Министерство высшего образования и науки Российской Федерации
Санкт-Петербургский политехнический университет Петра Великого
Институт прикладной математики и механики
Высшая школа теоретической механики

Работа допущена к защите

Директор высшей школы

А.М. Кривцов

«___»_____2021 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

Аутентификация пользователей по ЭЭГ головного мозга при моргании с использованием методов машинного обучения

по направлению подготовки

01.03.03 «Механика и математическое моделирование»

профиль

01.03.03_02 Биомеханика и медицинская инженерия

Выполнил

студент гр. 3630103/70201 П. В. Беленко

Руководитель

к.т.н., доцент ВШ АиР Л. А. Станкевич

Консультант

ассистент ВШ КФСУ А. М. Журавская

Санкт-Петербург

2021

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

Институт прикладной математики и механики

УТВЕРЖДАЮ

Директор высшей школы

теоретической механики

А.М. Кривцов

« » 2021 г.

ЗАДАНИЕ

по выполнению выпускной квалификационной работы

студенту Беленко Павлу Вячеславовичу, гр. 3630103/70201

1. Тема работы: Аутентификация пользователей по ЭЭГ головного мозга при моргании с использованием методов машинного обучения

2. Срок сдачи студентом законченной работы: 14 июня 2021г.

3. Исходные данные по работе: справочная литература, актуальные публикации по теме исследования.

4. Содержание работы (перечень подлежащих разработке вопросов): реализация алгоритма распознавания пользователей по записям ЭЭГ вынужденных морганий, снятым на немедицинском оборудовании с низкой частотой дискретизации записываемого сигнала. Обработка полученных результатов и сравнение их с литературными данными.

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

6. Консультанты по работе: А. М. Журавская

7. Дата выдачи задания 1 февраля 2021г.

Руководитель ВКР Л. А. Станкевич

Задание принял к исполнению 1 февраля 2021г.

Студент П. В. Беленко

РЕФЕРАТ

На 46 с., 21 рисунок

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО ЭЭГ ГОЛОВНОГО МОЗГА ПРИ МОРГАНИИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

В статье приведены результаты исследования в области применения электроэнцефалографии (ЭЭГ) в качестве метода биометрической аутентификации человека. Реализованы два алгоритма аутентификации, основанные на записях ЭЭГ вынужденных морганий. Для сбора данных используется электроэнцефалограф NeuroPlay-8Cap, записывающий сигнал с частотой дискретизации 125 Гц. Предобработка данных основана на вейвлет-преобразовании Добеши 2-го порядка (DWT DB2) и на распределении спектральной плотности мощности анализируемого сигнала, находимой методом Уэлша (PSD, Welch Method). Распознавание ведётся с помощью классификаторов на основе метода опорных векторов (Support Vectors Classifier), случайного леса (Random Forest Classifier) и k ближайших соседей (k Nearest Neighbors Classifier). Обе вариации алгоритма дают хороший показатель точности в 90–95% в зависимости от используемого метода классификации.

THE ABSTRACT

46 pages, 21 pictures

AUTHENTICATION OF USERS BY EEG OF THE BRAIN WHEN BLINKING USING MACHINE LEARNING METHODS

The article presents the results of a study on the use of electroencephalography (EEG) as a method of biometrical authentication of a person. Implemented two authentication algorithms based on EEG recordings of forced blinks. For data collection, the NeuroPlay-8Cap electroencephalograph is used, which records a signal with a sampling frequency of 125 Hz. Data preprocessing is based on the 2nd-order Daubechies wavelet transform (DWT DB2) and on the distribution of the spectral power density of the analyzed signal (PSD), found by the Welsh method. Recognition is performed using classifiers based on the Support Vectors Classifier (SVC), Random Forest (RF), and k Nearest Neighbors (kNN). Both variations of the algorithm give an accuracy rate of 90-95%, depending on the classification method used.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 5
ГЛАВА 1. ОПИСАНИЕ АЛГОРИТМОВ ЭЭГ-АУТЕНТИФИКАЦИИ 7
1.1. Анализ существующих методик ЭЭГ-аутентификации 7
1.2. Структура алгоритма ЭЭГ-аутентификации 10
1.3. Алгоритм аутентификации на основе вейвлет-преобразования 11
1.3.1. Сбор данных 11
1.3.2. Предобработка записанных сигналов 11
1.3.3. Формирование признаков 16
1.3.4. Аутентификация 18
1.3.5. Обучение и тестирование 20
1.4. Алгоритм аутентификации на основе спектральной плотности 24
1.4.1. Сбор данных 24
1.4.2. Предобработка записанных сигналов 24
1.4.3. Формирование признаков 26
1.4.4. Обучение модели и аутентификация 27
1.5. Выводы по главе 28
ГЛАВА 2. РЕАЛИЗАЦИЯ АЛГОРИТМОВ АУТЕНТИФИКАЦИИ 29
2.1. Описание используемого программного обеспечения 29
2.2. Реализация алгоритма на основе вейвлет-преобразования 30
2.3. Реализация алгоритма на основе спектральной плотности 36
2.4. Выводы по главе 40
ГЛАВА 3. АНАЛИЗ РЕЗУЛЬТАТОВ 41
1.1. Описание результатов 41
1.2. Выводы по главе 43
ЗАКЛЮЧЕНИЕ 44
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 45

ВВЕДЕНИЕ

В наше время мы сталкиваемся с необходимостью подтверждения своей личности практически каждый день. Аутентификация требуется, к примеру, при использовании социальных сетей, мобильных приложений, банковских сервисов для совершения денежных переводов, а также и во многих других сферах.

Наиболее распространенными в настоящее время являются системы аутентификации на основе паролей. Потенциальный пользователь получает доступ к работе, вводя в компьютер пароль, например, в виде заранее определенного для него слова или фразы, чтобы подтвердить свою личность. Надежность пароля определяется его длиной и ограничениями на используемые символы, поэтому каждому пользователю необходимо сначала сформировать, а затем и запомнить длинную (более 8 букв и цифр) последовательность символов, что на практике не всегда оказывается удобным.

Альтернативой аутентификации на основе паролей является биометрическая аутентификация. Этот метод использует уникальные биологические характеристики каждого человека для распознавания, спектр применяемых для аутентификации характеристик при этом по истине огромен. К примеру, в качестве характеристик могут быть использованы: отпечаток пальца руки или ладони, тембр голоса, рисунок иридиевой оболочки глаза, фотография лица и другие подобные характеристики [11]. Существуют некоторые требования, которые необходимо выполнить, чтобы биометрические признаки можно было применять в реальных приложениях. В частности, признаки должны быть универсальны, постоянны и измеримы, а системы идентификации должны обладать высокой точностью распознавания и воспроизводимостью [14].

В качестве биометрической аутентификации также могут быть использованы и сигналы биоэлектрической активности головного мозга, регистрируемые при помощи электродов с поверхности головы в виде электроэнцефалограмм (ЭЭГ). При этом каждый электрод, наложенный на зону

скальпа, регистрирует суммарный биопотенциал, образованный изменениями потенциалов действия множества нервных клеток, находящихся под ним. Если подобный электрод соединить с нулевым потенциалом, находящимся на некотором удалении (на практике нулевой потенциал как правило берут на мочке уха), то в этой системе возникнет электрическое напряжение, которое возможно усилить и зарегистрировать на соответствующей аппаратуре.

В силу невообразимого количества биологических процессов, влияющих на форму и характер ЭЭГ, данная характеристика для каждого человека является уникальной и может быть использована для аутентификации [5]. В данном методе аутентификации сигналы ЭЭГ, зарегистрированные на определенном отрезке времени и в определённых зонах головного мозга, выступают в роли носителя биометрической информации.

ЭЭГ-аутентификация имеет ряд недостатков по сравнению с другими биометрическими методами. В частности, амплитуда записываемых сигналов зачастую зависит от физического состояния человека и времени суток, в которое была сделана запись [2]. Поэтому запись ЭЭГ следует привязывать к некоторому типовому событию – к примеру, снимать сигналы только в первой половине дня и максимально изолировать человека, с которого снимаются сигналы, от негативных внешних факторов, таких как резкие звуки, вибрации, вспышки света и т. д.

Также немаловажную роль для качества записи играет отсутствие влияния внешних электрических и магнитных полей. В лабораторных условиях это требование удовлетворяется засечёт удаления на время записи испытуемого от электрических приборов, розеток и других людей.

Отмечу, что несмотря на описанные выше негативные аспекты, у данного вида биометрической идентификации есть существенное преимущество: сигналы ЭЭГ не могут быть подделаны, поскольку генерируются только тем человеком, который должен быть идентифицирован.

ГЛАВА 1. ОПИСАНИЕ АЛГОРИТМОВ ЭЭГ-АУТЕНТИФИКАЦИИ

1.1. Анализ существующих методик ЭЭГ-аутентификации

При разработке методики ЭЭГ-аутентификации прежде всего требуется определить, какие сигналы ЭЭГ могут быть использованы. Для решения этой проблемы были проанализированы существующие работы в данной области.

Исследования, описанные в работе [8], основаны на использовании сигналов ЭЭГ, записываемых в фоновом режиме, т. е. при отдыхе и отсутствии целенаправленной мыслительной активности. Полученные сигналы ЭЭГ обрабатывались с целью вычисления коэффициентов авторегрессии. Идентификация проводилась с использованием предварительно обученной на коэффициентах авторегрессии соревновательной нейронной сети. В эксперименте приняли участие 10 человек с оценкой точности для каждого человека отдельно. При этом минимальная точность идентификации была 80%, а максимальная – 90%.

В исследовании [22] приняло участие 10 человек, в течение 40 секунд каждому предъявляли фотографии лиц. Периодически перед собой они видели свою фотографию, что создавало особую форму волны, по которой и велось распознавание своего лица. Точность распознавания своего лица составила 86%.

В работе [9] велась запись сигнала ЭЭГ по 4 минуты. В это время человек, сидя в расслабленном состоянии, должен был воображать движения сначала левой рукой, потом правой. В эксперименте принимали участие 9 человек, при этом точность классификации движений рук составила 80%.

Работа [12] основывалась на состоянии покоя. 23 человека в течение одной минуты должны были находиться в расслабленном состоянии. Результаты классификации показали лишь 79% точности. Общая ошибка аутентификации 42%.

Работа [13] аналогична работе [22] с фотографиями самого себя. Точность распознавания своего лица была около 85%, но время записи стало намного короче.

Исследование, проведённое в работе [19] похоже на исследование [9], однако за счёт использования методов спектрального анализа сигнала, удалось сильно повысить точность распознавания

Статья [20] описывает алгоритм аутентификации на основе естественных морганий, совершаемых в течение 20 секунд. Эксперимент проводился с участием 10 человек, а в результате эксперимента максимальная точность аутентификации составила 95%.

Таким образом, можно выделить ряд особенностей разных методик ЭЭГ-аутентификации:

1. Распознавание на основе сигналов ЭЭГ, записанных в состоянии покоя, даёт малую точность в сравнении с другими методиками.
2. Аутентификация на основе визуальных образов имеет более высокую точность, но также требует высокой концентрации внимания исследуемых субъектов.
3. Анализ моторных образов занимает много времени, но может давать неплохие результаты в зависимости от методов обработки сигнала.
4. Распознавание на основе анализа ЭЭГ морганий даёт наивысшую точность, в сравнении с другими методиками.

Опираясь на результаты рассмотренных исследований, было принято решение о реализации системы ЭЭГ-аутентификации на основе морганий. Данный вариант имеет ряд преимуществ, поскольку относительно просто реализуется и, как показано в работах [1] и [20], может дать хорошую точность распознавания.

Также стоит отметить, что процесс моргания сопровождает и биоэлектрическая мышечная активность (глазодвигательный артефакт),

графическое изображение которой называют электроокулограммой (ЭОГ) [7]. В теории ЭЭГ данный вид активности считается дефектом, поскольку не является истинной биоэлектрической активностью головного мозга, однако исследования показывают, что моргания с интервалом не менее 300 миллисекунд генерируют уникальный сигнал ЭОГ для каждого человека [15]. Поэтому при построении алгоритма аутентификации имеет смысл работать непосредственно с ЭОГ, как это сделано в работе [20].

В целях оптимизации процесса в описанном выше подходе, вместо естественных морганий планируется рассматривать вынужденные, совершаемые с фиксированной частотой. При прочих равных, у такого подхода будет преимущество по количеству выделяемых морганий на одной записи, поскольку естественные моргания совершаются в среднем около 10 штук в минуту. Данный аспект должен положительно сказаться на точности распознавания.

