування штучних завдань такого штибу. Проте, практично навчити RNN таким параметрам видається неймовірним.

2.2.1 LSTM

Є специфічним різновидом RNN, котрі придатні до навчання залежностей із тривалим строком. Їм вдається прекрасно вирішувати цілий набір різних задач, що дозволяє їх зараз широко застосовувати.

LSTM створені навмисно, щоб обійти проблеми довготривалої залежності. Їх традиційна поведінка якраз і полягає в запам'ятовуванні даних упродовж тривалих часових термінів.

Будь-яка RNN є ланцюжком модулів ШНМ, котрі повторюються. У традиційній RNN конструкція одного такого елемента є надзвичайно простою

(рис. 2.6), наприклад, він може бути одним шаром з ФА tanh.

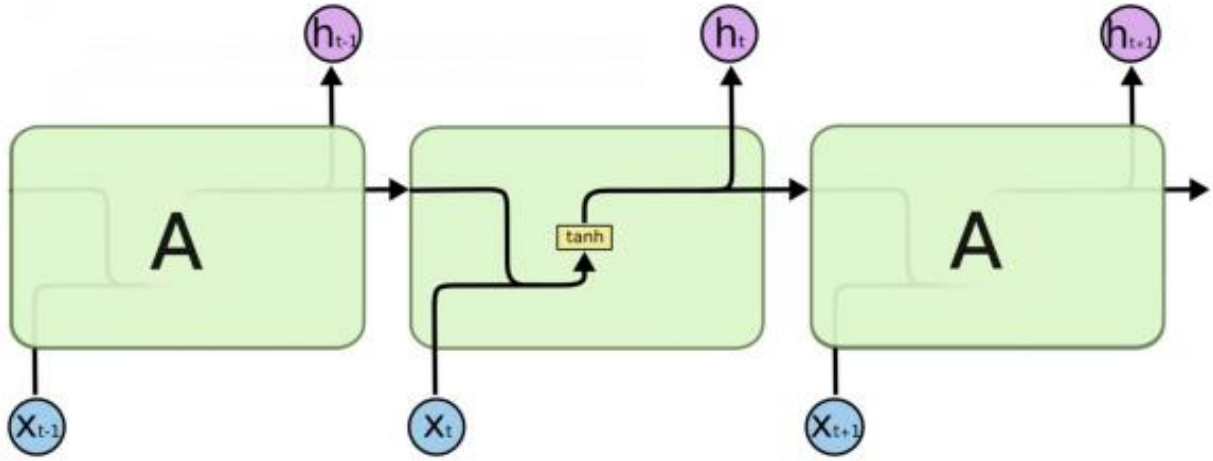


Рисунок 2.6 – Структура комірки RNN з ФА tanh

Конструкція LSTM також схожа на ланцюжок, проте модулі мають інший вигляд. Взамін одного шару ШНМ вони мають 4, і вони співпрацюють по особливому. На рис. 2.7 наведено приклад комірки LSTM. На рис. 2.8 представлені операції, що відбуваються в комірці LSTM.

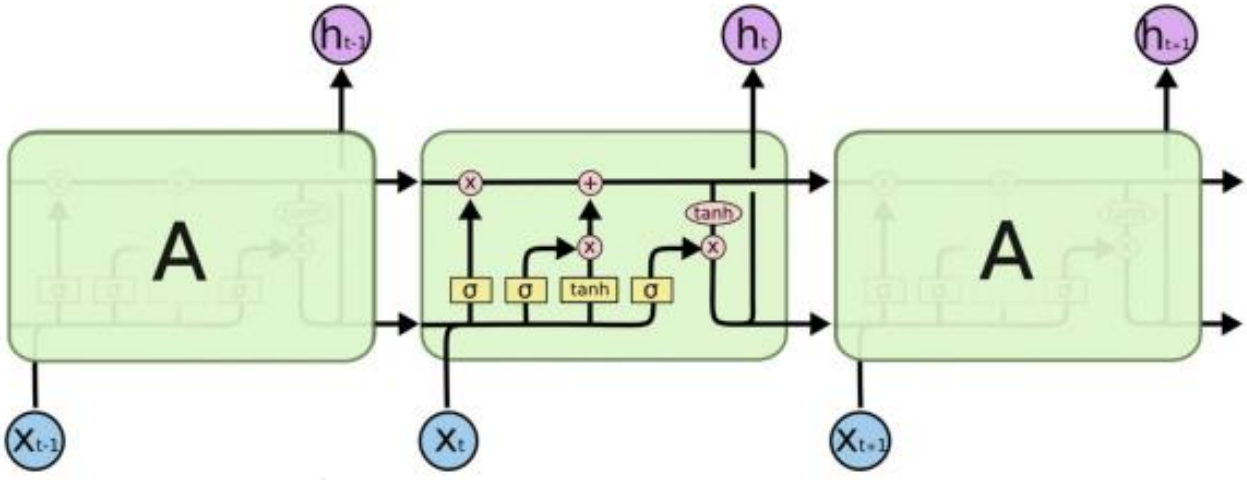


Рисунок 2.7 – Структура комірки LSTM мережі містить 4 взаємодіючі шари

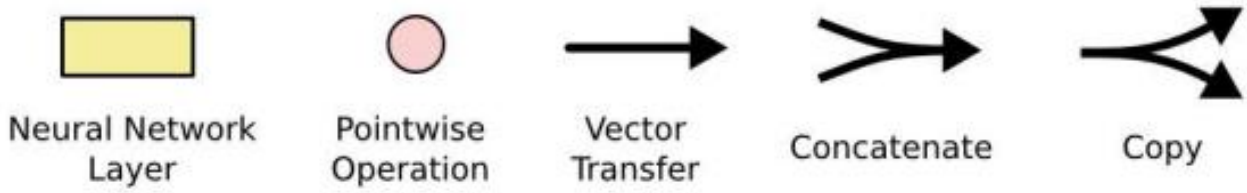


Рисунок 2.8 – Шар ШНМ; поточкова операція; векторне переміщення; об'єднання; копіювання

На рис. 2.7 кожна лінія переміщує весь вектор від властиво виходу вузла до входу вже іншого. Рожеві кружальця – це поточкові операції, такі, як додавання векторів, а прямокутники жовтого кольору - це навчені шари ШНМ. Лінії, що зводяться разом, значать об'єднання, а стрілки, котрі розходяться, свідчать про те, що інформація повторюється і репліки переміщуються до різних частин мережі.

Основна частина LSTM – це СК, позначається горизонтальною лінією, котра зображена у верхній частині рисунка. Цей СК схожий на стрічку конвеєра, рис. 2.9. Вона проходить прямо по всьому ланцюжку, і є застосованою лише до декількох лінійних перетворень. Дані спроможні легко проходити по ній, не зазнаючи змін у процесі.

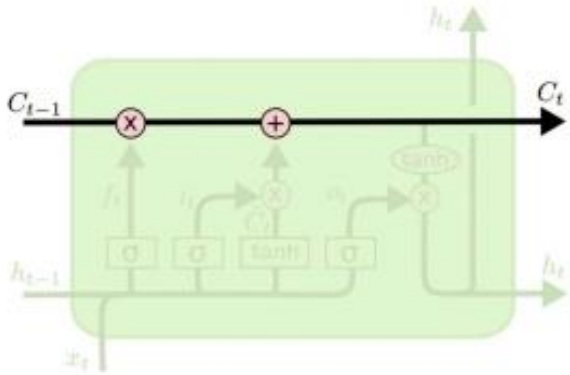


Рисунок 2.9 – СК

Тим не менш, LSTM спроможна знищувати дані зі СК; це регламентується структурами, які називаються фільтрами.

