УДК 621.395

ИССЛЕДОВАНИЕ ПОМЕХОУСТОЙЧИВОЙ И ЗАЩИЩЕННОЙ СИСТЕМЫ ПЕРЕДАЧИ РЕЧЕВЫХ СИГНАЛОВ НА ОСНОВЕ ПРЕДСТАВЛЕНИЯ ХУРГИНА – ЯКОВЛЕВА

В. Т. Дмитриев, к.т.н., доцент, заведующий кафедрой РУС РГРТУ, Рязань, Россия;
orcid.org/0000-0001-5521-6886, e-mail: vol77@rambler.ru
М. С. Смирнов, студент РГРТУ, Рязань, Россия;
orcid.org/0000-0003-0064-8379, e-mail: smirms@mail.ru

Приведено исследование качества восстановленной речи на выходе помехоустойчивых и защищенных систем передачи речевых сигналов на основе теоремы В.А. Котельникова и представления Хургина – Яковлева при действии различных помех в канале связи. Задачей исследования является определение наилучших сочетаний алгоритмов шифрования и первичного кодирования для достижения наилучшего качества восстановленной речевой информации на выходе первичного декодера при действии помех в канале связи, а также исследование применения представления В.А. Котельникова и представления Хургина – Яковлева при построении первичных кодеков. ***Целью работы*** *является выбор и обоснование алгоритмов первичного кодирования и шифрования помехоустойчивой и защищенной системы передачи речевых сигналов, которая обеспечивает наиболее высокое значение оценки качества речи на выходе системы передачи в заданном диапазоне скоростей передачи и действии помех в канале связи. В результате исследования осуществлен выбор наилучших сочетаний алгоритмов первичного кодирования и шифрования, а также обосновано применение представления Хургина – Яковлева с целью повышения качества восстановленной речи, а также помехоустойчивости и защищенности передаваемой информации на выходе системы передачи речевой информации.*

Ключевые слова: *помехоустойчивость, защищенность, криптографические алгоритмы, шифрование, первичное кодирование, передача речевых сигналов, кодеки речевых сигналов, представление Хургина – Яковлева.*

DOI: 10.21667/1995-4565-2022-82-27-37

Введение

В современных телекоммуникационных системах возрастают требования к защищённости и помехоустойчивости передаваемой информации, а также качеству речи на приемной стороне. Это обусловлено коммерческой ценностью передаваемой информации, так как большинство коммерческих переговоров сейчас производятся по телефону. Передаваемая речь обладает высокой информативностью, и условный перехват такой информации является нарушением безопасности и подразумевает под собой получение злоумышленником наиболее ценной информации. Одним из возможных решений повышения защищенности системы передачи при передаче речевого трафика является применение алгоритмов шифрования речевых сигналов (РС) с помощью наиболее распространенных криптографических алгоритмов, основанных на симметричном алгоритме DES или ассиметричном алгоритме RSA [1, 2]. В то же время применение алгоритмов шифрования приводит к дополнительному снижению качества восстановленной речи на приемной стороне при действии различных искажений в канале связи.

Работа посвящена исследованию известных защищенных систем передачи РС (СПРС) при совместном использовании алгоритмов шифрования и первичного кодирования, что обеспечивает анализ влияния на параметры СПРС каждого алгоритма и учет их параметров при разработке СПРС [2, 3]. Поэтому возникает необходимость в выборе алгоритмов первичного кодирования РС, а также шифрования для СПРС, обеспечивающих высокое качество восстановленной речи на выходе СПРС при высокой защищенности, обеспечиваемой за

счет применения алгоритма шифрования, и помехоустойчивости при действии различных возможных помех в канале связи. Исследование алгоритмов первичного кодирования и защиты целесообразно проводить при фиксированных параметрах и алгоритме модуляции чтобы обеспечить достоверность результатов.

Вызывает интерес в целях повышения качества восстановленной речи и помехоустойчивости системы передачи применение в помехоустойчивых и защищенных СПРС представления Хургина – Яковлева [4-6], которое рассматривает РС в виде прореженных отсчетов сигнала и его производной. Как показано в [7], возможно применение представления Хургина – Яковлева для увеличения защищенности передаваемой информации за счет перемешивания отсчетов сигнала и производной в общем канале. Построение первичных кодеков на основе представления Хургина – Яковлева обеспечивает дополнительное повышение качества восстановленной речи, а также увеличение помехоустойчивости за счет фазового сдвига между отсчетами сигнала и производной [8]. Поэтому необходимо провести сравнение защищенных СПРС, построенных на основе теоремы В.А. Котельникова и представления Хургина – Яковлева, при действии помех в канале связи.

Таким образом, **целью работы** является выбор и обоснование алгоритмов и параметров первичного кодирования и шифрования помехоустойчивой и защищенной системы передачи речевых сигналов, которая обеспечивает наиболее высокое значение оценки качества речи на выходе системы передачи в заданном диапазоне скоростей передачи и действии помех в канале связи, а также выбор представления РС на основе теоремы В.А. Котельникова и представления Хургина – Яковлева.

Постановка задачи

На рисунке 1 показана известная структурная схема защищенной СПРС на основе теоремы В.А. Котельникова для проведения экспериментальных исследований по выбору алгоритмов первичного кодирования, а также шифратора. Проведем исследование оценки качества восстановленной речи на выходе низкоскоростных (при скоростях передачи 1…2,4 кбит/с), среднескоростных (при скоростях передачи 4…8 кбит/с) и высокоскоростных (при скоростях передачи 16…64 кбит/с) первичных кодеков для известных алгоритмов шифрования.

