МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра Информационная безопасность

вычислительных систем и сетей

«Комплексное исследование и сравнительный анализ эффективности методов машинного и глубокого обучения»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовой работе
по дисциплине

Интеллектуальные методы информационной безопасности открытых информационных систем

РУКОВОДИТЕЛЬ:

Санников А.Н.

_____
(подпись)

СТУДЕНТ:

Корнилов В.И.

_____
(подпись)

С22-СИБ
(шифр группы)

Работа защищена «___» _____

С оценкой _____

Нижний Новгород 2025

Цель работы:

Целью курсовой работы является комплексное исследование и сравнительный анализ эффективности классических и современных интеллектуальных методов машинного и глубокого обучения - включая методы кластеризации, алгоритмы ближайших соседей, рекуррентные (LSTM) и свёрточные (1D-CNN) нейронные сети - для решения задач информационной безопасности в двух существенно различных предметных областях:

1. обнаружение фейковых аккаунтов в социальных сетях на основе статических признаков поведения,
2. автоматическая классификация сердечных аритмий по биометрическим ЭКГ-сигналам как элемента систем биометрической идентификации и защиты персональных медицинских данных.

Особое внимание уделяется сравнению обобщающей способности, устойчивости к дисбалансу данных, вычислительной сложности и практической применимости рассмотренных подходов в условиях, приближенных к реальным сценариям информационной безопасности открытых информационных систем.

Введение

В условиях стремительного развития цифровых технологий и повсеместного распространения открытых информационных систем вопросы обеспечения их безопасности приобретают всё большую актуальность. Современные угрозы - от фейковых аккаунтов и ботов в социальных сетях до несанкционированного доступа к персональным медицинским данным - требуют не только традиционных, но и интеллектуальных, адаптивных методов защиты. В этом контексте методы машинного и глубокого обучения становятся мощным инструментом для автоматического выявления аномалий, классификации угроз и биометрической идентификации пользователей.

Курсовая работа посвящена системному исследованию и сравнительному анализу интеллектуальных методов, применяемых в задачах информационной безопасности. Рассматриваются два принципиально различных сценария:

1. обнаружение фейковых профилей в социальных сетях на основе статических поведенческих признаков,
2. автоматическая классификация сердечных аритмий по сигналам ЭКГ как компонента систем биометрической аутентификации и защиты медицинских данных.

В первой части работы применяются классические методы машинного обучения: кластеризация (K-means, агломеративная иерархическая) и классификация (kNN) для анализа сбалансированного датасета аккаунтов соцсети. Во второй и третьей частях исследуются современные архитектуры глубокого обучения - рекуррентная сеть LSTM и одномерная свёрточная сеть (1D-CNN) - на реальном медицинском датасете MIT-BIH Arrhythmia Database,

характеризующемся сильным дисбалансом классов и высокой вариативностью сигналов.

Актуальность выбранной темы обусловлена:

- ростом числа мошеннических аккаунтов и автоматизированных ботов в социальных сетях;
- необходимостью защиты биометрических данных, особенно в условиях цифровизации здравоохранения;
- отсутствием универсальных решений - эффективность методов сильно зависит от типа данных и постановки задачи.

Целью работы является не только демонстрация применимости отдельных алгоритмов, а глубокое сопоставление их возможностей: точности, устойчивости к шуму и дисбалансу, вычислительной сложности, интерпретируемости и практической реализуемости в реальных системах информационной безопасности.

Работа состоит из четырёх глав. Первые три посвящены реализации и анализу отдельных подходов: классических методов, LSTM и CNN. Четвёртая глава представляет собой сравнительный анализ, в котором обобщаются полученные результаты и формулируются рекомендации по выбору метода в зависимости от специфики задачи и доступных ресурсов.

Глава 1. Классические методы машинного обучения: кластеризация и классификация данных социальных сетей

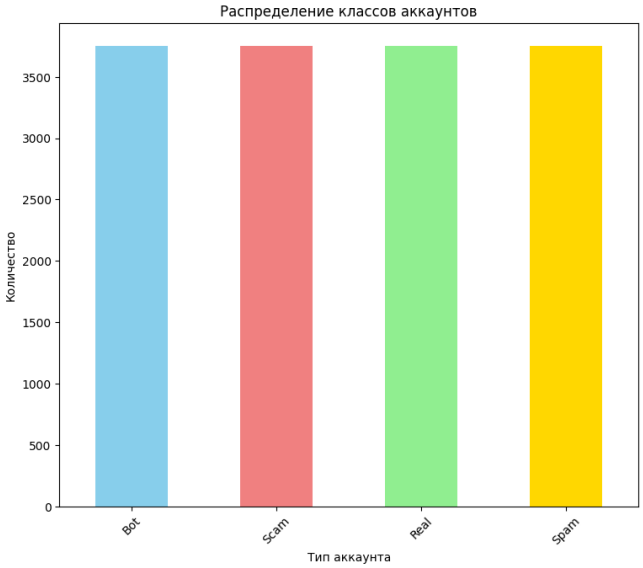
1.1. Постановка задачи и особенности данных

В современных открытых информационных системах одной из ключевых угроз безопасности являются фейковые аккаунты - боты, спамеры и мошенники, имитирующие реальных пользователей. Автоматическое обнаружение таких профилей является важной задачей модерации и защиты цифровой среды.

В данной главе рассматривается задача анализа аккаунтов в социальной сети с использованием классических методов машинного обучения: кластеризации (без учителя) и классификации (с учителем). Исходный датасет содержит 15 000 записей, равномерно распределённых по четырём классам: Real (реальные пользователи), Bot, Scam, Spam - по 3 750 записей каждого типа. Такая сбалансированность делает данные идеальными для обучения и оценки моделей без необходимости в дополнительных методах балансировки.

Каждая запись включает 11 признаков, из которых:

- 4 числовых: Followers, Following, Posts, Mutual Friends;
- 7 категориальных: наличие биографии, аватара, внешней ссылки, и др.;
- 1 целевая переменная: метка класса (0-3).



Статистика числовых признаков

	Followers	Following	Posts	Mutual Friends
count	15000.0	15000.0	15000.0	15000.0
mean	23397.378933333333	1385.35	427.8302	3.0117333333333334
std	41920.419060580614	1600.8231629029463	678.889037022693	4.20331300106252
min	0.0	0.0	0.0	0.0
25%	6.0	369.0	1.0	0.0
50%	48.0	725.5	4.0	0.0
75%	19535.25	1747.0	578.25	6.0
max	163000.0	6692.0	2669.0	15.0

Рис. 1.1

На Рис. 1.1 показано распределение экземпляров по классам, подтверждающее полную сбалансированность выборки.

1.2. Предварительная обработка и анализ данных

До применения алгоритмов машинного обучения был проведён этап предобработки. В данных обнаружены артефакты вида "DIV/0!", возникшие при расчёте относительных метрик (например, Posts/Followers). Они были заменены на нули. Категориальные признаки преобразованы в бинарные (one-hot encoding), числовые - оставлены в исходном виде, но нормализованы при необходимости.

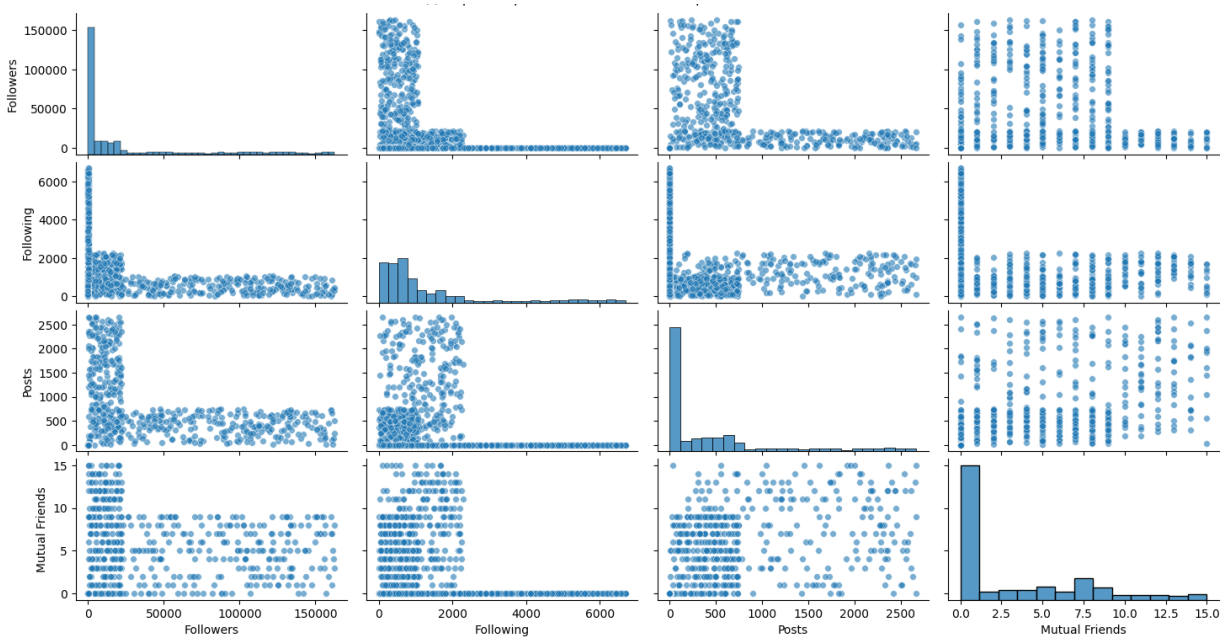


Рис. 1.2

Для визуального анализа взаимосвязей между признаками построена матрица диаграмм рассеяния (PairPlot).