Вони дають змогу пропускати інформацію з урахуванням деяких

закономірностей, рис. 2.10. До їх складу входять шар нейронної сигмоїдної мережі та операція поточкового множення.

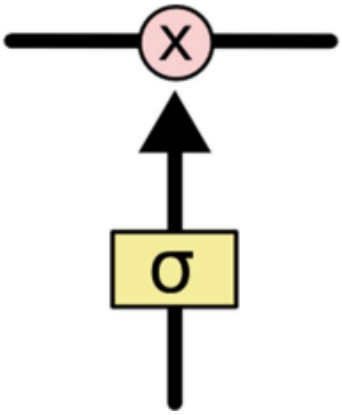


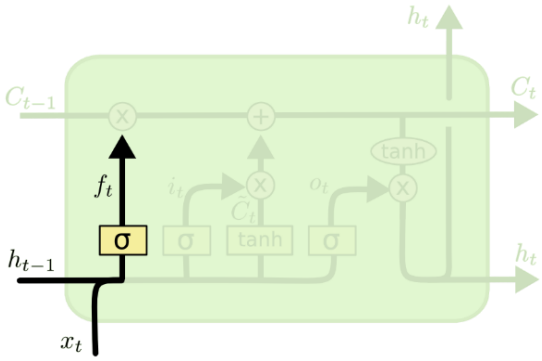
Рисунок 2.10 – Приклад фільтра в комірці LSTM

Величини від нуля до одиниці повертаються СШ. Вони позначають, який відсоток кожного блоку даних треба пропустити далі через мережу. 0 у цьому випадку відповідає за “нічого не пропускати”, 1 - “все пропустити”.

LSTM володіє трьома такими фільтрами, котрі дають змогу керувати СК.

Найпершим кроком у LSTM буде визначення, які саме дані ймовірно видалити зі СК. Відповідальність за це рішення лежить на СШ, котрий носить назву шара фільтра забування.

Цей шар опрацьовує h_{t-1} і x_t та повертає значення від 0 до 1 для кожної величини зі СК. 1 відповідає за "зберегти все повністю ", а 0 - " викинути все повністю ", рис. 2.11.

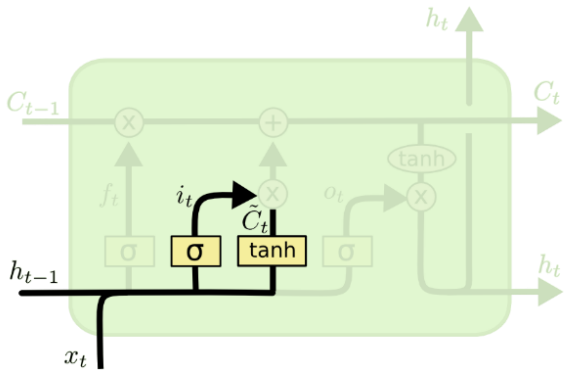


$$f_t = \sigma\left(W_f \cdot [h_{t-1}, x_t] \; + \; b_f\right)$$

Рисунок 2.11 – Шар фільтру забування

Наступним кроком буде вирішення того, яка властиво нова інформація

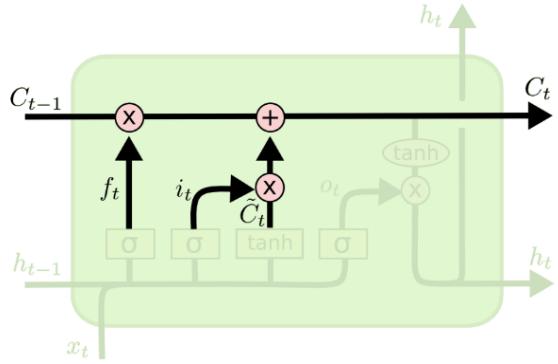
зберігатиметься у СК. Цей етап містить дві частини. Спочатку СШ, котрий носить назву шару вхідного фільтра, формулює, котрі значення підпадають під оновлення. Вподальшому tanh -шар створює вектор оновлених значень, котрі дозволено помістити до СК, рис. 2.12.



$$i_t = \sigma\left(W_i \cdot [h_{t-1}, x_t] \; + \; b_i\right)$$
$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] \; + \; b_C)$$

Рисунок 2.12 – Формування нових значень

Для переміни старого СК на новий СК, треба помножити старий СК на f_t, одночасно забуваючи про ту інформацію, котру було вирішено забути раніше. Опісля треба додати $i_t * \tilde{C}_t$. Ось це і будуть нові значення-кандидати, котрі домножені на t – на яку величину по часі потрібно оновити будь-яке значення СК, рис. 2.13.

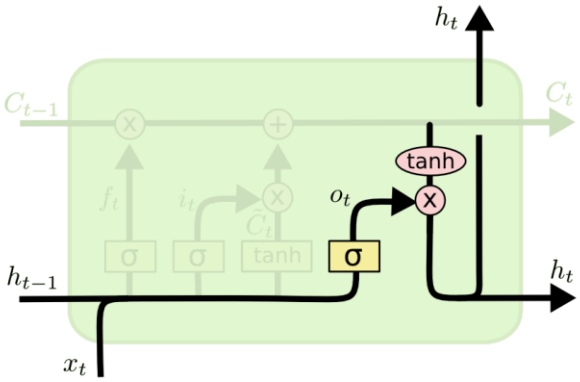


$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$

Рисунок 2.13 – Заміна старого СК

Потім потрібно з’ясувати, котру саме інформацію прагнемо одержувати на виході. Такі дані будуть базуватися на СК, до них будуть прикладені окремі фільтри. Спочатку варто використати СШ, який з’ясовує, яка саме інформація зі

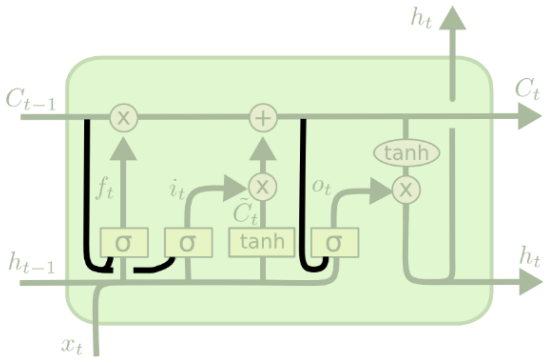
СК виводитиметься. Потім значення СК проходитимуть через tanh-шар. Це здійснюється з метою отримання на виході велчини від -1 до 1, котрі будуть перемножені з вихідними величинами СШ. Це дасть змогу виводити тільки ту інформацію, котра є необхідною, рис. 2.14.



$$o_t = \sigma\left(W_o\ [h_{t-1}, x_t]\ +\ b_o\right)$$
$$h_t = o_t * \tanh\left(C_t\right)$$

Рисунок 2.14 – Застосування СШ

Одна з найпопулярніших варіацій LSTM, описується додаванням “оглядових вічок” [18]. З їх застосуванням шари фільтрів здатні бачити СК, рис. 2.15.