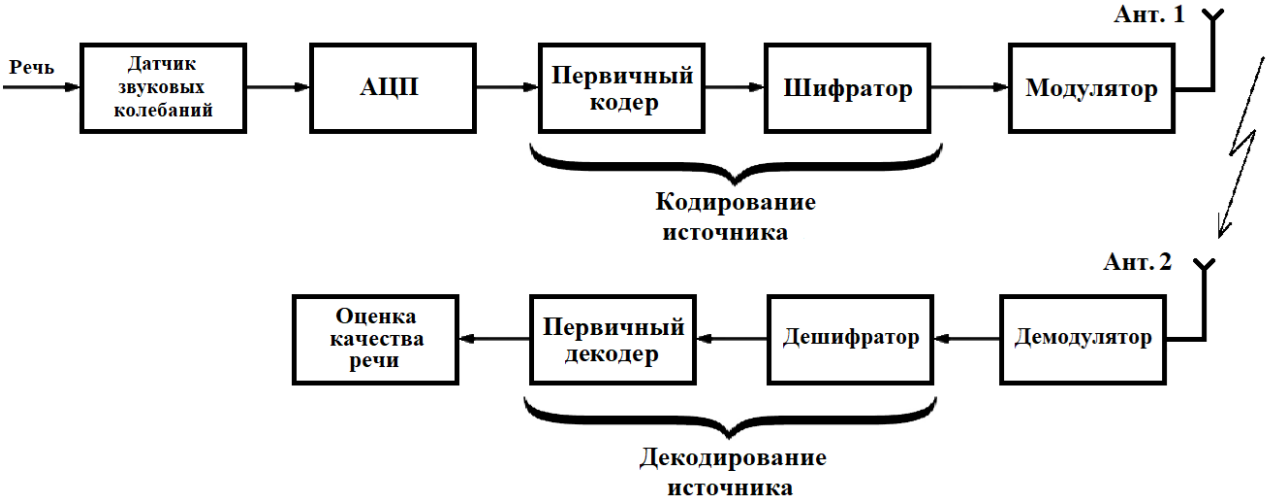

Рисунок 1 – Структурная схема защищенной системы передачи речевых сигналов
Figure 1 – Structural diagram of a secure voice transmission system

Исследование осуществляется путем математического моделирования СПРС, представленной на рисунке 1, в программе MATLAB. Приведенная структурная схема включает стандартные элементы, характерные для цифровых СПРС: датчик звуковых колебаний, в качестве которого выступает микрофон, аналого-цифровой преобразователь (АЦП), первичный кодер, шифратор, модулятор и антенну. На приемной стороне соответственно: демодулятор,

дешифратор, первичный декодер, а также блок объективной оценки качества речи. Так как целью исследований являлось исследование помех на сигнал с выхода первичного кодера и шифратора. Влияния помехоустойчивого кодера для системы не рассматривалось. В качестве критерия эффективности СПРС используется оценка качества речи на выходе первичного декодера, которая производилась при действии различных помех и искажений в канале связи. Для оценки качества РС при проведении экспериментальных исследований использовалась шкала MOS-LQO и алгоритм оценки качества речи PESQ [9]. Показанная на рисунке 1 структурная схема позволяет провести анализ различных алгоритмов первичного кодирования и шифрования и выбрать сочетание алгоритмов, обеспечивающих наилучшие оценки качества речи.

Целью экспериментальных исследований является определение сочетаний алгоритмов первичного кодирования на основе теоремы В.А. Котельникова и представления Хургина – Яковлева и наиболее распространённых алгоритмов шифрования, которые при действии различных помех в канале связи обеспечивают наилучшее качество восстановленной речи на приемной стороне.

Описание эксперимента

В качестве критерия оценки воздействия помех и искажений в канале связи на СПРС для различных алгоритмов первичного кодирования и шифрования, а также представлений РС на основе теоремы В.А. Котельникова и представления Хургина – Яковлева, использовалась оценка качества восстановленной речи на приемной стороне. При проведении экспериментальных исследований использовалось усредненное значение оценки качества речевых образцов по 10 испытаниям, заранее записанным аудиофайлам формата «.wav», согласно рекомендациям МСЭ-Т P.800.1 [9]. Для записи аудиофайлов использовался профессиональный диктофон *OlimpusLS-10 (Linear PCM recorder)*, обеспечивающий возможность записи РС в формате «.wav» со следующими параметрами: частота дискретизации – 44,1 кГц; разрядность квантования – 16 бит; тип кодирования ИКМ.

Диктофон устанавливался на расстоянии 0,5 м перед диктором на уровне лица. Записанные на диктофон РС конвертировались программным конвертором при помощи программы редактирования аудиофайлов *Cool Edit Pro 2.0*. Аудиофайл формата «.wav» выравнивался по амплитуде; затем полосовым фильтром выделялась речь в диапазоне частот 0,3 – 3,4 кГц и сохранялся образец речи с частотой дискретизации ($f_д$), равной 8000 кГц, в формате аудио – *Mono*, с разрядностью квантования 16 бит.

С помощью программы *SpeechPro VoceDEMO* исходный РС пропускался через первичный кодек. Всего в работе рассмотрено три основные группы кодеков: низкоскоростные, среднескоростные и высокоскоростные. В качестве алгоритмов первичного кодирования рассматриваются низкоскоростные алгоритмы (MMBE со скоростями передачи 1,2 кбит/с и 2,4 кбит/с; RMMBE со скоростью передачи 2,4 кбит/с; LBRAMR со скоростями передачи 1 кбит/с, 1,2 кбит/с, 2 кбит/с, 2,4 кбит/с), среднескоростные алгоритмы (ICELP со скоростями передачи 4,8 кбит/с, 6 кбит/с, 8 кбит/с; G.723.1 со скоростями передачи 5,3 кбит/с и 6,3 кбит/с; G729a со скоростью передачи 8 кбит/с), высокоскоростные алгоритмы (G.722 со скоростями передачи 48 кбит/с, 56 кбит/с, 64 кбит/с; G.726 со скоростями передачи 16 кбит/с, 24 кбит/с, 32 кбит/с, 40 кбит/с, а также G.728i со скоростью передачи 16 кбит/с).

В качестве методов шифрования рассмотрено два алгоритма, которые положены в основу большинства современных криптографических алгоритмов: DES и RSA. Данные алгоритмы, как и их модификации нашли широкое распространение в защищенных системах связи и обладают различными характеристиками и криптостойкостью (10^{23} у RSA по сравнению с $7*10^{16}$ у DES). После преобразований в шифраторе зашифрованный сигнал поступает на модулятор, в котором используется метод частотной манипуляции сигнала FSK.