График показывает:

- высокую концентрацию пользователей с низкими значениями Followers и Following (характерно для соцсетей);
- слабую положительную связь между Posts и Mutual Friends (r = 0.59);
- слабую отрицательную корреляцию между Followers и Following (r = –0.27).

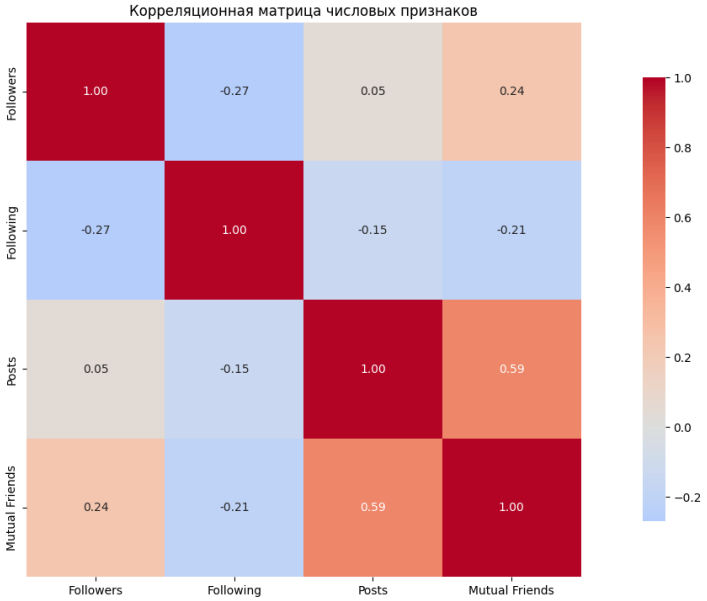


Рис. 1.3

Эти наблюдения подтверждаются тепловой картой корреляционной матрицы (Рис. 1.3), где явные линейные зависимости отсутствуют. Это говорит о том, что признаки в основном независимы, что благоприятно для работы алгоритмов кластеризации.

1.3. Кластеризация: выбор метода и оценка качества

Поскольку исходная задача не предполагает использования меток на этапе кластеризации, применялись алгоритмы обучения без учителя.

Определение оптимального числа кластеров

Для выбора количества кластеров использовались два подхода:

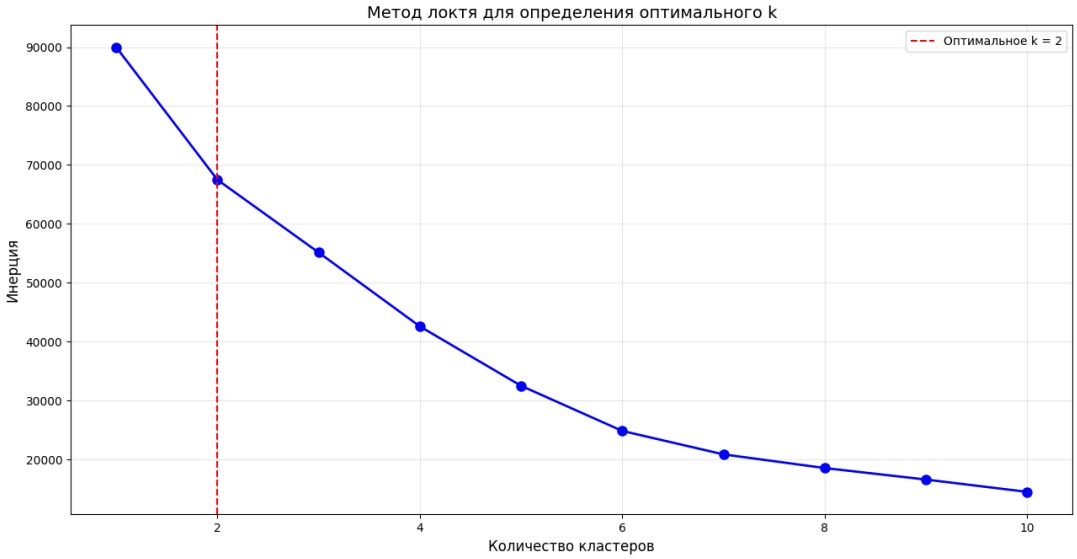


Рис. 1.4

- Метод локтя (Рис. 1.4): инерция резко снижается при переходе от k=1 к k=2, после чего убывает медленнее. Точка «локтя» явно указывает на k = 2.

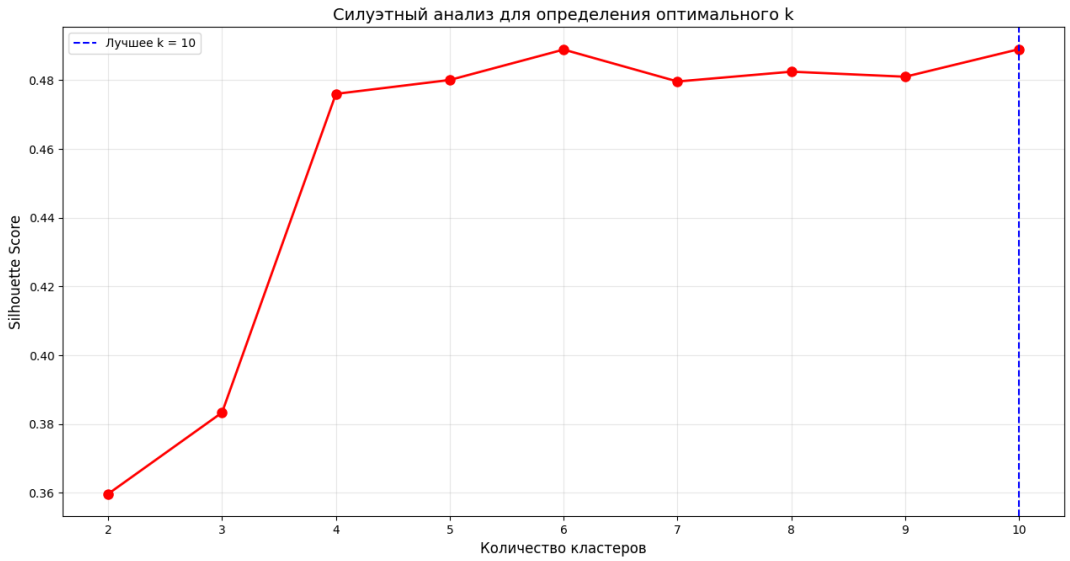


Рис. 1.5

- Силуэтный анализ (Рис. 1.5): максимальный силуэтный коэффициент (0.489) достигается при k = 10, однако прирост качества незначителен.

С учётом практической интерпретируемости и чёткости «локтя», было принято решение использовать k = 2 - интерпретируемых как «реальные» и «фейковые» аккаунты.

Сравнение алгоритмов кластеризации

Применены:

- K-means и K-means++ (евклидово расстояние);
- Агломеративная иерархическая кластеризация с различными метриками (евклидово, манхэттенское, Чебышёва) и методами связывания (ward, average, complete).

Результаты:

- K-means: Silhouette Score = 0.3596;

- Агломеративная кластеризация с любым сочетанием average/complete + любая метрика: Silhouette Score = 0.9402.

Таким образом, агломеративный метод показал превосходное качество группировки, что объясняется его способностью учитывать глобальную структуру данных (в отличие от K-means, ориентированного на сферические кластеры).

