Министерство образования и науки Российской Федерации

Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и технологий

Работа допущена к защите

И. о. заведующего кафедрой КИТ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Щукин

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2019 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА**

**ПРИМЕНЕНИЕ ИССКУСТВЕННОЙ НЕЙРОННОЙ СЕТИ ДЛЯ ОЦЕНКИ РИСКОВ ЗАРАЖЕНИЯ КОМПЬЮТЕРА ВРЕДОНОСНЫМ ПРОГРАМНЫМ ОБЕСПЕЧЕНИЕМ**

по направлению 09.03.03 Прикладная информатика

Выполнил

студент гр.43506/3 А.В. Заднепровский

Руководитель

доцент, к. ф.-м. н. В.Г. Пак

Санкт-Петербург

2019

**САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО**

**ИНСТИТУТ КОМПЬЮТЕРНЫХ НАУК И ТЕХНОЛОГИЙ**

УТВЕРЖДАЮ

И.О. заведующего кафедрой КИТ

А.В. Щукин

« » 2019 г.

ЗАДАНИЕ

по выполнению выпускной квалификационной работы

студенту

Заднепровскому Андрею Владимировичу 43506/3

1. Тема работы: «Применение искусственной нейронной сети для оценки рисков заражения компьютера вредоносным программным обеспечением».

2. Срок сдачи студентом законченной работы: май 2019.

3. Исходные данные по работе: Microsoft Malware Prediction Dataset, модели ИНС, применимые для решения задачи предсказания, алгоритмы обучения ИНС.

4. Содержание работы (перечень подлежащих разработке вопросов):

1. Постановка задачи, обоснование актуальности;
2. Обзор моделей ИНС применимых для решения задачи, алгоритмов обучения, существующих решений;
3. Выбор и разработка архитектуры ИНС применительно к задаче с обоснованием, описание архитектуры, алгоритмов обучения;
4. Анализ и предварительная обработка исходных данных;
5. Реализация ИНС;
6. Настройка гиперпараметров модели ИНС;
7. Экспериментальное исследование эффективности разработанной ИНС;
8. Сравнение с существующими решениями;
9. Выводы об эффективности разработанной ИНС, перспективы улучшения.

5. Перечень графического материала (с указанием обязательных чертежей): графики.

6. Консультанты по работе:

7. Дата выдачи задания: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) инициалы, фамилия

Задание принял к исполнению

(дата)

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) инициалы, фамилия

# РЕФЕРАТ

99 с., 9 рисунков, 9 таблиц, 9 приложений

МАШИННОЕ ОБУЧЕНИЕ, ИСКУССТВЕННЫЕ НЕЙРОННЫЕ СЕТИ, ОБУЧЕНИЕ С УЧИТЕЛЕМ, БОЛЬШИЕ ДАННЫЕ, ВРЕДОНОСНОЕ ПРОГРАМНОЕ ОБЕСПЕЧЕНИЕ

Данная работа относится к сфере машинного обучения. В первой главе ставится задача оценки рисков заражения компьютера вредоносным ПО и делается обзор подходов, применимых для решения этой задачи. Во второй и третей главах разрабатывается и реализуется модель ИНС. В четвертой главе оценивается эффективность полученной модели в задаче оценки рисков заражения компьютера вредоносным ПО, производится тестирование модели ИНС при различных наборах гиперпараметров, в результате которого в финальную модель ИНС вносятся необходимые улучшения. По итогам работы делается вывод об эффективности полученного решения и перспективах его улучшения.

# THE ABSTRACT

99 p., 9 pictures, 9 tables, 9 applications

# СОДЕРЖАНИЕ

[ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 6](#_Toc7516506)

[ВВЕДЕНИЕ 7](#_Toc7516507)

[ГЛАВА 1. ОПИСАНИЕ ЗАДАЧИ И ОБЗОР ПОДХОДОВ ДЛЯ ЕЕ РЕШЕНИЯ 10](#_Toc7516508)

[1.1. Задача оценки рисков заражения компьютера вредоносным ПО 10](#_Toc7516509)

[1.2. Метрика для оценки эффективности решения 10](#_Toc7516510)

[1.3. Подходы, применяющиеся для решения задачи 12](#_Toc7516511)

[1.3.1. Деревья решений 12](#_Toc7516512)

[1.3.2. Случайные леса 15](#_Toc7516513)

[1.3.3. Градиентный бустинг 17](#_Toc7516514)

[1.3.4. Логистическая регрессия 18](#_Toc7516515)

[1.3.5. Искусственные нейронные сети 19](#_Toc7516516)

[1.4. Выводы по первой главе 21](#_Toc7516517)

[ГЛАВА 2. РАЗРАБОТКА МОДЕЛИ ИНС 22](#_Toc7516518)

[2.1. Анализ исходных данных 22](#_Toc7516519)

[2.1.1. Обнаружение избыточных признаков 23](#_Toc7516520)

[2.1.2. Подготовка данных 24](#_Toc7516521)

[2.2. Тип слоев 26](#_Toc7516522)

[2.3. Функция потерь 27](#_Toc7516523)

[2.4. Оптимизатор 27](#_Toc7516524)

[2.5. Топология сети 27](#_Toc7516525)

[ГЛАВА 3. ПРОГРАМНАЯ РЕАЛИЗАЦИЯ ИНС 28](#_Toc7516526)

[3.1. Используемые программные средства 28](#_Toc7516527)

[3.1. Предварительная обработка данных 28](#_Toc7516528)

[3.3. Реализация ИНС 28](#_Toc7516529)

[ГЛАВА 4. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ИНС 29](#_Toc7516530)

[ЗАКЛЮЧЕНИЕ 30](#_Toc7516531)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 31](#_Toc7516532)

[Приложение 1. Набор признаков в исходных данных 33](#_Toc7516533)

[Приложение 2. Код предварительной обработки исходных данных 37](#_Toc7516534)

[Приложение 3. Код реализованой ИНС на языке Python 38](#_Toc7516535)

# ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИНС Искусственная нейронная сеть

ОС Операционная система

ПО Программное обеспечение

ПК Персональный компьютер

# ВВЕДЕНИЕ

Искусственные нейронные сети являются одним из методов машинного обучения, которое «позволяет справляться с задачами, которые слишком сложны для решения с помощью фиксированных программ, спроектированных и написанных людьми.» [1, с. 97] Характерной чертой алгоритмов машинного обучения является процедура обучения, а не прямое решение задачи. В ходе обучения происходит тренировка алгоритма на большом количестве примеров решения конкретной задачи.