Затем происходила имитация канала связи, в котором сигнал с выхода модулятора смешивался с одной из помех. В работе рассмотрены три основных вида помех. Узкополосная

(сосредоточенная) помеха представляет собой случайный гауссовский процесс с равномерной спектральной плотностью мощности в действительной и комплексной областях. Широкополосная (импульсная) помеха – одиночный импульс высокой мощности длительностью во много раз меньше, чем длительность полезного сигнала. Структурная помеха – сигнал с таким же видом манипуляции, как и у полезного сигнала, но отличный по переносимому сообщению и со сдвигом по фазе. Вероятности ошибки символов p_e рассчитывались на входе первичного декодера на основе сравнения искаженного и неискаженного сигналов.

Далее, сигнал поступал на приемную сторону, где происходила демодуляция сигнала, после чего, поступал на блок оценки качества речи. Для получения объективной оценки качества РС производились экспериментальные исследования с помощью специального алгоритма автоматизированной оценки качества принимаемой речи *PESQ* (указанного в рекомендациях МСЭ-Т Р.800.1 [9]), в котором осуществлялась объективная оценка качества восстановленной речи по пятибалльной шкале. Полученные оценки качества РС приведены по шкале MOS-LQO (PESQ) [9].

Для защищенной СПРС, структурная схема которой показана на рисунке 2, проводились аналогичные исследования.

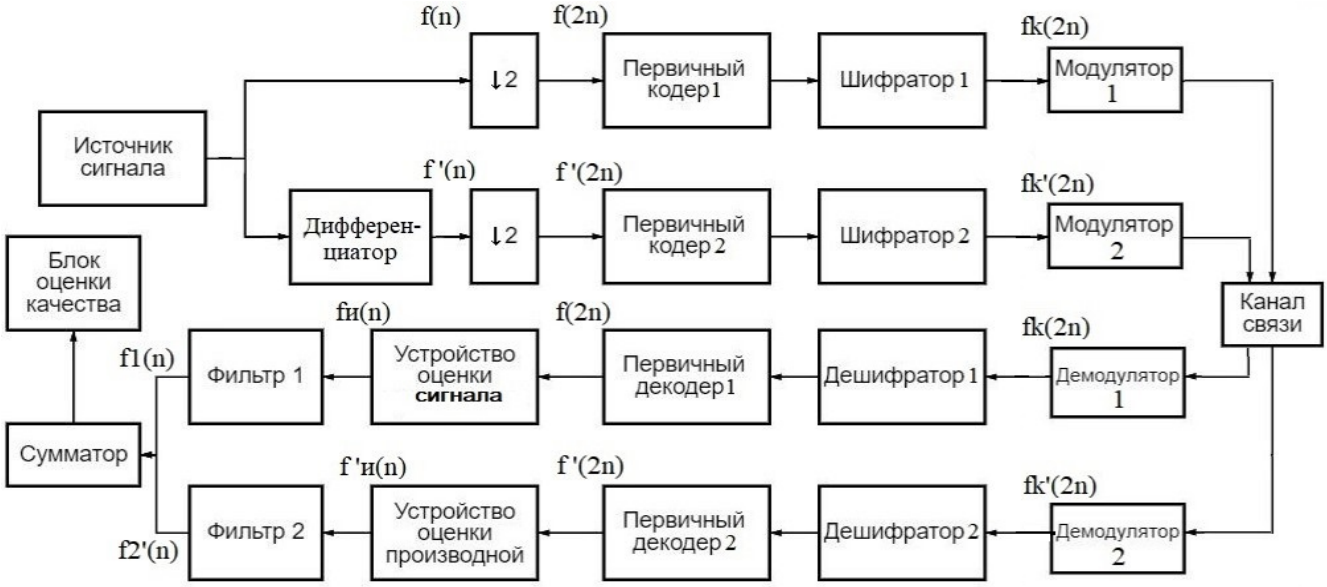

Рисунок 2 – Структурная схема защищенной системы передачи речевых сигналов для экспериментальных исследований на основе представления Хургина – Яковлева
Figure 2 – Structural diagram of a secure voice signal transmission system for experimental studies based on Khurgin – Yakovlev representation

В ходе экспериментальных исследований помехоустойчивой и защищенной СПРС на основе представления Хургина – Яковлева осуществлялась дискретизация исходного РС с частотой дискретизации, определенной в соответствии с теоремой В.А. Котельникова. Затем отсчеты дискретизированного РС поступали на дифференциатор, где происходило получение отсчетов производной. Далее полученные дискретные отсчеты сигнала и производной поступали в дециматор (↓2), где происходил отброс каждого второго отсчета сигнала и производной для сохранения общего объема передаваемой информации [6].

Затем отсчеты сигнала и производной проходили через первичный кодер, шифратор и далее в канал связи. Искаженные в канале связи кодированные отсчеты сигнала и производной поступали в приемник. После демодуляции и всех этапов декодирования отсчеты сигнала и производной поступал на интерполяторы, где происходила вставка между соседними отсчетами входного сигнала нулевых отсчетов. Затем, отсчеты сигнала и производной поступали на синтезирующие фильтры (фильтр 1 и фильтр 2) и далее на сумматор, на выходе которого были получены отсчеты восстановленного РС [6].

Экспериментальные исследования

Проведены экспериментальные исследования влияния известных первичных кодеков на основе теоремы В.А. Котельникова и представления Хургина – Яковлева на качество восстановленной речи при действии различных помех в канале связи для структурной схемы СПРС на основе теоремы В.А. Котельникова, представленной на рисунке 1. По совокупности исследуемых помех и кодеков, обеспечивающих наилучшие оценки качества РС, полученные данные сведены в таблицу 1. Более подробно оценки качества восстановленной речи на выходе систем передачи при действии ошибок в канале связи для различных низкоскоростных кодеков представлены в [10].

В таблице 1 приведены первичные кодеки, обеспечивающие лучшие показатели качества восстановленной речи, для низкоскоростных первичных кодеков – алгоритм RMMBE 2,4 кбит/с, для среднескоростных – алгоритм G.729a 8 кбит/с и высокоскоростных первичных кодеков – G.722 56 кбит/с. Также приведены оценки качества восстановленной речи при вероятности ошибки p_e = 0,5 % согласно оценке MOS-LQO (PESQ).

