В Республике Беларусь самым распространённым видом детекторов транспорта являются индуктивные рамки, хотя, как представляется, будущее принадлежит видеодетекции.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Врубель Ю.А. Организация дорожного движения.- Мн.: Фонд безопасности движения МВД Республики Беларусь, 1996.
2. Луконин В.Н. и др. Автотранспортные потоки и окружающая среда.- М.: ИНФРА-М, 2001.
3. Врубель Ю.А. Потери в дорожном движении. – Минск: БНТУ, 2003.
4. Кременец Ю.А., Печерский М.П. Технические средства регулирования дорожного движения. – М.: Транспорт, 1981.

Материал поступил в редакцию 23.10.2008

SHENDER A.V., PUSTOVOJT E.N., KARPILOVICH V.Y. Research of technologies of detecting of transport flows

There is a possibility to more effective usage of existing roads instead of building new ones. This is possible due to use of Intellectual Transport Systems, that allow to bring down time of travel, idle time in traffic jams and at crossroads, harmful influence of automobiles.

Transport detectors are integral part of any ITS. In some sense, they are eyes of a system and they report main parameters of transport streams to control system.

УДК 004.8.032.26

Шевеленков В.В.

СТЕГОКОДИРОВАНИЕ ЗВУКОВОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Введение. В распределенных системах передачи информации одна из проблем - обеспечение информационной конфиденциальности. Для того, чтобы решать эту проблему, как правило, используются различные методы криптографии. Криптографическая защита, однако, сама по себе не достаточна для обеспечения секретности информации. Необходимо не только закодировать, но также и скрыть закодированную информацию. Для этого можно использовать методологию компьютерной стеганографии. Стеганография – это методика сокрытия небольшого количества конфиденциальной информации в больших информационных массивах так, чтобы непосвященный наблюдатель не мог заметить ее наличия. Анализируя стеганографические системы, доступные сегодня, видно, что для сокрытия информации в звуковых файлах создано всего несколько программ. Методов стеганографии, использующих нейронные сети, пока нет. В этой работе будет показано, как мы можем скрыть информацию в звуковых файлах, используя нейронную сеть.

1. Общие принципы стеганографии. Для звуковых файлов применимы такие же методы, что и для других видов стеганографии. Процесс стеганографии можно разделить на несколько этапов:

1) Выбор информационного файла;
2) Выбор файла-контейнера;
3) Выбор алгоритма стеганографической защиты;
4) Кодирование файла.

После того, как выбран информационный файл, файл-контейнер и метод стеганографии, необходимо установить защиту нового файла по паролю. В нашем случае для этих целей будет использован открытый ключ.

5) Отправление сокрытого сообщения по электронной почте и его декодирование.

Например: мы можем скрыть информацию кодированием наименее значимого бита (LSB – Least Significant Bit): записывая секретное сообщение в наименьшие биты, или изменяя параметры звукового сигнала: изменяя коэффициенты дискретного косинуса преобразования.

В этой работе будет представлен метод сокрытия информации в звуковых файлах, использующий стеганографический подход и нейронные сети. Прежде всего, несколько слов о существующих методах звуковой стеганографии [1, 2].

1.1. Метод LSB. Метод кодирования наименее значимого бита (LSB) - самый простой способ встроить данные в другие структуры данных. Заменяя наименее значащий бит каждой информационной единицы, мы можем закодировать большое количество данных в звуковом сигнале.

Главный недостаток этого метода - его низкая робастность. Закодированная информация может быть разрушена простейшими манипуляциями с файлом: изменением частоты, перекодированием, изменением формата и т.д. Этот метод может быть полезен, в основном, в закрытых информационных средах, т.к. воспроизведенный и вновь записанный с микрофона стегокодированный файл полностью теряет секретное сообщение.

При переквантовании аудиосигнала из 16-битного в 8-битный и обратно, внедренный сигнал сохраняется, несмотря на частичную потерю информации.

1.2. Кодирование расширением спектра. Метка либо скрываемый файл (ЦВЗ – цифровой водяной знак) внедряется в аудиосигналы (последовательность 8- или 16-битных отсчетов) путем незначительного изменения амплитуды каждого отсчета. Для обнаружения ЦВЗ не требуется исходного аудиосигнала.