Также, поскольку имеющийся в наличии прибор NeuroPlay-8Cap не является профессиональным медицинским и обладает невысокой частотой дискретизации (равной 125 Гц), стоит рассмотреть систему аутентификации по ЭЭГ вынужденных морганий на основе спектрального анализа сигнала, как это делалось в работе [19] с записями воображаемых движений рук. Для данной методики также планируется рассматривать только записи ЭЭГ с фиксированной частотой морганий на них.

Таким образом, в данной работе было решено реализовать два алгоритма аутентификации по записям ЭЭГ вынужденных морганий, основанные на идее нахождении паттернов морганий из ЭОГ при помощи вейвлет-преобразования, и на идее анализа спектральной плотности мощности рассматриваемого сигнала.

1.2. Структура алгоритма ЭЭГ-аутентификации

Задача аутентификации человека по записи его ЭЭГ вынужденных морганий, решалась при помощи двух подходов, в основе которых лежали дискретное вейвлет-преобразование (Discrete Wavelet Transform - DWT) и анализ спектральной плотности мощности сигнала (Power Spectral Density - PSD). Процесс создания идентификатора для обоих подходов включает в себя 4 основных этапа: **сбор данных**, **предобработку**, **выделение признаков** и, непосредственно, блок **аутентификации** (рис. 1):

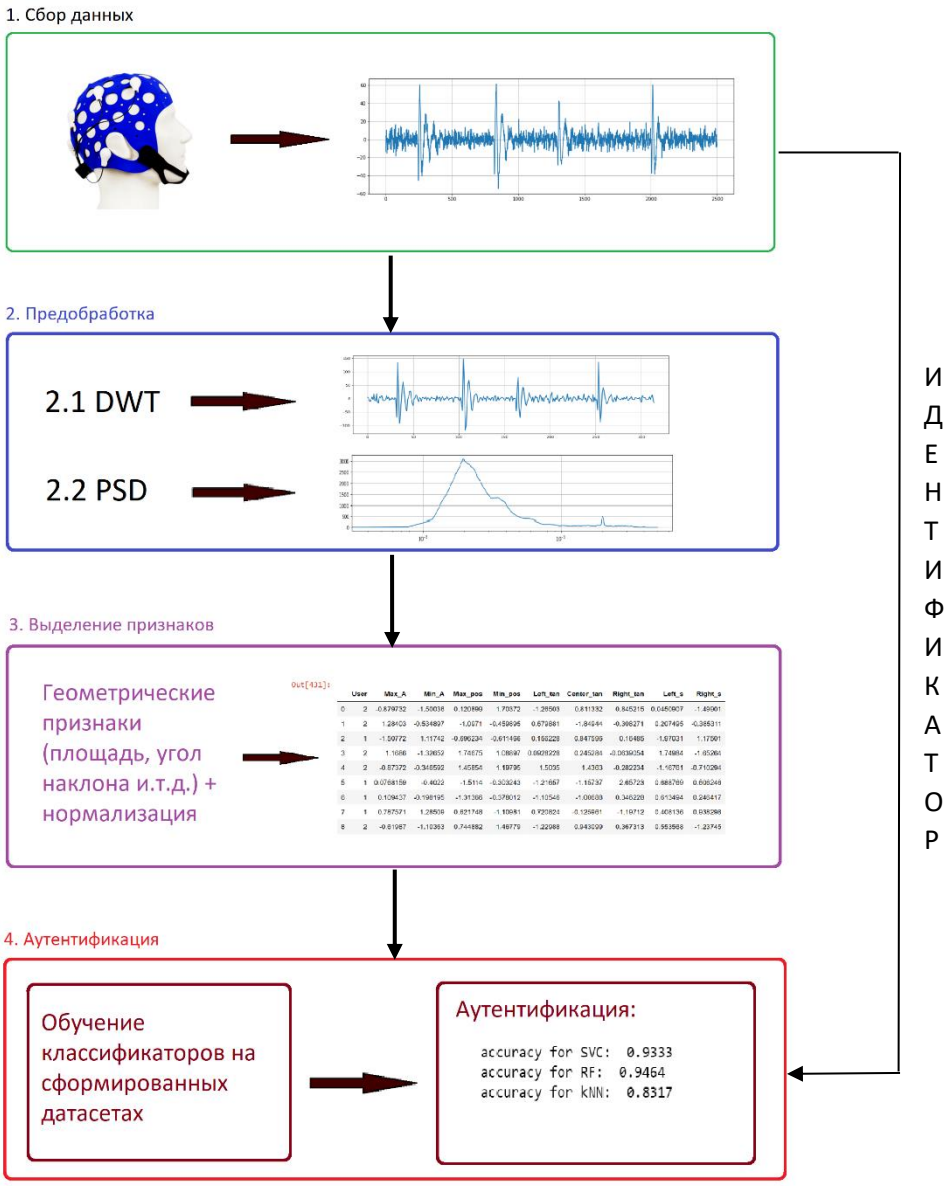

Рис. 1 – Блок-схема работы рассматриваемых алгоритмов аутентификации

1.3. Алгоритм аутентификации на основе вейвлет-преобразования

1.3.1. Сбор данных

На данном этапе происходит запись ЭЭГ вынужденных морганий при помощи электроэнцефалографа**.** Из всех каналов записи выбираются только те, что находятся в наибольшей близости к лобным долям – два фронтальных электрода, поскольку, как говорилось ранее, при работе с морганиями по отдельности наибольшую ценность для нас имеет ЭОГ (глазодвигательный артефакт), а он наиболее чётко прослеживается именно на двух фронтальных каналах записи.

1.3.2. Предобработка записанных сигналов

Цель данного этапа – сделать записанные сигналы ЭЭГ пригодными к дальнейшему выделению из них геометрических признаков для обучения классификатора.

Для этого к записанным сигналам применяется дискретное вейвлет-преобразование, в результате чего на имеющейся записи становится возможным выделение каждого конкретного моргания. При этом сигнал разбивается на две составляющие – аппроксимирующую и детализирующую. Сильно обобщая, аппроксимирующая часть содержит информацию, которую необходимо извлечь, детализирующая – маловажные элементы сигнала. Осуществляется это путем вычисления скалярного произведения анализируемого сигнала и анализирующего вейвлета на заданном масштабе.

В зависимости от того, какую именно информацию необходимо извлечь из сигнала, могут быть использованы вейвлеты разного типа. В нашем случае для разложения оказалось лучше использовать в качестве материнского - Вейвлет Добеши [6] второго порядка (db2), поскольку по форме он наиболее близок к паттерну моргания (рис. 2).

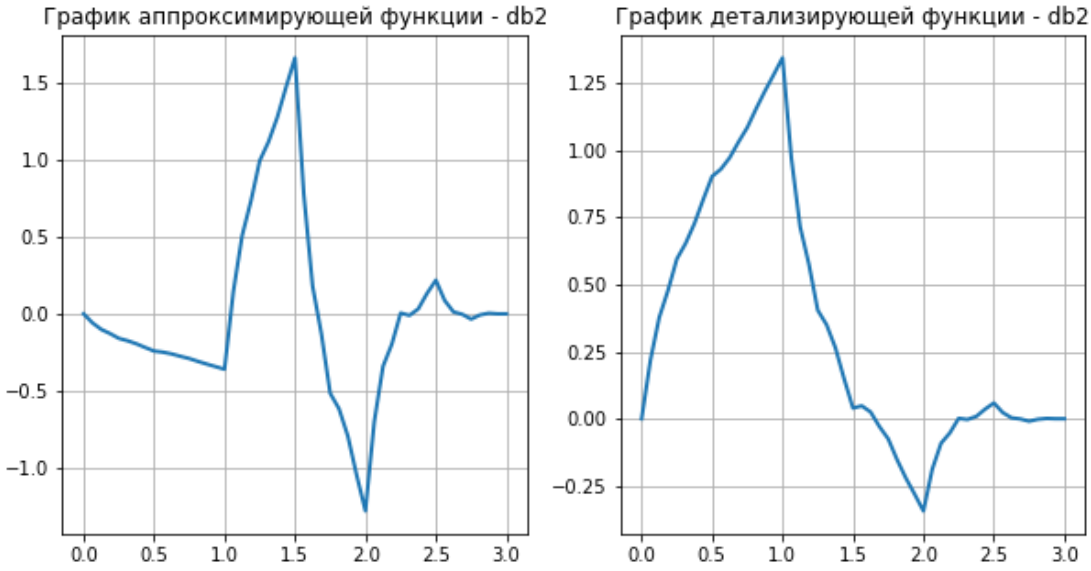

Рис.2 – Аппроксимирующая и детализирующая составляющие вейвлета Добеши 2-го порядка в осях «условная амплитуда-условное время»

Аппроксимирующая составляющая вейвлета Добеши задаётся рекуррентно соотношением:

$$\varphi(r) = [\varphi(2r), \quad \varphi(2r-1), \quad \varphi(2r-2), \quad \varphi(2r-3)] \cdot \begin{bmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \end{bmatrix}$$

при заданных начальных значениях:

$$\varphi(0) = 0, \qquad \varphi(1) = \frac{1+\sqrt{3}}{2}, \qquad \varphi(2) = \frac{1-\sqrt{3}}{2}, \qquad \varphi(3) = 0.$$

Детализирующая составляющая задаётся при помощи аппроксимирующей, используя те же коэффициенты h_i:

$$\psi(r) = [\varphi(2r-1), \quad \varphi(2r), \quad \varphi(2r+1), \quad \varphi(2r+2)] \cdot \begin{bmatrix} -h_1 \\ h_2 \\ -h_3 \\ h_4 \end{bmatrix}$$

Возвращаясь к поставленной задаче, для получения искомой аппроксимирующей последовательности требуется разбить исходный сигнал $S = \{S_i\}$ на группы по четыре элемента, смещаясь каждый раз на два. Элементы аппроксимирующей последовательности вычисляются по формуле:

$$a_i = c_1 \cdot S_{2i} + c_2 \cdot S_{2i+1} + c_3 \cdot S_{2i+2} + c_4 \cdot S_{2i+3},$$

где $c_1, .., c_4$ – табличные коэффициенты вейвлета, получаемые из $h_1, .., h_4$ нормировкой на $\sqrt{2}$:

$$c_1 = \frac{1+\sqrt{3}}{4\sqrt{2}} = 0.48296$$

$$c_2 = \frac{3+\sqrt{3}}{4\sqrt{2}} = 0.83651$$

$$c_3 = \frac{1+\sqrt{3}}{4\sqrt{2}} = 0.22414$$

$$c_4 = \frac{1-\sqrt{3}}{4\sqrt{2}} = -0.12941$$

Соответственно, элементы детализирующей последовательности вычисляются по формуле:

$$d_i = c_4 \cdot S_{2i} - c_3 \cdot S_{2i+1} + c_2 \cdot S_{2i+2} - c_1 \cdot S_{2i+3}.$$

Процедуру получения детализирующей и аппроксимирующей последовательностей также можно представить и в матричном виде:

$$\begin{bmatrix} a_1 \\ d_1 \\ a_2 \\ d_2 \\ \dots \\ a_{n/2} \\ d_{n/2} \end{bmatrix} = \begin{bmatrix} c_1 & c_2 & c_3 & c_4 & 0 & 0 & & 0 & 0 \\ c_4 & -c_3 & c_2 & -c_1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & c_1 & c_2 & c_3 & c_4 & & 0 & 0 \\ 0 & 0 & c_4 & -c_3 & c_2 & -c_1 & & 0 & 0 \\ & & & \vdots & & & \ddots & \vdots & \\ 0 & 0 & 0 & 0 & 0 & 0 & \dots & c_2 & -c_1 \end{bmatrix} \cdot \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \\ \dots \\ S_{n-1} \\ S_n \end{bmatrix}$$

Или, в упрощённом виде:

$$\langle cA|cD\rangle = M \cdot S,$$

Где $cA = \{a_i\}$, $cD = \{d_i\}$, – вектора аппроксимирующей и детализирующей последовательностей, соответственно, а M – матрица преобразования.

Нетрудно заметить, что при данном преобразовании согнал прорежается вдвое – длинна каждой из последовательностей $\{a_i\}$, $\{d_i\}$ становится в два раза меньше длины исходного сигнала S.