В настоящее время ИНС находится в наиболее активной фазе развития за всю свою историю, хотя ключевые алгоритмы были уже известны в 90-х годах ХХ века. Это связано с влиянием следующих факторов:

* Значительным приростом вычислительной мощности оборудования. Так как обучение ИНС очень требовательно к вычислительным ресурсам компьютера;
* Накоплением больших объемов данных, благодаря бурному росту сети Интернет и емкости устройств хранения информации.

Так же было разработано и много новых алгоритмов, однако этого бы не случилось без практических экспериментов, которые стали возможными благодаря описанным выше причинам. [2, c. 45]

За последнее время число задач для которых применяются ИНС значительно возросло, это стало возможным за счет демократизации инструментов разработки, то есть появления высокоуровневых фреймворков для реализации моделей ИНС.

Одной из новых задач, для решения которых можно применить нейронные сети является оценка рисков заражения компьютера вредоносным программным обеспечением по его параметрам, которая относится к категории бинарной классификации. Данная задача актуальна, так как разработка вредоносного ПО продолжает оставаться организованной и хорошо финансируемой сферой, которая наносит значительный вред мировой экономике, исчисляющийся в миллиардах долларов.

Объектом исследования в данной работе являются искусственные нейронные сети.

Предмет исследования – методы и алгоритмы применения искусственной нейронной сети в задаче оценки вероятности заражения компьютера вредоносным ПО.

Целью дипломной работы является разработка и обучение искусственной нейронной сети, способной эффективно оценивать вероятность заражения компьютера вредоносным ПО. После тестирования реализованной ИНС требуется сделать выводы о ее эффективности по сравнению с существующими решениями, и предложить возможные способы ее улучшения. Для достижения данной цели были выделены следующие задачи:

1. Исследовать методы машинного обучения, которые в настоящее время применяются для задачи оценки вероятности заражения компьютера;
2. Разработать архитектуру ИНС;
3. Реализовать ИНС;
4. Протестировать полученную сеть и добиться улучшения ее эффективности подобрав оптимальную комбинацию гиперпараметров;
5. Сделать вывод о эффективности реализованной сети по сравнению с существующими решениями, и предложить возможные способы ее улучшения.

Гипотеза исследования: ИНС способна эффективно справиться с задачей оценки вероятности заражения компьютера вредоносным ПО.

В соответствии с намеченной целью и задачами исследования были определены следующие методы:

* теоретический анализ научной и методический литературы по теме исследования;
* изучение документации необходимых языков программирования и библиотек;
* экспериментальный метод, включающий проведение констатирующего эксперимента, анализ и обобщение полученных данных.

Практическая значимость исследования, проведенного в дипломной работе, состоит в реализации эффективного решения задачи оценки вероятности заражения компьютера с помощью ИНС.

# ГЛАВА 1. ОПИСАНИЕ ЗАДАЧИ И ОБЗОР ПОДХОДОВ ДЛЯ ЕЕ РЕШЕНИЯ

В настоящей главе представлено описание задачи оценки рисков заражения компьютера вредоносным ПО и сделан обзор методов машинного обучения, которые применяются для решения этой задачи.

## 1.1. Задача оценки рисков заражения компьютера вредоносным ПО

В 2018 году компания Microsoft предоставила научному сообществу беспрецедентный набор данных о вредоносных программах, чтобы стимулировать прогресс в разработке эффективных методов прогнозирования заражения компьютера вредоносными программами. Эти данные были предоставлены в рамках соревнования Microsoft Malware Prediction Challenge для специалистов в области анализа данных. [3]

Цель соревнования заключается в разработке эффективного метода предсказания вероятности заражения компьютера под управлением ОС Windows, основываясь на различных свойствах компьютера, например: версии ОС, версии антивируса, наличии файрволла, производителе оборудования ПК и т.д. Всего набор содержит 82 характеристики для каждого ПК.

Описанная задача относится к категории симметричной бинарной классификации, решением которой должна быть непрерывная величина от 0 до 1, являющаяся степенью уверенности в том, что данный компьютер будет заражен в будущем.

## 1.2. Метрика для оценки эффективности решения

Для оценки эффективности полученных решений в рамках данной работы будет использоваться метод подсчета площади под кривой рабочей характеристики приемника или ROC-кривой (Area Under Receiver Operating Characteristic Curve). Данный метод находит свое применение аж с 40-х годов ХХ века, и в настоящее время широко применяется для сравнения алгоритмов бинарной классификации.

Рассмотрим на примере работу данного метода. Пусть некоторый алгоритм классификации выдал оценки, как показано в таблице 1.1. Упорядочим строки таблицы 1.1 по убыванию ответов алгоритма – получим таблицу 1.2.

Таблица 1.1

Пример оценок некоторого алгоритма классификации

|  |  |  |
| --- | --- | --- |
| Номер | Оценка | Класс |
| 1 | 0.1 | 0 |
| 2 | 0.9 | 1 |
| 3 | 0.3 | 1 |
| 4 | 0.2 | 0 |
| 5 | 0.5 | 0 |
| 6 | 0.4 | 0 |
| 7 | 0.8 | 1 |

Таблица 1.2

Упорядоченные оценки некоторого алгоритма классификации

|  |  |  |
| --- | --- | --- |
| Номер | Оценка | Класс |
| 2 | 0.9 | 1 |
| 7 | 0.8 | 1 |
| 5 | 0.5 | 0 |
| 6 | 0.4 | 0 |
| 3 | 0.3 | 1 |
| 4 | 0.2 | 0 |
| 1 | 0.1 | 0 |

Чтобы нарисовать ROC-кривую, надо взять единичный квадрат на координатной плоскости, разбить его на m равных частей горизонтальными линиями и на n – вертикальными, где m – число правильно классифицированных единиц, а n – нулей. В результате квадрат разбивается сеткой на m×n блоков, рисунок 1.1 а).

