ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И АНАЛИЗА СЕТЕВОГО ТРАФИКА

Ю. А. Крыжановская
Воронежский государственный университет, г. Воронеж, Российская Федерация
ORCID: https://orcid.org/0000-0002-7420-1900, ✍ jak@mail.ru

Аннотация: статья посвящена практическому применению нейронных сетей для решения задач генерации криптографических ключей и анализа сетевого трафика с целью обнаружения вторжений. В качестве средства реализации использовались язык Python и ряд библиотек. Для задачи генерации ключей применялся многослойный персептрон, включающий три слоя и обучавшийся на наборе случайных векторов, каждый из которых состоял из десяти случайных чисел. На выходе получается 128-битная бинарная последовательность, которая может использоваться в качестве криптографического ключа. Модель для анализа сетевого трафика обучалась на наборе данных, который был предварительно обработан с целью сокращения размерности, повышения точности обнаружения сетевых атак. Каждая из моделей обучалась в сто эпох. В ходе выполнения работы также анализировалось качество предложенных решений. Для сгенерированных ключей энтропия оценивалась по формуле Шеннона. Для построенной модели энтропия оказалась близка к единице, что говорит о возможности применения такого подхода. Для оценки качества модели анализа сетевого трафика применялась метрика accuracy. Анализ показал, что предложенная модель не переобучается, ее точность превышает 99%, что означает, что она хорошо подходит для классификации сетевого подключения.

Ключевые слова: многослойный персептрон, нейронная сеть, криптографический ключ, сетевой трафик.

Для цитирования: Крыжановская Ю. А. Применение нейронных сетей для генерации криптографических ключей и анализа сетевого трафика. *Успехи кибернетики*. 2025;6(4):50–54.

Поступила в редакцию: 14.10.2025. *В окончательном варианте: 20.11.2025.*

NEURAL NETWORKS FOR CRYPTOGRAPHIC KEY GENERATION AND NETWORK-TRAFFIC ANALYSIS

Yu. A. Kryzhanovskaya
Voronezh State University, Voronezh, Russian Federation
ORCID: https://orcid.org/0000-0002-7420-1900, ✍ jak@mail.ru

Abstract: we studied the practical application of neural networks to cryptographic key generation and network traffic analysis. The latter task plays a key role in intrusion detection systems. We implemented our approach in Python using specialized libraries. For key generation, we employed a three-layer multilayer perceptron trained on random vectors containing ten random numbers each. The network produced a 128-bit binary sequence suitable for use as a cryptographic key. The entropy of the generated keys was estimated using Shannon's formula; the resulting entropy was close to one, indicating the feasibility of the proposed approach. For network traffic analysis, we trained a model on a preprocessed dataset. The preprocessing reduced dimensionality and improved attack-detection accuracy. Each model was trained for one hundred epochs. Model performance was evaluated using the accuracy metric. The results showed no signs of overfitting, and the model achieved an accuracy exceeding 99%, demonstrating its suitability for network connection classification.

Keywords: multilayer perceptron, neural network, cryptographic key, network traffic.

Cite this article: Kryzhanovskaya Yu. A. Neural Networks for Cryptographic Key Generation and Network-Traffic Analysis. *Russian Journal of Cybernetics*. 2025;6(4):50–54.

Original article submitted: 14.10.2025. *Revision submitted: 20.11.2025.*

Введение

К настоящему моменту нейронные сети [1] получили широкое распространение в самых различных областях человеческой деятельности, таких как обработка мультимедиа [2], судебная медицина [3], прогнозирование потребности в лекарственных препаратах [4], анализ кредитных рисков [5, 6]

библиотечное дело [7], судостроение [8], информационная безопасность [9, 10] и других. В области информационной безопасности нейронные сети находят применение, например, в задачах криптоанализа, при обнаружении аномалий и вторжений в системах защиты информации [11], в генерации псевдослучайных последовательностей и ключей. В данной статье предложен вариант решения задачи генерации криптографических ключей и бинарной классификации сетевых подключений.

Постановка задачи

Целью работы являлась реализация применения нейронных сетей для генерации криптографических ключей и анализа сетевого трафика. Для этого было необходимо решить следующие задачи:

1. Сгенерировать криптографический ключ с помощью многослойного персептрона (MLP).
2. Оценить характеристику сгенерированного ключа (энтропию).
3. Использовать нейросетевую модель для анализа датасета, содержащего данные сетевого трафика (IDS).
4. Оценить качество обученной модели.