Для улучшения качества обработки, на аппроксимирующем наборе данное преобразование повторяется еще дважды, в результате чего получается разложение сигнала до третьего уровня с уменьшенным шумом и хорошо выделяемыми морганиями. Сигнал при этом прорежается ($\downarrow 2$ – оператор прорежения) в 8 раз, соответственно (рис. 3).

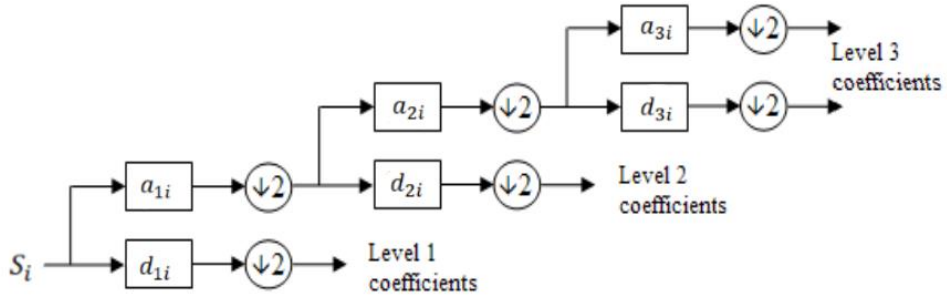

Рис. 3 - Блок-схема дискретного вейвлет-разложения 3 уровня, используемого в работе

Далее происходит извлечение морганий из полученных сигналов. Для этого каждый сигнал подвергается следующей поэтапной обработке (рис. 4).

1. Определяется максимальное положительное значение сигнала. Ожидается, что это будет положительный пик одного из морганий.
2. Идет поиск начала положительного пика путем уменьшения индекса сигналов, пока значение амплитуды не станет меньше 5% от обнаруженного положительного пика на этапе1.

3. Находится максимальное отрицательное значение в течение 400 мс от положения положительного пика, обнаруженного на этапе 1. Предполагается, что это будет отрицательный пик моргания.
4. Обнаруживается завершение отрицательного пика путем увеличения индекса сигналов до тех пор, пока значение амплитуды не станет менее 5% от обнаруженного отрицательного пика на этапе 3.
5. Если значение обнаруженного отрицательного пика (на этапе 3) составляет менее 35% от обнаруженного положительного пика (на этапе 1), то этот сигнал отбрасывается, поскольку обнаруженная форма не соответствует шаблону моргания. В противном случае сигнал от начала до завершения (этапы 3 и 4) сохраняется, а в исходном сигнале этот участок обнуляется.
6. Этапы 1–5 повторяются до тех пор, пока значение обнаруженного положительного пика не станет менее 50% от первого обнаруженного положительного пика.

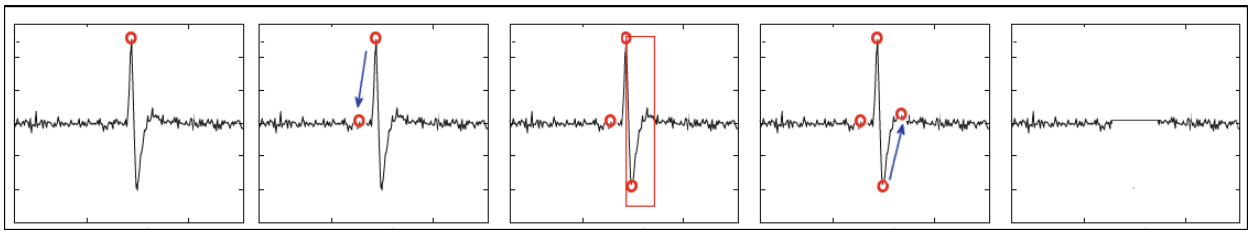

Рис. 4 - Этапы процесса извлечения морганий

После последовательного выполнения всех этапов процесса получаются выделенные моргания (а вернее, становятся известны положения их положительных и отрицательных пиков, а также точки их начала и окончания). Теперь данные подготовлены к дальнейшему анализу и извлечению уникальных признаков.

1.3.3. Формирование признаков

В качестве признаков были выбраны геометрические характеристики каждого выделенного моргания, так как оно является уникальным. Выделенные моргания обрабатываются для получения признаков, таких как: амплитуда максимального позитивного или негативного пика, позиция максимального позитивного или негативного пика и т.д. При построении шаблона морганий вычисляются следующие признаки:

M_p – Амплитуда позитивного пика;

I_p – Позиция позитивного пика;

M_n – Амплитуда негативного пика;

I_n – Позиция негативного пика;

I_z – Позиция точки пересечения нуля;

S_p – Площадь под позитивным импульсом;

S_n – Площадь под негативным импульсом;

Av_p – Среднее значение позитивного импульса;

Av_n – Среднее значение негативного импульса;

D_p – Длительность позитивного импульса;

D_n – Длительность негативного импульса;

Tg_{sp} – Угол наклона от начала позитивного импульса;

Tg_{ep} – Угол наклона от конца позитивного импульса;

Tg_{sn} – Угол наклона от начала негативного импульса;

Tg_{en} – Угол наклона от конца негативного импульса;

M_{p1} – Амплитуда позитивного пика первой производной волны;

I_{p1} – Позиция позитивного пика первой производной волны;

M_{n1} – Амплитуда негативного пика первой производной волны;

I_{n1} – Позиция негативного пика первой производной волны;

N_{z1} – Количество пересечений нуля первой производной волны.

Исходные значения признаков могут изменяться в большом диапазоне, поэтому работа классификатора с такими данными может оказаться некорректной. Для решения этой проблемы производится нормализация признаков, т. е. значения признаков, приводятся к некоторому заданному диапазону. В нашем случае каждый признак приводится к единичному среднеквадратичному отклонению и нулевому среднему. Для этого среднее значение столбца (признака) μ вычисляется по следующей формуле (где N – количество элементов в столбце; x_i – элемент столбца):

$$\mu = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (1)$$

Выражение для вычисления стандартного отклонения σ имеет вид:

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2} \qquad (2)$$

Новые нормализованные признаки по каждому из столбцов вычисляем с помощью найденных среднего значения и стандартного отклонения для данного столбца по формуле:

$$z_i = \frac{x_i - \mu}{\sigma} \qquad (3)$$

где z_i – новые нормализованные значения признака.

1.3.4. Аутентификация

Аутентификация производится с использованием машинного обучения, которое позволяет создать модели распознавания и классификации путём обучения на основе накопленных данных. В данном случае создаётся модель классификации выделенных ранее ЭЭГ-паттернов, соответствующих вынужденным морганиям людей из тестовой группы.

Модель получает на вход столбец признаков, соответствующих ЭЭГ вынужденных морганий тестируемого человека и, далее, используя шаблоны признаков тех людей, на которых велось обучение (тестируемый человек обязательно должен быть среди них), на выходе выдаёт идентификатор (имя, метку и.т.д в зависимости от специфики применения) тестируемого человека.

Формально задачу можно описать следующим образом: если $X = \{X_i\}_{i=1}^{n}$ – множество векторов признаков (X_{i_k} – вектор признаков какого-то конкретного выделенного моргания) , $Y = \{Y_i\}_{i=1}^{n}$ – множество ответов (Y_{i_k}– идентификатор человека, которому это моргание принадлежит), то модель классификации описывается отображением $X \to Y$, строящимся в процессе так называемого обучения модели.

Для обучения используется обучающая выборка, представляющая из себя набор примеров правильного отображения, то есть такие $\{X_i \to Y_i\}_{i=1}^{n}$, в которых любые выбранные X_{i_k} и Y_{i_k} в действительности соответствуют одному человеку. Найденное с использованием обучающей выборки отношение $X \to Y$ в дальнейшем используется для определения класса Y_0 для каждого нового ЭЭГ-паттерна, описываемого вектором X_0, если он достаточно близок к элементам одного из множеств X_i, т. е. если $X_0 \in X_i$.

Таким образом, для аутентификации необходим обученный классификатор, способный предсказать класс ЭЭГ-паттерна конкретного человека по его признакам.

В данной работе исследовались классификаторы, основанные на разных методах машинного обучения, таких как: метод опорных векторов, деревья решений и метод k ближайших соседей. Разберём в общих чертах механизм работы каждого из методов.

Метод опорных векторов *(Support Vectors Classifier – SVC)* основан на идее аналитического представления отображения $X \to Y$ как набора точек в пространстве размерности n, (соответствующей количеству используемых признаков), принадлежащих разным классам, в зависимости от значения Y_i. Суть метода заключается в поиске двух параллельных гиперплоскостей между каждыми двумя классами, причём таких, чтобы зазор между этими гиперплоскостями был максимальным.

В случае же мультиклассовой классификации, строится всего $\frac{M\cdot(M-1)}{2}$ бинарных классификаторов ($M -$ общее количество классов). Каждый из них предназначен для определения принадлежности текущей точки (точки в пространстве набора признаков) к конкретному классу, выбранному для данного классификатора. Итоговый же классификатор основывается на решениях бинарных о принадлежности точки к каждому из классов или к их отрицанию.

Из классификаторов на основе решающих деревьев был выбран метод случайного леса (*Random Forest– RF)*, основная идея которого заключается в построении как можно менее зависимых друг от друга деревьев с последующим принятием решения путем голосования. Деревья принятия решений (*Decision trees*) имеют листы, внутренние узлы и ребра. В листах записаны значения классов, а в узлах — признаки, по которым различаются случаи при спуске по дереву. Чтобы вычислить значение класса для набора признаков, надо спуститься по дереву до листа и выдать соответствующую метку.

Random Forest использует ансамбль решающих деревьев. Он сочетает метод случайных подпространств с усреднением решений локальных классификаторов по методу Будстрепа. Будстреп — статистический метода формирования *m* новых выборок размером *n* из *n* объектов исходной выборки.

При этом производится *n* раз выбор объекта в одну из *m* выборок с возвратом предмета в исходное множество, т. е. некоторые предметы могут попасть в выборку несколько раз, некоторые могут не попасть вообще. При классификации выборки формируются описанным подходом, на каждой выборке обучается свой (локальный) классификатор, а итоговый классификатор усредняет решения всех локальных классификаторов.

Для снижения корреляции между деревьями при их обучении на случайно выбранных признаках, вместо всего набора используется метод случайных подпространств. Дерево строится до полного исчерпания подвыборки.

Классификация объектов проводится путём голосования: каждое дерево комитета решающих деревьев относит классифицируемый объект к одному из классов, и побеждает класс, за который проголосовало наибольшее число деревьев.

Метод k ближайших соседей (k Nearest Neighbors – kNN) использует идею о том, что класс классифицируемого объекта должен наиболее часто встречающийся среди k штук ближайших соседей данного объекта. Таким образом для классификации каждого из объектов тестовой выборки необходимо последовательно выполнить следующие операции: вычислить расстояние до каждого из объектов обучающей выборки; отобрать k (заданное число) объектов обучающей выборки, расстояние до которых минимально.

1.3.5. Обучение и тестирование

Перед аутентификацией необходимо произвести обучение и тестирование описанных выше классификаторов на имеющемся наборе признаков, выделенных из сигналов ЭЭГ.

Для начала набор признаков требуется поделить на обучающую (используемую для обучения модели) и тестовую (используемую для тестирования модели) в каком-либо заданном соотношении. Чаще всего используют деление 70/30, поскольку оно позволяет и получить достаточно

хорошо обученную модель, и корректно определить показатели качество обученной модели.

Говоря о показателях качества модели, стоит ввести в рассмотрение следующие обозначения. Пусть модель уже обучена, тогда результаты классификации тестовых данных можно разбить на четыре группы:

1. TP — истинно-положительные решения, то есть те решения, которые были правильно определены классификатором как положительные;
2. TN — истинно-отрицательные решения, то есть те, которые, были верно распознаны классификатором как отрицательные;
3. FP — ложноположительные решения – те, которые были ошибочно распознаны классификатором как положительные;
4. FN — ложноотрицательные решения – те, которые были ошибочно определены в класс отрицательных.