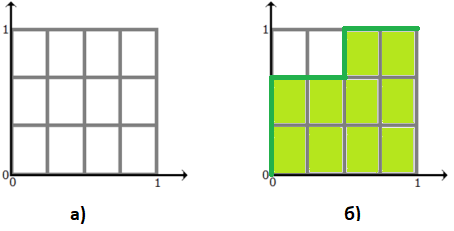


Рисунок 1.1. Построение ROC-кривой

Теперь будем просматривать строки таблице 1.2 сверху вниз и прорисовывать на сетке линии, переходя их одного узла в другой. Стартуем из точки (0, 0). Если значение метки класса в просматриваемой строке 1, то делаем шаг вверх; если 0, то делаем шаг вправо, результат представлен на рисунке 1.1 б). Ясно, что в итоге мы попадём в точку (1, 1), т.к. сделаем в сумме m шагов вверх и n шагов вправо. [4]

Площадь под ROC-кривой для этого примера будет равна 10/12 ~ 0.83.

## 1.3. Подходы, применяющиеся для решения задачи

Задача бинарной классификация является классической задачей машинного обучения, для ее решения существуют следующие наиболее распространенные методы:

* деревья решений,
* случайные леса,
* градиентный бустинг,
* логистическая регрессия,
* ИНС.

Далее следует подробный обзор всех представленных выше методов.

### 1.3.1. Деревья решений

Деревья решений — это весьма распространенный метод, который используется для решения разного класса задач:

* Классификации: распределение объектов по заранее определенным классам;
* Регрессии: предсказания целевой переменной, которая имеет непрерывную область значения, например численное прогнозирование;
* Описания данных: для хранения информации в компактной форме и быстрого поиска. [5]

Далее будем говорить о деревьях решений применительно к задаче классификации.

Итак, «дерево решений – это модель, представляющая собой совокупность правил для принятия решений.» [6] Графически она может быть предствленна в виде дерева (рис. 1.2), в котором моменты принятия решений соответствуют узлам дерева (англ.: decision nodes). В них происходит ветвление процесса (англ.: branching), т.е. деление его на ветви (англ.: branches) в зависимости от сделанного выбора. Конечные узлы называют листьями (англ.: leaf nodes), при этом каждый лист – это конечный результат последовательного принятия решений.

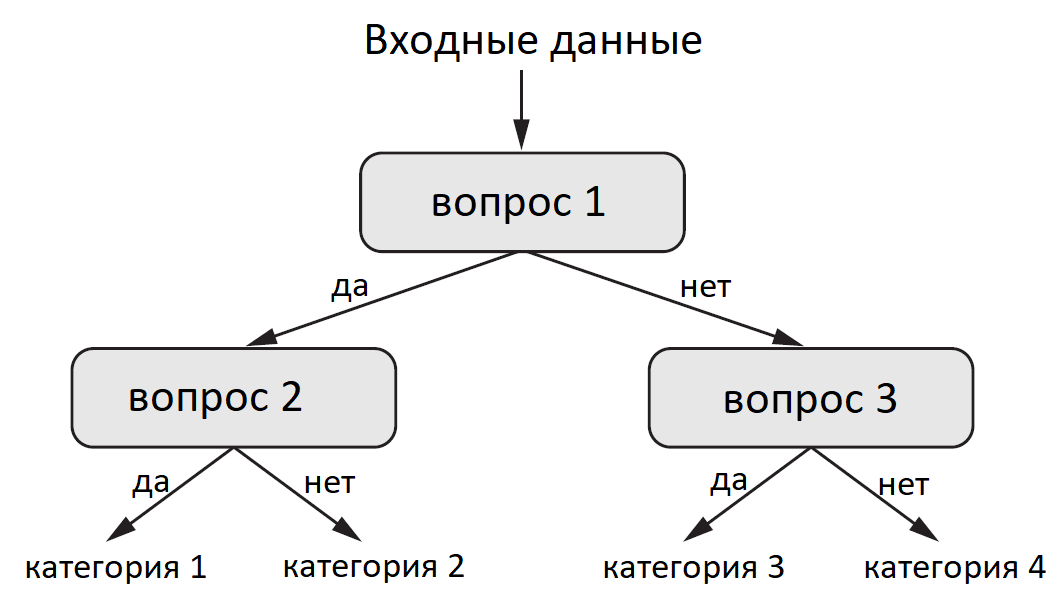


Рисунок 2.2. Визуализация дерева решений

Данные, подлежащие классификации, находятся в корне дерева (англ.: root). При построении дерева в каждом из узлов его узлов выбирается признак, значение которого используется для разбиения всех данных на 2 класса. Условия для такого разбиения являются обучаемыми параметрами метода. Пример такого вопроса: признак номер 3 в данных больше 0,5.

Таким образом, для того чтобы построить дерево, мы добавляем все новые узлы, с новыми вопросами о данных, до тех пор, пока не выполнится один из возможных критериев остановки. Это возможно в следующих ситуациях:

* Все, или практически все, данные узла принадлежат одному и тому же классу;
* Закончились признаки, по которым можно построить новое разбиение;
* Достигнут лимит роста дерева, если это параметр был задан. [6]

Проиллюстрируем работу уже построенного решающего дерева высоты 2 на простом примере классификации трех типов объектов (круг, квадрат, треугольник) на координатной плоскости (рис 1.3). Как можно заметить каждый из вопросов делит оставшееся множество объектов на 2 группы, пока большая часть из них не окажется однотипными.

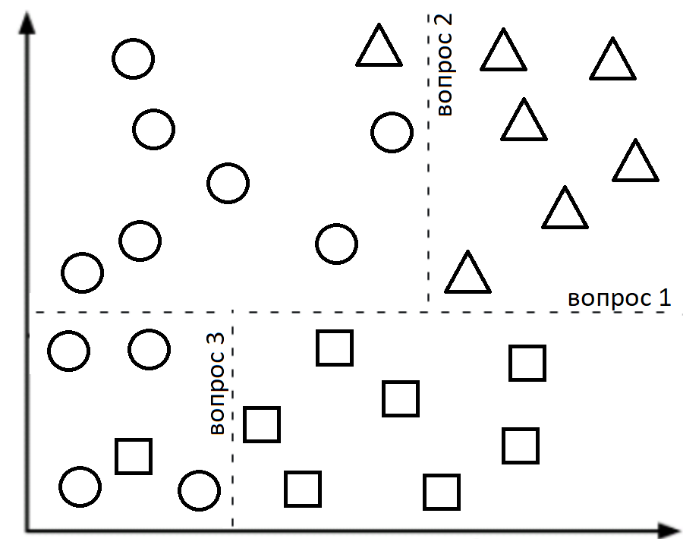


Рисунок 1.3. Иллюстрация работы дерева решений на координатной плоскости

Преимущества метода решающий деревьев:

* Легко визуализируется и интерпретируется;
* Не требует подготовки данных, поддерживает порядковые и номинальные признаки;
* Быстрое обучение и прогнозирование;
* Использует модель «белого ящика». Любое решение можно объяснить с помощь булевой логики;
* Позволяет оценить модель при помощи статистических тестов, что даёт возможность оценить надёжность модели;
* Метод хорошо работает даже в том случае, если были нарушены первоначальные предположения, включённые в модель.