Таблица 1 – Алгоритмы первичного кодирования, обеспечивающие максимальную оценку качества восстановленной речи

Table 1 – Primary coding algorithms providing maximum estimate of the reconstructed speech quality

Группа кодеков	Форма эксперимента			
	Алгоритм шифрования DES	Алгоритм шифрования DES + алгоритм Хургина – Яковлева	Алгоритм шифрования RSA	Алгоритм шифрования RSA + алгоритм Хургина – Яковлева
Низкоскоростные	RMMBE 2,4 кбит/с. K=2,2 балла	RMMBE 2,4 кбит/с. K=2,6 балла	RMMBE 2,4 кбит/с. K=2,1 балла	RMMBE 2,4 кбит/с. K=2,33 балла
Среднескоростные	G.729a 8 кбит/с. K= 2,46 баллов	G.729a 8 кбит/с. K=2,96 балла	G.729a 8 кбит/с. K= 2,35 балла	G.729a 8 кбит/с. K=2,65 балла
Высокоскоростные	G.722 56 кбит/с. K= 3,19 баллов	G.722 56 кбит/с. K=3,64 балла	G.722 64 кбит/с. K=3,05 балла	G.722 64 кбит/с. K=3,26 балла

В результате экспериментальных исследований проведена оценка влияния первичных кодеков РС, алгоритмов симметричного и ассиметричного шифрования DES и RSA, а также представления Хургина – Яковлева и теоремы В.А. Котельникова на качество восстановленной речи на выходе исследуемых СПРС при действии различных помех в канале связи.

С учетом полученных экспериментальных данных, приведенных в таблице 1, наибольший интерес с точки зрения дальнейшего исследования представляют кодеки, обеспечивающие наилучшее качество восстановленной речи в своем классе: низкоскоростной кодек RMMBE со скоростью 2,4 кбит/с, среднескоростной – G.729a со скоростью 8 кбит/с, а среди высокоскоростных – кодеки G.722 со скоростью 56 кбит/с и G.722 со скоростью 64 кбит/с.

Для выбранных алгоритмов первичного кодирования, обеспечивающих максимальное качество восстановленной речи, приведенных в таблице 1, проведем сравнение оценки качества восстановленной речи для выбранных первичных на основе теоремы В.А. Котельникова и представления Хургина – Яковлева.

Исследование влияния алгоритма Хургина – Яковлева на качество речевого сигнала для низкоскоростных кодеков при действии различных помех в канале связи

На рисунке 3 приведены зависимости выигрыша оценки качества речи при использовании представления Хургина – Яковлева, относительно теоремы В.А. Котельникова (ΔK) на выходе декодера в помехоустойчивой и защищенной СПРС, от вероятности ошибки в канале связи (p_e) для низкоскоростных кодеков (НСК) с учетом алгоритмов RSA и DES. Значения качества речи получены при вероятности ошибки в канале связи в пределах 0,1…5 %. Так как в ходе проведенных исследований, результаты которых приведены в таблице 1, наилучшее качество вос-

становленной речи среди НСК обеспечивает кодек RMMBE со скоростью передачи 2,4 кбит/с, дальнейшие исследования НСК проводились для данного кодека.

Под цифрой *1* приведены зависимости при использовании алгоритма шифрования DES низкоскоростного алгоритма первичного кодирования RMMBE со скоростью передачи 2,4 кбит/с (при использовании представления Хургина – Яковлева); под цифрой *2* – зависимости при использовании алгоритма первичного кодирования RMMBE со скоростью передачи 2,4 кбит/с (при использовании алгоритма шифрования RSA и представления Хургина – Яковлева).