В этих обозначениях качество классификации можно определить по следующим метрикам:

1. Доля верных ответов (метрика *Accuracy*):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

2. Точность (метрика *Precision*) в пределах класса – это доля записей, действительно принадлежащих данному классу относительно всех записей, которые классификатор отнес к этому классу:

$$Precision = \frac{TP}{TP + FP}.$$

3. Полнота (метрика *Recall*) в пределах класса – это доля найденных классификатором записей, принадлежащих классу относительно всех записей этого класса в тестовой выборке.

$$Recall = \frac{TP}{TP + FN}$$

4. F-мера – представляет собой гармоническое среднее между точностью и полнотой и определяется по формуле:

$$F = \frac{Precision \cdot Recall}{Precision\ +\ Recall}$$

Также, для более равномерного использования данных и, следовательно, получения более устойчивого результата относительно разделения на обучающую и тестовую выборки, используют кросс-валидацию [17]. При этом данные разбиваются на k (заранее выбранное число) частей. $k-1$ часть используется для обучения модели, а оставшаяся одна – для тестирования. Данная процедура повторяется k раз, пока каждая из k частей данных не будет использована для тестирования.

В данной работе будут использованы стандартное разделение данных на обучающую и тестовую выборки, кросс-валидация с перемешиванием (при этом обучающие выборки на разных шагах могут иметь ненулевое пересечение) и без него. Исходя из полученных результатов, выбирается наилучший метод классификации.

Беря за основу классификатор, обладающий наибольшей точностью, для аутентификации используется следующий алгоритм (рис. 5):

1. Модуль аутентификации получает идентификатор пользователя (User_id) и набор признаков (EEG_data), выделенных из сигнала ЭЭГ того пользователя, которого надо аутентифицировать.
2. С помощью обученного ранее классификатора находится значение p, характеризующее уровень соответствия биометрических данных имеющемуся идентификатору.
3. Если $\frac{p}{1-p} \geq T$, ($T -$ некое пороговое значение), то считается, что пользователь подтверждён. Если же $\frac{p}{1-p} < T$ - не подтверждён, соответственно. Параметр T в этом неравенстве называют порогом подобия, ведь его значение определяет степень безопасности системы

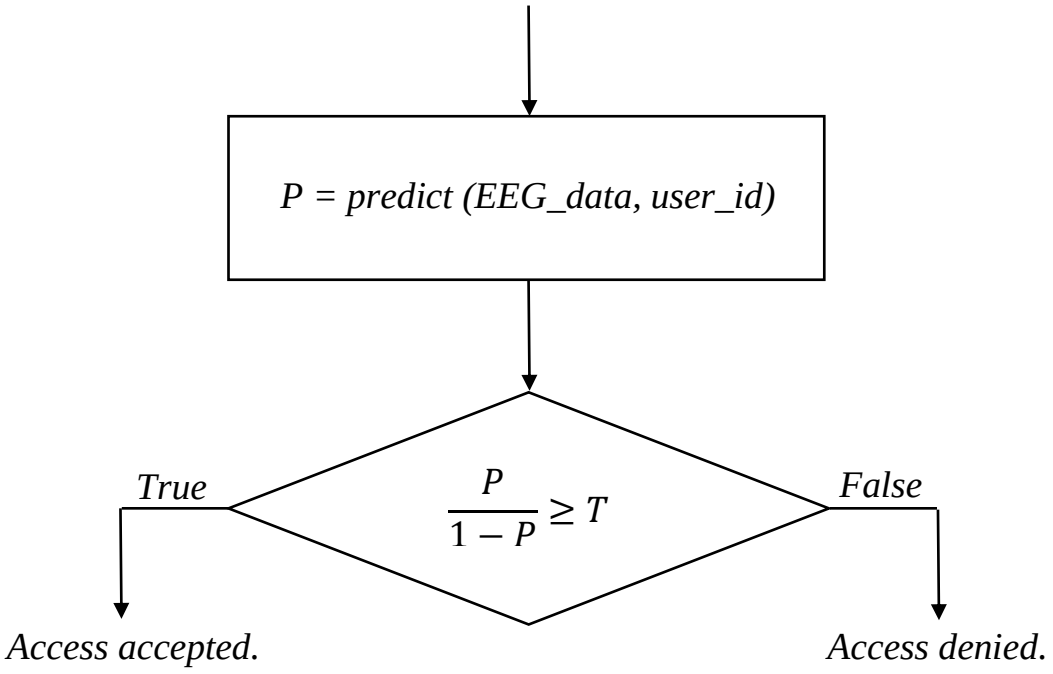

Рис. 5 – Схема работы алгоритма аутентификации

В такой схеме аутентификации возможны две основные ошибки:

1. FRR (False Reject Rate) – коэффициент ложного отказа, характеризующий случаи, когда истинный пользователь не допущен.
2. FAR (False Acceptance Rate) – коэффициент ложного допуска, характеризующий те случаи, когда допущен не истинный пользователь.

Из устройства модуля аутентификации следует, что значение обеих ошибок напрямую зависит от выбранного порога подобия системы. Так, например, уменьшив T, значение FFR также уменьшится, но увеличивается FAR (система станет более уязвима), и, наоборот, увеличив T, уменьшится FAR (система станет более безопасной), однако при этом увеличится и FFR.

Необходимо подобрать значение порога подобия для системы таким, чтобы свести ошибки к минимуму. Этим значением является так называемы равный уровень ошибок (Equal Error Rate - EER) – коэффициент, при котором обе ошибки (FFR и FAR) эквивалентны.

1.4. Алгоритм аутентификации на основе спектральной плотности

1.4.1. Сбор данных

Так же, как и в алгоритме, основанном на вейвлет-преобразовании, на данном этапе при помощи электроэнцефалографа производится запись ЭЭГ вынужденных морганий, однако в данном случае берутся все каналы, а не только те, на которых наиболее чётко прослеживается ЭОГ. В данном случае работа будет идти не с каждым конкретным морганием, а со всей записью в целом.

1.4.2. Предобработка записанных сигналов

На данном этапе, как и раньше, записанные данные приводились к виду, пригодному для выделения из них геометрических признаков, однако предобработка основывалась уже на распределении спектральной плотности мощности (СПМ) сигнала - функции распределения мощности сигнала в зависимости от частоты, или, иными словами, функции, характеризующая мощность, приходящуюся на единичный интервал частоты.

В основе СПМ лежит преобразование Фурье, однако поскольку в сигнале ЭЭГ распределение частот во времени непостоянно, нахождение спектра напрямую с помощью преобразования Фурье не имеет смысла: результат будет сильно варьироваться от записи к записи, причём и само распределение будет представлять собой набор некоего “шума”, аналогичного тому, что можно увидеть в записанном сигнале. По этой причине используется именно спектральная плотность мощности сигнала, так как она является своеобразным усреднением преобразования Фурье [16], а также является достаточно гладкой, что упрощает дальнейшее выделение признаков.

Математически, спектральная плотность мощности (power spectral density - PSD) сигнала $f(t)$ на промежутке $[-\frac{T}{2};\frac{T}{2}]$ находится следующим образом:

$$PSD(\omega) = \lim_{T \to +\infty} \frac{|F_T(\omega)|^2}{T} \qquad (10),$$

Где $F_T(\omega)$ – преобразование Фурье рассматриваемого сигнала:

$$F_T(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-T/2}^{T/2} f(t) e^{-i\omega t} dt \qquad (11)$$

В данной же работе предполагается использовать дискретный вариант СПМ, вычисляемый методом Уэлша[?], заключающийся в оценке спектральной плотности мощности путем разделения данных на перекрывающиеся сегменты, вычисления модифицированной периодограммы для каждого сегмента и усреднения по всем периодограммам. Под периодограммой в данном случае подразумевается усреднение квадрата модуля преобразования Фурье по рассматриваемой выборке измерений:

$$PSD_D(\omega) = E\left[\frac{|F_{DT}(\omega)|^2}{T}\right] \qquad (12)$$

Здесь $|F_{DT}(\omega)|$ - амплитуда преобразования Фурье от дискретной функции $f(t)$ на конечном временном интервале длиной T, а $E[\dots]$ — оператор статистического усреднения (математическое ожидание).

В отличие от варианта предобработки с использованием вейвлет-преобразования, СПМ не требует выделения паттернов конкретных морганий, а применяется ко всей записи (Рис. 5). Таким образом, СПМ характеризует, скорее, общую ЭЭГ-активность испытуемого, моргания в данном случае являются тем самым типовым событием, обеспечивающим корректность проводимого исследования.

Поскольку в данной работе рассматриваются записи ЭЭГ с разной частотой морганий, разумно будет нормировать получаемые распределения спектральной плотности мощности на максимальное её значение по каждой конкретной записи. Так как СПМ в данном случае характеризует не только

моргания, но и фоновую ЭЭГ-активность, форма распределения при анализе записей с разными частотами морганий не должна измениться.

1.4.3. Формирование признаков

В качестве признаков используется площадь секторов полученного распределения нормированной спектральной плотности мощности (рис. 6). Количество используемых секторов (то есть, соответственно, количество выделяемых признаков) может настраиваться в зависимости от требуемой точности дальнейшей классификации.

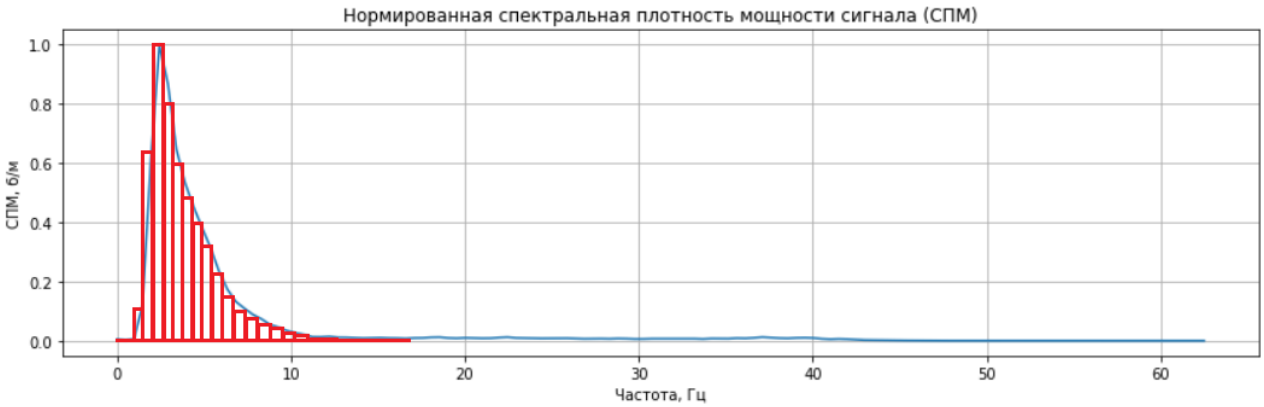

Рис. 6 – графическое представление механизма выделения признаков из СПМ

Для большей точности вычислений, при нахождении площадей использовался метод Симпсона, суть которого заключается в приближении подынтегральной функции $f(x)$ на каждом из рассматриваемых отрезков $[a, b]$ интерполяционным многочленом второй степени $p_2(x)$, то есть приближение графика функции на отрезке параболой.

Формула Симпсона имеет вид:

$$\int_a^b f(x)dx \approx \int_a^b p_2(x)dx = \frac{b-a}{6}\left(f(a) + 4f\left(\frac{a+b}{2}\right) + f(b)\right)$$

где $f(a), f(b), f(\frac{a+b}{2})$ - значения исследуемой функции на концах отрезка и в его середине, соответственно.

Для более точного вычисления интеграла интервал $[a, b]$ разбивают на $N = 2n$ элементарных отрезков одинаковой длины и применяют формулу Симпсона на составных отрезках. Каждый составной отрезок состоит из соседней пары элементарных отрезков. Значение исходного интеграла является суммой результатов интегрирования на составных отрезках:

$$\int_a^b f(x)dx \approx \frac{h}{3} \cdot \left(\frac{1}{2} f(x_0) + \sum_{k=1}^{N-1} f(x_k) + 2 \sum_{k=1}^{N} f\left(\frac{x_{k-1} + x_k}{2} \right) + \frac{1}{2} f(x_N) \right)$$

где $h = \frac{b-a}{N}$ – шаг интегрирования, а $x_k = a + kh$ – чередующиеся границы и середины составных отрезков, на которых применяется формула Симпсона.

1.4.4. Обучение модели и аутентификация

Аутентификация в данном алгоритме происходит абсолютно аналогично алгоритму на основе вейвлет-преобразования. Точно так же рассматриваются метод опорных векторов, случайный лес и k ближайших соседей. Аналогичным же образом используется кросс-валидация и разделение на обучающую и тестовую выборки. Меняется только фактическая длина векторов признаков X_i, зависящая в данном случае от количества секторов, на которых вычисляются площади.