Средства реализации

В качестве средства реализации использовались язык Python и такие библиотеки, как pandas, numpy, random, tensorflow, keras, matplotlib.pyplot.

Генерация криптографического ключа

Для генерации ключа построена простая модель нейронной сети — многослойный персептрон (MLP) [1], принимающая на вход случайный шум и генерирующая 128-битный бинарный ключ. Обучение проводится на случайных данных. В результате генерируется новый ключ. Для оценки качества полученного ключа использовалась энтропия, под которой понимается мера неопределенности или случайности. В криптографии высокая энтропия ключа означает хорошую устойчивость к атакам. Энтропия рассчитывается по формуле Шеннона (1):

$$H = -\sum p(x)\log_2 p(x), \tag{1}$$

где p(x) — вероятность появления символа в ключе. Приемлемым показатель считается, если его значение приближается к 1.

На первоначальном этапе было необходимо спроектировать многослойный персептрон (MLP), который будет использоваться для обучения и генерации новых ключей. MLP содержит три слоя:

- слой, принимающий на вход вектор из 10 случайных чисел (применяется функция активации — relu);
- скрытый слой (применяется функция активации — relu);
- слой, возвращающий 128-битный ключ (применяется функция активации — sigmoid).

Затем производится генерация 1000 случайных векторов чисел для обучения. В качестве целевой переменной выступают случайно сгенерированные ключи. Модель обучается 100 эпох.

Для генерации (предсказания) нового ключа необходимо сгенерировать случайный шум (вектор длиной 10) и подать на вход обученной модели нейронной сети. Модель выдаст предсказание, при интерпретации которого получается новый сгенерированный криптографический ключ.

Для оценки качества используется энтропия, рассчитанная по специальной формуле (1). Результат отображается на экране. В качестве примера рассмотрим результаты трех тестов.

Результат 1:

*** Генерация и анализ ключа ***

Сгенерированный криптографический ключ:

00011111110011010010000010101110001110110000110100000100001100000000001101100111100110101110000101011100100011000010010001001111

Энтропия ключа: 0.9887

Результат 2:

*** Генерация и анализ ключа ***

Сгенерированный криптографический ключ:

10100100001111100101000011001111111111101100010010100010001101010110100101101001110000001000100111111100010111110101001111101101 1

Энтропия ключа: 0.9972

Результат 3:

*** Генерация и анализ ключа ***

Сгенерированный криптографический ключ:

10011000001001001110011111100110110100000111111011111101111111000000010010001110011 10100001100110010010001100011000010111001111

Энтропия ключа: 0.9998

Как можно видеть, в каждом из случаев был сгенерирован уникальный 128-битный ключ с очень высоким (близким к 1) показателем энтропии, что позволяет считать, что построенная модель нейронной сети пригодна для генерации криптографических ключей.

Анализ трафика с помощью нейронной сети

Нейронные сети также могут использоваться для анализа датасетов, содержащих информацию о сетевых подключениях. В рамках данной работы будет использоваться набор данных NSL-KDD, применимый для задач систем обнаружения вторжений (IDS). Данный датасет включает более 100000 предназначенных для обучения и более 20000 предназначенных для тестирования записей о сетевых соединениях, происходящих с использованием протоколов TCP, UDP, ICMP, каждое из которых определяется как «нормальное» или как один из видов атак. Фрагмент данных с выделенной характеристикой вида «нормальное / один из видов атаки» приведен на рис. 1.