1.3. Модификация фазы аудиосигнала. Метод заключается в использовании слабой чувствительности системы слуха человека к незначительным изменениям фазы сигнала. Внедрение информации модификацией фазы аудиосигнала – это метод, при котором фаза начального сегмента аудиосигнала модифицируется в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с ним для сохранения разности фаз. Это необходимо потому, что к разности фаз человеческое ухо более чувствительно. Фазовое кодирование, когда оно может быть применено, является одним из наиболее эффективных способов кодирования по критерию отношения сигнал-шум. В экспериментах пропускная способность канала варьировалась от 8 до 32 бит в секунду.

1.4. Метод изменения времени задержки эхо сигнала. Этот метод позволяет внедрять данные в сигнал прикрытия, изменяя параметры эхо сигнала. К параметрам эхо, несущим внедряемую информацию относятся: начальная амплитуда, время спада и сдвиг (время задержки между исходным сигналом и его эхо). При уменьшении сдвига два сигнала смешиваются. В определенной точке человеческое ухо перестает различать два сигнала, и эхо воспринимается, как добавочный резонанс. Эту точку трудно определить точно, так как она зависит от исходной записи, типа звука и слушателя. В общем случае, для большинства типов сигналов и для большинства слушателей слияние двух сигналов происходит при расстоянии между ними около 0,001 секунды.

***Шевеленков Виталий Вячеславович**, ассистент кафедры интеллектуальных информационных технологий Брестского государственного технического университета.*
Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

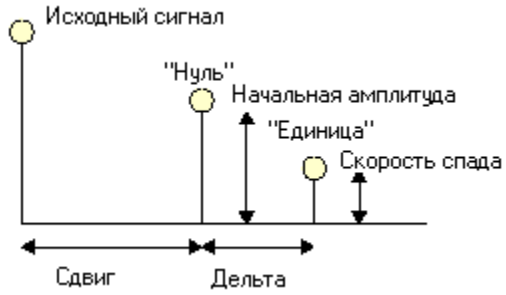

Рис. 1. *Сокрытие данных эха*

Кодировщик использует два времени задержки: одно для кодирования нуля, другое для кодирования единицы. И то, и другое время задержки меньше того, на котором человеческое ухо может распознать эхо. Кроме уменьшения времени задержки необходимо добиться установлением начальной амплитуды и времени спада того, чтобы внедренная информация не могла быть воспринята системой слуха человека [3].

Общая схема встраивания и извлечения скрытой информации в звуковом файле представлена на рис. 2. и рис. 3.:

Рис. 2. *Общая схема встраивания информации*

Рис. 3. *Общая схема извлечения информации*

Ключ - любое слово или число (Пример: Цветы, Tim1362, 12.1998).

Контейнер – звуковой файл WAV, Mp3 или другого формата.

Встраиваемое сообщение - любой файл любого типа (Пример: Документ MS Word, картинка, файл, текстовый файл).

Стегокодированный файл - звуковой файл со встроенным скрытым сообщением.

Алгоритм дешифровки сообщения – алгоритм, определяющий факт наличия скрытого сообщения в звуковом файле и дешифрующий встроенное сообщение посредством открытого ключа.

2. Методология нейросетевой стеганографии. В этой главе приведено описание разработанного алгоритма.

1. Программа открывает звуковой файл, в который мы должны встроить скрываемое сообщение и делит его на наименьшие информационные части - байты звукового файла.

2. Аналогично программа открывает файл скрываемого сообщения, и делит его на наименьшие информационные части.

3. Строится таблица соответствия (ТС), в которой записываются соответствия между каждыми байтами скрываемого сообщения и аналогичными байтами звукового файла (контейнера). Например: первый информационный байт скрываемого сообщения равен «00», следовательно, программа ищет такой же байт в файле контейнере и запоминает его положение (4, т.е. четвертая позиция). Затем выбирается второй байт сообщения, ищется аналогичный байт в контейнере и т.д. После просмотра всего сообщения мы создаем таблицу соответствия между байтами сообщения и контейнера.

Графическое представление процесса создания таблицы соответствия показано на рис. 4.

4. Создается нейронная сеть встречного распространения и обучается на прогнозирование ТС. Причем таблица соответствия это и есть обучающая выборка, размер которой напрямую зависит скрываемого сообщения.