Значение оптимального порогового коэффициента точно так же, как и в алгоритме на основе вейвлет-преобразования планируется подбирать перебором, добиваясь равенства значений коэффициента значений коэффициентов ложного допуска (FRR) и ложного отказа (FAR).

1.5. Выводы по главе

В результате анализа литературы была выбрана методика распознавания, основанная на вынужденных морганиях, совершаемых под такт метронома. В данной главе предложены и описаны два алгоритма аутентификации, основанные на вейвлет-преобразовании и на распределении спектральной плотности мощности сигнала соответственно. Каждый из алгоритмов содержит по 4 блока: сбор данных, предобработку выделение признаков, и, непосредственно, блок аутентификации.

ГЛАВА 2. РЕАЛИЗАЦИЯ АЛГОРИТМОВ АУТЕНТИФИКАЦИИ

2.1. Используемое программное обеспечение и оборудование

Для реализации обоих алгоритмов использовалась среда разработки **JupyterLab** и язык программирования **Python**. Данный язык программирования был выбран, поскольку для него существует большое количество научных и технических библиотек. Так, например, для чтения записанных файлов использовалась библиотека **pyEDFlib**, для вейвлет-преобразования – библиотека **pywavelets**, для нахождения спектральной плотности мощности сигнала – библиотека **scipy**, для машинного обучения, оценки эффективности и последующего тестирования – библиотека **sklearn**. Также для оптимизации вычислительного процесса использовались библиотеки **numpy**, **pandas** и **matplotlib**.

Запись ЭЭГ велась при помощи портативного электроэнцефалографа **NeuroPlay-8Cap,** имеющего 8 сухих электродов**.** Во время записи электроды были установлены в положения O1, P3, C3, F3 – для левого полушария и в положения O2, P4, C4, F4 – для правого (рис. 7). Нулевой потенциал, относительно которого велась запись, брался на мочке левого и правого уха для каждого из полушарий, соответственно.

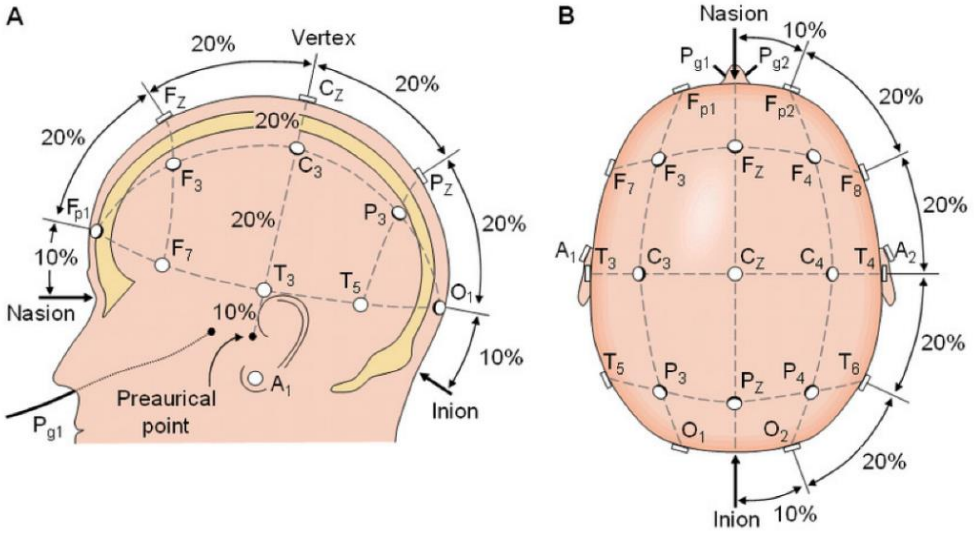

Рис. 7 – Схема всех возможных расположений электродов

2.2. Реализация алгоритма на основе вейвлет-преобразования

Всего в записи учувствовали 5 человек - двое женщин и трое мужчин, в возрасте от 21 до 27 лет. За один подход с каждого из них снималось по 5 записей длинной в минуту, содержащих моргания с частотой 15 морганий в минуту. Моргания совершались в такт метроному. Всего было сделано 3 подхода с разницей во времени между первыми двумя примерно в месяц, и, между вторым и третьим – в 3 месяца. Для обучения и тестирования использовались только данные, снятые в первый день – остальные данные использовались исключительно для проведения сравнительного анализа.

С целью избежать возникновения нежелательных атрибутов на записи, снятие ЭЭГ велось в условиях отсутствия посторонних шумов, в удалении от бытовых электроприборов, электрических розеток, а также других людей. Во время записи испытуемые смотрели в одну точку, стараясь не двигать глазами без необходимости.

С помощью библиотеки pyEDFlib, снятые данные преобразовывались во внутренний тип языка Python, на котором и описывались все дальнейшие операции, производимые над сигналом. В алгоритме распознавания решено было использовать только два фронтальных канала из записей (F3 и F4), поскольку, как говорилось ранее, именно на них ЭОГ (глазодвигательный артефакт) проявляются наилучшим образом (рис. 8).

Для вейвлет-преобразования Добеши 2-го порядка использовалась библиотека **pywavelets** и метод **downcoef** с аппроксимацией на краях типа **reflect**, применяемой во избежание возникновения там нежелательных артефактов, которые на последующих шагах могут быть ошибочно восприняты алгоритмом как моргания. Метод применялся последовательно три раза: сперва непосредственно к снятым данным, а в последующие два раза - к полученной на предыдущем шаге детализирующей последовательности. Обработанный сигнал представлен на рис. 9.

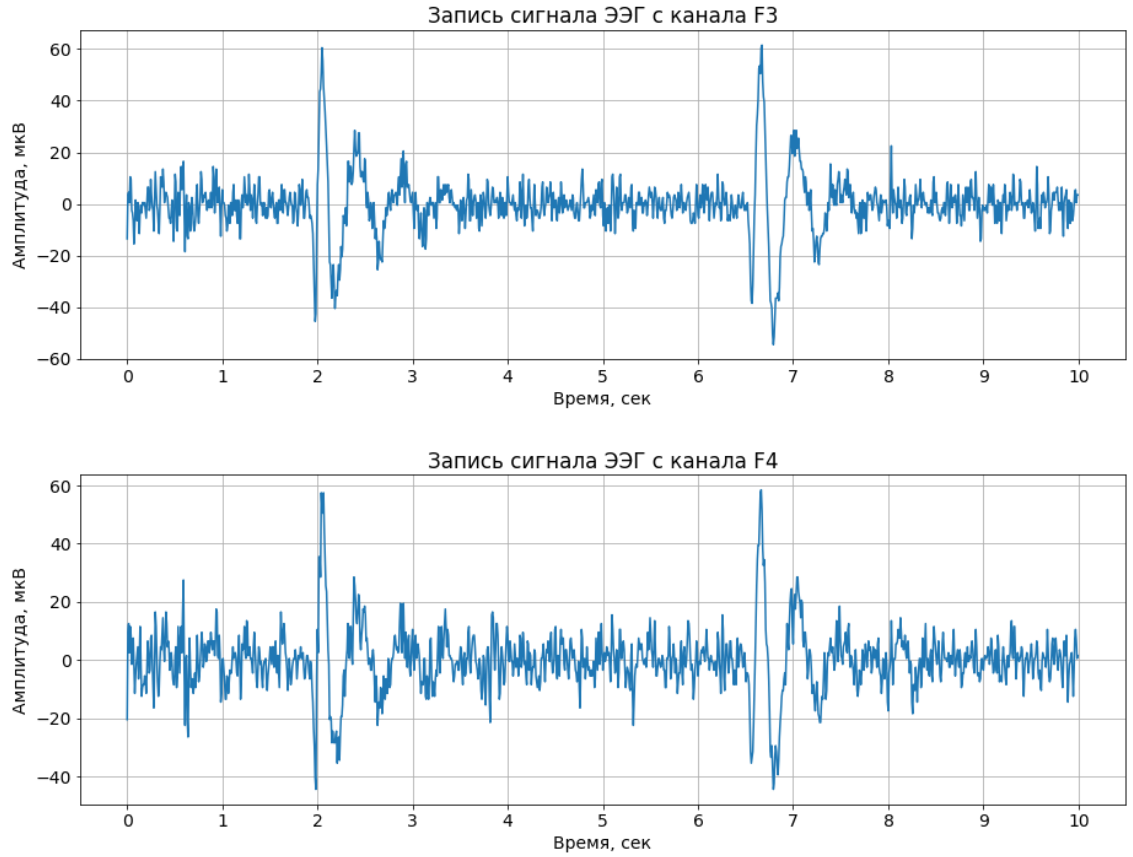

Рис. 8 – Вид необработанной записи ЭЭГ с двух фронтальных каналов

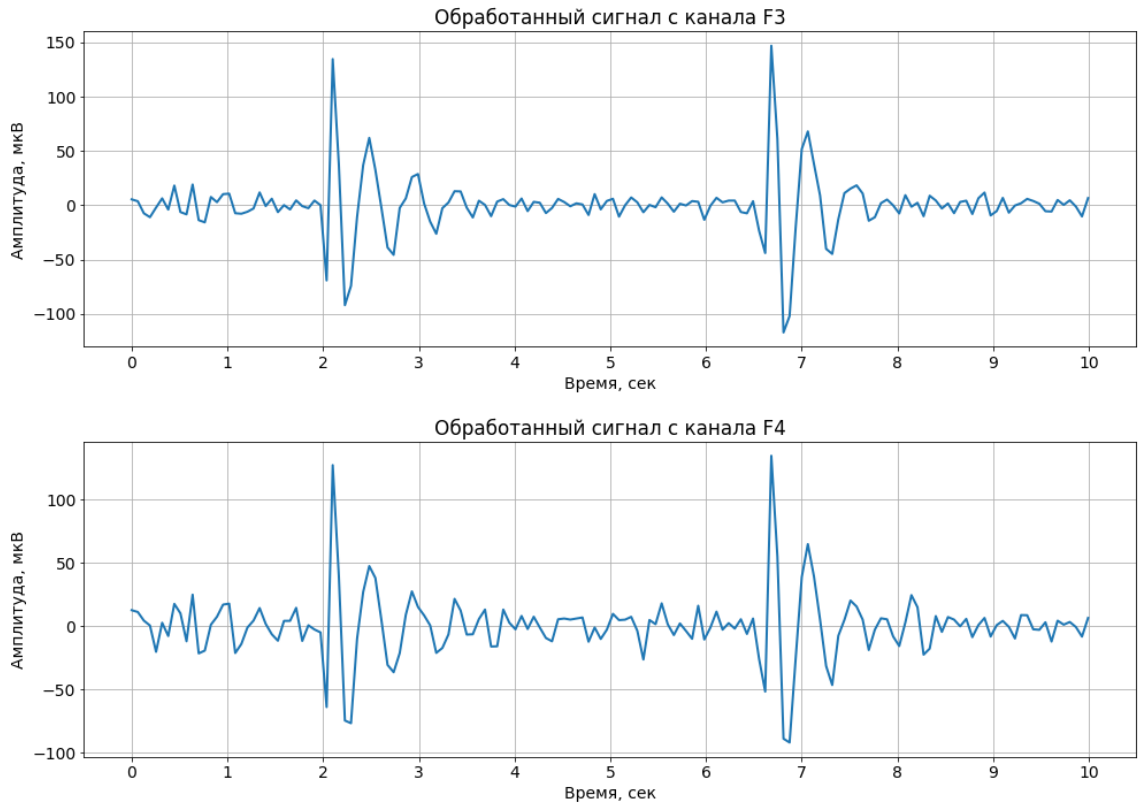

Рис. 9 - Сигнал с фронтальных каналов после трёхуровневого применения вейвлет-преобразования Добеши 2-го порядка

Далее из обработанных записей выделялись положительный и отрицательный пики, а также координаты их начала и конца, соответственно. Ниже приведена визуализация найденных точек на одном из каналов (рис. 10), на втором канале они выглядит аналогично.