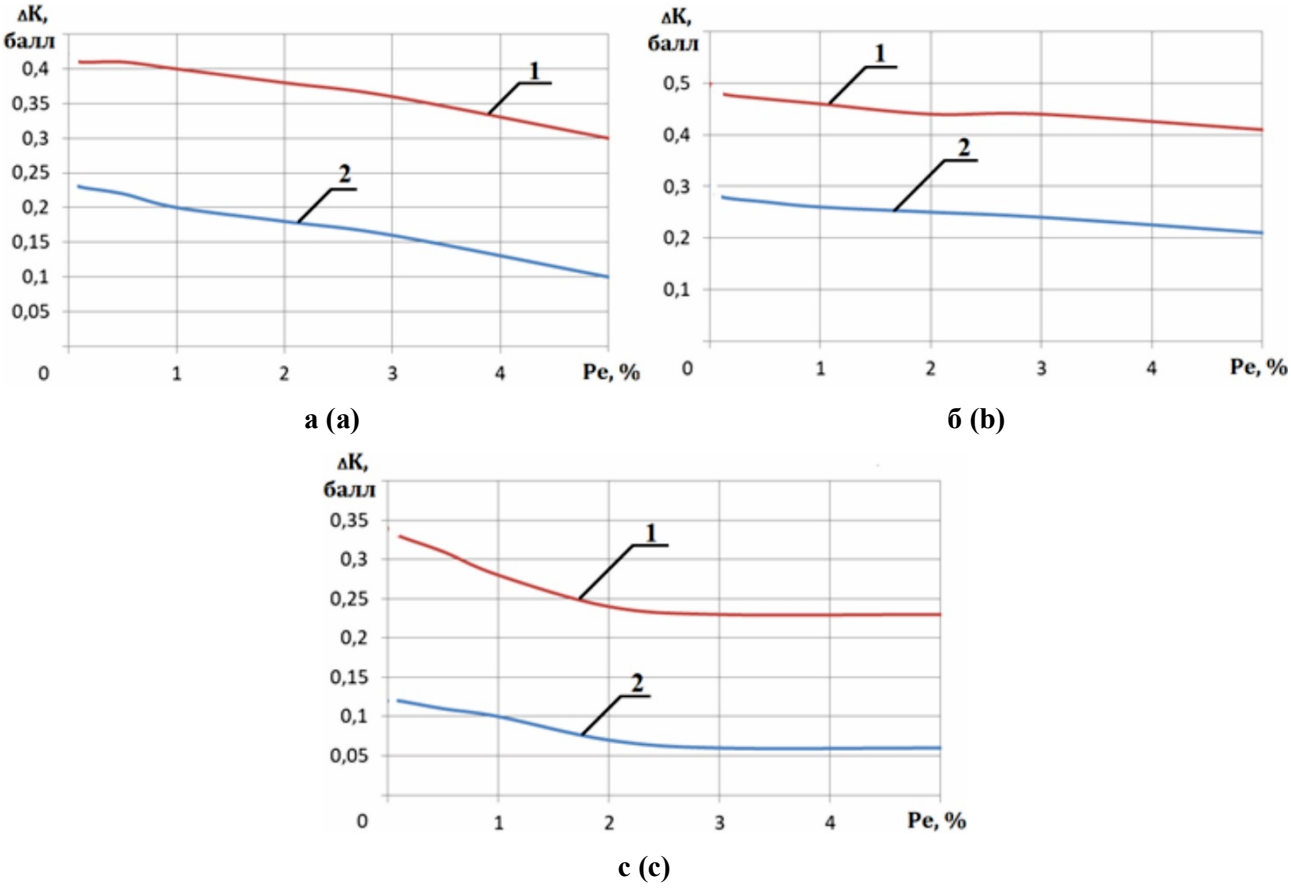

Рисунок 3 – Выигрыш качества восстановленной речи при использовании представления Хургина-Яковлева, относительно теоремы В.А. Котельникова для низкоскоростных кодеков при действии широкополосной помехи (а), узкополосной помехи (б), структурной помехи (в)
Figure 3 – Gain in the reconstructed speech quality when using Khurgin – Yakovlev representation, relative to V.A. Kotelnikov for low-speed codecs under the action of broadband interference (a), narrow-band interfer-ence (b), structural interference (c)

Из полученных зависимостей следует, что наилучшее качество восстановленной речи для НСК RMMBE со скоростью передачи 2,4 кбит/с обеспечивает использование алгоритма шифрования DES, а также применение на входе первичного кодека представления Хургина – Яковлева, которое позволяет улучшить качество восстановленного РС на 0,2…0,3 балла согласно шкалы MOS-LQO (PESQ) при скорости передачи 2,4 кбит/с, по сравнению с аналогичной СПРС на основе теоремы В.А. Котельникова.

Лучшее качество восстановленной речи при использовании алгоритма DES можно объяснить меньшим размером блока – 64 бита по сравнению с 1024 битами у алгоритма RSA, что приводит к большему поражению отдельных блоков при одинаковой вероятности ошибок в канале связи. Выигрыш для систем на основе представления Хургина – Яковлева объясняется частичной возможностью восстановления информации за счет отсчетов сигнала и производной и фазовым сдвигом между отсчетами [8].

Исследование влияния алгоритма Хургина – Яковлева на качество речевого сигнала для среднескоростных кодеков при действии различных помех в канале связи

На рисунке 4 приведены зависимости выигрыша оценки качества восстановленной речи на выходе первичного декодера в помехоустойчивой и защищенной СПРС при использовании представления Хургина-Яковлева относительно теоремы В.А. Котельникова (ΔК), от вероятности ошибки в канале связи (p_e) для среднескоростных кодеков (ССК) для алгоритмов RSA и DES. Значения получены при вероятности ошибки в канале связи в пределах 0,1… 5 %.