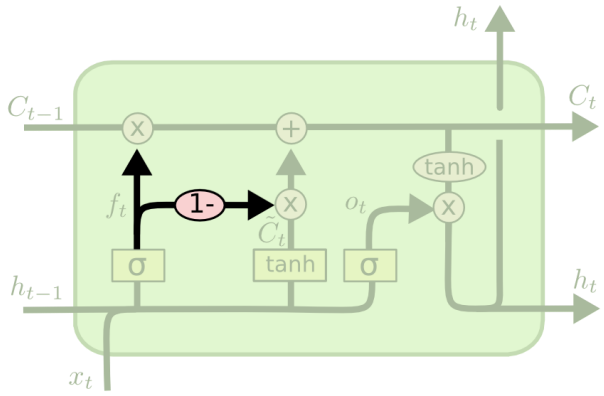
$$f_t = \sigma\left(W_f \cdot [\boldsymbol{C_{t-1}}, h_{t-1}, x_t]\ +\ b_f\right)$$
$$i_t = \sigma\left(W_i \cdot [\boldsymbol{C_{t-1}}, h_{t-1}, x_t]\ +\ b_i\right)$$
$$o_t = \sigma\left(W_o \cdot [\boldsymbol{C_t}, h_{t-1}, x_t]\ +\ b_o\right)$$

Рисунок 2.15 – Оглядові вічка

На рис. 2.15 такі “вічка” є в кожного шару, але в багатьох літературних працях вони додаються лише до деяких шарів.

Інші видозміни містять об'єднані фільтри "забуття" та вхідні фільтри. І тут рішення, котру саме інформацію варто забути, а котру - запам'ятати, ухвалюються разом. Забувається якась інформація лише тоді, коли треба

помістити на її місце що небудь. Додавання нової інформації зі СК проходить лише тоді, коли забуваємо стару, що показано на рис. 2.16.

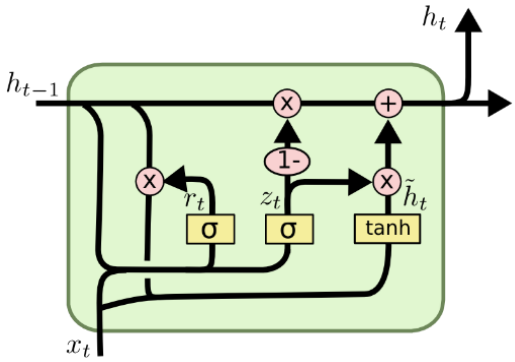


$$C_t = f_t * C_{t-1} + (\mathbf{1} - \boldsymbol{f_t}) * \tilde{C}_t$$

Рисунок 2.16 – Забування під час переписування

GRU. Такий варіант ШНМ було згадано вперше у [19]. У GRU фільтри «забуття» та входу поєднують в один фільтр «оновлення». До того ж, СК поєднується із прихованим станом.

Сформована в результаті модель є простішою, ніж стандартна LSTM, і її використання неомінно зростає, на рис . 2.17 наведено приклад комірки GRU.



$$z_t = \sigma\left(W_z \cdot [h_{t-1}, x_t]\right)$$
$$r_t = \sigma\left(W_r \cdot [h_{t-1}, x_t]\right)$$
$$\tilde{h}_t = \tanh\left(W \cdot [r_t * h_{t-1}, x_t]\right)$$
$$h_t = (1 - z_t) * h_{t-1} + z_t * \tilde{h}_t$$

Рисунок 2.17 – Комірка GRU

2.2.2 TCN

У роботі [20] було вперше запропоновано використовувати TCN для сегментації дій на основі відео.

Зазвичай процес розбивається на два етапи:

– обчислення низькорівневих ознак з використанням (найчастіше) CNN,

яка кодує просторово-тимчасову інформацію;

– введення низькорівневих ознак у класифікатор, який отримує високорівневу тимчасову інформацію за допомогою (найчастіше) RNN.

Головним недоліком такого підходу є потреба у двох окремих моделях. TCN пропонує уніфікований підхід, щоб покрити обидва рівні інформації за принципом ієрархії.

На рис. 2.18 представлена структура енкодера-декодера. Найбільш критичні питання вирішуються наступним чином: TCN може взяти ряд будь-якої довжини і на виході отримати ту саму довжину. Казуальна (casual) згортка використовується там, де є повністю згорткова одновимірна архітектура мережі. Ключовою характеристикою є те, що вихідне значення в момент часу *t* згортається лише з тими елементами, що відбулися за часом до нього.