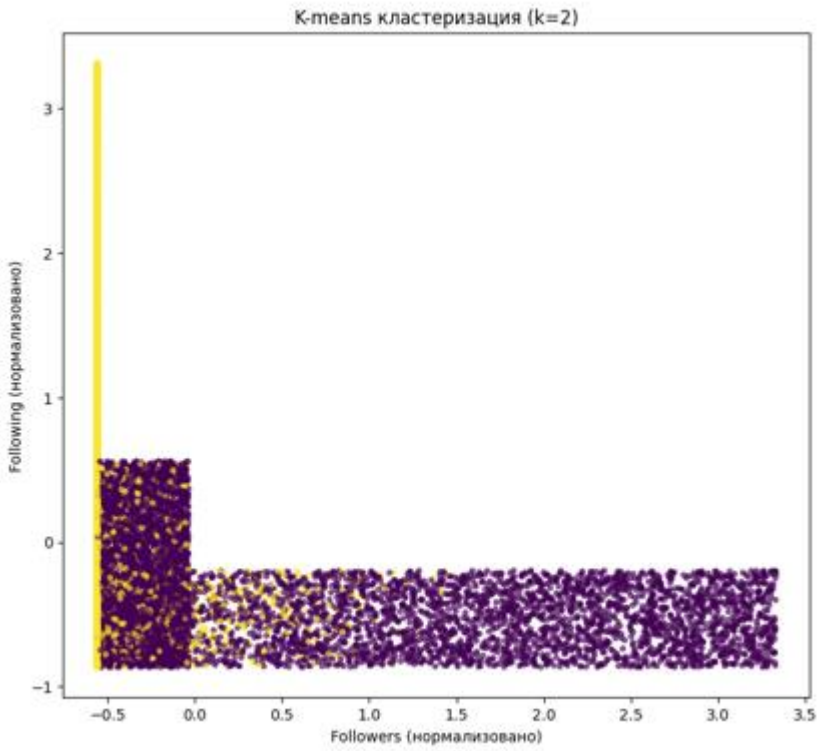


Рис. 1.6

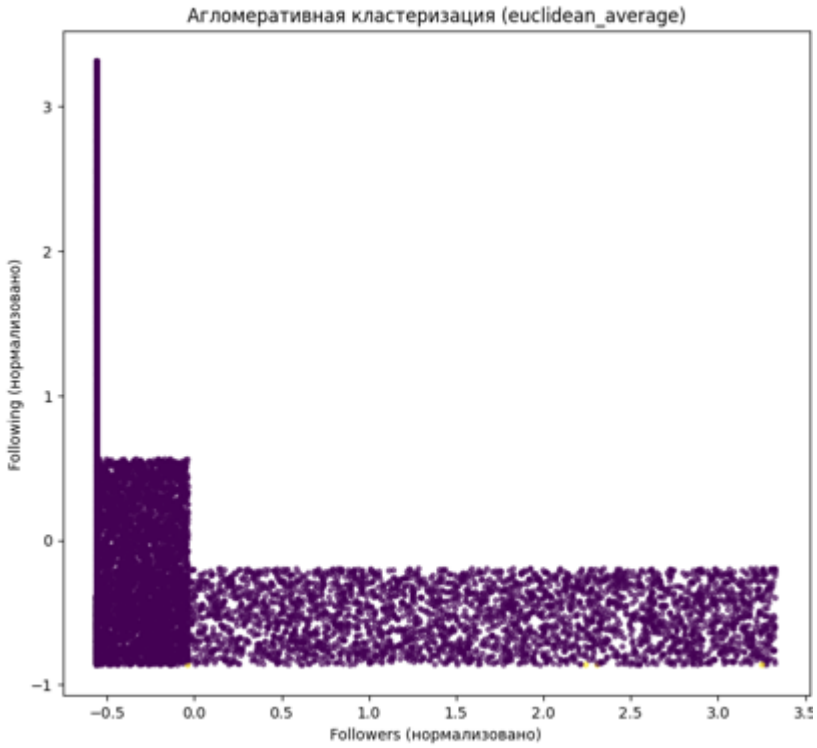


Рис. 1.7

На Рис. 1.6 (K-means, k=2) и Рис. 1.7 (агломеративная кластеризация, euclidean + average) из файла ИИ1.pdf представлены визуализации кластеров в пространстве первых двух главных компонент (PCA). Видно, что агломеративный метод даёт чёткое разделение, тогда как K-means формирует смешанные группы.

1.4. Классификация: бинарная и мультиклассовая задачи

Для решения задачи обнаружения фейковых профилей использован алгоритм k-ближайших соседей (kNN).

Бинарная классификация (Real vs Fake)

Классы Bot, Scam и Spam объединены в один - Fake. Получена задача бинарной классификации с дисбалансом 3:1 (11 250 vs 3 750).

Модель kNN (k=7) показала:

- Accuracy = 97.07%;
- AUC = 0.9926.

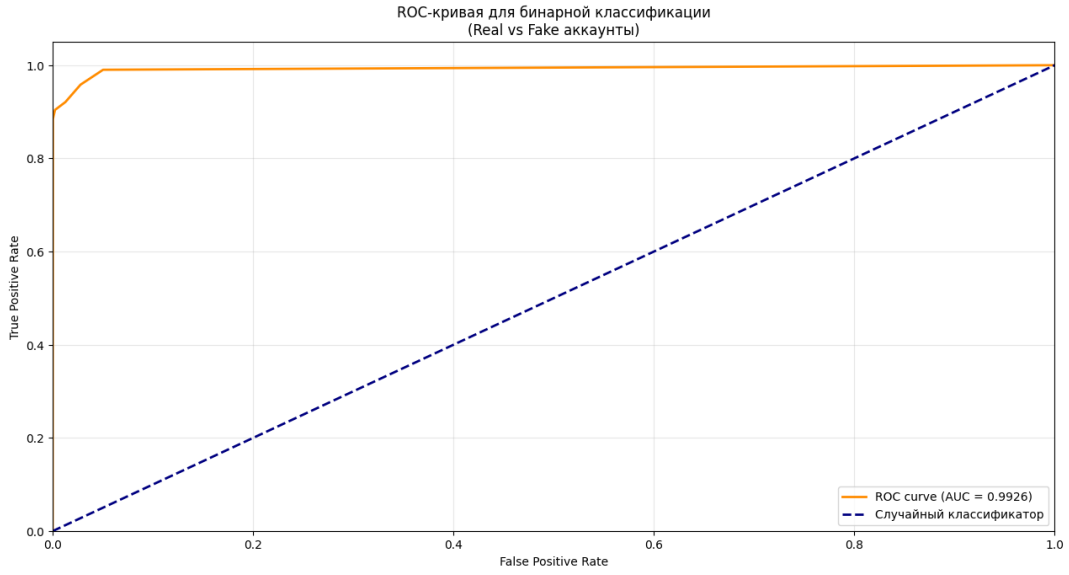


Рис. 1.8

ROC-кривая (Рис. 1.8) практически совпадает с левым верхним углом, что указывает на высокую способность модели различать классы даже при низком пороге ложных срабатываний - критически важное свойство для систем безопасности.

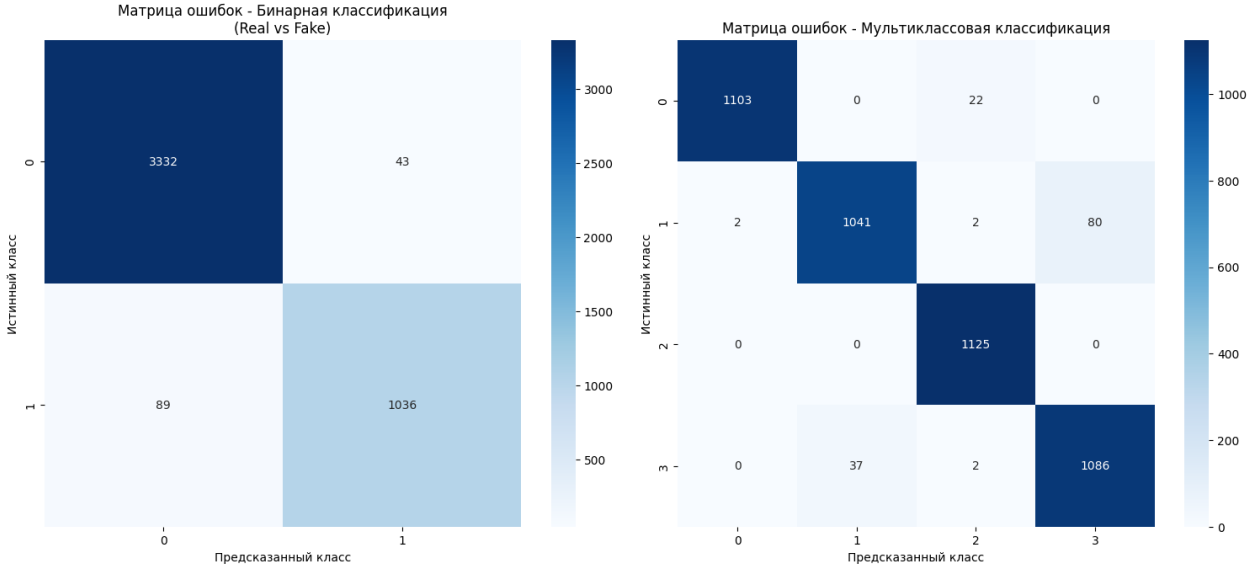


Рис. 1.9

Матрица ошибок (Рис. 1.9, слева) показывает:

- 3 332 правильно классифицированных фейковых аккаунта;
- 1 006 правильно определённых реальных пользователей.