Недостатки метода решающий деревьев:

* Большая чувствительность к шумам во входных данных, «лишние» данные сильно ухудшают точность метода;
* Плохо справляется с разреженными значениями признаков;
* Нестабильность. Небольшие изменения данных приводят к существенным изменениям построенного дерева;
* Задача построения оптимального дерева решений является NP-полной. Поэтому для построения деревьев используются жадные алгоритмы, где единственно оптимальное решение выбирается локально в каждом узле. Однако такие алгоритмы не могут обеспечить оптимальность всего дерева в целом;
* Склонность к переобучению, с которым необходимо боротся регулированием максимальной глубины дерева;
* Не умеет экстраполировать, только интерполировать, из-за чего уступает по качеству классификации некоторым другим методам.

Резюмируя, отметим, что в чистом виде деревья решений хоть и показывают не плохую эффективность, особенно в небольших задачах с низкой размерностью пространства признаков, однако они уступают по эффективности более сложным алгоритмам, которые основываются на деревьях решений. О наиболее распространенных из таких алгоритмов речь пойдет ниже.

### 1.3.2. Случайные леса

Алгоритм случайный лес (англ.: Random Forest) предлагает надежный и практичный подход к обучению на основе деревьев решений, его основная идея заключается в использовании большого ансамбля решающих деревьев (это число является параметром метода) с последующим объединением выдаваемых ими результатов. Случайные леса применимы к задачам регрессии, классификации и кластеризации, селекции признаков и т.д. Являются достаточно универсальным алгоритмом, можно сказать, что они почти всегда являются оптимальным алгоритмом для любых задач поверхностного машинного обучения.

«В отличие от классических алгоритмов построения деревьев решений в методе случайных лесов при построении каждого дерева на стадиях расщепления вершин используется только фиксированное число случайно отбираемых признаков обучающей выборки (второй параметр метода) и строится полное дерево (без усечения), т. е. каждый лист дерева содержит наблюдения только одного класса.» [7]

Результат классификации определяется путем голосования полученных классификаторов, определяемых отдельными деревьями. При этом точность ансамблей классификаторов существенно зависит от разнообразия (англ.: diversity) классификаторов, входящих в ансамбль или, т. е. от того, насколько их решения взаимозависимы. А именно, чем более разнообразны классификаторы ансамбля, тем выше эффективность классификации. [7]

Достоинства алгоритма «случайный лес»:

* Не подвержен переобучению, что выделяет этот метод среди большинства методов классификации;
* Обеспечивает большую точность, чем просто решающие деревья;
* Есть возможность распараллелить вычисления, что существенно при большом объеме обучающих данных;
* Одинаково хорошо обрабатываются порядковые, номинальные и дискретные признаки;
* Существует естественная оценка вероятности ошибочной классификации – метод Out-Of-Bag, рассчитывающаяся на образцах обучающих данных, не использовавшихся при построении решающего дерева.

Недостатки алгоритма «случайный лес»:

* Большой объем получающихся моделей;
* В отличие от одного дерева, результаты случайного леса сложнее интерпретировать;
* Для данных, включающих категориальные переменные с различным количеством уровней, случайные леса предвзяты в пользу признаков с большим количеством уровней;
* Метод случайных лесов, так же, как и решающие деревья, не умеет экстраполировать.

На основании всего вышеизложенного, можно сказать, что метод «случайный лес» можно использовать для решения поставленной задачи, однако существуют более интеллектуальные методы, основанные на том же принципе (построения ансамбля решающих деревьев), об одном из которых речь пойдет далее.

### 1.3.3. Градиентный бустинг

Градиентный бустинг (англ.: Gradient Boosting Machine), во многом схож с случайным лесом, этот метод машинного обучения основывается на объединении слабых моделей прогнозирования, чаще всего деревьев решений в ансамбли. «Он использует градиентный бустинг, способ улучшения любой модели машинного обучения путем итеративного обучения новых моделей, специализированных для устранения слабых мест в предыдущих моделях.» [5] Прием градиентного бустинга использующий деревья решений позволяет получить модели, которые как правило превосходят случайные леса при сохранении аналогичных свойств. На данный момент это один из лучших алгоритмов, для решения большинства задач машинного обучения, за исключением задач распознавания образов. [2, с. 41]

Для задачи оценки рисков заражения компьютера метод градиентного бустинга является одним из наиболее оптимальных, и он нашел широкое применение в рамках соревнования Microsoft Malware Prediction Challenge. [3]

### 1.3.4. Логистическая регрессия

Логистическая регрессия (англ.: logistic regression) — «метод построения линейного классификатора, позволяющий оценивать апостериорные вероятности принадлежности объектов классам.» [8] Суть линейной регрессии состоит в анализе связи между несколькими независимыми переменными (называемыми также регрессорами) и зависимой переменной .

Для этого делается предположение, о том, что вероятность наступления события равно:

где , – коэффициенты регрессии, а функция так же называемая логистической функцией (или сигмоид) имеет следующий вид (рис. 1.4):

Процесс обучения модели логистической регрессии заключается в подборе коэффициентов регрессии, для этого существует несколько способов. Чаще всего применяется метод максимального правдоподобия, цель которого максимизировать значение функции правдоподобия для обучающей выборки . [9]

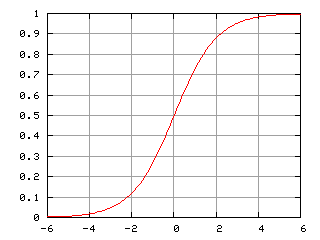


Рисунок 1.4. График логистической функции [10]

Преимущества логистической регрессии:

* Прозрачность моделирования, т. е. доступность для анализа всех промежуточных вычислений;
* Скорость и простота получения модели.