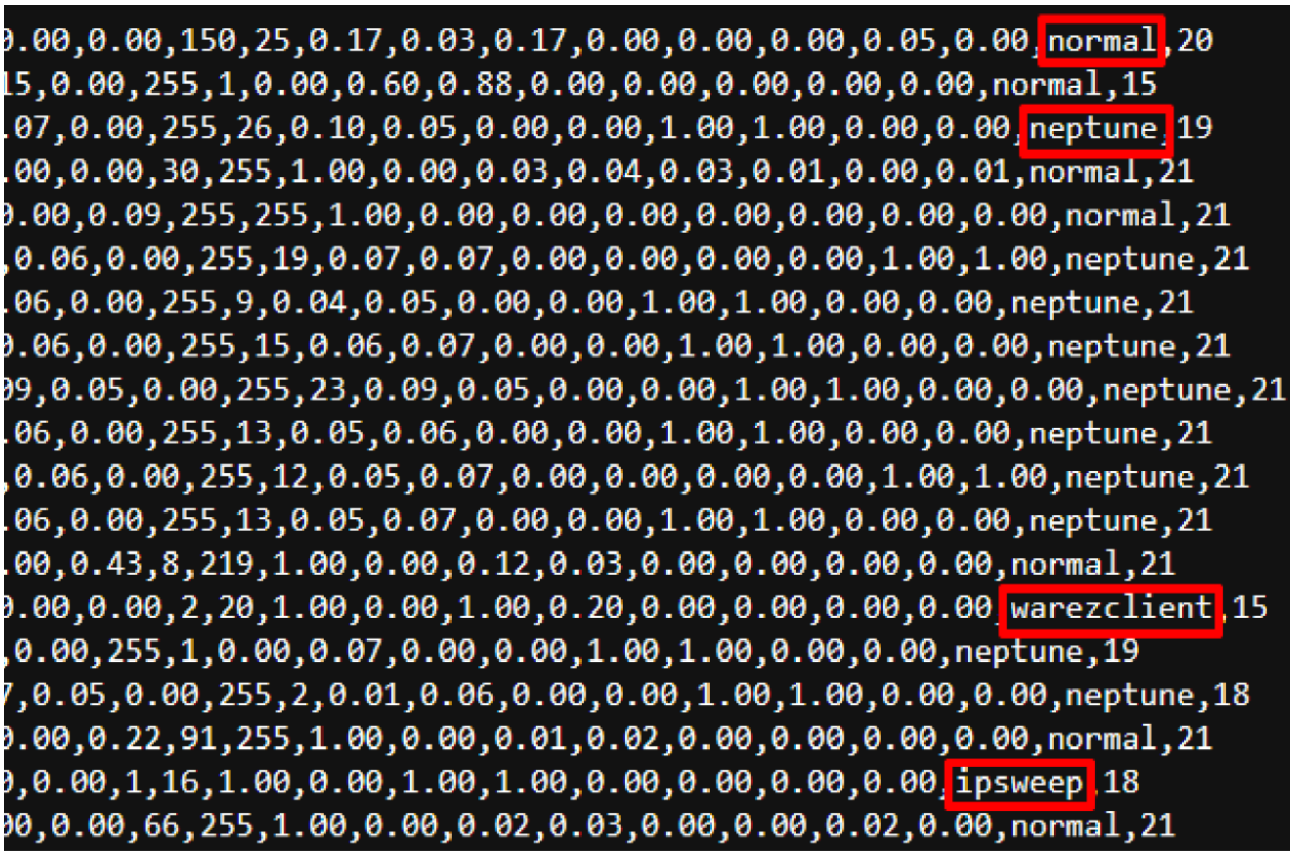

Рис. 1. *Фрагмент данных датасета*

Данная последовательность представляет собой поток данных между источником и адресатом сетевых пакетов в соответствии с IP-адресом, указанным в заголовке пакета, и содержит числовые и нечисловые данные. В рамках данной работы модель нейронной сети обучалась классифицировать сетевое соединение как нормальное (normal) или содержащее какую-либо атаку.

Перед использованием данного набора требуется выполнить предобработку, проведя кодирование меток и сокращение размерности. Для этих целей исключаются нечисловые признаки (например, TCP кодируется 0, UDP — 1, SMTP — 2), метки «normal» заменяются на 0, метки атак заменяются на 1. Также производится сокращение размерности за счет устранения малозначимых параметров, что позволит ускорить вычисления, производимые нейронной сетью, поскольку сокращается число нейронов входного слоя и тем самым повышается точность обнаружения сетевых атак благодаря концентрации обучения нейронной сети только на значимых параметрах. Важность параметров оценивалась эмпирически: за один раз удалялся один параметр и на полученном наборе данных обучалась и тестировалась нейронная сеть [12]. Во время тестирования фиксировались показатели качества нейронной сети по метрике: точность классификации — precision (2), так как данная метрика не зависит от соотношения классов и потому применима в условиях несбалансированных выборок, к которым относится и NSL-KDD:

$$precision = \frac{TP}{TP + FP}, \tag{2}$$

где *TP — True Positive* — классификатор верно отнес объект к рассматриваемому классу, *FP – False Positive* — классификатор неверно отнес объект к рассматриваемому классу.