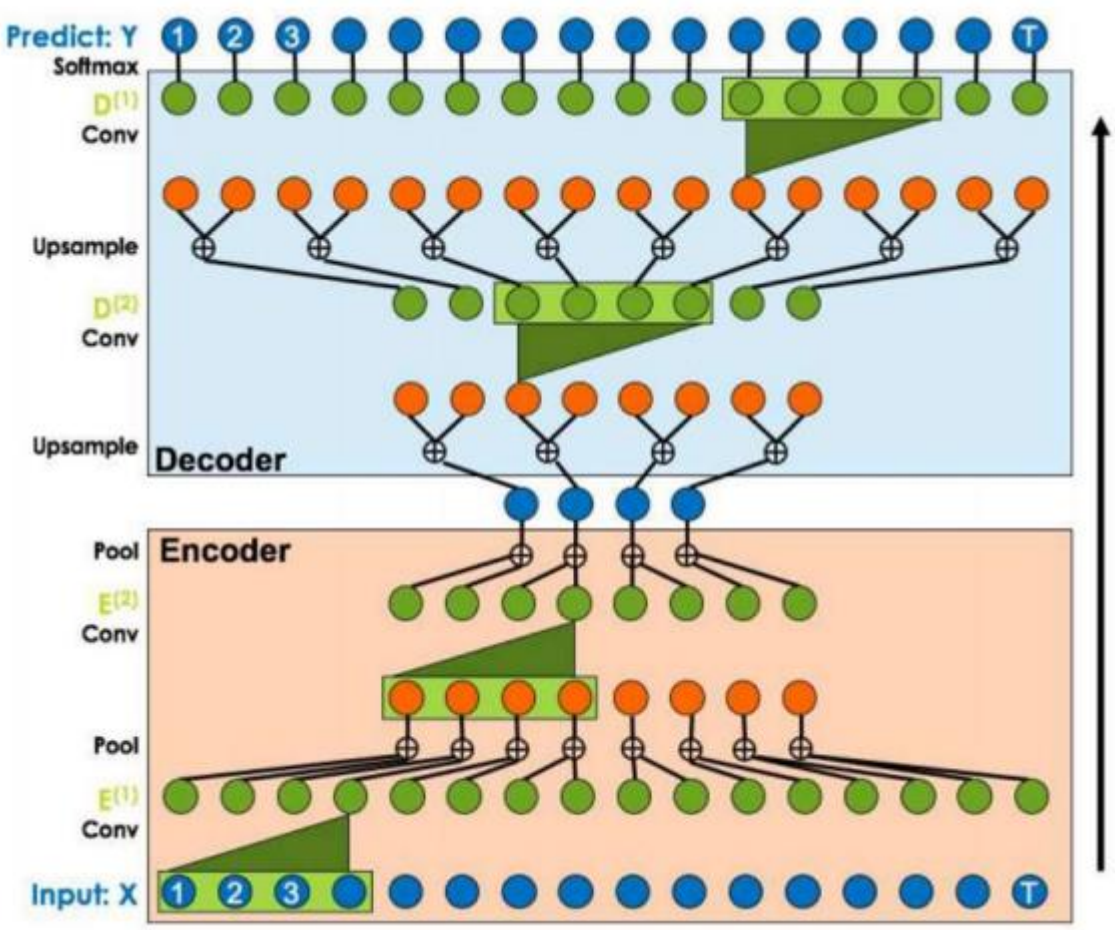
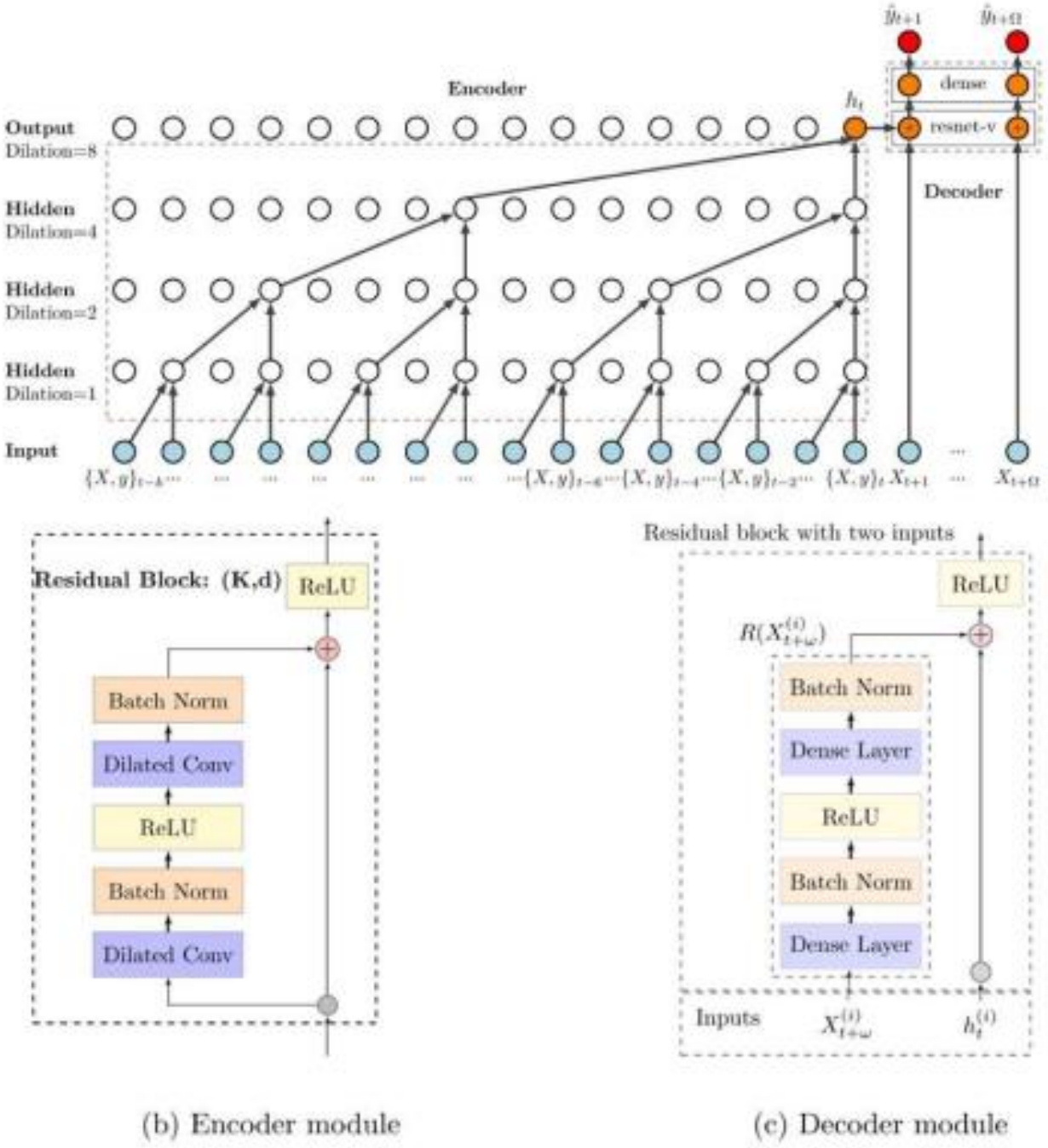


Рисунок 2.18 – Архітектура TCN

У роботі [21] показано можливість застосування TCN з метою оцінки

щільності ймовірності. Прогнозування часових рядів покращує багато сценаріїв прийняття бізнес-рішень (наприклад, управління ресурсами). Імовірнісне прогнозування дозволяє отримувати інформацію з історичних даних та мінімізувати невизначеність майбутніх подій. Коли завдання прогнозування полягає в тому, щоб передбачити мільйони пов'язаних часових рядів (як у роздрібному бізнесі), потрібні непомірно великі трудові та обчислювальні ресурси для оцінки параметрів. Щоб розв'язати ці проблеми, автори запропонували систему оцінки щільності і прогнозування з урахуванням CNN. Їхня структура може вивчити приховану кореляцію між рядами. Наукова новизна в їх роботі полягає в запропонованій ними глибокій TCN. Рис. 2.19 описує представлену архітектуру.

Реалізація модулів енкодера/декодера може допомогти в розробці прикладних великомасштабних програм.



(b) Encoder module (c) Decoder module

Рисунок 2.19 – Архітектура TCN для часових рядів

2.2.3 GAN

Є засобом для генеративного моделювання із застосуванням методів глибинного навчання.

Зі свого боку, генеративне моделювання є властиво некерованою навчальною задачею в МН, котре визначає в автоматичному режимі визначення та вивчення логіки необхідностей вхідних даних так, що модель ймовірно застосувати для формування або побудови нових моделей, котрі ймовірно

одержати з первісного набору даних.

GAN - це алгоритм МН, що входить до сімейства моделей, що породжують і побудований на комбінації з двох нейронних мереж: генеративна модель *G*, яка будує наближення розподілу даних, і дискримінативна модель *D*, котра оцінює ймовірність, що зразок прийшов з тренувальних даних, а не згенерованих моделлю *G* (рис. 2.20). Навчання для моделі *G* полягає у максимізації ймовірності помилки дискримінатора *D*. Вперше такий вид ШНМ був описаний у [22].

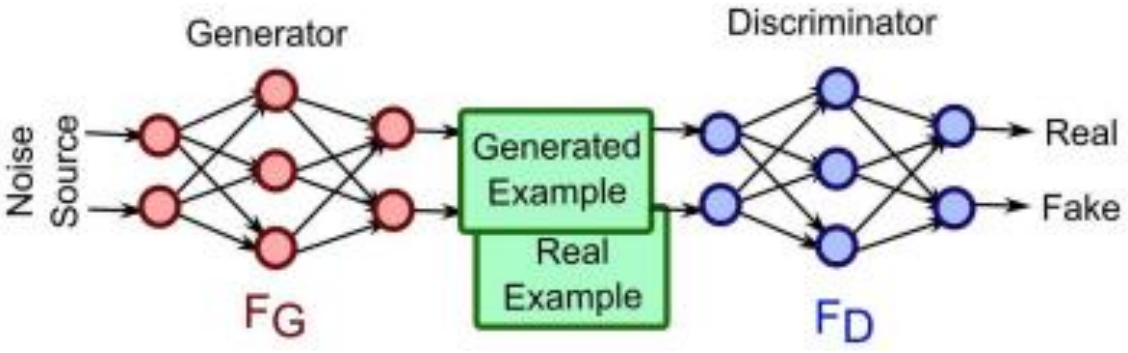


Рисунок 2.20 – Архітектура GAN

На рис. 2.21 представлена узагальнена схема GAN.