Недостатки логистической регрессии:

* Не подходит для моделирования нелинейных зависимостей;
* Чувствительность к шумам и «лишним» тренировочным данным;
* Чувствительность избыточным признакам;
* Трудоемкое нахождение коэффициентов регрессии.

Применительно к задаче этой работы данный метод не является подходящим. Это объясняется тем, что алгоритм логистической регрессии относится к категории линейных алгоритмов, которые плохо справляются с задачами, в которых зависимость результата от признаков нелинейная и сложная, т.е. пространство признаков нельзя эффективно разделить гиперплоскостью.

### 1.3.5. Искусственные нейронные сети

Структурно ИНС представляет из себя ориентированный ациклический граф, вершины которого называются нейронами – элементарными единицами обработки информации, а соединительные ребра графа – синапсами, каждый из которых имеет свой вес. Процедура обучения, применительно к ИНС, «выстраивает в определенном порядке синаптические веса нейронной сети для обеспечения необходимой структуры взаимосвязей нейронов.» [11]

// Описание процесса обучения [2, с. 71]

Преимущества ИНС:

* «Адаптивность. Нейронные сети обладают способностью адаптировать свои синаптические веса к изменениям окружающей среды. В частности, для работы в нестационарной среде (где статистика изменяется с течением времени) могут быть созданы нейронные сети, изменяющие синаптические веса в реальном времени»; [11]
* Масштабируемость. Параллельная структура нейронных сетей потенциально ускоряет решение некоторых задач и обеспечивает масштабируемость нейронных сетей;
* Устойчивость к шумам и «лишним» обучающим данным;
* Устойчивость к избыточным признакам;
* Позволяют эффективно строить нелинейные зависимости;
* Может одновременно решать несколько задач на едином наборе входных данных − имея несколько выходов, прогнозировать значения нескольких показателей.

Недостатки ИНС:

* Высокая требовательность к вычислительным ресурсам на стадии обучения сети, однако обученная сеть выдает результат достаточно быстро;
* Необходима тщательная предварительная обработки входных данных;
* Для высокой точности нужен большой объем обучающий данных;
* Работают по принципу «черного ящика», т.е. результаты сети очень трудно интерпретировать.

Основываясь на сказанном выше, стоит отметить, что ИНС хорошо подходят для решения поставленной задачи, из-за способности строить нелинейные зависимости, устойчивости к зашумленным и избыточным данным. Так же важна их способности адаптироваться к изменяющейся окружающей обстановке, так как предметная область подразумевает, что с течением времени характер входных данных будет претерпевать значительных изменений.

## 1.4. Выводы по первой главе

В данной главе были исследованы методы машинного обучения, позволяющие решать задачу оценки рисков заражения компьютера вредоносным ПО. На основании чего, можно сделать вывод, что для решения поставленной задачи наряду с градиентным бустингом подходят ИНС. Однако ИНС выглядят предпочтительнее так как:

* на данный момент не нашли широкого применения в рамках решения этой задачи,
* являются одним из самых быстроразвивающихся и популярных методов машинного обучения,
* полученная с его помощью модель имеет способность к адаптации с течением времени.

Это обосновывает применимость и потенциальную эффективность ИНС для решения поставленной задачи.

# ГЛАВА 2. РАЗРАБОТКА МОДЕЛИ ИНС

Разработка любой модели ИНС состоит из следующих ключевых пунктов:

* Выбора типа слоев, которые будут объединятся в сеть;
* Определения функции потерь, значение которой в процессе обучения будет уменьшатся;
* Определения оптимизатора, который определяет способ обучения.

На рисунке 2.1. представлена схематическая взаимосвязь между этими компонентами ИНС. Их выбор напрямую зависят от исходных данных и глобальных целей, которые должна решать сеть. Поэтому на одном из первых этапов конструирования модели ИНС необходимо проанализировать исходные данные предметной области, сконструировать признаки и определить необходимые преобразования.

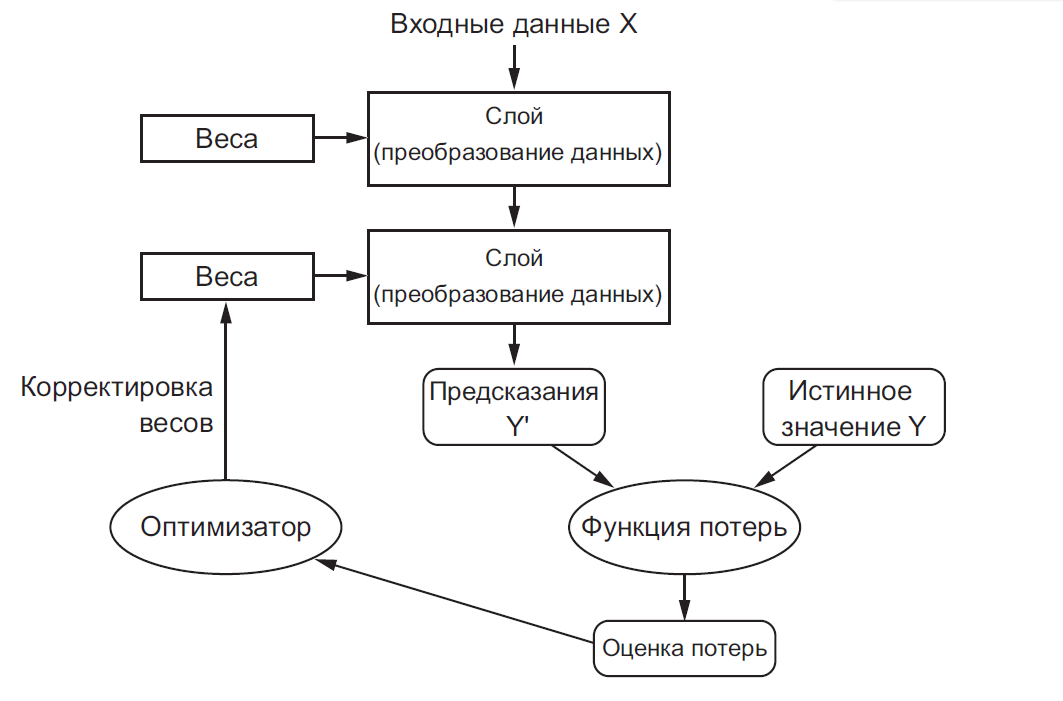


Рисунок 2.1. Связь между сетью, слоями, функцией потерь и оптимизатором [2]