Отделяется целевая переменная, данные нормализуются и делятся на обучающую и тестовую выборки: 80% — обучающая выборка, 20% — тестовая выборка. Затем строится аналогичная нейронная сеть для бинарной классификации, содержащая чуть меньшее количество нейронов.

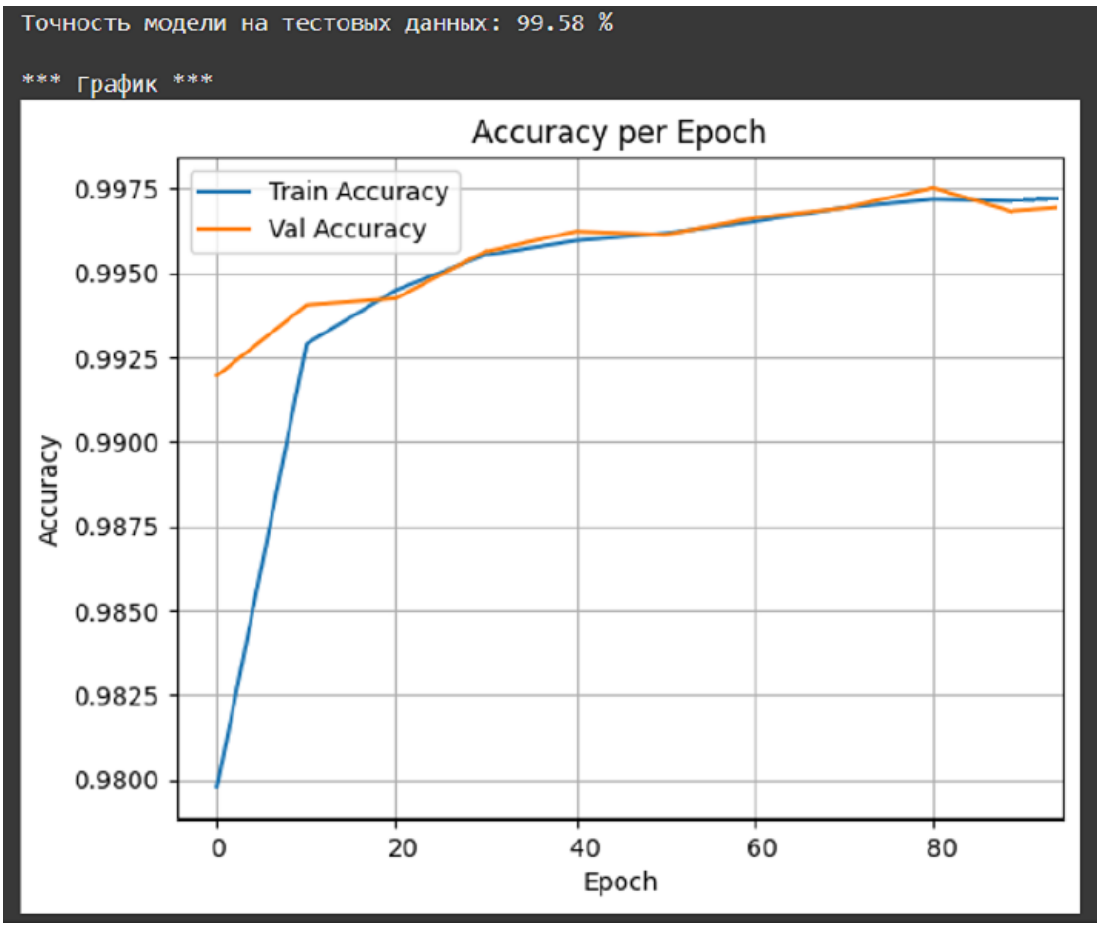

Рис. 2. *Точность модели*

Построенная модель обучается 100 эпох на предобработанных ранее данных. Для обученной сети применяется метрика accuracy, описываемая формулой (3):

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN}, \tag{3}$$

где *TP* и *FP* имеют тот же смысл, что и в формуле (2), а *TN* (*True Negative)* и *FN (False Negative)* означают, что классификатор верно и неверно утверждает, что объект не принадлежит к рассматриваемому

классу, соответственно. Полученная точность модели выводится на экран, а также визуализируется с помощью графиков (рис. 2).