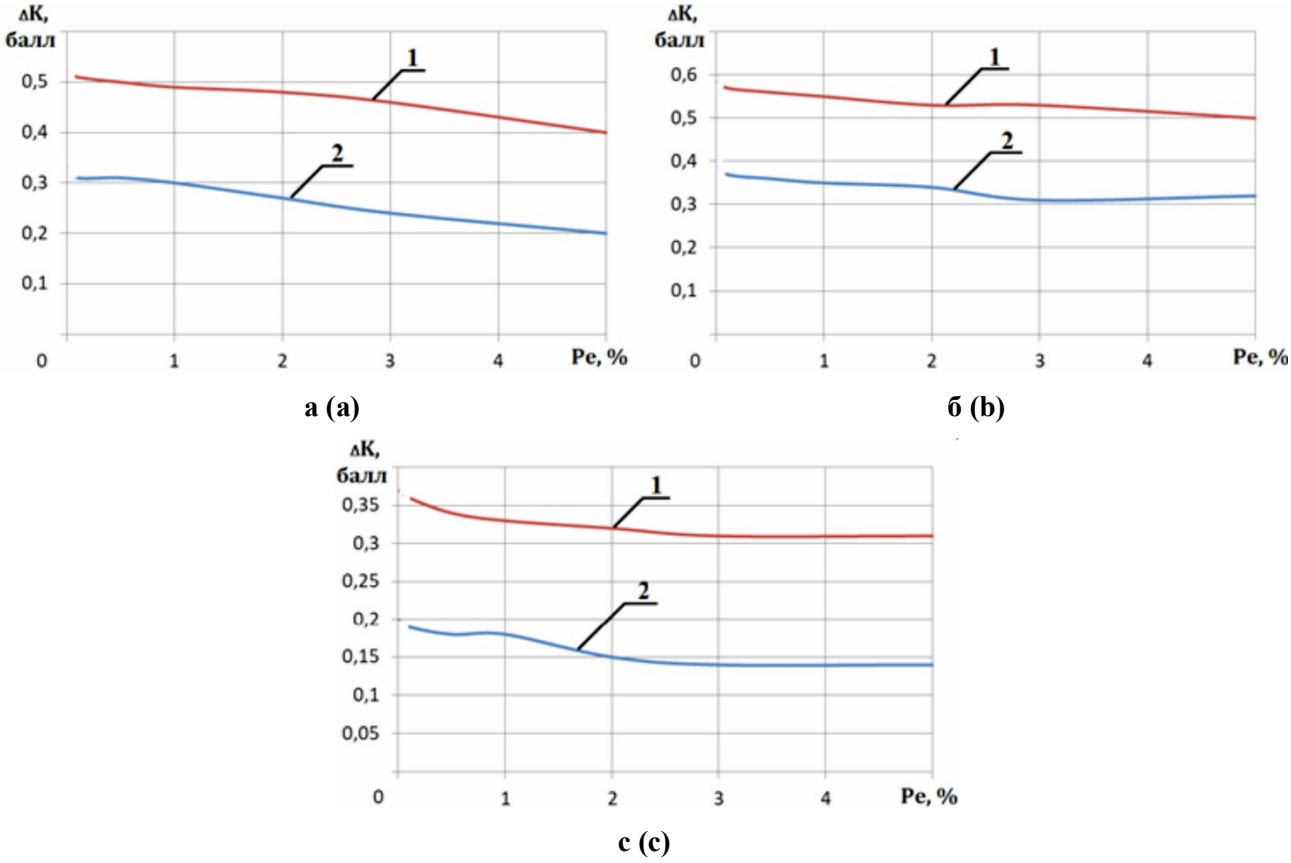

Рисунок 4 – Выигрыш качества восстановленной речи при использовании представления Хургина – Яковлева, относительно теоремы В. А. Котельникова для среднескоростных кодеков при действии широкополосной помехи (а), узкополосной помехи (б), структурной помехи (в)
Figure 4 – Gain in the reconstructed speech quality when using Khurgin – Yakovlev representation, relative to V.A. Kotelnikov for medium-speed codecs under the action of broadband interference (a), narrow-band in-terference (b), structural interference (c)

Так как, в ходе проведенных исследований, результаты которых приведены в таблице 1, наилучшее качество восстановленной речи среди ССК обеспечивает кодек G.729a со скоростью передачи 8 кбит/с, дальнейшие исследования ССК проводились для данного кодека.

Под цифрой *1* приведены зависимости для ССК G.729a со скоростью передачи 8 кбит/с (с учетом алгоритма шифрования DES и на основе представления Хургина-Яковлева); под цифрой *2* приведены зависимости при использовании алгоритма первичного кодирования G.729a со скоростью 8 кбит/с (с учетом алгоритма шифрования RSA и на основе представления Хургина – Яковлева).

С учетом приведенных на рисунке 4 зависимостей выигрыша качества восстановленной речи наилучшее качество восстановленной речи обеспечивает среднескоростной кодек G.729a со скоростью передачи 8 кбит/с, с учетом алгоритма шифрования DES, на основе представления Хургина – Яковлева, которое позволяет увеличить качество восстановленного

сигнала на 0,2…0,3 балла согласно шкале MOS-LQO (PESQ) при скорости передачи 8 кбит/с по сравнению с аналогичной СПРС на основе теоремы В.А. Котельникова.

Исследование влияния алгоритма Хургина – Яковлева на качество речевого сигнала для высокоскоростных кодеков при действии различных помех в канале связи

На рисунке 5 приведены зависимости выигрыша качества речи при использовании представления Хургина – Яковлева, относительно теоремы В. А. Котельникова (ΔК) в помехоустойчивой и защищенной СПРС, от вероятности ошибки в канале связи (p_e) для высокоскоростных кодеков (ВСК) для алгоритмов RSA и DES.

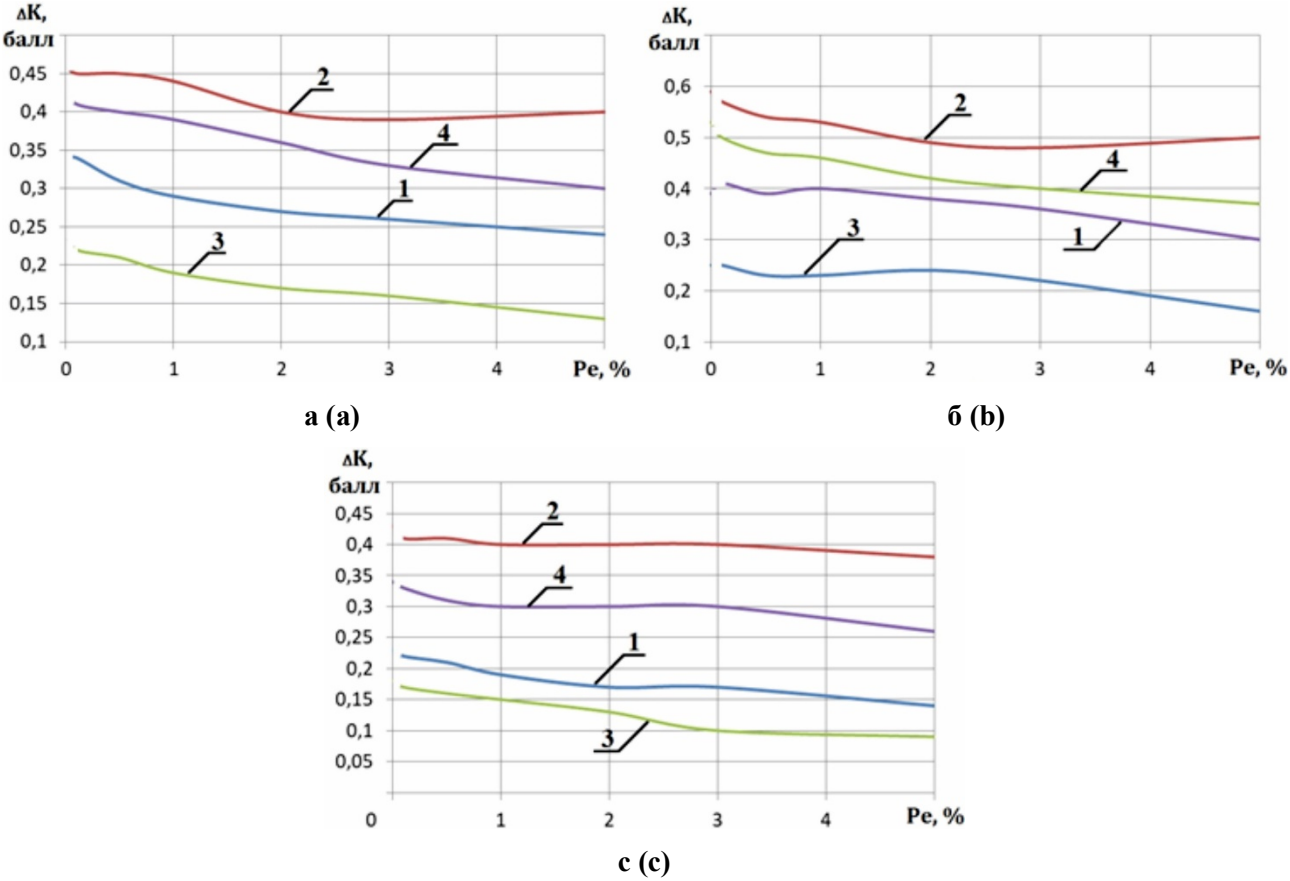

Рисунок 5 – Выигрыш качества восстановленной речи при использовании представления Хургина – Яковлева относительно теоремы В.А. Котельникова для высокоскоростных кодеков при действии широкополосной помехи (а), узкополосной помехи (б) и структурной помехи (в)
Figure 5 – Gain in the reconstructed speech quality when using the Khurgin – Yakovlev representation, relative to V.A. Kotelnikov for high-speed codecs under the action of broadband interference (a), narrow-band interference (b) and structural interference (c)

