Кафедра радиотехники МФТИ

Проект 3969

«Разработка теории и универсальных методов обработки и защиты информации для каналов с множественными источниками помех»

Научный руководитель
Габидулин Э.М.

- **Мероприятие № 2 «Проведение фундаментальных исследований в области естественных, технических и гуманитарных наук. Научно-методическое обеспечение развития инфраструктуры вузовской науки».**

- **Раздел № 2.1 «Проведение фундаментальных исследований в области естественных, технических и гуманитарных наук».**

- **Подраздел № 2.1.2 «Проведение фундаментальных исследований в области технических наук».**

- **Проект 3969: «Разработка теории и универсальных методов обработки и защиты информации для каналов с множественными источниками помех».**

План работ на 1 этапе 2006

- **Выбор и анализ модели канала с множественными источниками помех.**
- **Выбор методов кодирования и разработка методов декодирования для борьбы с множественными помехами.**

Кафедра радиотехники МФТИ

План работ на 2 этапе 2006

- **Выбор методов кодирования и разработка методов декодирования для борьбы с множественными помехами.**
- **Разработка методов сопряжения исправления ошибок и защиты от несанкционированного доступа.**

Кафедра радиотехники МФТИ

План работ на 3 этапе 2007

- **Исследование характеристик выбранных методов обработки и защиты информации.**

- **Моделирование избранных вариантов передачи по каналам с множественными помехами.**

Кафедра радиотехники МФТИ

План работ на 4 этапе 2007

- **Моделирование избранных вариантов передачи по каналам с множественными помехами.**

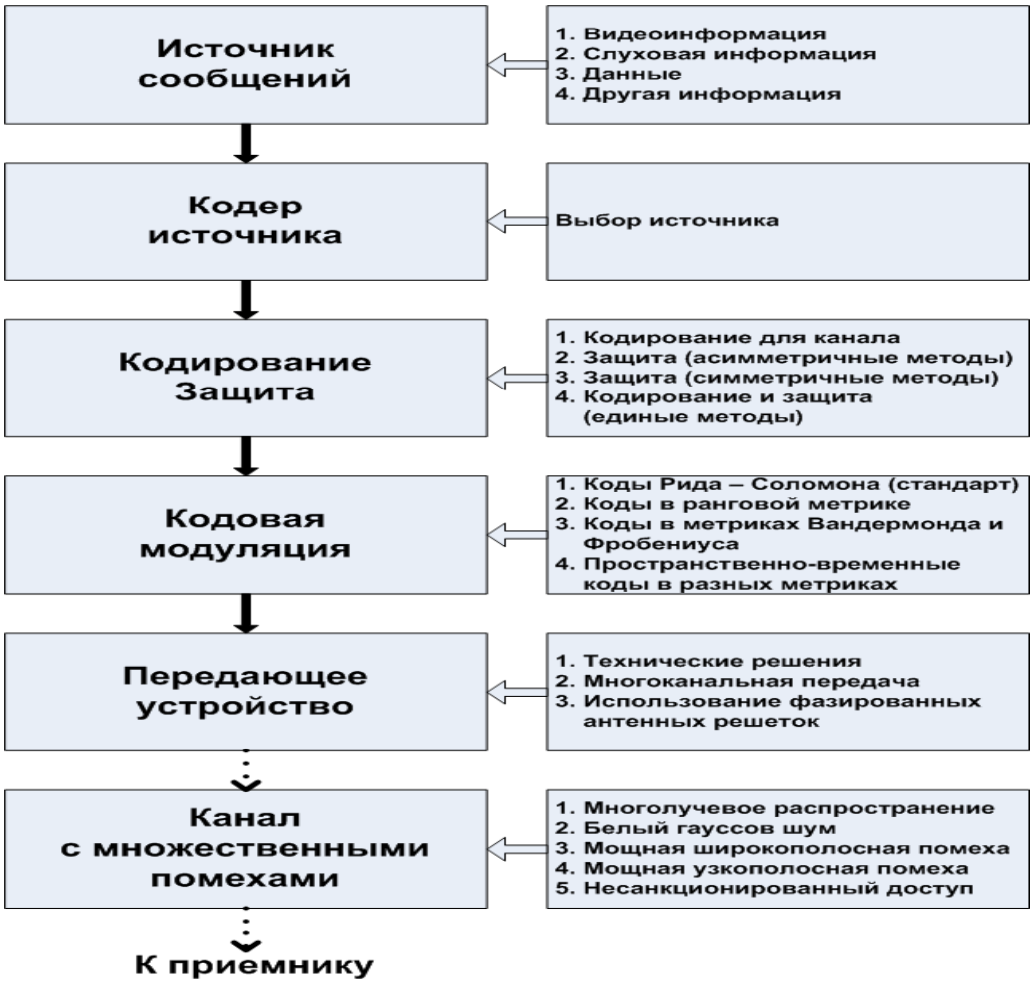
- **Разработка рекомендаций по применению полученных результатов.**
- **Рекомендации для дальнейших исследований.**