Анализируя полученный график, можно заметить, что обе кривые поднимаются вверх, что означает, что модель обучается и становится качественнее на обеих выборках. Также растет и стабилизируется валидационная точность: модель не переобучается. А маленький разрыв между обучающей и валидационной точностью также говорит об отсутствии переобучения. Таким образом, можно с уверенностью сказать о том, что построенная модель отлично справляется с задачей классификации статуса сетевого подключения в указанном наборе данных.

Заключение

В ходе выполнения данной работы реализован способ генерации криптографических ключей с приемлемой степенью случайности, что подтверждается рассчитанной энтропией, с использованием многослойного персептрона (MLP). Также построена и обучена нейросетевая модель для бинарной классификации сетевых атак, проведена оценка точности модели на тестовой выборке и построен график, визуализирующий качество обучения.

ЛИТЕРАТУРА

1. Галушкин А. И. *Нейронные сети: основы теории*. М.: Горячая линия-Телеком; 2024. 496 с. Режим доступа: https://e.lanbook.com/book/448412.
2. Молодяков С. А. *Применение нейронных сетей для обработки мультимедийного контента (100 примеров на Python):* монография. СПб.: ПОЛИТЕХ-ПРЕСС; 2025. 572 с. DOI: 10.18720/SPBPU/2/id25-4.
3. Крыжановский В. Д., Крыжановская Ю. А. Применение нейронной сети для решения задачи классификации в судебной медицине. *Вестник УрФО. Безопасность в информационной сфере.*2023;3:21–27. DOI: 10.14529/secur230302.
4. Крыжановский В. Д. Программный модуль прогнозирования плановой потребности в медицинской продукции. *Успехи кибернетики*. 2024;5(4):40–44. DOI: 10.51790/2712-9942-2024-5-4-05.
5. Munkhdalai, L., Munkhdalai T., Namsrai O., Lee J., Ryu K. An Empirical Comparison of Machine-Learning Methods on Bank Client Credit Assessments. *Sustainability*. 2019;11(3):699–722. DOI: 10.3390/su11030699.
6. Addo P., Guegan D., Hassani B. Credit Risk Analysis Using Machine and Deep Learning Models. *Risks.* 2018;6(2):38. DOI: 10.3390/risks6020038.
7. Нуждова Д. А. Нейросети в библиотечном деле: опыт проекта «Новые библиотекари». *Корпоративные библиотечные системы: технологии и инновации:* материалы Международной научно-практической конференции. 2023:59–65. DOI: 10.18720/SPBPU/2/k23-6.
8. Кирильчук С. П., Князева Д. С. Data mining в системе управленческих навыков (в приложении к сфере гражданского судостроения). *Современные информационные технологии и ИТ-образование*. 2022;8(1):98–106. DOI: 10.25559/SITITO.18.202201.98-106.
9. Власов К. А. Нейрокриптографическая система рекуррентных конвергентных нейросетей защиты информации. *Вопросы кибербезопасности*. 2020;4:44–55. DOI: 10.21681/2311-3456-2020-04-44-55.
10. George A., Marcel S. Learning One Class Representations for Face Presentation Attack Detection Using Multi-Channel Convolutional Neural Networks. *IEEE Transactions on Information Forensics and Security*. 2021;16:361–375. DOI: 10.1109/TIFS.2020.3013214.
11. Yu W., Wang Y., Song L. A Two Stage Intrusion Detection System for Industrial Control Networks Based on Ethernet/IP. *Electronics*. 2019;8(12):1545. DOI: 10.3390/electronics8121545.
12. Татарникова Т. М., Бимбетов Ф., Богданов П. Ю. Выявление аномалий сетевого трафика методом глубокого обучения. Известия СПБГЭТУ ЛЭТИ. 2021;4:36–41. Режим доступа: http://elibrary.ru/item.asp?id=45736639.