Значения получены при вероятности ошибки в канале связи в пределах 0,1… 5 %.

Так как, в ходе проведенных исследований, результаты которых приведены в таблице 1, наилучшее качество восстановленной речи среди ВСК обеспечивает кодек G.722 со скоростью 56 кбит/с, дальнейшие исследования ВСК следует проводить для данного кодека.

Под цифрой *1* приведены зависимости для ВСК G.722 со скоростью 56 кбит/с (с учетом алгоритма шифрования RSA и на основе представления Хургина – Яковлева); под цифрой *2* – зависимости при использовании алгоритма первичного кодирования G.722 со скоростью 56 кбит/с (с учетом алгоритма шифрования DES и на основе представления Хургина – Яковлева); под цифрой *3* – зависимости при использовании алгоритма первичного кодирования G.722 со скоростью 64 кбит/с (с учетом алгоритма шифрования RSA и на основе представления Хургина – Яковлева); под цифрой *4* – зависимости при использовании алгоритма пер-

вичного кодирования G.722 со скоростью 64 кбит/с (с учетом алгоритма шифрования DES и на основе представления Хургина – Яковлева).

С учетом приведенных на рисунке 5 графиков зависимостей, наилучшее качество восстановленной речи на приеме для высокоскоростных кодеков обеспечит применение в защищенных СПРС кодека G.722 со скоростью 56 кбит/с и алгоритма шифрования DES, а также на основе представления Хургина-Яковлева, которое позволяет увеличить качество восстановленного сигнала на 0,2…0,3 балла согласно MOS-LQO (PESQ) при скорости передачи 56 кбит/с, по сравнению с аналогичной СПРС на основе теоремы В. А. Котельникова.

Выводы по результатам экспериментальных исследований

С учетом результатов экспериментальных исследований осуществлён выбор алгоритмов первичного кодирования (НСК, ССК, ВСК), обеспечивающих максимально возможное качество восстановленной речи при использовании рассмотренных алгоритмов шифрования, обеспечивающих приемлемые значения качества восстановленной речи, помехоустойчивости и защищенности передаваемой информации при действии помех в канале связи. Полученные результаты сведены в таблицу 2.

Таблица 2 – Выбор алгоритмов на основе результатов экспериментальных исследований
Table 2 – Selection of the algorithms based on the results of experimental studies

Группа кодеков	Название кодека	Алгоритм шифрования	Применение алгоритма Хургина – Яковлева
Низкоскоростные	RMMBE 2.4 кбит/с	DES	Применяется
Среднескоростные	G.729a 8 кбит/с	DES	Применяется
Высокоскоростные	G.722 56 кбит/с	DES	Применяется

Заключение

В данной работе осуществлен выбор первичных кодеков, а также алгоритма защиты информации для СПРС, которая обеспечивает наилучшие показатели качества речи по проведенным экспериментальным исследованиям, при высоких показателях помехоустойчивости и защищенности.

Проведены исследования для НСК, ССК, ВСК для защищенных СПРС. Исследования проводились на основе представления Хургина – Яковлева и теоремы В.А. Котельникова. Показано, что применение симметричного криптографического алгоритма DES обеспечивает в среднем выигрыш качества восстановленной речи на приемной стороне на 0,2…0,3 балла согласно шкале MOS-LQO (PESQ) по сравнению с ассиметричным алгоритмом RSA. В то же время алгоритм RSA обеспечивает гораздо большую помехоустойчивость (10^{23} у RSA по сравнению с $7*10^{16}$ у DES), что подчеркивает необходимость использования адаптивных систем передачи.

Дополнительный выигрыш по помехоустойчивости для защищенных СПРС обеспечивает применение алгоритма Хургина – Яковлева, что дает согласно MOS-LQO (PESQ) выигрыш в качестве восстановленной речи относительно аналогичных СПРС на основе теоремы В. А. Котельникова в 0,2…0,3 балла. При вероятности ошибки $p_e = 0{,}5$ %, согласно оценке MOS-LQO (PESQ), наилучшие оценки качества восстановленной речи на приеме обеспечивают следующие первичные кодеки:

– для НСК – Spirit RMMBE при скорости передачи 2,4 кбит/с – 2-й класс качества речи (среднее значение качества восстановленной речи K = 2,6 балла согласно MOS-LQO (PESQ));

– для ССК – ITU G.729a при скорости передачи 8 кбит/с – 2-й класс качества речи (среднее значение качества восстановленной речи K = 2,96 балла согласно MOS-LQO (PESQ));

– для ВСК – ITU G.722 при скорости передачи 56 кбит/с – 1-й класс качества речи (ср. знач. K = 3,64 балла согласно MOS-LQO (PESQ)).

Таким образом, осуществлен выбор алгоритмов первичного кодирования и криптографического алгоритма DES для различных первичных кодеков РС при действии ошибок в канале

связи для защищенных СПРС. Также обосновано применение представления Хургина – Яковлева, обеспечивающее улучшение качества восстановленной речи в защищенной СПРС на 0,2…0,3 балла согласно MOS-LQO (PESQ).

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-07-00783.

Библиографический список

1. **Сердюков П. Н., Бельчиков А. В., Дронов А. В.** Защищенные радиосистемы цифровой передачи информации. М.: АСТ. 2006. 403 с.