Цели и задачи проекта

- Разработка **новых классов кодов** с умеренной сложностью реализации.
- **Моделирование передачи** в каналах с замираниями и с активными узкополосными и импульсными помехами, характерных для систем подвижной связи.
- **Интегрирование в единую систему** помехоустойчивого кодирования и защиты от несанкционированного доступа.

Кафедра радиотехники МФТИ

Передающая сторона



Кафедра радиотехники МФТИ

Приемная сторона

Результаты 1 этапа 2006

- Проведен анализ источников помех и построена модель канала с множественными мощными помехами.
- Выбраны методы кодирования для защиты от ошибок в канале.
- Построены оптимальные симметричные ранговые коды, обладающие повышенной корректирующей способностью.
- Предложено семейство новых алгоритмов декодирования на основе информационных совокупностей.

Результаты 2 этапа 2006

- Разработана рекурсивная конструкция ранговых кодов с уменьшенной сложностью кодирования.
- Проведен анализ методов криптозащиты, совместимых с методами помехоустойчивого кодирования.
- Улучшены характеристики системы криптозащиты с открытым ключом, основанной на приводимых ранговых кодах.
- Проведен анализ криптостойкости системы Габидулина-Парамонова-Третьякова.

Результаты 3 этапа 2007

- Получены характеристики адаптивного алгоритма декодирования ранговых кодов в условиях передачи с мощными негауссовыми шумами.
- Проведено моделирование в среде Matlab многоканальной системы связи с множественными помехами.
- Показано, что ранговые коды эффективны для работы в системах с ортогональным частотным разделением.