## 2.1. Анализ исходных данных

Исходные данные, представленные компанией Microsoft, содержат информацию о более чем 16 миллионах компьютеров. Каждый компьютер характеризуется 82 признаками (список представлен в приложении 1), среди которых есть как номинальные, так и порядковые. Весь объем исходных данных делится на две примерно равные части, это:

* Обучающая выборка, которая содержит в дополнение к 82 характеристикам, дополнительный бинарный признак, говорящий о том, было ли обнаружено заражение вредоносным ПО этого компьютера, или нет;
* Тестовая выборка, которая не содержит правильных ответов, для нее необходимо предсказать ответ. Эффективность классификатора оценивается по тестовой выборке, для этого выданные классификатором оценки отправляются для расчетов на сервер соревнования.

В общем случае, на первом этапе анализа данных следует произвести конструирование признаков. Это такое преобразование исходных данных, которое позволяет выделить более информативные показатели, которые улучшат обучаемость сети. Эти преобразования основываются на опыте и знаниях экспертов в предметной области. Однако в данном случае этот этап был выполнен специалистами компании Microsoft, и научному сообществу были предоставлены уже подготовленные данные.

### 2.1.1. Обнаружение избыточных признаков

Для ИНС избыточность признаков не является проблемой, и не приводит к уменьшению точности предсказаний конечной сети. Однако ИНС очень требовательны к вычислительной мощности и памяти, поэтому устранение лишних атрибутов позволит значительно уменьшить время обучения и размер сети.

Под избыточными признаками понимаются признаки, не обладающие статистической значимостью вследствие:

* критической разрежённости значений признаков,
* значительного перекоса распределения значений признаков,
* высокой степени зависимости от других признаков.

Чтобы удаление каких-то признаков не привело даже к малейшим потерям в эффективности будущей сети, отнесем к избыточным признакам только самые явные, которые имеют более 99%:

* пустых значений,
* одинаковых значений,
* зависимость от другого признака.

В результате применения такого подхода было обнаружено 17 избыточных признаков, которые можно смело не учитывать. Это позволило сократить весь объем исходных данных на 20%.

### 2.1.2. Подготовка данных

Как уже было отмечено в п. 1.3.5. искусственные нейронные сети накладывают сильные ограничения на входные данные. Так они могут работать только с тензорами (специальными многомерными массивами для числовых данных). Поэтому данные необходимо обработать перед передачей в ИНС.

Нейронные сети не умею обрабатывать пропущенные значения, поэтому необходимо заполнить пропущенные значения признаков. Для этого существует два основных подхода:

* Заполнить недостающие значения нулями, в этом случае они будут игнорироваться сетью;
* Заполнить недостающие значения средним значением, для порядковых признаков, или самой распространенной категорией, для номинальных.

Хорошим решением для ИНС считается заменить недостающие значения нулями, тогда сетью они будут игнорироваться. Главное в этом случае убедится, что в исходных данных ноль не является осмысленным значением, в этом случае для заполнения пропущенных значений можно взять другое число (например -1).

Для порядковых (числовых) признаков необходимо произвести масштабирование, то есть приведение значений к одному диапазону (обычно это диапазон [0, 1] или [-1, 1]). Это упрощает обучение сети так как из-за непропорционального диапазона значений, разные признаки будут вносить разный вклад в направление обучения сети и будут препятствовать сходимости сети.

Номинальные (категориальные) признаки необходимо векторизовать, для этого используются следующие подходы:

* Кодирование категорий целыми числами в интервале от [1, m], где m – число категорий. Применяется как в случае, если категории представлены строками (например ОС компьютера или город), так и в случае числового представления (например номер сборки ОС). Это позволяет равномерно распределить все категории по числовой прямую;
* Прямое кодирование (one-hot encoding). Каждое значение признака кодируется нулевым вектором размера m, с одной единицей на позиции равной номеру соответствующей категории.

На практике можно использовать либо только первый подход, либо оба. В данной работе будут использоваться оба подхода. Использование прямого кодирования часто затруднительно из-за многократного увеличения требуемой памяти, особенно при большом числе категорий. Однако оно дает лучшие результаты благодаря полному отделению категорий друг от друга, так как проецирование номинальных данных на числовую прямую привносит не существующие связи между категориями.

Чтобы уменьшить размер требуемой памяти при прямом кодировании следует ограничить максимальное число категорий m для всех номинальных признаков. В этом случае нужно оставить только самые популярные категории, а все остальные сделать одной пустой категорией. Само значение m должно быть подобрано экспериментальным путем. Так же все данные необходимо разделить на пакеты, размер пакета после кодирования должен соответствовать объему свободной оперативной памяти в процессе обучения.

## 2.2. Типы слоев

Слой – это фундаментальная структура обработки данных в ИНС. Его можно интерпретировать как функцию, которая принимает на вход тензор, и возвращает преобразованных тензор. Преобразование осуществляется, основываясь на значении весовых коэффициентов, типе и размере слоя.

Сначала все слои входящие в ИНС инициализируются небольшими случайными весовыми коэффициентами. На этом этапе сеть не способна выдавать сколько ни будь значимые предсказания. В процессе обучения весовые коэффициенты оптимизируются, критерием оптимизации является значение функции потерь.

Размер слоя определяется следующими параметрами:

* числом входных нейронов,
* числом внутренних (скрытых) нейронов,
* числом выходных нейронов.

Не существует четких руководств, для оптимального выбора этих параметров, поэтому они выбираются экспериментально.

Тип слоя выбираются в зависимости от класса решаемой задачи, он определяет характер внутренних связей нейронов в слое. Часто происходит комбинирование нескольких типов слоев в рамках одной ИНС.

### 2.2.1. Вычислительные слои

…существуют следующие основные типы слоев:

* Полносвязный. В нем каждый нейрон связан со всеми нейронами предыдущего уровня;
* Сверточный – каждый нейрон связан только с ограниченным числом нейронов предыдущего уровня, такая связь называется сверткой, благодаря ней ИНС может создавать позиционно независимую иерархию шаблонов. Применяются главным образом для решения задач распознавания образов;
* Рекурентный. Используются для распознавания речи, машинного перевода, …

// …

Для решаемой задачи самым подходящим является полносвязный тип слоя.