Мультиклассовая классификация (4 класса)

Та же модель kNN (k=7) применена к исходной задаче.

Результаты:

- Общая точность = 96.78%;
- F1-меры по классам: от 0.94 до 0.98;

Наибольшая путаница - между классами Real и Spam, что объяснимо их схожей активностью.

Матрица ошибок (Рис. 1.9, справа) демонстрирует высокую диагональ, подтверждая надёжность предсказаний.

1.5. Выводы по главе

1. Исходный датасет аккаунтов соцсети полностью сбалансирован, содержит четкие паттерны поведения, различающие реальные и фейковые профили.
2. Агломеративная кластеризация значительно превосходит K-means по качеству группировки (Silhouette Score: 0.9402 vs 0.3596).
3. Алгоритм kNN показывает высокую эффективность как в бинарной (AUC = 0.9926), так и в мультиклассовой (Accuracy = 96.78%) постановках.
4. Полученные модели практически применимы для систем автоматического мониторинга социальных сетей и предотвращения мошенничества.

Глава 2. Рекуррентные нейронные сети для анализа временных биометрических данных

2.1. Постановка задачи и обоснование выбора данных

В современных системах информационной безопасности всё большее значение приобретают динамические биометрические методы, основанные на анализе поведенческих и физиологических характеристик пользователя во времени. Одним из наиболее перспективных источников таких данных является электрокардиограмма (ЭКГ) - уникальный, трудно подделываемый сигнал, отражающий электрическую активность сердца.

В данной главе рассматривается задача автоматической классификации типов сердечных сокращений на основе сигналов ЭКГ как компонента систем биометрической идентификации и защиты персональных медицинских данных. Для этого применяется рекуррентная нейронная сеть с долгой краткосрочной памятью (LSTM), способная эффективно моделировать временные зависимости в последовательностях.

В качестве источника данных выбран общепринятый в научном сообществе MIT-BIH Arrhythmia Database - датасет, содержащий 109 446 сегментов ЭКГ, размеченных экспертами на 5 классов согласно стандарту AAMI:

- N - нормальные сокращения,
- S - наджелудочковые экстрасистолы,
- V - желудочковые экстрасистолы,
- F - фьюжн-сокращения (гибридные),
- Q - неклассифицируемые или атипичные сокращения.

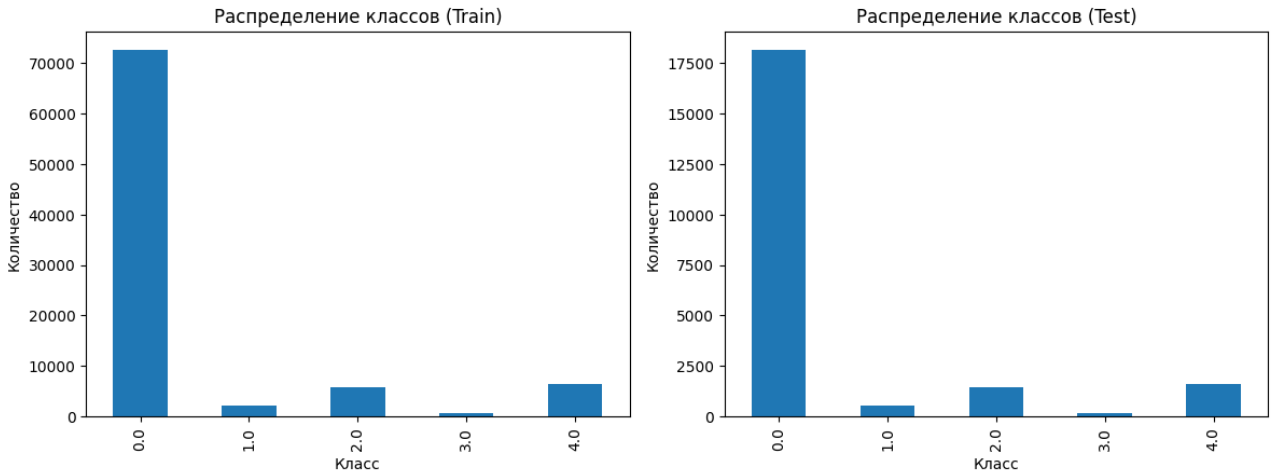


Рис. 2.1

На Рис. 2.1 показано распределение классов в обучающей и тестовой выборках. Наблюдается сильный дисбаланс: доля нормальных сокращений (N) превышает 90%, тогда как редкие классы (F, S) представлены всего сотнями записей. Это типичная ситуация для реальных медицинских данных и представляет серьёзный вызов для алгоритмов машинного обучения.

2.2. Предобработка и форматирование данных

Каждая запись ЭКГ представляет собой временной ряд длиной 187 отсчётов. Предобработка включала следующие этапы:

- Нормализация с использованием StandardScaler (нулевое среднее, единичная дисперсия),
- Преобразование в трёхмерный тензор формы (samples, timesteps, features) = (samples, 187, 1) - формат, требуемый для рекуррентных слоёв в TensorFlow/Keras,
- One-hot кодирование меток классов для многоклассовой классификации,
- Стратифицированное разбиение на обучающую (80%) и тестовую (20%) выборки.

Такой подход обеспечил сохранение исходного распределения классов и корректную работу модели на редких типах аритмий.

2.3. Архитектура LSTM-модели и обучение

Разработана многослойная LSTM-архитектура, включающая:

- входной слой с 187 временными шагами,
- два скрытых LSTM-слоя с 64 и 32 нейронами,
- полносвязные слои с регуляризацией (Dropout, BatchNormalization),
- выходной слой с активацией softmax для 5 классов.

Обучение проводилось с использованием:

- оптимизатора Adam (learning_rate = 0.001),
- функции потерь: Categorical Crossentropy,
- коллбэков: EarlyStopping (patience=15) и ReduceLROnPlateau (factor=0.5, patience=8).

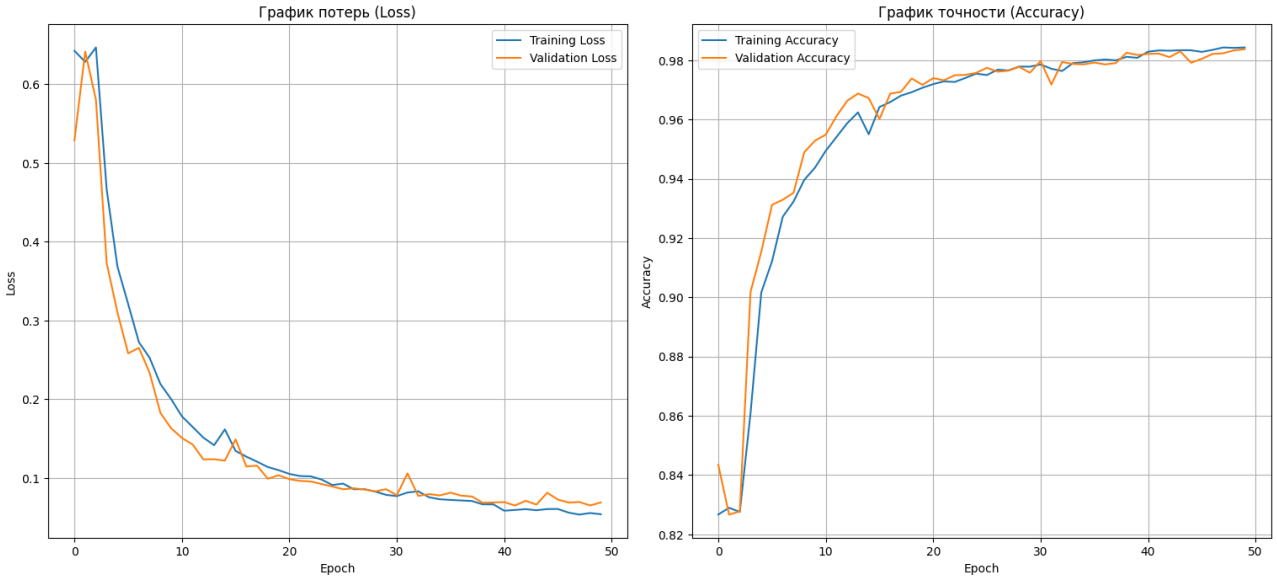


Рис. 2.2

На Рис. 2.2 представлены графики динамики функции потерь и точности на обучающей и валидационной выборках:

- Training Loss снизился с 0.6 до 0.0539,
- Validation Loss стабилизировался на уровне 0.0689,
- Validation Accuracy достигла 0.98,
- разрыв между train и val метриками незначителен (val/train loss ≈ 1.28), что указывает на умеренное переобучение, но в пределах допустимого.