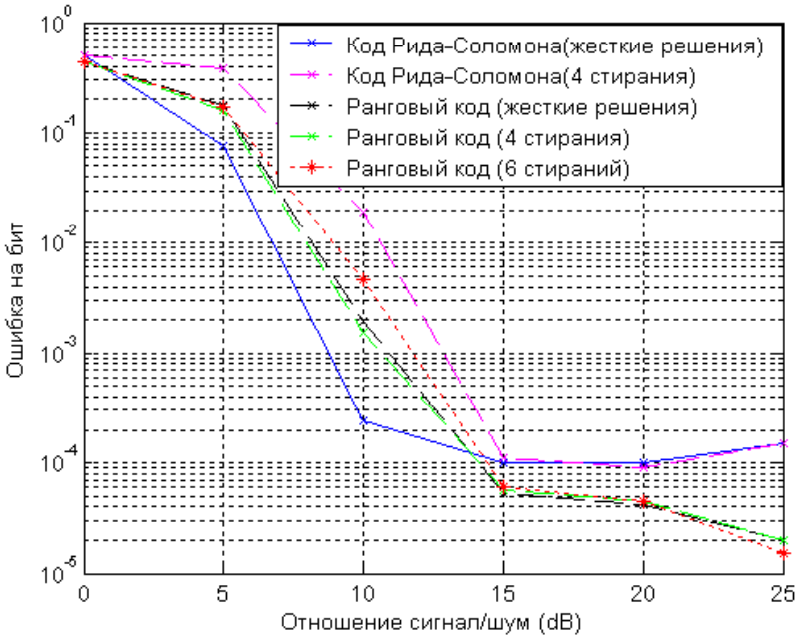
Результаты 4 этапа 2007

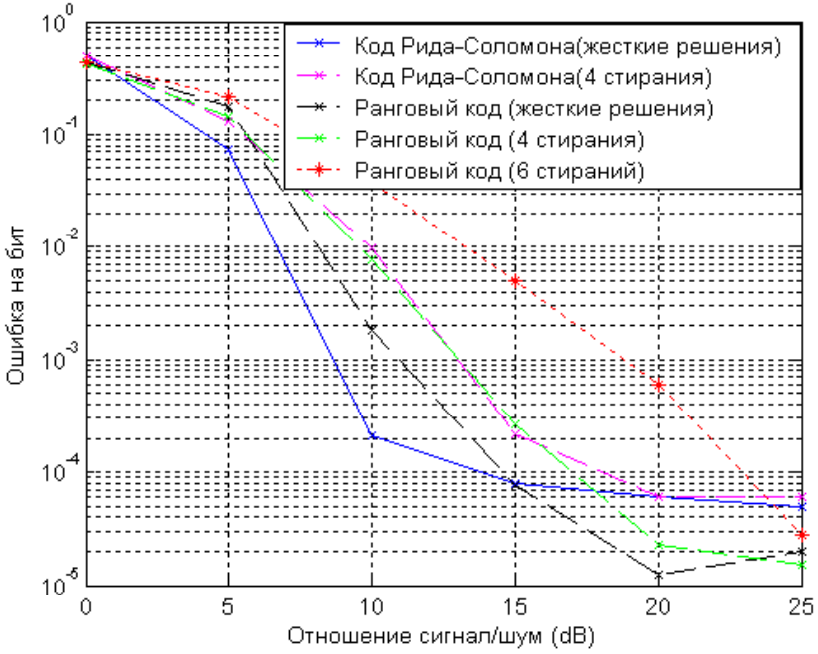
- Путем моделирования в среде Matlab подтверждена эффективность ранговых кодов применительно к крипто- и помехозащите.
- Разработана методика выбора оптимальных параметров универсальной системы крипто- и помехозащиты.

2. Полученные результаты тестового моделирования ранговых кодов и кодов Рида-Соломона применительно к многоканальной системе с шумами показали, что ранговые коды позволяют исправлять больше ошибок, чем широко применяемые коды Рида-Соломона.

Кафедра радиотехники МФТИ

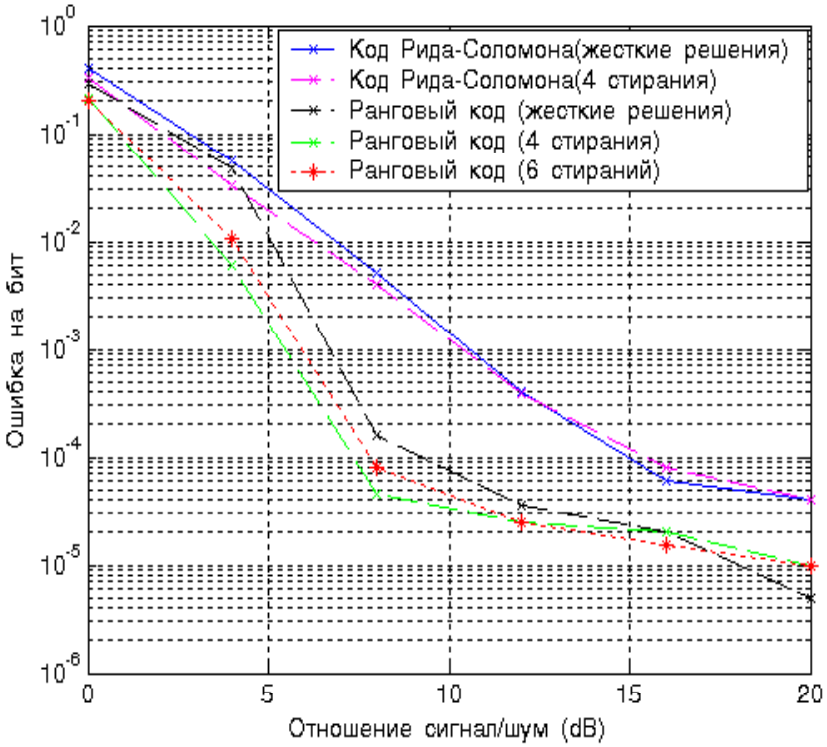
Влияние порога ненадежности на эффективность декодирования