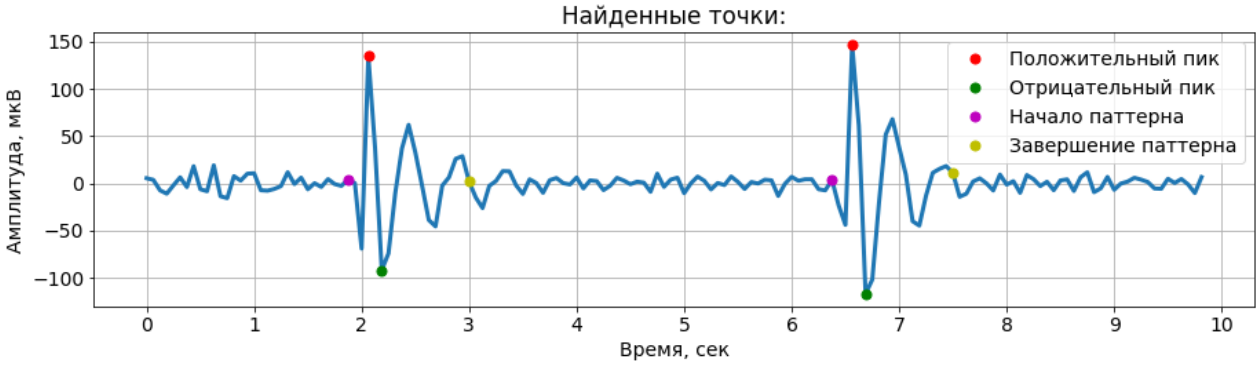

Рис. 10 - Сигнал с фронтальных каналов после трёхуровневого применения вейвлет-преобразования Добеши 2-го порядка

По алгоритму, описанному в прошлой главе, формировался датафрейм, содержащий признаки каждого из выделенных морганий для каждой из записей. Нормализация признаков производилось при помощи функции **scale** библиотеки **sklearn**. Для оптимизации дальнейших шагов идентификатор пользователя записывался в том же датафрейме в графе “User” (рис. 11).

	User	Max_A	Min_A	Max_pos	Min_pos	Left_tan	Center_tan	Right_tan	Left_s	Right_s
0	4	0.400841	-0.966933	-0.895116	-0.255408	-0.740186	-0.801579	0.67844	0.31893	-0.611582
1	5	-1.61375	0.351672	-0.213571	1.59984	-0.38679	0.889086	0.604102	-1.55328	0.300447
2	2	-1.44135	0.880901	-0.704107	-0.534413	-1.68746	0.561149	-0.901154	-0.803573	0.560871
3	5	0.198898	0.707092	2.28537	0.800411	-0.894067	0.900637	-0.409181	2.16701	0.478992
4	1	-1.27729	1.36153	2.3153	0.756689	-1.38729	1.27947	-0.822375	0.145364	1.02401
5	3	0.142528	0.274725	0.661452	0.321691	-0.297034	0.477403	-0.606425	0.60301	-0.136477
6	1	-1.04103	0.128128	-0.942549	-0.186122	-1.29017	0.12291	-0.217168	-0.871054	0.0863015
7	3	0.0258112	-1.85609	-0.412895	1.89099	-0.671282	-0.071382	1.13853	0.0930651	-2.18153
8	4	1.49531	-0.191188	-0.405977	-0.969891	-0.224455	-0.853131	0.0516717	1.50229	0.0636967
9	5	-0.346085	0.802571	2.11411	1.05057	-1.15388	1.01093	-0.802002	1.41785	0.322619

Рис. 11 – часть датафрейма признаков, выделенных из записи ЭЭГ морганий

Далее создавались классификаторы, основанные на методе опорных векторов (SVC), случайного леса (RF) и k ближайших соседей (kNN) - для этого снова использовалась библиотека **sklearn** и методы SVC, RandomForestClassifier и KNeighborsClassifier, соответственно. Путём перебора, с помощью метода GridSearchCV, выявлялись оптимальные параметры для каждого из классификаторов.

Ниже представлены результаты работы классификаторов при найденных оптимальных параметрах для стандартного разделения данных 70/30 (Default), а также для кросс-валидации типов K-Fold и ShuffleSplit при количестве разбиений k = 5 в обоих вариантах (рис. 12). В качестве метрики используется доля правильных ответов (Accuracy).

```
accuracy for SVC (Default):  0.9172
accuracy for RF (Default):  0.8935
accuracy for kNN (Default):  0.8639

accuracy for SVC (KFold):  0.9111
accuracy for RF (KFold):  0.9260
accuracy for kNN (KFold):  0.9054

accuracy for SVC (ShuffleSplit):  0.8824
accuracy for RF (ShuffleSplit):  0.9059
accuracy for kNN (ShuffleSplit):  0.8765
```

Рис. 12 – Точность обученных классификаторов при стандартном разделении данных и при использовании кросс-валидации

Из полученных результатов видно, что наибольшей точностью, находящейся в районе 90–92 %, обладает метод случайного леса. Поэтому на этапе непосредственно аутентификации разумно использовать именно его.

Наконец, тестируем аутентификатор на свежих данных по алгоритму, описанному в прошлой главе: подавая классификатору значение идентификатора пользователя (id) и запись ЭЭГ (EEG_data) вынужденных морганий, получим точность *P*, благодаря которой далее можно оценить принадлежность пользователя к заданному классу.

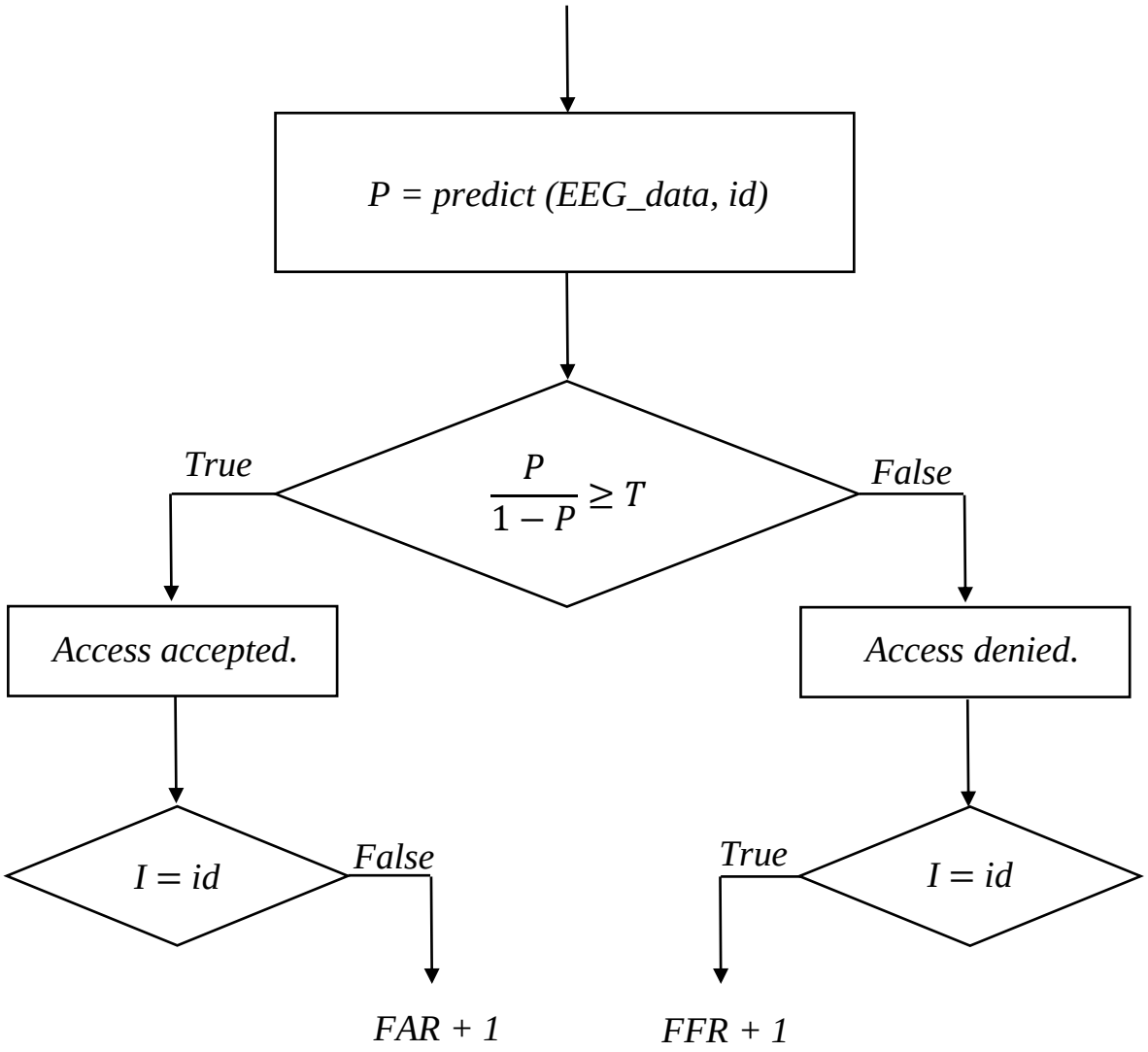

Рис. 13 – Схема для нахождения коэффициентов ложного отказа и ложного доступа

Теперь необходимо подобрать оптимальное значение порогового коэффициента T, при котором соотношение коэффициентов ложного отказа (FFR) и ложного допуска (FAR) будем ближе всего к единице. Схема для нахождения значений соответствующих коэффициентов представлена на рис. 13 (*I* - истинное значение идентификатора человека, которому принадлежит запись)

Тестируя работу алгоритма при различных значениях T согласно схеме (рис. 13), было установлено, что оптимальное значение коэффициента T равно 0.71, поскольку суммарная ошибка при этом значении минимальна (рис. 14).

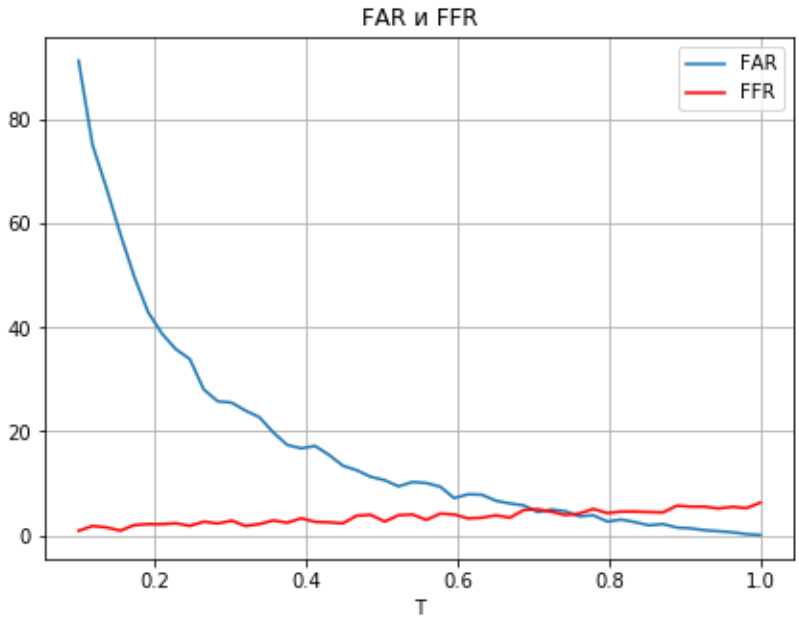

Рис. 14 – Коэффициенты ложного допуска (FAR) и ложного отказа (FFR) в зависимости от порога подобия T

2.3. Реализация алгоритма на основе спектральной плотности

Для данного алгоритма по схожей схеме с тех же испытуемых были записаны сигналы ЭЭГ вынужденных морганий с частотой 45 морганий в минуту. Число морганий было решено увеличить, поскольку при малом количестве морганий на записи, методика фактически становится ближе к анализу записей ЭЭГ людей в расслабленном состоянии. А, как было выяснено ранее, подобные методы, как правило, не дают желаемой в данной работе точности в 95%.