5. Секретный ключ используется в качестве первых элементов обучающей выборки.

6. После обучения нейронной сети встречного распространения и достижения желательной точности мы получаем обученную нейронную сеть с настроенными параметрами: коэффициенты, количество нейронов в слоях, количество слоев, шаги и т.д.

7. Следующий шаг заключается в сокрытии этих коэффициентов в контейнере. В данной работе был использован метод LSB. Алгоритм встраивания заключается в следующем: выбираются места для вставки раздробленных данных (каждый элемент данных - весовой коэффициент, порог, шаг, имеет вещественный тип и занимает в памяти 6 байт, поэтому предварительно пришлось разбить их на более мелки части) используя открытый ключ, доступный тем, кто авторизован встраивать и извлекать информацию. Ключ в нашем случае может принимать любые значения как числового, так и строкового типа (в случае строкового типа также необходимо ключ преобразовать к числовому виду используя таблицу ASCII). Таким образом, после преобразования ключа в число и нормализации встраиваемых параметров, происходит внедрение информации в звуковой файл-контейнер, причем места внедрения также выбираются при помощи ключа.

Для декодирования спрятанного сообщения из контейнера необходимо выполнить следующие шаги:

1. Преобразовать ключ в число и вычислить местоположение коэффициентов нейронной сети встречного распространения.
2. Используя эти параметры и ключ, мы восстанавливаем нейронную сеть и прогнозируем таблицу соответствия.
3. Последний шаг заключается в создании и выделении скрытого сообщения и сохранении его на диске.

Так, используя этот алгоритм, мы можем скрыть любую информацию в звуковом файле. Однако имеется одно важное ограничение: размер файла контейнера должен быть несколько больше, чем скрываемое сообщение.

3. Архитектура нейронной сети. В архитектуре нейронной сети встречного распространения объединены два хорошо известных алгоритма: самоорганизующаяся карта Кохонена и звезда Гроссберга. При этом появляются свойства, которых нет ни у одного из них в отдельности. Как и многие другие, сети встречного распространения функционирует в двух режимах:

- в нормальном режиме, при котором принимается входной вектор и выдается выходной вектор;
- в режиме обучения, при котором подается входной вектор и веса корректируются, чтобы дать требуемый выходной вектор [3], [4].

3.1. Нормальное функционирование. Слой Кохонена. В простейшей форме слой Кохонена функционирует в духе "победитель забирает все", т.е. для данного входного вектора один и только один нейрон Кохонена выдает на выходе логическую единицу, а все остальные выдают ноль. Подобно нейронам большинства сетей, выход каждого нейрона Кохонена является просто суммой взвешенных входов [4].

3.2. Нормальное функционирование. Слой Гроссберга. Слой Гроссберга функционирует аналогично предыдущему. Его выход является взвешенной суммой выходов нейронов слоя Кохонена. Фактически каждый нейрон слоя Гроссберга только выдает величину веса, связывающего этот нейрон с единственным ненулевым нейроном Кохонена [4], [5].

3.3. Обучение слоя Кохонена. Слой Кохонена классифицирует входные векторы в группы схожих. Это достигается с помощью такой подстройки весов слоя Кохонена, что близкие входные векторы активируют один и тот же нейрон данного слоя. Затем задачей слоя Гроссберга является получение требуемых выходов. Обучение Кохонена является самообучением, протекающим без учителя. Поэтому трудно (и не нужно) предсказывать, какой именно нейрон Кохонена будет активироваться для заданного входного вектора. Необходимо добиться гарантированного разделения несхожих входных векторов в результате обучения.