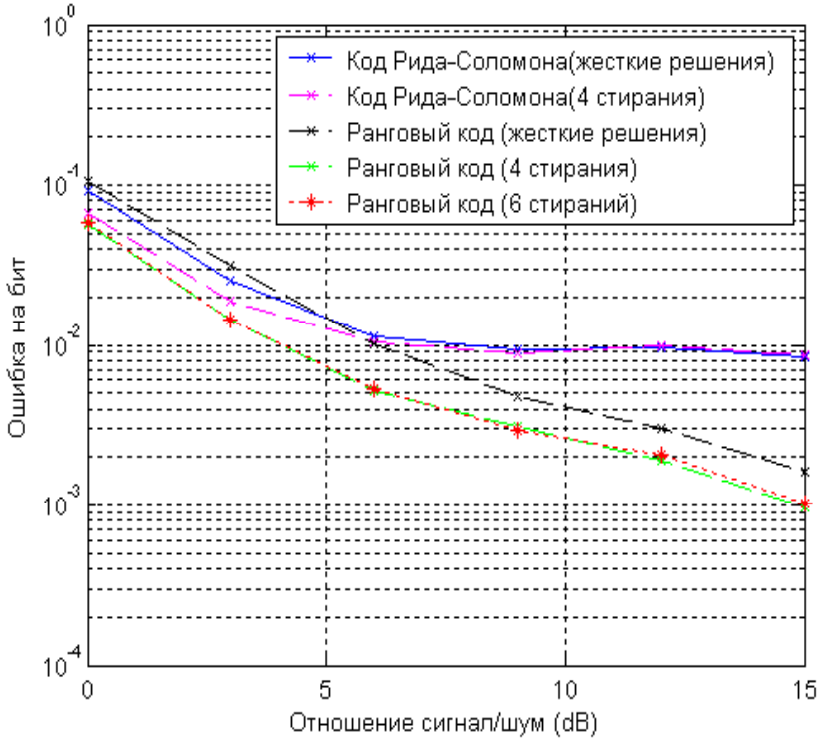




Кафедра радиотехники МФТИ

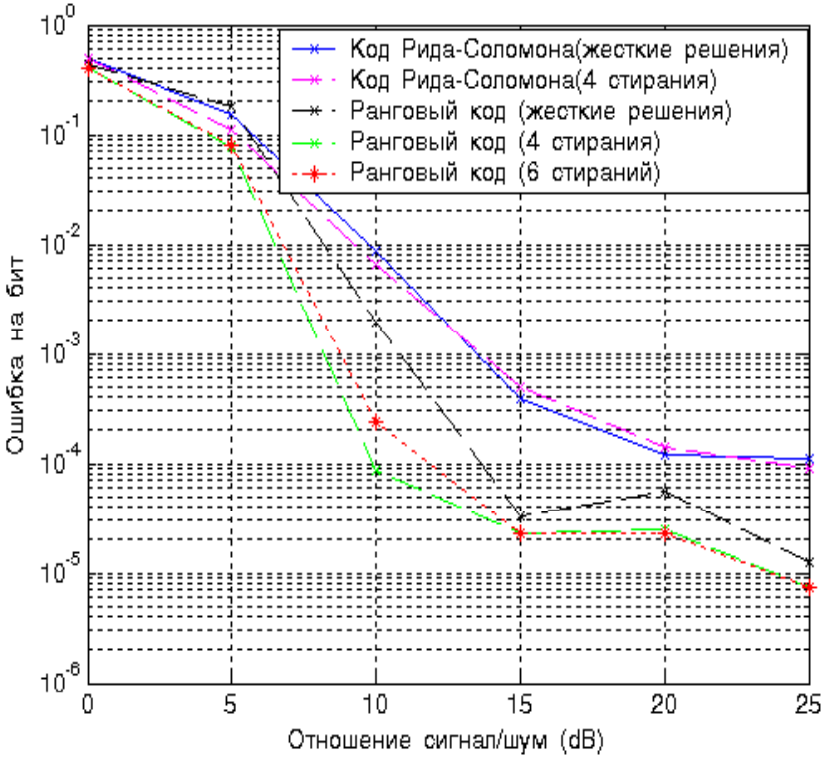
Декодирование при модуляции 2-PSK