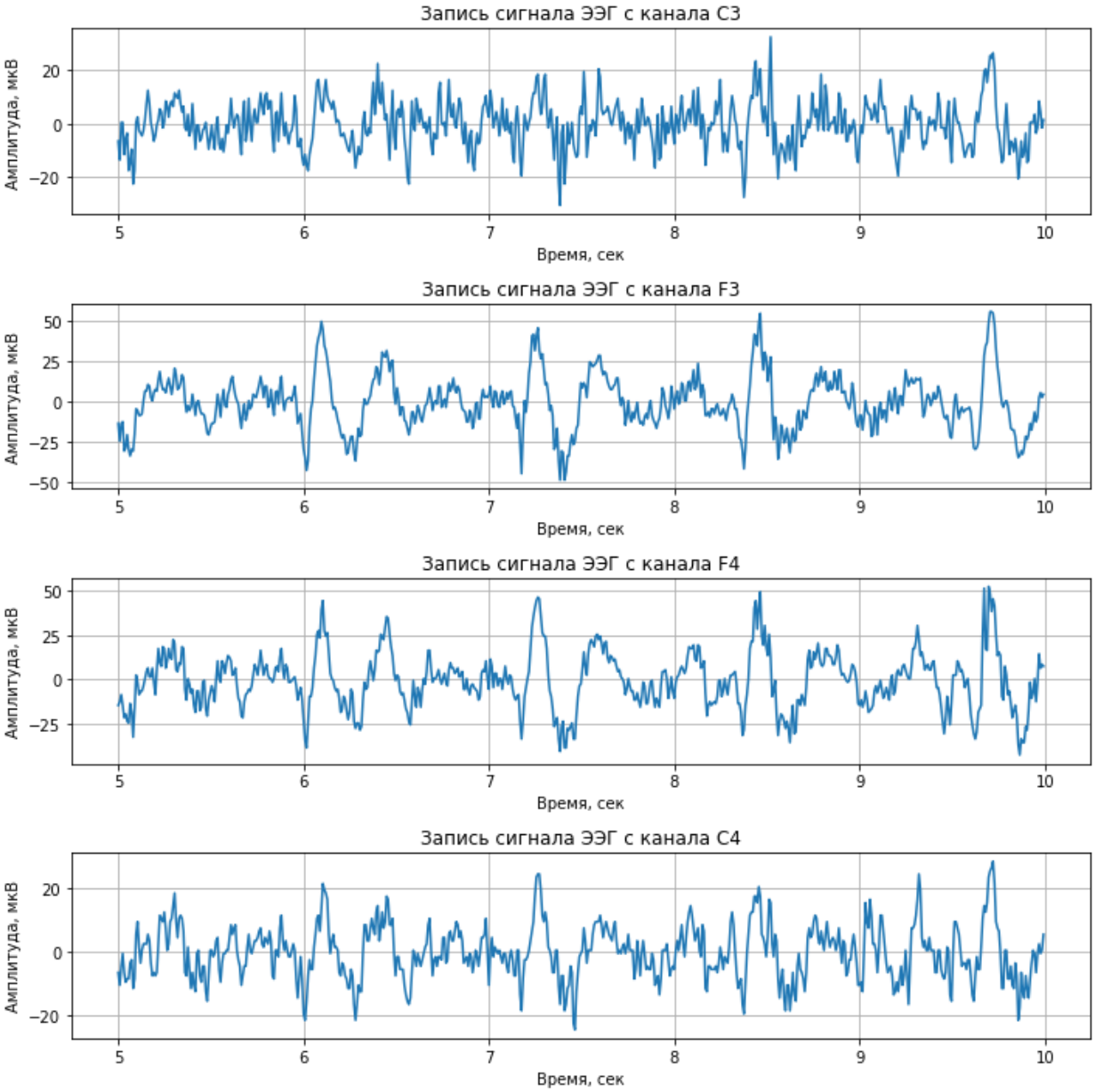

Рис.15 – Вид необработанной записи ЭЭГ с двух фронтальных и двух центральных каналов

Далее из снятых данных выбирались 4 канала – C3 и F3 с левого полушария, а C4 и F4 – с правого (Рис. 15). Остальные 4 канала не брались в рассмотрение, поскольку из-за неплотного прилегания шапки электроэнцефалографа (в профессиональных приборах используют разные размеры, но в моём распоряжении размер был только один) у некоторых испытуемых на каналах O1, O2, P3 и P4 запись велась некорректно. Таким образом пришлось отбросить записи с этих каналов у всех испытуемых и работать только с теми, что приведены на рис. 15.

Для нахождения спектральной плотности мощности сигнала использовалась библиотека **scipy** и метод **signal.welch** (рис. 16):

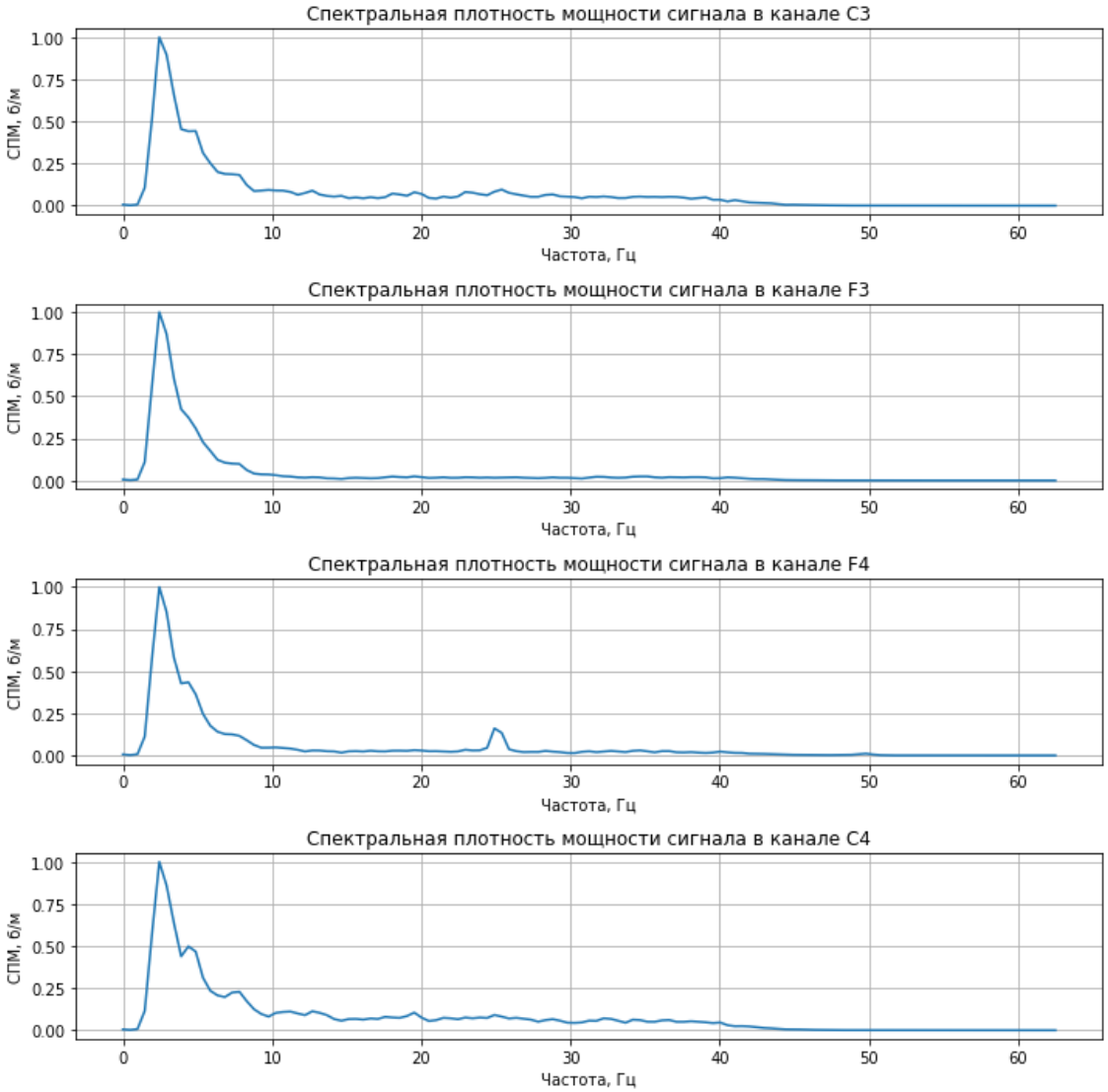

Рис. 16 – Вид нормированной спектральной плотности сигнала ЭЭГ по 4 рассматриваемым каналам

По алгоритму, описанному в прошлой главе, формировался датафрейм, содержащий признаки для каждого из выбранных каналов. Количество признаков (количество секторов, на которых вычислялась площадь под графиком) было выбрано равным 60, поскольку при этом алгоритм с одной стороны не тратит слишком много времени на выделение признаков и обучение, а с другой – даёт приемлемую точность.

Как и в случае с вейвлет-преобразованием, для нормализации признаков использовалась библиотека **sklearn** и метод **scale**. Для оптимизации дальнейших шагов идентификатор пользователя также записывался в датафрейме в столбце ‘User’.

	Users	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	...	S_51	S_52
0	2	0.314753	5.71325	69.7821	72.8244	49.4529	30.0791	33.0621	11.5353	8.0865	...	0.00257527	0.00233166
1	3	0.826598	19.7472	193.343	155.309	46.0108	31.3319	35.9685	9.73165	7.60588	...	0.00237725	0.00251238
2	5	0.257702	4.84342	62.7228	69.555	43.3885	28.6042	31.0186	8.90138	6.85603	...	0.00291893	0.00327886
3	1	0.296863	4.16334	60.5543	54.4929	29.7238	14.2429	18.5559	4.9696	3.93396	...	0.00222964	0.00220358
4	4	0.948434	12.6558	201.609	118.288	50.4886	29.5017	28.2242	7.54867	4.605	...	0.009921	0.00306434
5	1	0.385148	5.36136	51.0031	41.506	25.1781	14.7625	23.1024	5.86439	4.74364	...	0.0019749	0.00181107
6	4	0.932944	28.0285	210.74	131.8	46.2856	27.4406	30.0621	8.67999	8.27946	...	0.00246035	0.00208212
7	1	0.206793	3.07705	47.3246	39.8673	24.5466	14.8112	18.1441	5.41769	3.21577	...	0.00249449	0.00208305
8	1	0.168487	3.58226	42.4662	38.5941	26.2786	14.0186	15.0368	4.4987	3.56486	...	0.00244814	0.00237916
9	3	1.11931	16.648	181.22	132.565	82.4108	46.1427	37.1638	7.19316	5.61716	...	0.00291693	0.00184151
10	5	0.647763	33.3935	285.631	179.108	71.0466	30.5147	26.9976	7.74525	4.95145	...	0.00221737	0.00186781
11	2	0.373723	4.32462	61.5318	59.074	36.3699	21.7212	27.7602	10.8822	6.62231	...	0.00269091	0.00226261
12	2	0.485784	6.46489	79.0955	74.3308	44.564	31.8888	38.0453	11.5223	6.59334	...	0.00259504	0.00232505
13	2	0.336166	6.60179	81.7156	89.543	53.1481	37.3921	39.5255	15.9639	10.2789	...	0.002899	0.00273011
14	2	0.454194	6.00864	89.6793	80.0893	51.6438	33.7185	37.7987	14.1493	9.57829	...	0.00228308	0.00217372

Рис. 17 – Часть датафрейма признаков, выделенных из записи ЭЭГ морганий

На обработанных данных обучались классификаторы, основанные на методе опорных векторов (SVC), случайного леса (RF) и k ближайших соседей (kNN) - для снова использовалась библиотека **sklearn** и методы SVC, RandomForestClassifier и KNeighborsClassifier, соответственно. Путём перебора, с помощью метода GridSearchCV, выявлялись оптимальные параметры для каждого из классификаторов.

Ниже представлены результаты работы классификаторов при найденных оптимальных параметрах для стандартного разделения данных 70/30 (Default), а также для кросс-валидации типов K-Fold и ShuffleSplit при количестве разбиений k = 5 в обоих вариантах (рис. 18). В качестве метрики используется доля правильных ответов (Accuracy).

```
accuracy for SVC (Default):  0.9217
accuracy for RF (Default):  0.9565
accuracy for kNN (Default):  0.7913

accuracy for SVC (KFold):  0.9346
accuracy for RF (KFold):  0.9192
accuracy for kNN (KFold):  0.8056

accuracy for SVC (ShuffleSplit):  0.9538
accuracy for RF (ShuffleSplit):  0.9491
accuracy for kNN (ShuffleSplit):  0.8644
```

Рис. 18 – Точность обученных классификаторов при стандартном разделении данных и при использовании кросс-валидации.

Из полученных результатов видно, что наибольшей точностью обладает снова классификатор, основанный на методе случайного леса. Вычислив для него коэффициенты ложного допуска и ложного отказа при разных значениях коэффициента T, было найдено оптимальное значение: T = 0.68 (рис. 19).