### 2.2.2. Слои преобразования данных

// Dropout, Normalization, Flatten - слои

## 2.3. Функция потерь

Правильный выбор функции потерь играет во много определяющую роль при проектировании ИНС. Так как именно значение этой функции будет минимизировался в процессе обучения. Однако для большинства классических задач, к которым так же относится задача бинарной классификации, существуют конкретные рекомендации по оптимальной функции потерь.

// Оптимальная функция потерь для задачи бин. классификации

## 2.4. Оптимизатор

Функция оптимизации определяет то, как будет изменятся сеть, а именно весовые коэффициенты слоев в процессе обучения. Существуют разные оптимизаторы, каждый из которых реализует конкретный вариант стохастического (случайного) градиентного спуска.

Идея градиентного спуска состоит в вычислении градиента в многомерном пространстве признаков, для функции потерь, относительно каждого весового коэффициента, и затем незначительно сдвинуть каждый весовой коэффициент в сторону уменьшения градиента.

// Описание градиентного спуска

// Оптимальный алг. град спуска для задачи бин. классификации

## 2.5. Топология сети

// Предварительный выбор числа слоев, размера слоев, сколько входов сети, сколько выходов, как связаны слои.

# ГЛАВА 3. ПРОГРАМНАЯ РЕАЛИЗАЦИЯ ИНС

## 3.1. Используемые программные средства

// Почему был выбран язык Python, описание библиотек

## 3.1. Предварительная обработка данных

// Описание обработки данных на основе п.2.1.2 (код в приложении 2)

## 3.3. Реализация ИНС

// Описание базовой реализации (код в приложении 3)

# ГЛАВА 4. ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ИНС

// Подбор оптимальных значений большинства параметров сети

# ЗАКЛЮЧЕНИЕ

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Годфеллоу Я. Глубокое обучение [Текст] / И. [Бенджио](https://www.labirint.ru/authors/190834/), Я. [Гудфеллоу](https://www.labirint.ru/authors/190835/), А. [Курвилль](https://www.labirint.ru/authors/190836/); пер. с англ. А.А. Слинкин, ред. Д.А. Мовчан. 2-е изд., испр. – М.: ДМК Пресс, 2018. – 652 с.
2. Шолле Ф. Глубокое обучение на Python [Текст] / Ф. Шолле – СПб.: Питер, 2018 – 400 с.
3. Microsoft Malware Prediction Competition / [Электронный документ] (https://www.kaggle.com/c/microsoft-malware-prediction). Проверено 20.03.2019.
4. AUC ROC (площадь под кривой ошибок) / [Электронный документ] (https://dyakonov.org/2017/07/28/auc-roc-площадь-под-кривой-ошибок/). Проверено 03.03.2019.
5. Деревья решений – общие принципы работы / [Электронный документ] (https://basegroup.ru/community/articles/description). Проверено 16.04.2019.
6. Метод деревьев решений для задачи классификации / [Электронный документ] (https://edu.kpfu.ru/pluginfile.php/91556/mod\_resource/content /2/Decision%20trees\_1.pdf). Проверено 16.04.2019.
7. Чистяков С.П. Случайные леса: обзор / Труды Карельского научного центра РАН № 1. 2013. С. 117-136 [Электронный документ] (http://resources.krc.karelia.ru/transactions/doc/trudy2013/trudy\_2013\_1\_117-136.pdf). Проверено 17.04.2019.
8. Цыплаков А.А. Некоторые эконометрические методы. Метод максимального правдоподобия в эконометрии / Методическое пособие. – Новосибирск: НГУ, 1997. – 127 С.
9. Воронцов К.В. Лекции по линейным алгоритмам классификации / [Электронный документ] (http://www.machinelearning.ru/wiki/images/6 /68/voron-ML-Lin.pdf). Проверено 18.04.2019.
10. Логистическая регрессия / [Электронный документ] (https://ru.wikipedia.org/wiki/Логистическая\_регрессия). Проверено 18.04.2019.
11. Хайкин. С. Нейронные сети: полный курс, 2-е изд.: Пер. с англ. – М.: Вильямс, 2006 – 1104 с.
12. //общая теория по нейронным сетям
13. Keras Documentation. / [Электронный документ] (https://keras.io/). Проверено 13.03.2019.
14. Scicit-leart Library Documentation // [Электронный документ] (https://scikit-learn.org/stable/documentation.html). Проверено 03.03.2019.

Приложение 1

Набор признаков в исходных данных

Unavailable or self-documenting column names are marked with an "NA".