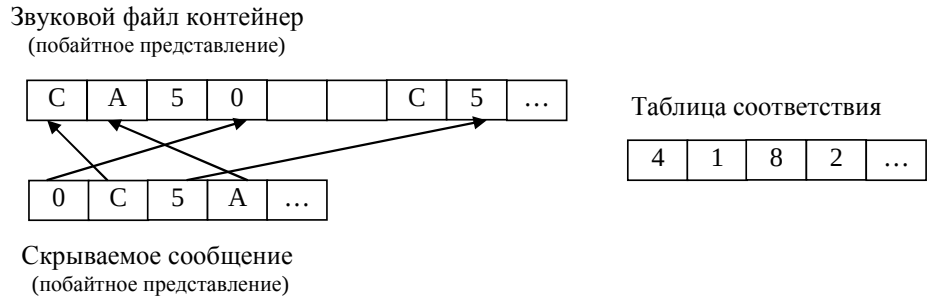

Рис. 4. *Создание таблицы соответствия*

Процесс является самообучением, выполняемым без учителя. Сеть самоорганизуется таким образом, что данный нейрон Кохонена имеет максимальный выход для данного входного вектора.

Каждый вес, связанный с выигравшим нейроном Кохонена, изменяется пропорционально разности между его величиной и величиной входа, к которому он присоединен. Направление изменения выбирается так, чтобы уменьшить разность между весом и его входом.

3.4. Выбор начальных значений весовых векторов. Всем весам сети перед началом обучения следует придать начальные значения. Общепринятой практикой при работе с нейронными сетями является присваивание весам небольших случайных значений. При обучении слоя Кохонена случайно выбранные весовые векторы следует нормализовать. Окончательные значения весовых векторов после обучения совпадают с нормализованными входными векторами. Поэтому нормализация перед началом обучения приближает весовые векторы к их окончательным значениям, сокращая, таким образом, продолжительность обучающего процесса.

3.5. Обучение слоя Гроссберга. Слой Гроссберга обучается относительно просто. Входной вектор, являющийся выходом слоя Кохонена, подается на слой нейронов Гроссберга, и выходы слоя Гроссберга вычисляются как при нормальном функционировании. Далее, каждый вес корректируется только в том случае, если он соединен с нейроном Кохонена, имеющим ненулевой выход.

Обучение слоя Гроссберга — это обучение с учителем, алгоритм располагает желаемым выходом, по которому он обучается (обратного распространения ошибки). Обучающийся без учителя, самоорганизующийся слой Кохонена дает выходы в недетерминированных позициях. Они отображаются в желаемые выходы слоем Гроссберга [4], [5].

4. Внедрение данных. Для корректной работы нейронной сети встречного распространения мы должны подготовить обучающую выборку. Как упоминалось ранее, в качестве обучающей выборки мы используем таблицу соответствия и открытый ключ, который пользователи используют при внедрении и декодировании информации. Полностью обучающая выборка может быть представлена как: Ключ + Таблица соответствия, где каждый компонент этой формулы – это числовой вектор. Используя алгоритм обучения, мы обучаем нейронную сеть встречного распространения прогнозировать обучающую выборку, зная лишь открытый ключ. После окончания процесса обучения мы получаем обученную сеть, ключевыми параметрами которой являются весовые коэффициенты. Их мы используем для прогнозирования таблицы соответствия. В качестве отправной точки используем открытый ключ. Количество нейронных элементов распределительного слоя выбирается в зависимости от открытого ключа, но не может быть меньше 5. Количество нейронов в слое Кохонена и Гроссберга зависит от файла контейнера и внедряемого сообщения, но не может быть меньше 10.

Используя полученные весовые коэффициенты обученной нейронной сети и открытый ключ, мы можем внедрить их в контейнер, используя метод LSB. Позиции изменяемых битов также вычисляются, используя векторное представление открытого ключа. Таким образом, после всех действий мы получаем звуковой файл, лишь со встроенными весовыми коэффициентами обученной нейронной сети. Само секретное сообщение не встраивается в файл контейнер.

Процесс декодирования происходит в обратном порядке.

На рис. 5. представлена общая структура нейронной сети встречного распространения [3].

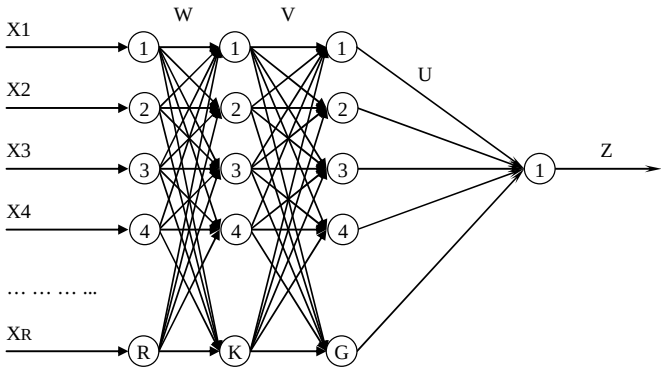

Рис. 5. *Структура нейронной сети встречного распространения*

5. Экспериментальные результаты. Для тестирования программы был использован в качестве контейнера Mp3 файл Eagles – Hotel California. Размер 3 365 407 байтов. В качестве секретного сообщения - документ MS Word размером 23 Кб. Секретный ключ - слово "Torch".