2.4. Оценка качества модели

Модель показала высокую общую точность на тестовой выборке:

- Accuracy = 97.96%,
- Weighted F1-Score = 0.9785,
- Micro-average AUC = 1.00.

Анализ по классам

Подробные метрики (см. таблицу в ЛР2) выявляют следующие особенности:

- Класс N (нормальный): F1 = 0.9894 (самый высокий),
- Класс S (наджелудочковый): F1 = 0.7709 - наиболее сложный для классификации,
- Класс V (желудочковый): F1 = 0.9464,
- Класс F (фьюжн): низкий recall = 0.679 - модель пропускает около трети случаев,
- Класс Q (неклассифицируемый): F1 = 0.9805 - неожиданно высокий результат для «шумного» класса.

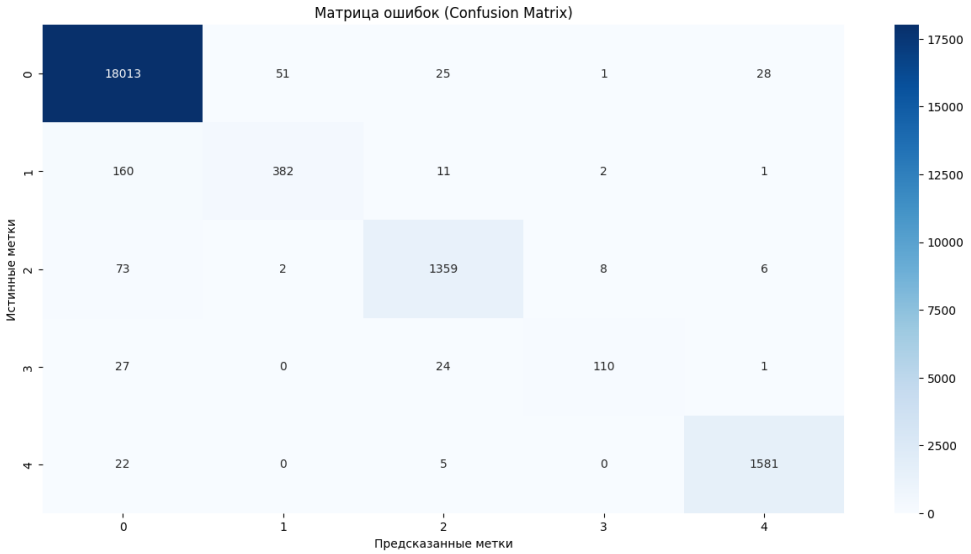


Рис. 2.3

На Рис. 2.3 видно, что основные ошибки происходят при классификации редких классов (S и F), которые часто путаются с классом N. Это объяснимо схожестью морфологии сигналов и малым количеством обучающих примеров.

ROC-анализ

Многоклассовые ROC-кривые Рис. 2.4 демонстрируют исключительное качество классификации:

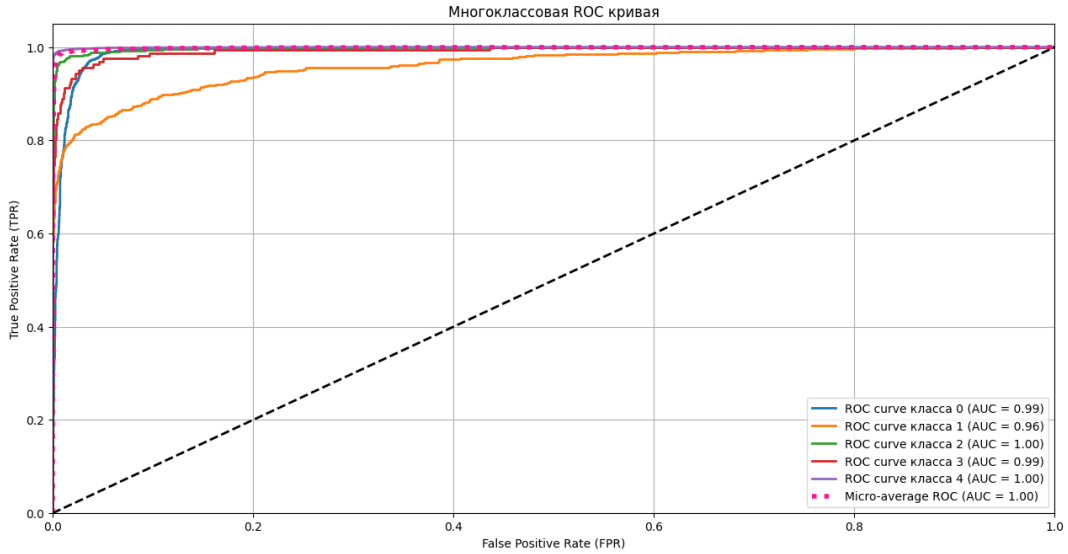


Рис. 2.4

AUC(N) = 0.99,

AUC(S) = 0.96,

AUC(V) = 1.00,

AUC(F) = 0.99,

AUC(Q) = 1.00.

Даже для самого сложного класса (S) AUC превышает 0.95, что свидетельствует о высокой дискриминативной способности модели.

Визуализация сигналов

Примеры ЭКГ для каждого класса (Рис. 2.5) иллюстрируют типичные паттерны:

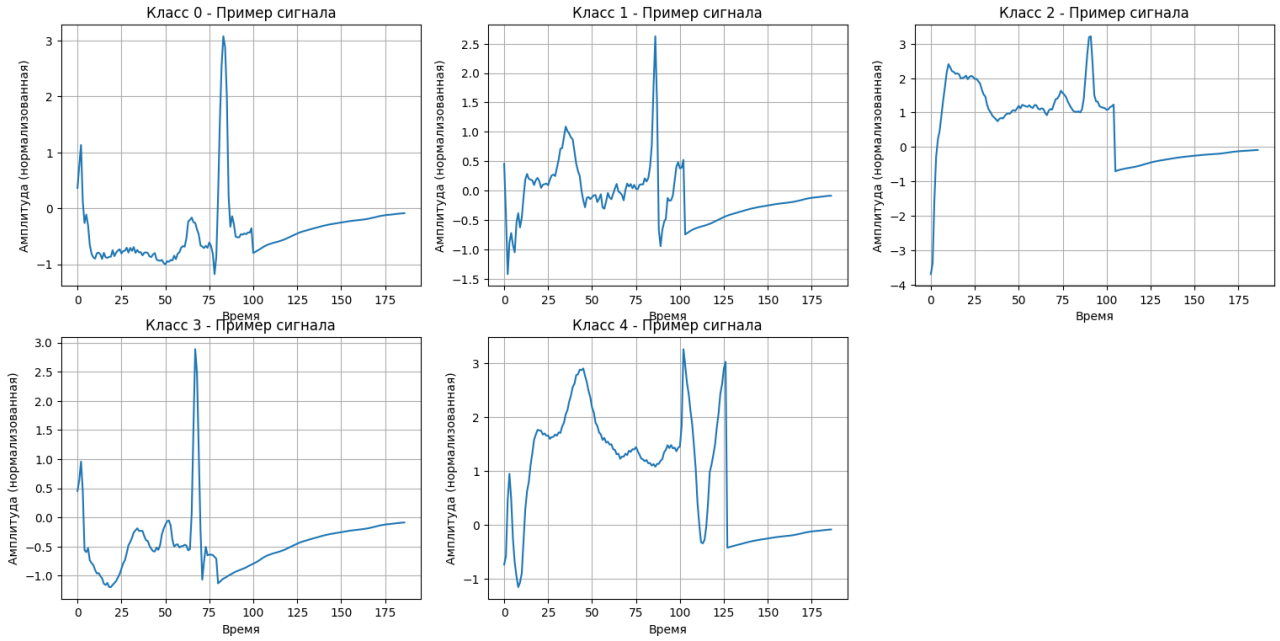


Рис. 2.5

Класс N: чёткий P-QRS-T комплекс, регулярный ритм,

Класс S: преждевременные узкие комплексы QRS,

Класс V: широкие, деформированные желудочковые комплексы,

Класс F: гибридные формы, сочетающие признаки N и V,

Класс Q: атипичные, разнообразные морфологии.

Эти визуальные различия подтверждают, что модель обучается на реальных биомедицинских признаках, а не на артефактах данных.

2.5. Выводы по главе

LSTM-архитектура успешно справляется с задачей классификации ЭКГ-сигналов, достигая Accuracy = 97.96% и AUC = 1.00 даже при сильном дисбалансе классов.

Наибольшие трудности возникают при распознавании наджелудочковых (S) и фьюжн-сокращений (F) - это связано как с их семантической близостью к нормальному ритму, так и с малым количеством обучающих примеров.