* MachineIdentifier - Individual machine ID
* ProductName - Defender state information e.g. win8defender
* EngineVersion - Defender state information e.g. 1.1.12603.0
* AppVersion - Defender state information e.g. 4.9.10586.0
* AvSigVersion - Defender state information e.g. 1.217.1014.0
* IsBeta - Defender state information e.g. false
* RtpStateBitfield - NA
* IsSxsPassiveMode - NA
* DefaultBrowsersIdentifier - ID for the machine's default browser
* AVProductStatesIdentifier - ID for the specific configuration of a user's antivirus software
* AVProductsInstalled - NA
* AVProductsEnabled - NA
* HasTpm - True if machine has tpm
* CountryIdentifier - ID for the country the machine is located in
* CityIdentifier - ID for the city the machine is located in
* OrganizationIdentifier - ID for the organization the machine belongs in, organization ID is mapped to both specific companies and broad industries
* GeoNameIdentifier - ID for the geographic region a machine is located in
* LocaleEnglishNameIdentifier - English name of Locale ID of the current user
* Platform - Calculates platform name (of OS related properties and processor property)
* Processor - This is the process architecture of the installed operating system
* OsVer - Version of the current operating system
* OsBuild - Build of the current operating system
* OsSuite - Product suite mask for the current operating system.
* OsPlatformSubRelease - Returns the OS Platform sub-release (Windows Vista, Windows 7, Windows 8, TH1, TH2)
* OsBuildLab - Build lab that generated the current OS. Example: 9600.17630.amd64fre.winblue\_r7.150109-2022
* SkuEdition - The goal of this feature is to use the Product Type defined in the MSDN to map to a 'SKU-Edition' name that is useful in population reporting. The valid Product Type are defined in %sdxroot%\data\windowseditions.xml. This API has been used since Vista and Server 2008, so there are many Product Types that do not apply to Windows 10. The 'SKU-Edition' is a string value that is in one of three classes of results. The design must hand each class.
* IsProtected - This is a calculated field derived from the Spynet Report's AV Products field. Returns: a. TRUE if there is at least one active and up-to-date antivirus product running on this machine. b. FALSE if there is no active AV product on this machine, or if the AV is active, but is not receiving the latest updates. c. null if there are no Anti Virus Products in the report. Returns: Whether a machine is protected.
* AutoSampleOptIn - This is the SubmitSamplesConsent value passed in from the service, available on CAMP 9+
* PuaMode - Pua Enabled mode from the service
* SMode - This field is set to true when the device is known to be in 'S Mode', as in, Windows 10 S mode, where only Microsoft Store apps can be installed
* IeVerIdentifier - NA
* SmartScreen - This is the SmartScreen enabled string value from registry. This is obtained by checking in order, HKLM\SOFTWARE\Policies\Microsoft\Windows\System\SmartScreenEnabled and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SmartScreenEnabled. If the value exists but is blank, the value "ExistsNotSet" is sent in telemetry.
* Firewall - This attribute is true (1) for Windows 8.1 and above if windows firewall is enabled, as reported by the service.
* UacLuaenable - This attribute reports whether or not the "administrator in Admin Approval Mode" user type is disabled or enabled in UAC. The value reported is obtained by reading the regkey HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA.
* Census\_MDC2FormFactor - A grouping based on a combination of Device Census level hardware characteristics. The logic used to define Form Factor is rooted in business and industry standards and aligns with how people think about their device. (Examples: Smartphone, Small Tablet, All in One, Convertible...)
* Census\_DeviceFamily - AKA DeviceClass. Indicates the type of device that an edition of the OS is intended for. Example values: Windows.Desktop, Windows.Mobile, and iOS.Phone
* Census\_OEMNameIdentifier - NA
* Census\_OEMModelIdentifier - NA
* Census\_ProcessorCoreCount - Number of logical cores in the processor
* Census\_ProcessorManufacturerIdentifier - NA
* Census\_ProcessorModelIdentifier - NA
* Census\_ProcessorClass - A classification of processors into high/medium/low. Initially used for Pricing Level SKU. No longer maintained and updated
* Census\_PrimaryDiskTotalCapacity - Amount of disk space on primary disk of the machine in MB
* Census\_PrimaryDiskTypeName - Friendly name of Primary Disk Type - HDD or SSD
* Census\_SystemVolumeTotalCapacity - The size of the partition that the System volume is installed on in MB
* Census\_HasOpticalDiskDrive - True indicates that the machine has an optical disk drive (CD/DVD)
* Census\_TotalPhysicalRAM - Retrieves the physical RAM in MB
* Census\_ChassisTypeName - Retrieves a numeric representation of what type of chassis the machine has. A value of 0 means xx
* Census\_InternalPrimaryDiagonalDisplaySizeInInches - Retrieves the physical diagonal length in inches of the primary display
* Census\_InternalPrimaryDisplayResolutionHorizontal - Retrieves the number of pixels in the horizontal direction of the internal display.
* Census\_InternalPrimaryDisplayResolutionVertical - Retrieves the number of pixels in the vertical direction of the internal display
* Census\_PowerPlatformRoleName - Indicates the OEM preferred power management profile. This value helps identify the basic form factor of the device
* Census\_InternalBatteryType - NA
* Census\_InternalBatteryNumberOfCharges - NA
* Census\_OSVersion - Numeric OS version Example - 10.0.10130.0
* Census\_OSArchitecture - Architecture on which the OS is based. Derived from OSVersionFull. Example - amd64
* Census\_OSBranch - Branch of the OS extracted from the OsVersionFull. Example - OsBranch = fbl\_partner\_eeap where OsVersion = 6.4.9813.0.amd64fre.fbl\_partner\_eeap.140810-0005
* Census\_OSBuildNumber - OS Build number extracted from the OsVersionFull. Example - OsBuildNumber = 10512 or 10240
* Census\_OSBuildRevision - OS Build revision extracted from the OsVersionFull. Example - OsBuildRevision = 1000 or 16458
* Census\_OSEdition - Edition of the current OS. Sourced from HKLM\Software\Microsoft\Windows NT\CurrentVersion@EditionID in registry. Example: Enterprise
* Census\_OSSkuName - OS edition friendly name (currently Windows only)
* Census\_OSInstallTypeName - Friendly description of what install was used on the machine i.e. clean
* Census\_OSInstallLanguageIdentifier - NA
* Census\_OSUILocaleIdentifier - NA
* Census\_OSWUAutoUpdateOptionsName - Friendly name of the WindowsUpdate auto-update settings on the machine.
* Census\_IsPortableOperatingSystem - Indicates whether OS is booted up and running via Windows-To-Go on a USB stick.
* Census\_GenuineStateName - Friendly name of OSGenuineStateID. 0 = Genuine
* Census\_ActivationChannel - Retail license key or Volume license key for a machine.
* Census\_IsFlightingInternal - NA
* Census\_IsFlightsDisabled - Indicates if the machine is participating in flighting.
* Census\_FlightRing - The ring that the device user would like to receive flights for. This might be different from the ring of the OS which is currently installed if the user changes the ring after getting a flight from a different ring.
* Census\_ThresholdOptIn - NA
* Census\_FirmwareManufacturerIdentifier - NA
* Census\_FirmwareVersionIdentifier - NA
* Census\_IsSecureBootEnabled - Indicates if Secure Boot mode is enabled.
* Census\_IsWIMBootEnabled - NA
* Census\_IsVirtualDevice - Identifies a Virtual Machine (machine learning model)
* Census\_IsTouchEnabled - Is this a touch device ?
* Census\_IsPenCapable - Is the device capable of pen input
* Census\_IsAlwaysOnAlwaysConnectedCapable - Retreives information about whether the battery enables the device to be AlwaysOnAlwaysConnected .
* Wdft\_IsGamer - Indicates whether the device is a gamer device or not based on its hardware combination.
* Wdft\_RegionIdentifier - NA

Приложение 2

Код предварительной обработки исходных данных

Приложение 3

Код реализованной модели ИНС на языке Python