После построения таблицы соответствия и внедрения документа Word в звуковой файл, размер последнего не изменился. При этом:

- Количество нейронов распределительно слоя равнялось 10.
- Слой Кохонена содержал 10 нейронов.
- Слой Гроссберга 10 нейронов.
- В выходном слое использовался 1 нейрон, хотя можно было и без него.
- Размер сгенерированной таблицы соответствия равнялся 23552 байт.
- Размер обучающей выборки составлял 23562 байт.
- Количество параметров нейронной сети, характеризующих ее обученное функционирование (прогнозирование числового ряда) равнялось 224 (веса, пороги и шаги).
- Количество итераций, необходимых для достижения желаемой ошибки (0,001) варьировалось от 5 до 100 раз. Т.е. каждый элемент обучающей выборки необходимо было подать на каждый нейрон распределительного слоя от 5 до 100 раз в зависимости от начальной инициализации весовых коэффициентов и правила нормализации их значений.

Во время многократного прослушивания файла изменений не замечено. Разница, замеченная в HEX-редакторе, ни каким образом не похожа ни на размер внедренного сообщения, не тем более, на само секретное сообщение.

Основная проблема любого стеганографического метода заключается в стабильности стегокодированного звукового файла. Если пользователь, распределенная система передачи информации, линия связи или модем внесут искажения в передаваемый звуковой файл, то внедренная информация не должна быть утрачена. Нейронная сеть встречного распространения способна восстановить прогнозируемые элементы даже в случае не совсем достоверных параметров (входов, подаваемых на нейроны распределительно

слоя). Но все имеет свои пределы. Поэтому данный метод удобно использовать для файлов, не подверженных искажениям, т.е. использующимся в закрытых информационных средах.

Заключение. В данной работе был представлен новый метод нейросетевой стеганографии. Он объединяет нейронную сеть встречного распространения и LSB метод. Результаты эксперимента показали, что этот метод подходит для различных звуковых файлов и типов скрываемых сообщений.

Кроме того, этот метод имеет много возможностей для дальнейших усовершенствований, и может быть легко изменен, специально для других типов файлов и структур нейронных сетей.

Следующий шагом будет использование этого метода с незначительными модификациями для стеганографии, работающей в реальном масштабе времени.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. IBM Systems Journal, 35(3 & 4), 1996.
2. E. Franz, A. Jerichow, S. Moller, A. Pfitzmann, I. Stierand. Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, In Information hiding: first international workshop, Cambridge, UK. Lecture Notes in Computer Science, vol. 1174, Berlin Heidelberg New York: Springer-Verlag, 1996.
3. Головко В. А. Нейроинтеллект: теория и применение. Книга 2: самоорганизация, отказоустойчивость и применение нейронных сетей. – Брест: БПИ, 1999. - 228с.
4. Boseniuk T., van der Meer M., Poschel T. A Multiprocessor system for high speed simulation of neural networks // Journal of New Generation Computer Systems.-1990, № 3.-pp. 65-71.
5. А.И. Змитрович. Интеллектуальные информационные системы. – Минск: ТетраСистемс, 1997.

Материал поступил в редакцию 24.10.08

SHEVELENKOV V.V. Neural network approach for sound file steganography

The neural network approach for sound file steganography is presented. The most used methods and algorithms of inserting and decoding information is examined. Neural network technique and steganography method is realized. Research results are submitted.

УДК 004.421

Быков В.Л.