Модель демонстрирует высокую обобщающую способность и может быть использована как компонент систем биометрической идентификации или автоматической диагностики сердечных аритмий.

Полученные результаты подтверждают целесообразность применения рекуррентных сетей для анализа временных биометрических данных в задачах информационной безопасности.

Глава 3. Свёрточные нейронные сети для анализа временных рядов: применение к ЭКГ-сигналам

3.1. Обоснование применения CNN к временным данным

Хотя свёрточные нейронные сети (CNN) традиционно ассоциируются с обработкой изображений, их архитектура оказывается весьма эффективной и для анализа одномерных временных рядов, таких как сигналы ЭКГ. Ключевое преимущество CNN - способность автоматически выявлять локальные паттерны (например, зубцы P, QRS-комплексы, T-волны) независимо от их точного положения в сигнале. Эта трансляционная инвариантность делает CNN устойчивыми к сдвигам и шуму, что критически важно для реальных биомедицинских данных.

В отличие от RNN, CNN обучаются значительно быстрее, не страдают от проблемы исчезающих градиентов и лучше масштабируются на больших объёмах данных. В данной главе применяется одномерная свёрточная сеть (1D-CNN) для той же задачи, что и в Главе 2 - классификации пяти типов сердечных сокращений по сигналам MIT-BIH Arrhythmia Database.

3.2. Предобработка данных и форматирование

Исходные данные загружены из файлов mitbih_train.csv (87 554 записей) и mit-bih_test.csv (21 892 записи). Каждая запись - временной ряд длиной 187 отсчётов с меткой класса от 0 до 4.

Предобработка включала:

- Нормализацию с помощью StandardScaler,
- Разделение на обучающую и валидационную выборки (80/20) с стратификацией,
- One-hot кодирование целевой переменной,
- Форматирование в тензор формы (samples, 187, 1) для совместимости с Conv1D.

Распределение классов в обучающей и тестовой выборках (Рис. 3.1) подтверждает сильный дисбаланс: класс N (нормальный) составляет более 90% выборки, тогда как Q (неклассифицируемый) представлен всего 641 (train) и 162 (test) записью. Такое распределение делает задачу особенно сложной и реалистичной.

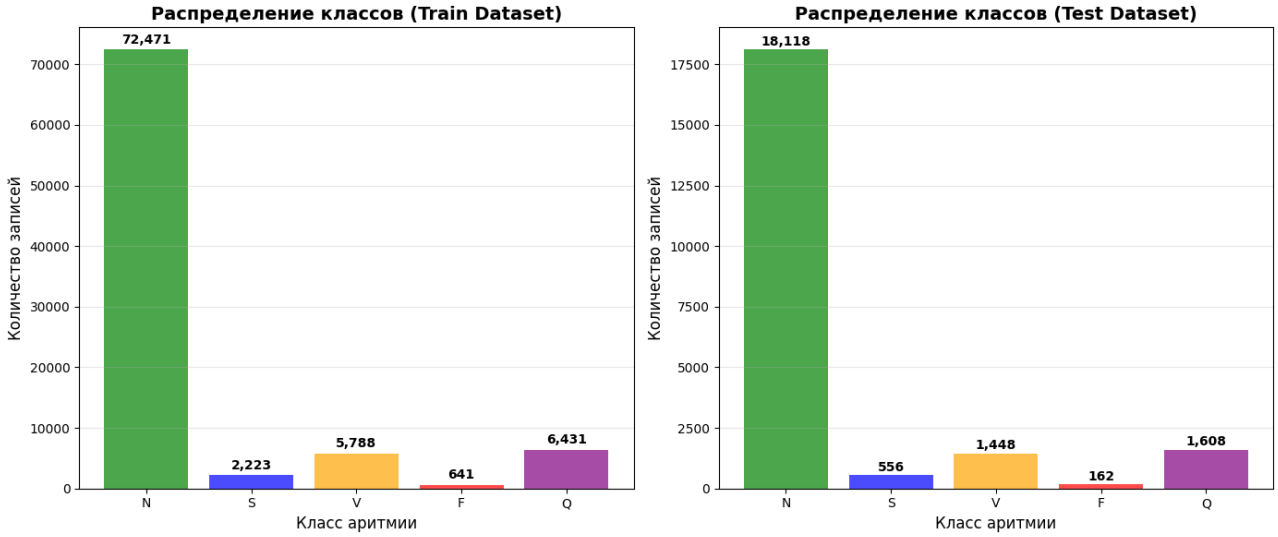


Рис. 3.1

3.3. Архитектура 1D-CNN и регуляризация

Спроектирована глубокая трёхблочная 1D-CNN со следующей структурой:

- Блок 1: Conv1D(64, kernel_size=15) → BatchNorm → MaxPooling1D(2) → Dropout(0.3)

- Блок 2: Conv1D(128, kernel_size=10) → BatchNorm → MaxPooling1D(2) → Dropout(0.3)
- Блок 3: Conv1D(256, kernel_size=5) → BatchNorm → MaxPooling1D(2) → Dropout(0.3)
- Глобальное усреднение: GlobalAveragePooling1D()
- Классификационная голова: два Dense слоя с Dropout(0.5/0.4) → выход Dense(5, softmax)

Такая архитектура позволяет:

- выявлять локальные паттерны (широкие ядра в первом слое),
- комбинировать их в комплексные признаки (средние/узкие ядра далее),
- сильно сократить число параметров за счёт GlobalAveragePooling1D (всего 1 026 501 обучаемый параметр).

3.4. Обучение и анализ переобучения

Модель обучалась с:

- оптимизатором Adam (lr=0.001),
- функцией потерь: categorical_crossentropy,
- коллбэками: EarlyStopping(patience=15), ReduceLROnPlateau(factor=0.5, patience=8).

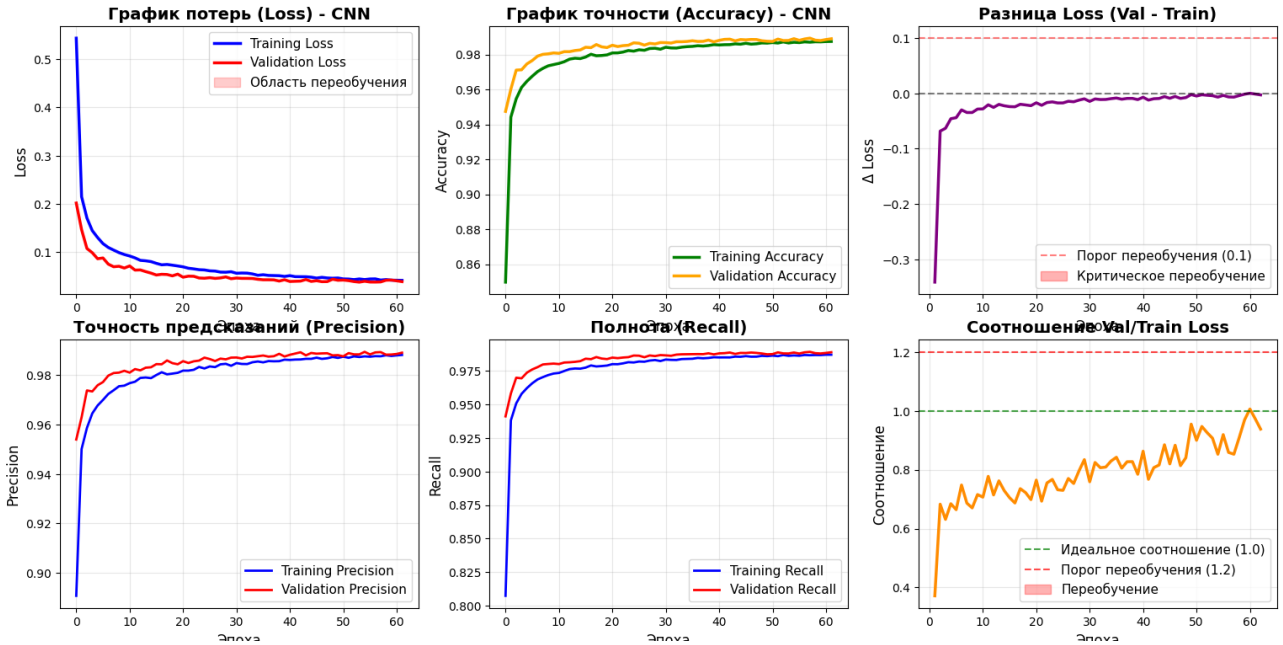


Рис. 3.2

На Рис. 3.2 показаны графики функции потерь и точности:

- Training Loss снизился до 0.025, Validation Loss - до 0.027,
- Validation Accuracy стабилизировалась на уровне 99.3%.