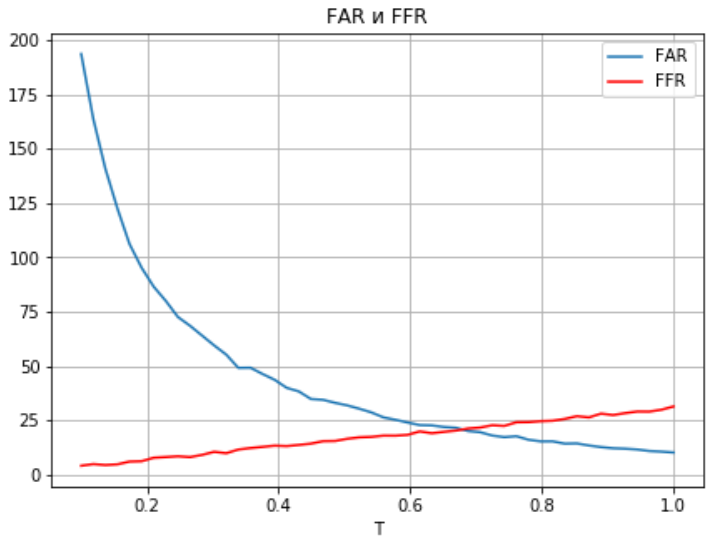

Рис. 19 – Коэффициенты ложного допуска (FAR) и ложного отказа (FFR) в зависимости от порога подобия T.

2.4. Выводы по главе

В данной главе при помощи языка Python в среде разработке JupyterLab были реализованы два алгоритма аутентификации на основе записей ЭЭГ вынужденных морганий. В обоих случаях наилучший результат дал классификатор на основе случайного леса (RF). Точность оказалась приемлемой в обоих случаях, однако алгоритм на основе спектральной плотности оказался более точным.

ГЛАВА 3. АНАЛИЗ РЕЗУЛЬТАТОВ

1.1. Описание результатов

Алгоритм аутентификации на основе спектральной плотности мощности (PSD) анализируемого сигнала показал большую точность в сравнении с алгоритмом на основе вейвлет-преобразования (DB2): 95,6% против 92,6% (рис. 20). Объяснить это можно тем, что в алгоритме на основе спектральной плотности количество используемых в обучении модели признаков было фактически в три раза больше, чем в алгоритме на основе вейвлет-преобразования.

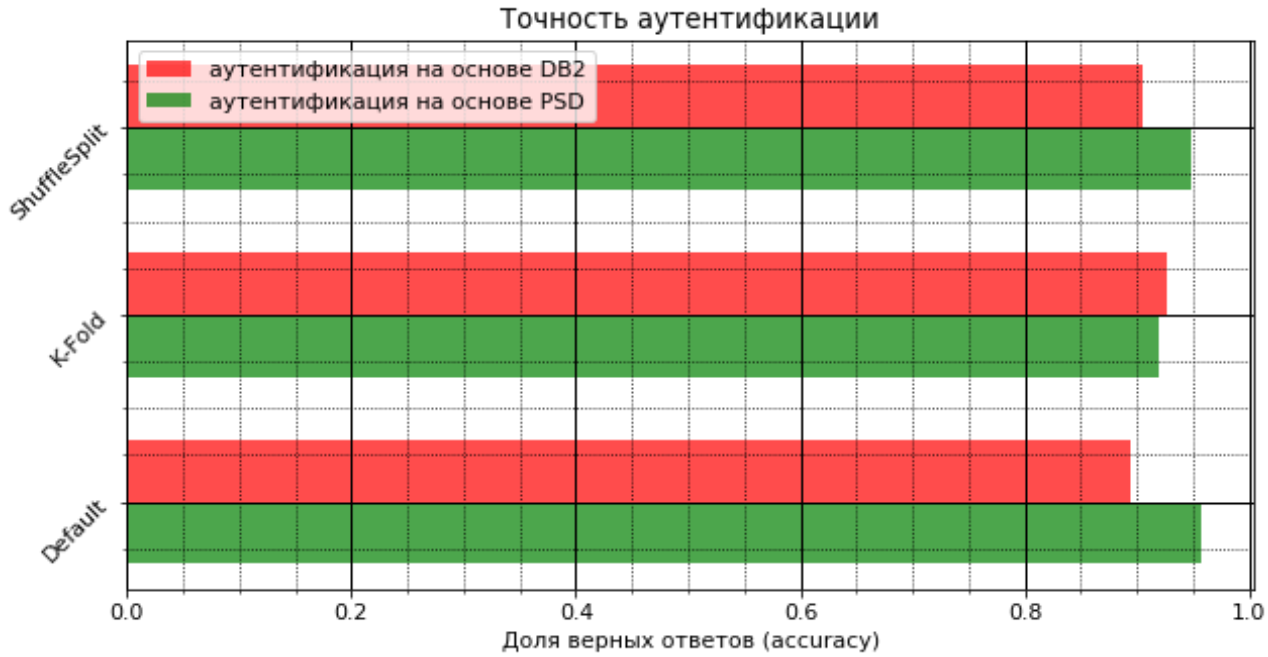

Рис. 20 – Визуализация точности алгоритмов аутентификации по метрике accuracy

Помимо этого, на результат сильно влияет и низкая частота дискретизации у используемого оборудования, равная 125 Гц. Как говорилось ранее, при вейвлет-преобразовании третьего уровня сигнал прорежается в 8 раз, и, соответственно, плотность точек на обработанном сигнале становится в 8 раз меньше. Этот факт может сильно влиять, к примеру, на результат обнаружения границ паттернов морганий, из-за чего некоторые из признаков (такие как площадь под положительным и отрицательным пиками паттерна) могут быть вычислены некорректно.

Несмотря на преимущество алгоритма на основе спектральной плотности перед алгоритмом на основе вейвлет-преобразования в точности, в перспективе он является менее устойчивым при распознавании записей ЭЭГ, взятых с одного и того же человека с течением времени.

Ниже приведена визуализация точности обоих алгоритмов (полученной усреднением по всем результатам в рассматриваемый день) при тестировании на данных записанных в тот же день (1-st day), что и данные, на которых велось обучение; через месяц (2-nd day) и через 4 месяца (3-rd day) со дня записи сигналов, на которых велось обучение моделей (рис. 21).

Рис. 21 – Точность аутентификации по записям, сделанным разные дни.

Данную закономерность, вероятно, можно объяснить тем фактом, что распределение частот на записи ЭЭГ не постоянное и их спектр у одного человека может меняться со временем. Таким образом, хотя для нормализации получаемых признаков и было использовано типовое событие в виде морганий, устойчивости алгоритма на основе спектральной плотности мощности сигнала всё же добиться не удалось.

Также стоит отметить, что аутентификация на основе спектральной плотности требует большего числа входных данных, поскольку из одного канала, по сути, можно выделить только одну строку с признаками для модели. При аутентификации на основе вейвлет-преобразования из одного канала записи можно было выделить по крайней мере 80% присутствующих в нём морганий (всего их в одном канале было 15), то есть не менее 12 строк с признаками для модели.

По времени работы алгоритмы отличаются не сильно: для обоих время работы лежит в диапазоне от 1.1 до 1.3 секунд в зависимости количества подаваемых данных.

1.2. Выводы по главе

В данной главе проведен сравнительный анализ результатов двух реализованных в работе алгоритмов аутентификации. Из построенных графиков видно, что хотя алгоритм на основе распределения спектральной плотности и даёт лучшие результаты на этапе обучения и тестирования, он является менее устойчивым к распознаванию сигналов, снятых с одного и того же испытуемого в разные моменты времени.

ЗАКЛЮЧЕНИЕ

В ходе данной работы были описаны и реализованы два алгоритма по распознаванию личности на основе ЭЭГ вынужденных морганий, обладающие точностью, доходящей до 92 и до 95 процентов соответственно.

Для реализации алгоритмов использовалась среда разработки JupyterLab и язык программирования Python. Для чтения записанных файлов использовалась библиотека pyEDFlib, для вейвлет-преобразования Добеши 2-го порядка – библиотека pywavelets, для нахождения спектральной плотности мощности сигнала – библиотека scipy, для машинного обучения и последующих тестов – библиотека sklearn. Для оптимизации вычислительного процесса также использовались библиотеки numpy, pandas и matplotlib.

В ходе сравнительного анализа реализованных алгоритмов выяснилось, что при выигрыше в точности, алгоритм на основе спектральной плотности мощности уступает алгоритму на основе вейвлет-преобразования по количеству требуемых для обучения данных. Также было выявлено, что хотя алгоритм на основе распределения спектральной плотности и даёт лучшие результаты на этапе обучения и тестирования, он является менее устойчивым при распознавании сигналов ЭЭГ, снятых с одного человека в разные моменты времени.

Реализованные алгоритмы можно использовать для аутентификации пользователей как альтернативу другим методам биометрической аутентификации, таких как анализ отпечатков пальца, сетчатки глаза, записи голоса и других аналогичных. К примеру, данные алгоритмы могут использоваться в сфере банковских услуг, для подтверждения денежных операций с особо крупными суммами.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Abo-Zahhad M. et. al., A new multi-level approach to eeg based human authentication using eye blinking. Pattern Recognition. Lett. 2016.
2. Alexandrov M. V., Ivanov L. B., Lytaev S. A., Electroencephalography: a guide / ed. by Alexandrov M. V., 3rd edition, reprinted, St. Petersburg, 2020.
3. Anoklin A. et. al., A genetic study of the human low-voltage electroencephalogram, Human Genetic, 1992.
4. Breiman L., Random Forest. Machine Learning, 2001.
5. Campisi P., Daria La Rocca., Scarano G., EEG for Automatic Person Recognition, IEEE Computer, July 2012, IEEE Computer Society.
6. Daubechies I., Ten lectures on wavelets. Philadelphia, Pa.: Society for Industrial and Applied Mathematics, 1992.
7. Denney D., Denney C., The eye blink electro-oculogram. Br. J. Ophthalmology, 1984.
8. Gelareh Mohammadi et. al., Person Identification by Using AR Model for EEG Signals. Proceedings of World Academy of Science, Engineering and Technology. Vol. 11, February 2006.
9. Marcel S., Millan J. D. R., Person authentication using brainwaves (EEG) and maximum a posteriori model adaptation. IEEE Trans. Pattern Anal. Mach. Intell. 2007.
10. Marple S. L., Digital Spectral Analysis: With Applications (Prentice-Hall Series in Signal Processing), January 1st, 1987, Prentice Hall, 492 pages.
11. Matsumoto T., Impact of Artificial "Gummy" Fingers on Fingerprint Systems. Optical Security and Counterfeit, 2002.
12. Miyamoto C. et. al., Biometric person authentication using new spectral features of electroencephalogram (EEG). Proceedings of the 2008 International Symposium on Intelligent Signal Processing and Communications Systems; Bangkok, Thailand. February 2009.

13. Mu Z., Hu J., Min J., — EEG-Based Person Authentication Using a Fuzzy Entropy-Related Approach with Two Electrodes. Entropy. 2016.
14. Nixon K. A. et. al., Handbook of Biometrics, chap. Spoof detection schemes, 2008.
15. Ohya T. et. al., Research of Operation Method of Accessibility Equipment for Severely Handicapped Based on Voluntary Eye Blink. In: Goh J. (eds.) The 15th International Conference on Biomedical Engineering. IFMBE Proceedings, vol. 43. Springer, Cham, 201.
16. Oppenheim A. V., Verghese G. C., Signals, systems, and inference - Introduction to Communication, Control and Signal Processing. Massachusetts Institute of Technology, 2010.
17. Pracki T., Pracka D., Narepski J., The meaning of EEG power density for the computer analysis of human sleep / Acta, neurobiol. exp., 1992, v. 52, p. 138.
18. Rangayan R. M., Analysis of biomedical signals; edited by Nemirno L. P., Moscow, 2007, 440 pages.
19. Saidatul A., Tze Zhi Chin, Ibrahim Z., Exploring EEG based Authentication for Imaginary and Non-imaginary tasks using Power Spectral Density Method, The 1st International Conference on Mechanical Electronic and Biosystem Engineering (MEBSE 2018) 15–16 December 2018, Bogor, Indonesia
20. Stankevich L.A., Amanbaeva S.S., Samochadin A.V., User authentication by electroencephalographic signals when blinking, Peter the Great St.Petersburg Polytechnic University, 2019.
21. Vogel F., The genetic basis of the normal EEG, Human Genetic, 1970.
22. Yeom S.K. et. al., Person authentication from neural activity of face-specific visual self-representation. Pattern Recognition. 2013.