Рисунок 2.21 – Схема GAN

Розглянуті вище ШНМ мають різну архітектуру зі своїми перевагами та недоліками. У роботі ШНМ застосовуються для генерації тексту.

3 ПРАКТИЧНА ЧАСТИНА

3.1 Опис стегосистеми та технології її роботи

Традиційні лінгвістичні стегосистеми ґрунтуються на модифікації існуючого тексту обкладинки, наприклад, з використанням заміни синонімів [23, 24]. Ідея полягає в тому, щоб закодувати секретну інформацію у перетворенні тексту контейнера, не впливаючи на зміст чи граматичну правильність, тобто без лексико-семантичних помилок. Прикладом такої системи є CoverTweet [25], стегосистема модифікації контейнера, яку використовує Твіттер як засіб приховування.

Модифікація контейнера може призвести до синтаксичної та семантичної неприродності [26], для вирішення цієї проблеми автори роботи запропонували альтернативну стегосистему, в якій людина генерує стеготекст вручну, тим самим покращуючи лінгвістичну природність за рахунок людських зусиль.

У нашій роботі використовуються різні варіації RNN та тимчасових згорткових нейронних мереж, оскільки вони пропонують кращу якість у галузі генерації тексту [27].

Одна із можлививх варіацій ШНМ наведена на рис. 3.1.

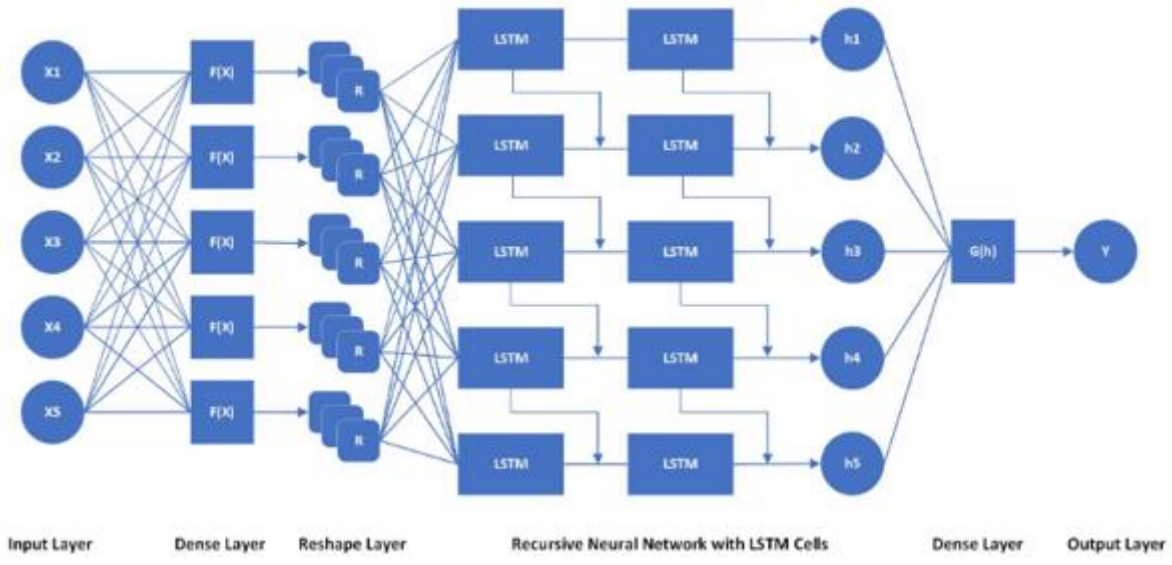


Рисунок 3.1 – Формування RNN з LSTM клітинами

Пропонується автоматично генерувати стеготекст з ШНМ, навченої завдання мовного моделювання. Неформально кажучи, метою моделювання мови є розрізнення можливих (імовірних) або неможливих (малоймовірних) ланцюжків слів у цій мові. Висновок ШНМ потім може бути використане безпосередньо як стеготекст.

Загальна технологія роботи стегосистеми представлена таким чином:

1. Навчання нейронної мережі для завдання мовного моделювання (набір текстових даних).

2. Перетворення секретного повідомлення, заданого відправником, на булевий вектор $S=x_1\ x_2 \ldots x_n$, де $x_i \in \{0,1\}$.

3. Побудова ключ-таблиці, яка ставить у відповідність бітовим блокам B_i набір токенів, тобто підмножина слів зі словника предметної області.

4. Генерація стеготексту $a = a_1 \ldots a_m$.

Секретний булевий вектор S розбивається на блоки з довжиною, котра відповідає довжині бітових блоків ключ-таблиці: $S=b_1\ b_2 \ldots b_m$,.

Поки не закінчився секретний булевий вектор S виконується таке:

5. Береться черговий блок b_i секретного булевого вектора S. Вибирається бітовий блок B_i ключ-таблиці, що збігається з ним. Цьому блоку B_i ключ-таблиці відповідає кошик W_{Bi} (набір токенів), з якого і вибирається чергове слово стеготексту. Для цього на основі поточного підслова $a_1 \ldots a_{i-1}$ за допомогою ШНМ генерується найбільш ймовірне продовження $a_i \in W_{Bi}$ Передача стеготексту одержувачу;

6. Вилучення прихованого повідомлення

– на основі ключ-таблиці, якою володіє одержувач, кожне слово (токен) зі стеготексту перетворюється на відповідний йому бітовий блок у ключ-таблиці;

– повторюємо перший крок до закінчення токенів стеготексту;

– секретний булевий вектор, що вийшов, перетворюється на вихідне секретне повідомлення.

3.2 Навчання нейромережі для завдання мовного моделювання

Навчання ШНМ відбувається наступним чином:

– береться текст із набору даних і розбивається на слова;

– на вхід нейронної мережі подається перше слово з тексту і вона вчиться передбачати друге слово;

– на вхід ШНМ подається два перші слова і вона вчиться передбачати третє;

– процес повторюється поки що у тексті є слова, які можна передбачити;

– здійснюється перехід до наступного тексту з набору даних та мережа продовжує навчання.

3.3 Перетворення секретного повідомлення (заданого відправником) на бітову послідовність

Секретні дані – це інформація, котру потрібно приховати. По-перше, секретні дані стискаються, або шифруються в секретний булевий вектор S. По-друге, S ділиться на менші бітові блоки довжиною $|B|$, у результаті виходить $|S| / |B|$ бітових блоків.

3.4 Побудова ключ-таблиці

Використовують ключ-таблицю відправник та одержувач разом спільно. Вона зіставляє бітові блоки з наборами токенів і стегоконтейнер будується таким чином:

– отримуємо словник V, який є набором всіх можливих токенів, котрі можуть з'явитися в стеготексті;

– токени, зазвичай, є словами, але також можуть бути розділовими знаками. Словник поділяється на $2^{|B|}$ кошиків, тобто набори токенів, що не перетинаються, випадково обрані зі словника без заміни;

– кожен токен з'являється рівно в одному кошику, і кожен кошик містить $|V| / 2^{|B|}$ токена. Далі кожному бітовому блоку зіставляється кошик, що позначається W_B .

3.5 Генерація стеготексту

Для генерації стеготексту використовується ШНМ лише на рівні слів для моделювання мовної моделі. Для приховування бітового рядка S, що містить секретне повідомлення, розглядається по одному бітовому блоку $|B|$ за раз, і нейронна мережа вибирає один токен з кошика W_B; отже, стеготекст-кандидат містить стільки токенів, скільки кількість бітових блоків в S.