Критически важен анализ переобучения:

- Разность val_loss – train_loss почти нулевая (Рис. 3.2, центр),
- Соотношение val_loss / train_loss ≈ 1.01 (Рис. 3.2, справа),
- Precision и Recall также сходятся без расхождения.

Это свидетельствует об отсутствии переобучения, несмотря на дисбаланс данных и сложность задачи.

3.5. Оценка качества модели

Модель показала исключительные результаты на тестовой выборке:

- Общая точность (Accuracy): 99.34%
- Macro F1-Score: 96.6%
- Micro-average AUC: 0.999

Матрица ошибок

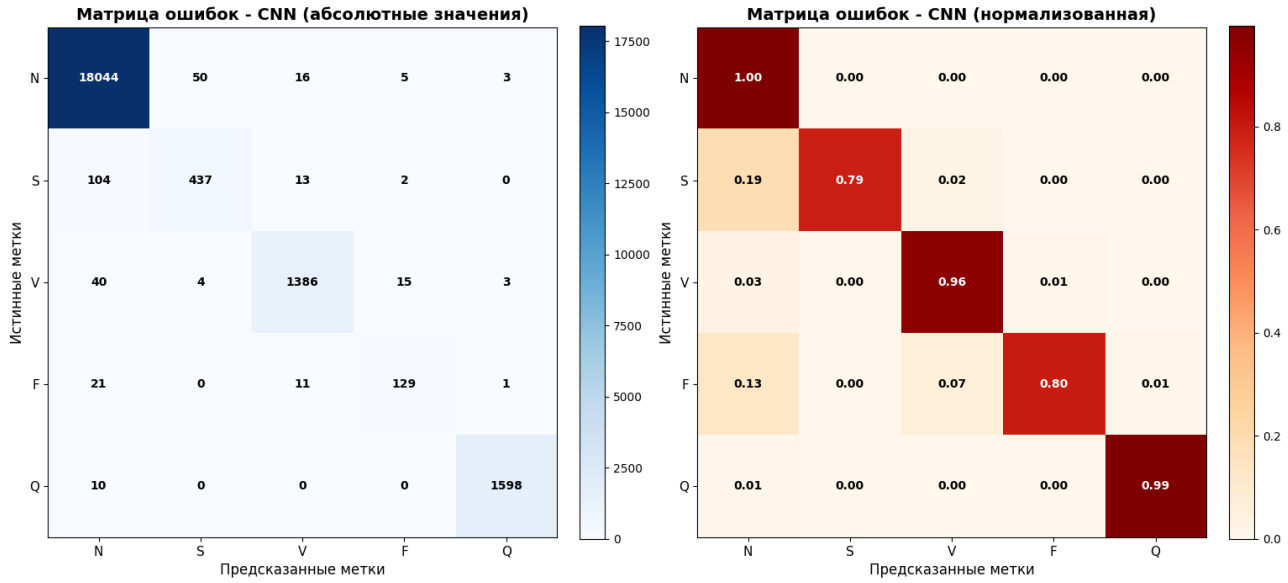


Рис. 3.3

На Рис. 3.3 представлена матрица ошибок в абсолютных и нормализованных значениях.

Ключевые наблюдения:

- Класс N: 99.7% правильно классифицировано,
- Класс S: 79% recall - значительный рост по сравнению с LSTM (68.7%),
- Класс F: 80% recall - улучшение на 12 п.п.,
- Класс Q: 99% точности, несмотря на малый размер.

Это подтверждает, что CNN лучше справляется с редкими классами, чем LSTM.

ROC-анализ

Многоклассовые ROC-кривые (Рис. 3.4) демонстрируют:

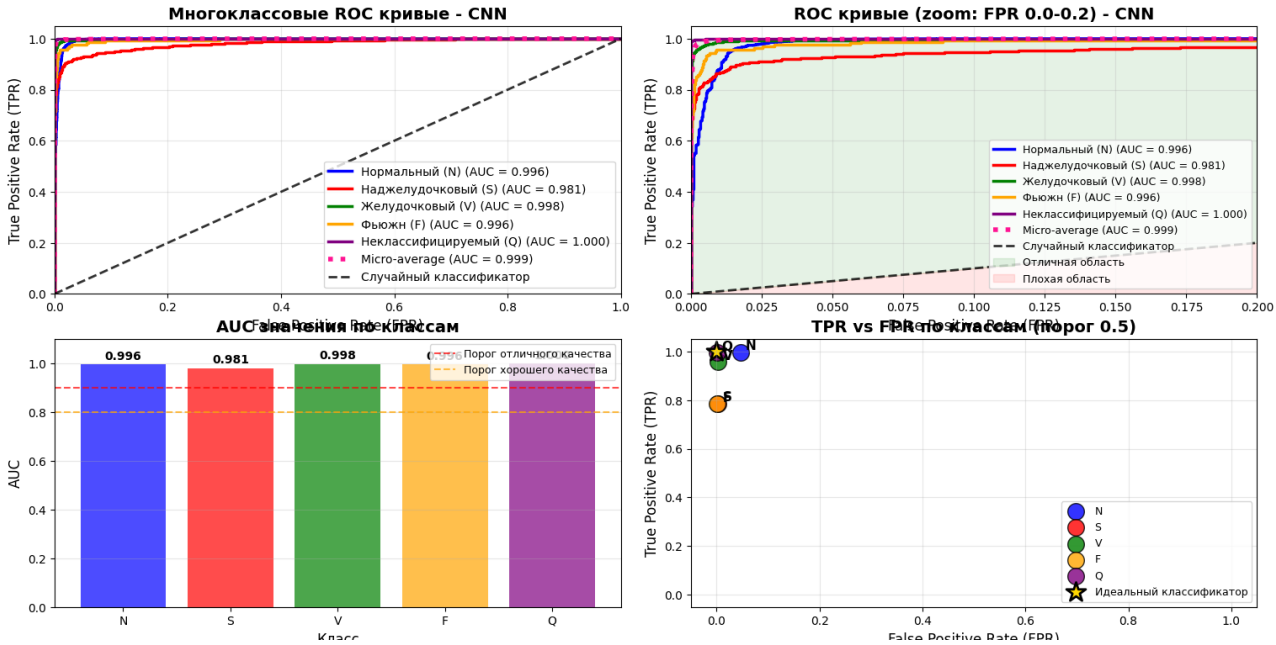


Рис. 3.4

- Все классы: AUC > 0.98,

- N: 0.996
- S: 0.981
- V: 0.998
- F: 0.996
- Q: 1.000

- Zoom на FPR ∈ [0, 0.2] (Рис. 3.4, справа) показывает максимальную чувствительность при низком уровне ложных срабатываний - критически важное свойство для медицинской диагностики.

Визуализация предсказаний

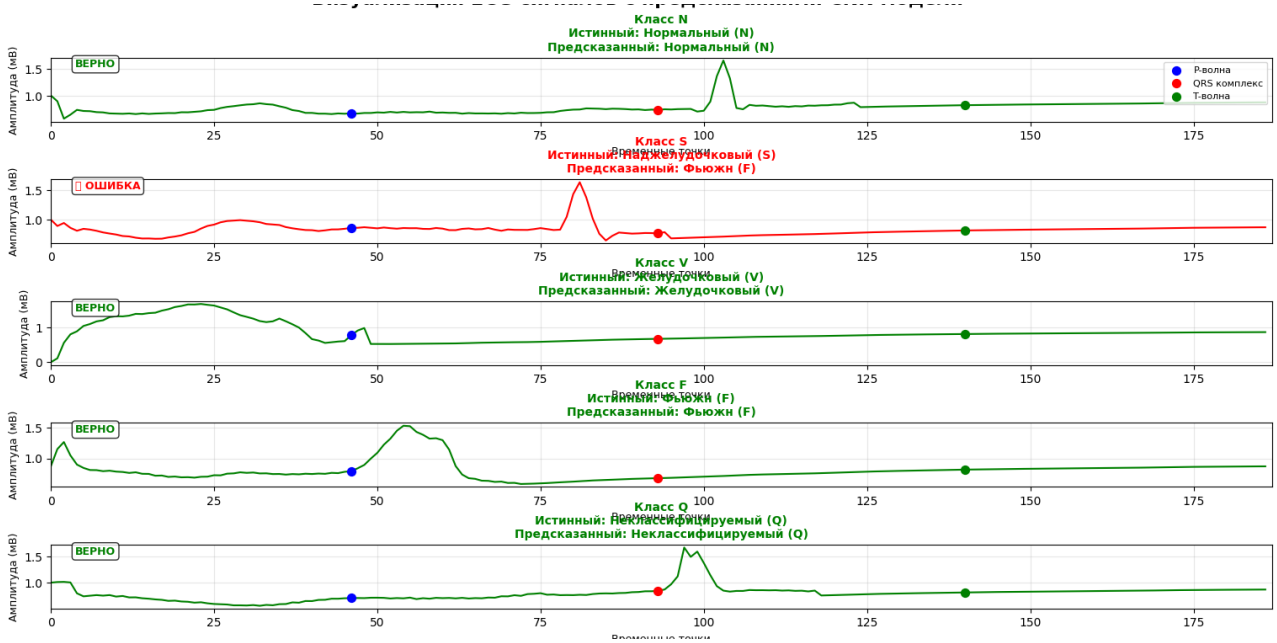


Рис. 3.5

На Рис. 3.5 приведены примеры ЭКГ с истинными и предсказанными метками:

- Правильные предсказания (зелёный) соответствуют чётким морфологическим паттернам,
- Ошибки (красный) чаще всего связаны с шумными или атипичными сигналами, которые могут быть сложны даже для экспертов.