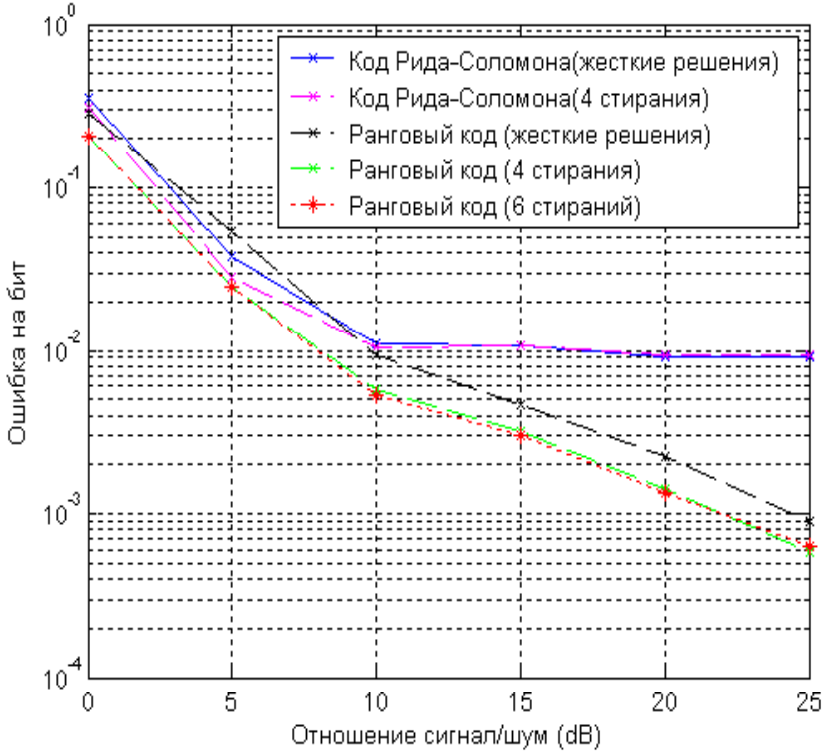




Кафедра радиотехники МФТИ

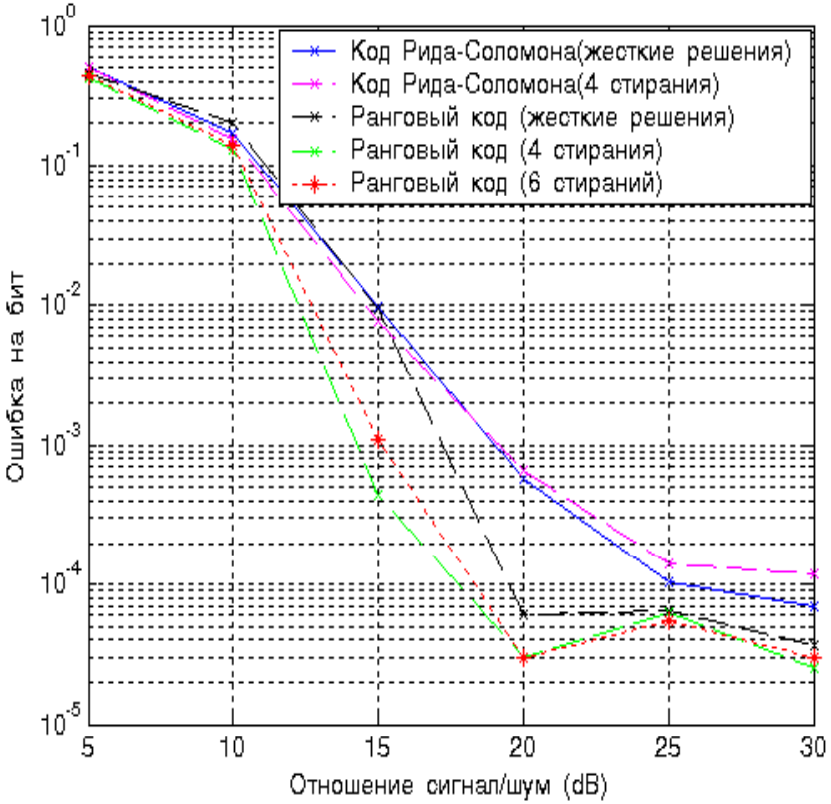
Декодирование при модуляции 4-PSK