3.6 Передача стеготексту одержувачу

Для передачі стеготексту одержувачу можуть використовуватися різні засоби, наприклад, якщо ми генеруємо стеготекст на основі набору даних зібраних з твіттера, то він може бути опублікований у цій соціальній мережі, аналогічно якщо ми генеруємо стеготекст на основі даних поштових повідомлень, то він може бути переданий засобами електронної пошти.

3.7 Вилучення прихованого повідомлення

Алгоритм вилучення відновлює вихідні дані наступним способом:

– приймає як вхідні дані згенерований стеготекст;
– розглядає по одному токену за раз;
– знаходить кошик токена в ключ-таблиці;
– відновлює вихідний бітовий блок.

Отримана послідовність біт може бути розшифрована та/або розтиснута в залежності від умов формування секретного повідомлення

3.8 Метрики оцінки

У роботі використовується перплексія (perplexity) для кількісної оцінки якості стеготексту та пропускна спроможність (capacity, тобто кількість захованих біт на слово стеготексту) для кількісної оцінки ефективності стегоконтейнера як каналу передачі секретної інформації.

Перплексія є стандартною метрикою якості мовних моделей [30] та визначається як середнє значення логарифмічної ймовірності кожного слова у наборі даних [31]:

$$Perp(W) = e^{-\frac{1}{N*\sum_i \ln(p[w_i])}}, \quad (3.1)$$

де W - множина всіх слів, w_i - ймовірність слова, N - кількість слів у наборі даних.

У нашому випадку не можна використовувати цю метрику як є: оскільки ймовірність $p[w_i] = 0$ для слів w_i не з набору даних W_B і відповідний $ln(p[w_i])$ стає невизначеним в цьому випадку.

Натомість вимірюється ймовірність w_i як середнє значення $p[w_i]$ по всіх можливих секретних бітових блоках у припущенні, що бітові блоки розподілені рівномірно. За законом великих чисел [32], якщо виконується множина випробувань з генерації стеготексту з використанням різних випадкових секретних даних як вхідні дані, ймовірність P кожного слова буде прагнути до очікуваному значенню $\frac{\sum p[w_i,B]}{2^{|B|}}$, отже, можна встановлювати $p[w_i] = \frac{p[w_i,B]}{2^{|B|}}$ замість $p[w_i] = 0$ для w_i, що не належать W_B.

Найменша перплексія вказує на найкращу модель.

Пропускна здатність нашої системи – це кількість зашифрованих бітів на вихідне слово. Пропускна здатність завжди $|B|$ біт/слово (оскільки кожен бітовий блок розміром $|B|$ завжди відображається в одне вихідне слово).

Пропускна здатність нашої стегосистеми - це кількість прихованих бітів на

вихідне слово. Пропускна здатність дорівнює $|B|$ біт/слово, оскільки кожен бітовий блок розміром $|B|$ завжди відображається в одне слово стеготексту.

3.9 Набори даних

Твіти та електронні листи є досить популярними засобами спілкування і, отже, забезпечують широкі можливості приховування інформації. Таким чином, ШНМ навчаються на цих даних, тобто на повідомленнях з Твіттера та електронних листів Enron [28], які сильно відрізняються за довжиною повідомлень та розміром словника. Також у роботі використовувався набір даних Penn -tree bank [33], який зазвичай використовується завдання автоматичної морфологічної розмітки.

Для Твіттера використовувався токенізатор NLTK для перетворення твітів [29] у слова та розділові знаки. Вміст нормалізується, заміняться ім'я користувача та URL -адреси на маркер імені користувача (<user>) та маркер URL -адреси (<url>) відповідно. Використано 600 тисяч твітів із загальним обсягом 45 мільйонів слів та словниковим запасом розміром 225 тисяч.

Для набору даних Enron очищені та вилучені тіла повідомлень електронної пошти. Було взято 500 тисяч листів отриманих повідомлень із 16,8 мільйонами токенів та обсягом словника 406 тисяч.

Для набору даних Penn-tree bank використовувалася стандартна передобробка текстових даних.

3.10 Результати експериментів

Були оцінені результуючі повідомлення, що згенеровані різними моделями нейронних мереж для 1 (не стеганографічний варіант), 2, 4, 8 кошиків. У табл. 3.1 показано взаємозв'язок між пропускною здатністю (біт на слово) та кількісною якістю тексту (перплексія).

Таблиця 3.1 – Аналіз нейромережевих архітектур для генерації стеготекстів

Нейронна мережа	Кількість кошиків	Пропускна здатність	Перплексія
RNN	1	0	147
	2	1	211
	4	2	408
	8	3	858
LSTM	1	0	134
	2	1	190
	4	2	381
	8	3	833
GRU	1	0	134
	2	1	185
	4	2	377
	8	3	824
TCN	1	0	131
	2	1	181
	4	2	369
	8	3	801

Зазначимо деякі цікаві з практичної точки зору нюанси роботи з повідомленнями твіттера під час генерації стеготексту.

Наприклад, у згенерованому стеготексті тег <user> замінений на фіктивне ім'я користувача більш реалістичного подання у табл. 3.2. Також можна замінювати токени <user>, випадковим чином вибираючи передплатників відправника цього твіта. Повторний твіт повідомлень, що починається з тега

“RT”, може викликати проблеми, оскільки можна буде легко перевірити, чи існує вихідне повідомлення по повідомленню, що пересилається. При цьому слід виключати повідомлення з тегом "RT" із навчальної вибірки (або при генерації стеготексту). Оскільки на етапі попередньої обробки всі твіти переведені в нижній регістр, можна проводити післяобробку згенерованого стеготексту, щоб поліпшити його адекватність.

3.11 Приклад апробації технології роботи стегосистеми

1. Навчання нейронної мережі LSTM (100 прихованих шарів) на наборі текстових даних Penn-tree bank (250 тисяч речень, 7 мільйонів слів, 10 тисяч токенів розмір словника).
2. Відправник поставив секретне повідомлення "me". Воно перетворюється на бітову послідовність - 01101101 01100101 (ASCII код).
3. Виконується побудова ключ-таблиці з розміром кошика – чотири та ємністю – два (табл. 3.2).

Таблиця 3.2 – Приклад ключ-таблиці

Бітовий блок	Токени
00	This, am, weather, other, old, little, do, way, ...
01	was, attaching, today, new, heat, large, “.”, art, ...
10	I, better, an, dog, good, big, whole, kit, person, ...
11	great, than, NDA, high, long, free, time, end, ...

4. Генерація стеготексту в 8 ітераціях (табл. 3.3).

Таблиця 3.3 – Згенерований стеготекст

Рядок бітів	01	10	11	01	01	10	01	01
Токен	today	I	end	new	large	kit	heat	.

5. Передача стеготексту (табл. 3.4) одержувачу.

6. Вилучення прихованого повідомлення

– на основі ключ-таблиці (табл. 3.2) вибираємо токен "today", якому відповідає бітовий блок "01";

– повторюємо перший крок 8 ітерацій, формуючи бітову послідовність - 01101101 01100101;

– бітову послідовність перетворюємо на вихідне секретне повідомлення - «me».

