ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ФРАНКА
ФАКУЛЬТЕТ ПРИКЛАДНОЇ МАТЕМАТИКИ ТА ІНФОРМАТИКИ
КАФЕДРА ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

КУРСОВА РОБОТА

на тему:

# Аналіз атак на лінійні моделі машинного навчання

студента III курсу
групи ПМп-31
Середовича Віктора

Науковий керівник:
доцент Ю.А.Музичук

Завідуючий кафедри
обчислювальної математики
проф.

Львів — 2020

# Зміст

# Розділ 1

# Вступ

Машинне начання та штучний інтелект активно використовується у різних областях нашого життя, та допомагає у вирішенні таких задач як розпізнавання дорожніх знаків, облич, визначення ризику захворювання та багато іншого. А з поширенням його використання, також збільшуєтья і ризик нападів зловмисників на ці алгоритми, що може привести, до трагічних наслідків. Тому варто досліджувати тему нападів на алгоритми машинного навчання, та знати як захистити свою модель.

В межах теми цієї роботи будуть розглядатись різні атаки на лінійні моделі машинного начання, та методи їх захисту.

## 1.1 Постановка задачі

*Мета* даної роботи полягає у тому, щоб дослідити ефективність атак на лінійні моделі машинного навчання, та визначити методи захисту від них.

Виходячи з мети, визначені завдання роботи:

- Практична реалізація та дослідження методів атак
- Визначення методів захисту

# Розділ 2

# Класифікація атак

## 2.1 Цілеспрямовані атаки

Основна частина даної роботи полягала у написанні програми. Нижче наводимо основний алгоритм її роботи, на мові C:

```
% ========================================== %
#include &lt;stdio.h&gt;
int main()
{
printf("Hello, world!\n");
return 0;
}

```

[language=Python]

```
    def fit(self, X, w, b, y, alpha, max_iters, predict_func):
# Check that X and y have correct shape
self.w = w
self.b = b

self.y_ = np.expand_dims(y.T, axis=1)
self.X_ = X.T

self.num_iters = 0
```

## 2.2 Нецілеспрямовані атаки

Основна частина даної роботи полягала у написанні програми. Нижче наводимо основний алгоритм її роботи, на мові C:

```
self.X_ = self._gradient_descent(self.X_, self.y_, self.w, self.b, alpha
    , max_iters, predict_func)

def _cost_function(self, X, Y, A):
m = X.shape[0]
if m == 0:
return None

J = (1 / m) * np.sum(-Y * np.log(A) - (1 - Y) * np.log(1 - A))
return J

```

# Розділ 3

# Альтернативні рішення

Деякі дослідники пишуть свої роботи в програмах типу Microsoft Word. Але то не є труйово[1].

# Розділ 4

# Висновок

Дана робота містить значний мій вклад, і перевершує попередні досягнення в багатьох напрямках. Окрім того, даний напрямок досліджень має значні перспективи подальшого розвитку. (Особливо добре було б, якби хтось вирішив проблему кирилиці в listings).

# Бібліоґрафія

[1] Вікіпідручник *Як написати курсову?* (http://uk.wikibooks.org/wiki/%D0%AF%D0%BA_%D0%B2%D1%87%D0%B8%D1%82%D0%B8%D1%81%D1%8C_%D0%BA%D1%80%D0%B0%D1%89%D0%B5%3F/%D0%9A%D1%83%D1%80%D1%81%D0%BE%D0%B2%D1%96)