2. **Банков Е. А.** Влияние криптопреобразований по ГОСТ Р 28147-89 на субъективное качество речи в системе радиосвязи // Фундаментальные проблемы радиоэлектронного приборостроения. 2009. Том 9. № 4. С. 178-181.

3. **Леонович Г. И., Логвинов Л. М**. Космические и наземные системы радиосвязи и сети телерадиовещания. Самара: изд-во Самарского научного центр РАН. 2008. С. 48-62.

4. **Хургин Я. И., Яковлев В. П.** Методы теории целых функций в радиофизике, теории связи и оптике. М.: Государственное издательство физико-математической литературы, 1962. 220 с.

5. **Хургин Я. И., Яковлев В. П.** Финитные функции в физике и технике. М.: Наука, 1971. 408 с.

6. **Кириллов С. Н., Дмитриев В. Т.** Реализационные возможности и помехоустойчивость процедуры восстановления сигналов на основе алгоритма Хургина-Яковлева // Радиотехника. 2003. № 1. С. 73-75.

7. **Кириллов С. Н., Дмитриев В. Т.** Асинхронное маскирование речи на основе алгоритма Хургина-Яковлева / Новые информационные технологии. 2004. № 1. С.46-48.

8. **Дмитриев В. Т.** Помехоустойчивость кодеков речи на основе алгоритма Хургина-Яковлева // Вестник Рязанского государственного радиотехнического университета. 2003. № 12. С.133-136.

9. Рекомендация МСЭ-Т P.800.1 (07/2006) [Электронный ресурс] / URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8860&lang=en (Дата обращения: 29.12.2021).

10. **Kirillov S. N. Dmitriev V. T.** Algorithm to Control Primary Codec Under the Influence of Interference in Communication Channel. International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA) DOI (CrossRef): 10.1109/SUMMA53307.2021.9632238.

UDK 621.395

STUDY OF NOISE-RESISTANT AND PROTECTED SPEECH SIGNAL TRANSMISSION SYSTEM BASED ON KHURGIN – YAKOVLEV REPRE-SENTATION

V. T. Dmitriev, Ph.D. (Tech.), head of department, RSREU, Ryazan, Russia;
orcid.org/0000-0001-5521-6886, e-mail: vol77@rambler.ru
M. S. Smirnov, student RSREU, Ryazan, Russia;
orcid.org/0000-0003-0064-8379, e-mail: smirms@mail.ru

The research of reconstructed speech quality at the output of noise-immune and protected speech signal transmission systems based on V.A. Kotelnikov theorem and Khurgin – Yakovlev representation under the action of various interferences in a communication channel is made. The task of the study is to determine the best combinations of encryption and primary coding algorithms to achieve the best quality of restored speech information at the output of primary decoder under the influence of interference in a communication channel, as well as to study the application of V.A. Kotelnikov and Khurgin – Yakovlev representations in the construction of primary codecs. ***The aim of the work*** *is to select and justify the algorithms for primary coding and encryption of noise-resistant and protected system for transmitting speech signals, which provides the highest value for assessing the quality of speech at the output of transmission system in a given range of transmission rates and interference in a communication channel. As a result of study, the best combinations of primary coding and encryption algorithms were selected, and the use of Khurgin – Yakovlev representa-*

tion was substantiated in order to improve restored speech quality, as well as noise immunity and security of transmitted information at the output of speech information transmission system.

Keywords: *noise immunity, security, noise-correcting coding algorithms, cryptographic algorithms for symmetric and asymmetric encryption, primary coding, speech signal transmission, speech signal codecs.*

DOI: 10.21667/1995-4565-2022-82-27-37

References

1. **Serdyukov P. N., Belchikov A. V., Dronov A. V.** *Zashchishchennye radiosistemy cifrovoj peredachi informacii* (Protected radio systems for digital transmission of information). Moscow: AST. 2006. 403 p. (in Russian).

2. **Bankov E. A.** Vliyanie kriptopreobrazovanij po GOST R 28147-89 na sub"ektivnoe kachestvo rechi v sisteme radiosvyazi. *Fundamental'nye problemy radioelektronnogo priborostroeniya*. 2009, vol. 9, no. 4, pp. 178-181. (in Russian).

3. **Leonovich G. I., Logvinov L. M.** *Kosmicheskie i nazemnye sistemy radiosvyazi i seti teleradioveshchaniya*. (Space and terrestrial radio communication systems and television and radio broadcasting networks). Samara: izd-vo Samarskogo nauchnogo centr RAN. 2008, pp. 48-62. (in Russian).

4. **Khurgin Ya. I., Yakovlev V. P.** Metody teorii celyh funkcij v radiofizike, teorii svyazi i optike (Methods of the theory of entire functions in radiophysics, communication theory and optics). Moscow: State publishing house of physical and mathematical literature. 1962, 220 p. (in Russian).

5. **Khurgin Ya. I., Yakovlev V. P.** Finitnye funkcii v fizike i tekhnike (Finite functions in physics and technology). Moscow: Nauka, 1971. 408 p. (in Russian).

6. **Kirillov S. N., Dmitriev V. T.** Realizacionnye vozmozhnosti i pomekhoustojchivost' procedury vosstanovleniya signalov na osnove algoritma Hurgina-Yakovleva. *Radiotekhnika*. 2003, no. 1, pp. 73-75. (in Russian).

7. **Kirillov S. N., Dmitriev V. T.** Asinhronnoe maskirovanie rechi na osnove algoritma Hurgina-Yakovleva. *Novye informacionnye tekhnologii*. 2004, no. 1, pp.46-48. (in Russian).

8. **Dmitriev V. T.** Pomekhoustojchivost' kodekov rechi na osnove algoritma Hurgina-Yakovleva. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta*. 2003, vol. 12, pp. 133-136. (in Russian).

9. Rekomendaciya MSE-T P.800.1 (07/2006) [Elektronnyj resurs] / URL: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=8860&lang=en (Data obrashcheniya: 29.12.2021).

10. **Kirillov S. N. Dmitriev V. T.** Algorithm to Control Primary Codec Under the Influence of Interference in Communication Channel. *International Conference on Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA)* DOI (CrossRef): 10.1109/SUMMA53307.2021.9632238.