Таким чином, у цьому розділі описані деталі апробації створеної стегосистеми та проведено порівняльний аналіз нейромережевих моделей для генерації стеготексту. Крім того, продемонстровано працездатність стеганосистеми, що показує, що нейромережеві моделі створюють реалістичні повідомлення, приховуючи інформацію. При цьому показники перплексії дають змогу дійти висновку, що різні апробовані архітектури нейронних мереж показали не значні відмінності результатів щодо адекватності генерованого стеготексту.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Стихійні лиха та їх класифікація

Стихійні дії сил природи, поки що не повною мірою підвладні людині та щорічно завдають державі і населенню величезних збитків. Стихійні лиха - це такі явища природи, що викликають екстремальні ситуації, порушують нормальну життєдіяльність населення, роботу безлічі об'єктів. Стихійні лиха є трагедією для будь-якої держави. Через стихійні лиха страждає економіка країни, бо при цьому руйнуються виробничі підприємства, знищуються матеріальні цінності, гинуть люди.

Стихійні лиха - небезпечні природні явища, як правило раптового походження, хоча іноді і прогнозовані за допомогою метеорогогії, але на інтенсивність яких люди впливати не можуть. Їх можна класифікувати: за швидкістю переміщення - землетруси, зсуви, цунамі, снігопади, ожеледі - швидкі; підвищення рівня води в ріках через інтенсивні опади або танення снігу, льоду (повіні), звільнення внутрішньої енергії Землі, виверження вулканів - повільні. Часто виникають потужні, високошвидкісні потоки повітря через швидкий перепад значень атмосферного тиску (урагани, смерчі і т.п.). Стихійні лиха речовинного характеру можуть ініціювати виникнення різноманітних полів, які негативно впливають на здоров'я, самопочуття людини. [34].

Стихійні явища часто виникають в комплексі, що значно посилює їх негативний вплив. Небезпечні природні явища визначаються трьома основними групами процесів - ендогенні, екзогенні та гідрометеорологічні.

Стихійні лиха, які характерні для України, за структурою можна поділити на прості, що включають один елемент - наприклад, сильний вітер, зсув або землетрус та складні. Вони складаються з декількох процесів однієї групи або кількох груп. Найбільші збитки спричиняють повені - 40%, на другому місці - циклони (20%), на третьому - посухи та землетруси (15%). Деякі стихійні лиха (пожежі, обвали, зсуви і навіть землетруси) можуть виникати в результаті дій самих людей, тобто мають антропогенне походження, але наслідки їх завжди є

діями сил природи. Для кожного стихійного лиха характерна наявність властивих йому вражаючих чинників, що несприятливо впливають на стан здоров'я, життя людини [35].

Причинами стихійних лих можуть бути:

– швидке переміщення речовини (землетрусу, зсуви);

– вивільнення внутриземної енергії (вулканічна діяльність, землетруси);

– підвищення рівня вод річок, ставків і морів (повені, цунамі);

– вплив надзвичайно сильного вітру (урагани, торнадо, циклони).

Важливо своєчасно провести роботи, спрямовані на локалізацію природного лиха, щоб зменшити зони руйнувань, звести до мінімуму кількість загиблих та постраждалих.

В Україні найчастіше спостерігаються такі надзвичайні ситуації природного характеру:

– небезпечні геологічні явища (зсуви, обвали, осипки, просадки земної поверхні);

– небезпечні метеорологічні явища (зливи, урагани, сильні снігопади, сильний град, ожеледь);

– небезпечні гідрологічні явища (повені, паводки);

– природні пожежі лісових та торф’яних масивів;

– масові інфекції та хвороби людей, тварин, рослин.

В останні роки кількість стихійних лих в Україні та в світі в цілому значно збільшилася. Найчастіше в Україні виникають такі природні катастрофи як землетруси, повені, посухи (на Півдні України), лісові пожежі в літню пору року, снігові замети, зсуви поверхні.

Є серйозні підстави вважати, що масштабність впливу лиха й катастроф на соціальні, економічні, політичні та інших процесів сучасного нашого суспільства та їх драматизм вже перевищили такий рівень, який дозволяв ставитися до них як до локальних збоїв у розміреному функціонуванні державних та громадських структур [34].

Отже, перед людиною та громадськістю в XXI в. вимальовується нова мета - глобальна безпека. Досягти цього можна, в першу чергу, за допомогою зміни

світогляду людини, а також покращення системи профілактичних заходів у боротьбі зі стихійними лихами, а саме: вдосконалення рятувальних служб та рятувальної техніки, проведення попереджувальних заходів та пропагандистської роботи з громадянами щодо правил поведінки та дій під час стихійних лих. Це допоможе в майбутньому зменшити кількість загиблих та постраждалих від природних катастроф, а також зменшить матеріальні збитки, що були завдані стихійним лихом.

Природні лиха з часом нікуди не зникнуть. Будуть виникати землетруси в геологічно активних районах, будуть виникати повені, а штормові припливи стануть, раз у раз затопляти морські узбережжя, не обійдеться і пожеж. Людина безсила запобігти природним процесам, але тільки в наших силах зменшити кількість жертв і матеріальних втрат.

4.2 Соціальне значення охорони праці

Соціальне значення охорони праці полягає в сприянні росту ефективності суспільного виробництва шляхом безперервного вдосконалення і поліпшення умов праці, підвищення їх безпеки, зниження виробничого травматизму і профзахворювань [36]. Соціальне значення охорони праці проявляється в зростанні продуктивності праці, збереженні трудових ресурсів і збільшенні сукупного національного продукту.

Охорона праці полягає в сприянні росту ефективності виробництва, яке досягається шляхом безперервного вдосконалення і поліпшення умов праці, підвищення їх безпеки, зниження виробничого травматизму і профзахворювань.

Зростання продуктивності праці відбувається в результаті збільшення фонду робочого часу завдяки скороченню внутрішньо-змінних простоїв шляхом ліквідації мікротравм або зниження їх кількості, а також завдяки запобіганню передчасного стомлення шляхом раціоналізації і покращення умов праці та введенню оптимальних режимів праці і відпочинку та інших заходів, які сприяють підвищенню ефективності використання робочого часу.

Важливим питанням є зростання продуктивності праці, яка відбувається в

результаті збільшення фонду робочого часу завдяки скороченню внутрішньозмінних простоїв шляхом ліквідації мікротравм або зниження їх кількості, а також завдяки запобіганню передчасного стомлення шляхом раціоналізації і покращення умов праці та введенню оптимальних режимів праці і відпочинку та інших заходів, які сприяють підвищенню ефективності використання робочого часу [36].

Особливої уваги заслуговує те, що збереження трудових ресурсів і підвищення професійної активності працюючих відбувається завдяки покращенню стану здоров’я і подовженню середньої тривалості життя шляхом покращення умов праці, що супроводжується високою трудовою активністю і підвищенням виробничого стажу. Підвищується професійний рівень також завдяки зростанню кваліфікації і майстерності. Відповідно і збільшення сукупного національного продукту відбувається завдяки покращенню вищеперелічених показників та їх складових компонентів [29]. Збереження трудових ресурсів і підвищення професійної активності працюючих відбувається завдяки покращенню стану здоров'я і подовженню середньої тривалості життя шляхом покращення умов праці, що супроводжується високою трудовою активністю і підвищенням виробничого стажу. Підвищується професійний рівень також завдяки зростанню кваліфікації і майстерності. Збільшення сукупного національного продукту відбувається завдяки покращенню вищеперелічених показників та їх складових компонентів. Крім того, соціальне значення охорони праці проявляється в зростанні продуктивності праці, збереженні трудових ресурсів.

Комплекс заходів з поліпшення умов праці може забезпечити приріст продуктивності праці на 15-20%. Так, нормалізація освітлення робочих місць збільшує продуктивність на 6-13% та скорочує брак на 25%. Раціональна організація робочого місця підвищує продуктивність праці на 21%, раціональне фарбування робочих приміщень – на 25% [37]. Збільшення ефективного фонду робочого часу може бути досягнуто за рахунок скорочення тимчасової непрацездатності працівників внаслідок хвороб та виробничого травматизму.