О РЕАЛИЗАЦИИ ОДНОГО ИЗ МЕТОДОВ ВЕКТОРНОЙ ОПТИМИЗАЦИИ В ЭЛЕКТРОННОЙ ТАБЛИЦЕ EXCEL

Введение. Вопрос принятия решения в условиях неопределенности при наличии множества факторов всегда был и остается сложной задачей. Здесь присутствуют как технические трудности связанные с формированием целевых функций, так и трудности связанные собственно с принятие решения в условиях неопределенности. Задачи подобного рода возникают при исследовании и проектировании больших систем. Это могут быть как технические системы, так и модели исследования экономических систем. Большой интерес к данной проблеме проявлялся в 80-е годы прошлого столетия, не ослабевает интерес к данной проблеме и в настоящее время как в академической, так и в студенческой среде. В настоящей статье приведено краткое описание одного из методов многокритериальной оптимизации и приведен пример реализации данного метода в электронной таблице Excel.

Краткие теоретические сведения. Известно достаточно много методов многокритериальной оптимизации, сводимых к созданию безразмерных взвешенных критериев и поиску оптимального варианта на множестве допустимых альтернатив по некоторому предпочтению лица принимающего решение [1-5]. Такие методы получили название векторная оптимизация. При решении задач данного вида всегда присутствует эвристический аспект. Он связан как с выбором самих целевых функций, так и с заданием вектора предпочтения на множестве целевых функций. Вектор предпочтения задается либо самим исследователем проектируемой системы, либо формируется с использованием экспертных оценок специалистов в соответствующей области знаний.

Суть рассматриваемого метода состоит в следующем [1, 2].

Пусть имеется система, которая описывается множеством целевых функций (критериев), одна часть из которых максимизируется, а другая часть минимизируется (обязательное условие для данного метода), а также имеется множество допустимых вариантов[1] построения такой системы

$$f = \{f_i(\alpha\} \quad \alpha \in A, i \in I, \quad I = \{1,...,M\},$$

где A – множество допустимых альтернатив, I – множество индексов, соответствующих совокупности целевых функций, с учетом которых осуществляется выбор выходных параметров в исследуемой ситуации принятия решения.

Вычисление значений целевых функций при различных значениях входных параметров позволяет определить эффективную альтернативу. Эффективной называют альтернативу α_0, если на множестве допустимых альтернатив A не существует такой альтернативы $\hat{\alpha}$, для которой выполнялись бы неравенства

$$f_i(\hat{\alpha}) \geq f_i(\alpha_0) \qquad \forall i \in I_1.$$

$$f_i(\hat{\alpha}) \leq f_i(\alpha_0) \qquad \forall i \in I_2$$

$$I_1 \in I, \quad I_2 \in I, \quad I_1 \cap I_2 = \varnothing, \quad I_1 \cup I_2 = I.$$

Здесь I_1 – подмножество максимизируемых целевых функций, I_2 - подмножество минимизируемых целевых функций. Если эффективная альтернатива единственная, то задачи выбора не возникает. При выборе входных параметров наилучшими могут быть только эффективные альтернативы, которые не сравнимы между собой по множеству функций цели в смысле отношения

$$\alpha_1 \succ= \alpha_2, \quad \text{когда} \quad \begin{cases} f_i(\alpha_1) \geq f_i(\alpha_2) & \forall i \in I_1 \\ f_i(\alpha_1) \leq f_i(\alpha_2) & \forall i \in I_2, \end{cases}$$

где $\succ=$ - отношение слабого предпочтения.

Для двух альтернатив α_1, $\alpha_2 \in A$ существует отношение слабого предпочтения, если $f_i(\alpha_1) \geq (\leq) f_i(\alpha_2)$, и строгого предпочтения, если $f_i(\alpha_1) > (<) f_i(\alpha_2)$. Альтернативы эквивалентны, если $f_i(\alpha_1) = f_i(\alpha_2)$.

Ввиду того, что целевые функции имеют, как правило, разную физическую размерность, то рекомендуется рассматривать не само множество функций цели *f*, а эквивалентное ему множество функций *w,* представляющих собой монотонные преобразования, приводящие функции цели к безразмерному виду и позволяющие сравнивать

***Быков Вячеслав Леонидович**, к.т.н., доцент кафедры информатики и прикладной математики Брестского государственного технического университета.*

Беларусь, БрГТУ, 224017, г. Брест, ул. Московская, 267.

[1] *Вопрос построения допустимых вариантов в рамках данной статьи не рассматривается*