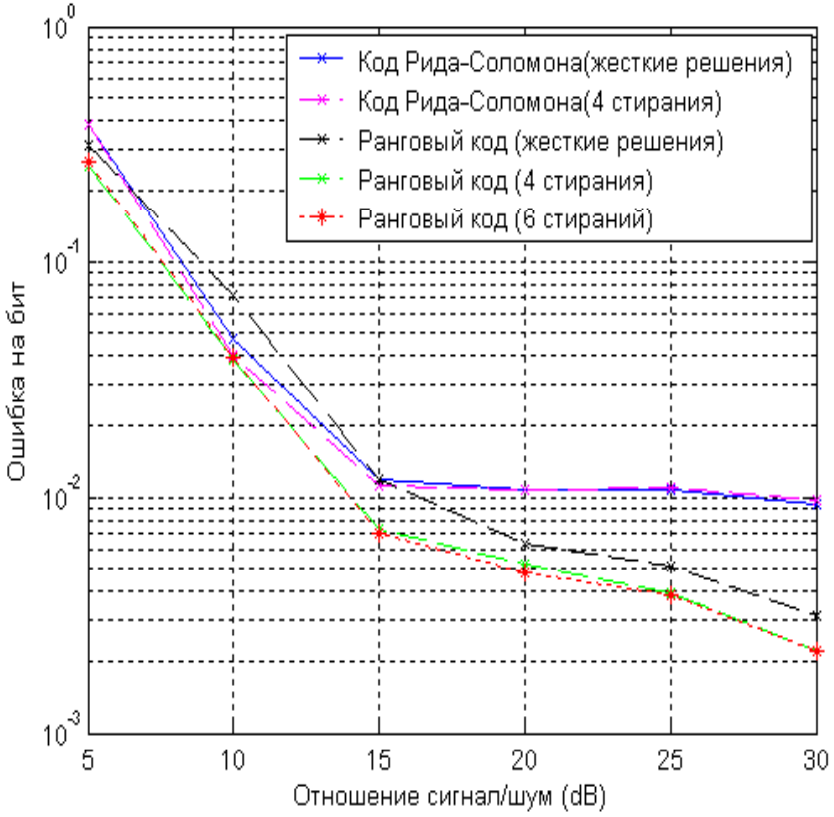




Кафедра радиотехники МФТИ

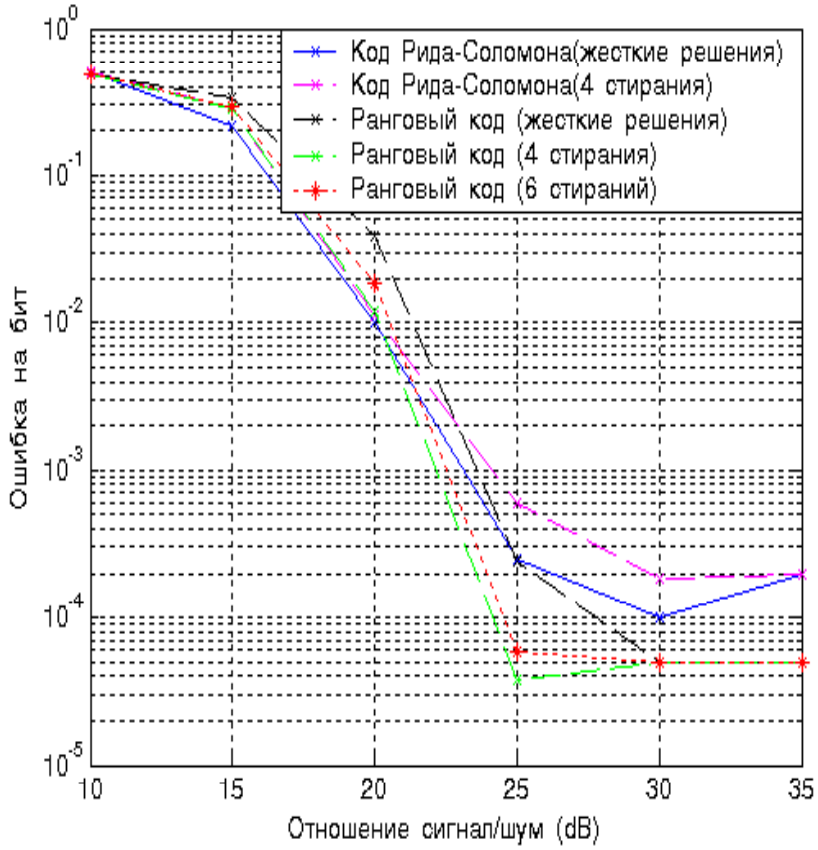
Декодирование при модуляции 16-QAM