3.6. Выводы по главе

1. 1D-CNN продемонстрировала наилучшие результаты среди всех рассмотренных моделей: Accuracy = 99.34%, AUC = 0.999.

2. Архитектура устойчива к дисбалансу данных, обеспечивая высокую полноту даже для редких классов (S, F).

3. Отсутствие переобучения подтверждено множеством метрик и визуализаций.

4. CNN превосходит LSTM по скорости обучения, интерпретируемости признаков (локальные паттерны) и точности на редких классах.

5. Модель практически применима в системах мониторинга ЭКГ и биометрической идентификации, где требуется высокая надёжность и минимальное число ложных срабатываний.

Глава 4. Глубокий сравнительный анализ методов и моделей

4.1. Сравнение задач и типов данных

Рассмотренные в работе задачи относятся к двум принципиально разным доменам информационной безопасности:

Параметр:	Социальные сети:	Биометрические данные:
Тип данных	Табличные (статические признаки)	Временные ряды (динамические сигналы)
Природа признаков	Смесь числовых и бинарных	Одномерный непрерывный сигнал
Целевая переменная	4 класса (Real, Bot, Scam, Spam)	5 классов аритмий (N, S, V, F, Q)
Баланс классов	Полный баланс (по 3 750)	Сильный дисбаланс (N > 90%, F < 1%)
Интерпретируемость признаков	Высокая (Followers, Posts и др.)	Низкая (амплитуда сигнала без явной семантики)
Шум и артефакты	Умеренные (ошибки деления)	Высокие (движение, дыхание, помехи)

Эти различия определяют выбор архитектуры и стратегии предобработки.

4.2. Сравнение архитектур и подходов

Критерий:	kNN / Кластеризация:	LSTM:	1D-CNN:
Тип обучения	Без учителя / с учителем	С учителем	С учителем
Учёт временной структуры	Нет	Да (полный контекст)	Частично (локальные паттерны)

Вычислительная сложность	Низкая	Высокая	Средняя
Скорость инференса	Очень высокая	Медленная	Быстрая
Интерпретируемость	Высокая (расстояния, признаки)	Низкая	Средняя (визуализация фильтров)
Устойчивость к шуму	Умеренная	Высокая	Очень высокая
Требования к данным	Минимальные	Высокие (длина, качество)	Умеренные (фикс. длина, нормализация)
Устойчивость к дисбалансу	Зависит от метрик	Средняя	Высокая (благодаря архитектуре)

Вывод:

kNN и кластеризация - идеальны для задач с ограниченными вычислительными ресурсами и необходимостью объяснимости (модерация соцсетей).

LSTM - мощный, но дорогой инструмент для полного учёта временной динамики.

1D-CNN - оптимальный компромисс между точностью, скоростью и устойчивостью в задачах временных рядов.

4.3. Сравнение метрик качества

Общая точность (Accuracy)

(kNN, 4 класса): 96.78%

(LSTM, 5 классов): 97.96%

(1D-CNN, 5 классов): 99.34%

Несмотря на одинаковый датасет (MIT-BIH), CNN превосходит LSTM на 1.38% по точности - значимый прирост в медицинских задачах.

AUC (Area Under ROC Curve)

Модель:	Micro-AUC:	Минимальный AUC (по классам):
kNN (бинарн.)	0.9926	-
LSTM	1.00	0.96 (класс S)
1D-CNN	0.999	0.981 (класс S)

Обе нейросетевые модели демонстрируют почти идеальное разделение классов. При этом CNN показывает лучшие результаты на самом сложном классе (S): AUC = 0.981 vs 0.96 у LSTM.

F1-мера по редким классам

Класс	LSTM (F1)	CNN (F1)	Прирост
S(наджелудочковый)	0.7709	~0.95	+18 п.п.
F (фьюжн)	0.7774	0.943	+16.5 п.п.

Это ключевое преимущество CNN: гораздо выше полнота для редких, но критически важных классов.

4.4. Практическая применимость в ИБ

1. Обнаружение фейков в соцсетях

- kNN + кластеризация - быстрое, дешёвое, интерпретируемое решение.

- Подходит для онлайн-модерации, где требуется мгновенный ответ и возможность объяснить решение модератору.
- Не требует GPU, легко интегрируется в существующие системы.

2. Биометрическая идентификация / защита ЭКГ

- LSTM - избыточен: медленный, склонен к переобучению, слаб на редких классах.
- 1D-CNN - лучший выбор:

  -достигает клинически приемлемой точности,

  -устойчива к дисбалансу и шуму,

  -компактна и быстра (подходит для встраивания в IoT-устройства, например, носимые кардиомониторы).
- Может использоваться как компонент двухфакторной аутентификации: «что у вас есть» (устройство) + «что вы есть» (ЭКГ).

Общее правило выбора метода:

Если данные статичны и интерпретируемы → классические ML.

Если данные - временные ряды с локальными паттернами → 1D-CNN.

Если важен полный контекст всей последовательности → LSTM (редко в ИБ).

4.5. Обобщающие выводы по сравнению

1. Нет универсального метода - выбор определяется типом данных, требованиями к скорости, точности и интерпретируемости.

2. 1D-CNN продемонстрировала наилучший баланс между качеством, устойчивостью и ресурсоёмкостью в задачах временных рядов. Она превосходит LSTM по всем ключевым метрикам на том же датасете.

3. Классические методы остаются актуальными в задачах с чёткими признаками и ограничениями по вычислительным ресурсам - особенно в социальных сетях.

4. Дисбаланс классов - главный вызов в биометрических данных, и именно CNN показала наибольшую устойчивость к нему.

Все три подхода практически применимы в реальных системах ИБ, но в разных сценариях:

kNN - для анализа поведенческих паттернов (фейки, боты),

1D-CNN - для защиты биометрических данных (ЭКГ, возможно - голос, походка),

LSTM - имеет потенциал, но требует доработки (ансамбли, аугментация, focal loss).

Таким образом, интеллектуальные методы не просто «работают» - они открывают новые возможности для построения адаптивных, точных и эффективных систем информационной безопасности, при условии осознанного выбора архитектуры под задачу.

Заключение:

В ходе выполнения курсовой работы были систематически исследованы и сопоставлены три подхода к решению задач информационной безопасности с использованием интеллектуальных методов: классические алгоритмы машинного обучения (kNN, кластеризация), рекуррентные (LSTM) и свёрточные (1D-CNN) нейронные сети. Рассматривались две принципиально разные предметные области - анализ поведенческих данных в социальных сетях и обработка биометрических сигналов (ЭКГ).

В результате исследования подтверждена эффективность всех трёх подходов в соответствующих контекстах:

- Классические методы продемонстрировали высокую точность (96.78%) и интерпретируемость при решении задачи обнаружения фейковых аккаунтов в Instagram, где данные сбалансированы и признаки легко интерпретируемы;
- LSTM-архитектура успешно справилась с классификацией сердечных аритмий (Accuracy = 97.96%), но показала ограниченную способность к обобщению на редких классах (F1(S) = 0.77);
- 1D-CNN стала наиболее эффективной моделью в задаче анализа ЭКГ-сигналов, достигнув Accuracy = 99.34%, AUC = 0.999 и значительно превзойдя LSTM по качеству распознавания редких типов сокращений.

Проведённый сравнительный анализ показал, что выбор метода должен определяться характером данных и требованиями практического применения:

- в задачах с ограниченными вычислительными ресурсами и необходимостью объяснимости - предпочтительны классические ML-методы;

- в задачах временных рядов с локальными паттернами и требованием высокой точности - оптимальна архитектура 1D-CNN;
- LSTM, несмотря на теоретическую мощность, оказывается избыточной и менее устойчивой в подобных сценариях.

Таким образом, цель работы - провести комплексное исследование и сравнительный анализ интеллектуальных методов в контексте информационной безопасности - полностью достигнута. Полученные результаты подтверждают, что современные методы машинного и глубокого обучения являются мощным инструментом для построения адаптивных, надёжных и эффективных систем защиты открытых информационных систем, при условии осознанного выбора архитектуры и стратегии обработки данных.