ВИСНОВКИ

Враховуючи зростаючий інтерес до застосування ШНМ для різних прикладних завдань, включаючи завдання інформаційної безпеки, з'являються спроби застосування нейромереж і в такій перспективній галузі, як стеганографія. Однак, досі не до кінця зрозумілі прикладні аспекти застосування нейронних мереж для подібних завдань, їхня вдала архітектура, а також ключові показники ефективності таких рішень. Ця робота спрямовано деяке усунення цих неуточнених моментів.

В результаті виконаної роботи реалізована стеганосистема з контейнером у вигляді тексту. в основі якої лежить ШНМ. Експериментально продемонстровано, що нейромережеві мовні моделі створюють реалістичні тексти та добре приховують інформацію.

Порівняно з деякими іншими стеганографічними системами, реалізована система має перевагу в пропускній здатності (від близько 2 біт на слово), що робить її більш застосованою на практиці.

Надалі слід оцінити безпеку розглянутої стегосистеми щодо різних методів стегоаналізу. Ще одним напрямом майбутніх досліджень є створення стеготекстів, персоналізованих для певного типу користувачів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Jordan M. I., Mitchell T. M. Machine learning: Trends, perspectives, and prospects //Science. – 2015. – Т. 349. – №. 6245. – С. 255-260.

2. Гбур З. В. Використання штучного інтелекту в інформаційній безпеці України. Державне управління: удосконалення та розвиток. 2022. № 1. – [Електронний ресурс] - Режим доступа: http://www.dy.nayka.com.ua/ ?op=1&z=2601 (дата звернення: 14.04.2023).

3. Управління інформаційною безпекою: конспект лекцій : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: Носок С.О., Фаль О.М., Ткач В.М. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

4. Федотова-Півень І., Тарасенко Я. Шляхи задоволення потреб сучасної кібербезпеки в рамках протидії методам комп'ютерної лінгвістичної стеганографії // Безпека інформації, №23(3), с. 190-196, 2017.

5. Meng P., Hang L., Chen Z., Hu Y., Yang W., «STBS: A Statistical Algorithm for Steganalysis of Translation-Based Steganography», 12th International Conference «Information Hiding», Calgary, Canada, June 28-30, Vol. 6387, pp. 208-220, 2010.

6. Стеганографія : навчальний посібник / Кузнецов О. О., Євсеєв С. П., Король О. Г. – Х. : Вид. ХНЕУ, 2011. – 232 с.

7. Xiang L. et al. Novel linguistic steganography based on character-level text generation //Mathematics. – 2020. – Т. 8. – №. 9. – С. 1558.

8. Niu Y. et al. A hybrid r-bilstm-c neural network based text steganalysis //IEEE Signal Processing Letters. – 2019. – Т. 26. – №. 12. – С. 1907-1911.

9. Bao Y. J. et al. Text Steganalysis with Attentional L STM-CNN //2020 5th International Conference on Computer and Communication Systems (ICCCS). – IEEE, 2020. – С. 138-142.

10. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain //Psychological review. – 1958. – Т. 65. – №. 6. – С. 386

11. Hecht-Nielsen R. Theory of the backpropagation neural network //Neural networks for perception. – Academic Press, 1992. – С. 65-93.

12. Medsker L., Jain L. C. (ed.). Recurrent neural networks: design and applications. – CRC press, 1999.

13. Graves A., Mohamed A., Hinton G. Speech recognition with deep recurrent neural networks //2013 IEEE international conference on acoustics, speech and signal processing. – Ieee, 2013. – С. 6645-6649.

14. Sundermeyer M., Schlüter R., Ney H. LSTM neural networks for language modeling //Thirteenth annual conference of the international speech communication association. – 2012.

15. Venugopalan S. et al. Translating videos to natural language using deep recurrent neural networks //arXiv preprint arXiv:1412.4729. – 2014.

16. Liang M., Hu X. Recurrent convolutional neural network for object recognition //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2015. – С. 3367-3375.

17. Hochreiter S., Schmidhuber J. Long short-term memory //Neural computation. – 1997. – Т. 9. – №. 8. – С. 1735-1780.

18. Gers F. A., Schmidhuber J. Recurrent nets that time and count //Proceedings of the IEEE-INNS-ENNS International Joint Conference on Neural Networks. IJCNN 2000. Neural Computing: New Challenges and Perspectives for the New Millennium. – IEEE, 2000. – Т. 3. – С. 189-194.

19. Cho K. et al. Learning phrase representations using RNN encoder-decoder for statistical machine translation //arXiv preprint arXiv:1406.1078. – 2014.

20. Lea C. et al. Temporal convolutional networks: A unified approach to action segmentation //European Conference on Computer Vision. – Springer, Cham, 2016. – С. 47-54.

21. Yan J. et al. Temporal convolutional networks for the advance prediction of ENSO //Scientific reports. – 2020. – Т. 10. – №. 1. – С. 1-15.

22. Goodfellow I. et al. Generative adversarial nets //Advances in neural information processing systems. – 2014. – Т. 27.

23. Topkara U., Topkara M., Atallah M. J. The hiding virtues of ambiguity: quantifiably resilient watermarking of natural language text through synonym

substitutions //Proceedings of the 8th workshop on Multimedia and security. – 2006. – С. 164-174.

24. Chang C. Y., Clark S. Practical linguistic steganography using contextual synonym substitution and a novel vertex coding method //Computational linguistics. – 2014. – Т. 40. – №. 2. – С. 403-448.

25. Wilson A., Blunsom P., Ker A. D. Linguistic steganography on twitter: hierarchical language modeling with manual interaction //Media Watermarking, Security, and Forensics 2014. – International Society for Optics and Photonics, 2014. – Т. 9028. – С. 902803.

26. Grosvald M., Orgun C. O. Free from the Cover Text: A Human-generated Natural Language Approach to Text-based Steganography //J. Inf. Hiding Multim. Signal Process. – 2011. – Т. 2. – №. 2. – С. 133-141.

27. Sutskever I., Martens J., Hinton G. E. Generating text with recurrent neural networks //ICML. – 2011.

28. Zhou Y. et al. Strategies for cleaning organizational emails with an application to enron email dataset //5th Conf. of North American Association for Computational Social and Organizational Science. – 2007. – №. 0621303.

29. Loper E., Bird S. Nltk: The natural language toolkit //arXiv preprint cs/0205028. – 2002.

30. Daniel J., James H. M. Speech and language processing. – 2000.

31. Jozefowicz R. et al. Exploring the limits of language modeling //arXiv preprint arXiv:1602.02410. – 2016.

32. Révész P. The laws of large numbers. – Academic Press, 2014. – Т. 4.

33.Marcus M., Santorini B., Marcinkiewicz M. A. Building a large annotated corpus of English: The Penn Treebank. – 1993.

34. Стеблюк М.І. Цивільна оборона: Підручник. – Знання, 2006. – 487 с.

35. Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навч. посібник. – 2011. – 215 с.

36. Агєєв Є .Я. Основи охорони праці: Навчально-методичний посібник для самостійної роботи– Львів: «Новий Світ – 2000», 2009. – 404 с.

37. Основи охорони праці: Підручник.; 3-те видання / За ред. Ткачука К. Н. – К.: Основа, 2011. – 480 с.