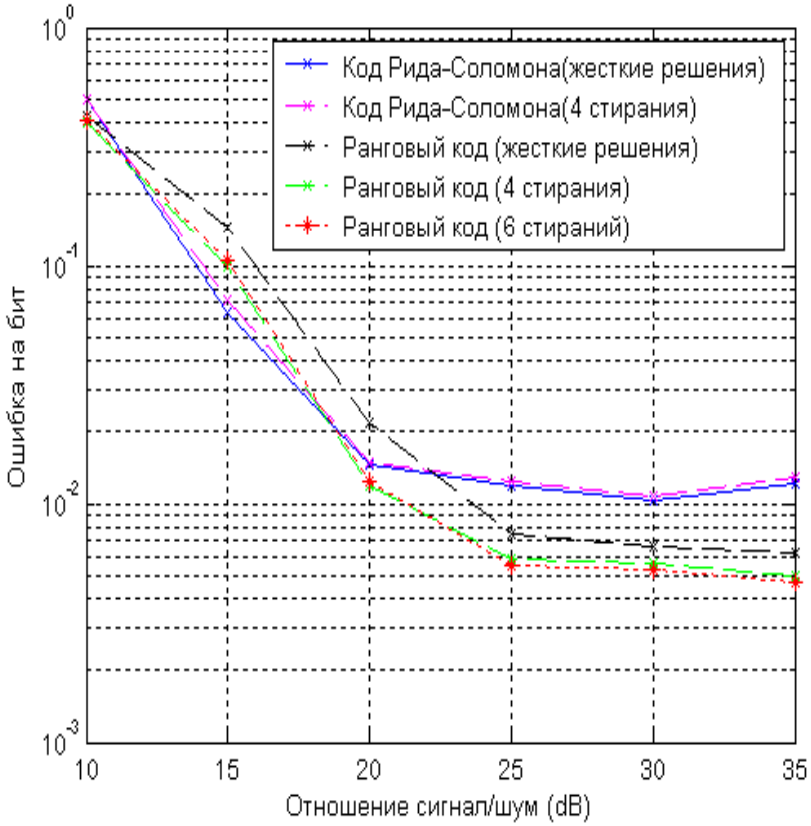




Кафедра радиотехники МФТИ

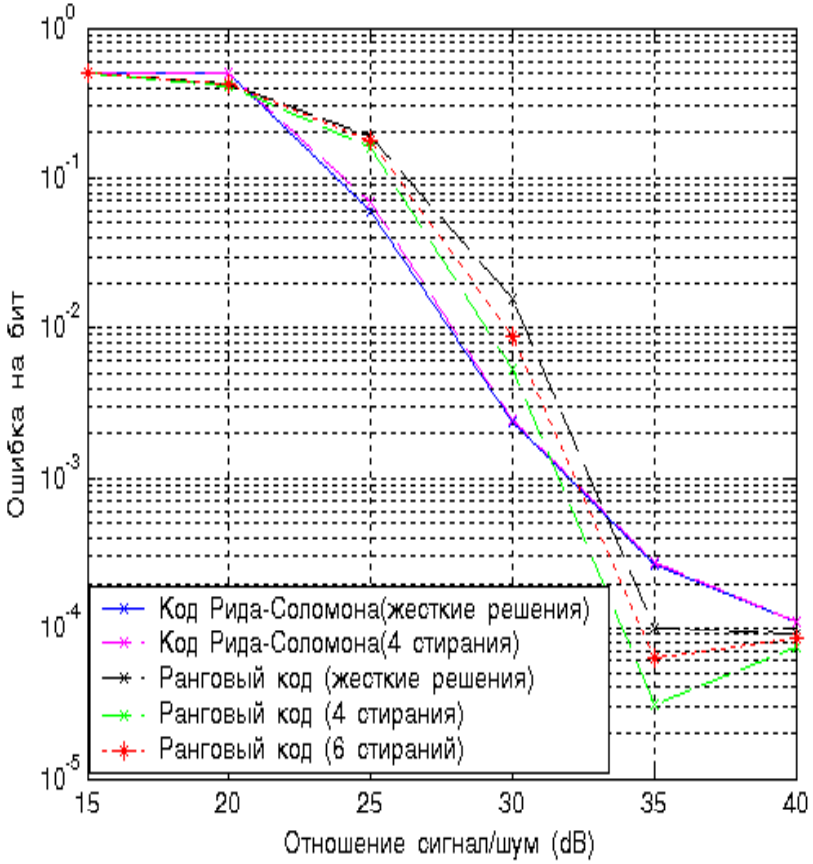
Декодирование при модуляции 64-QAM

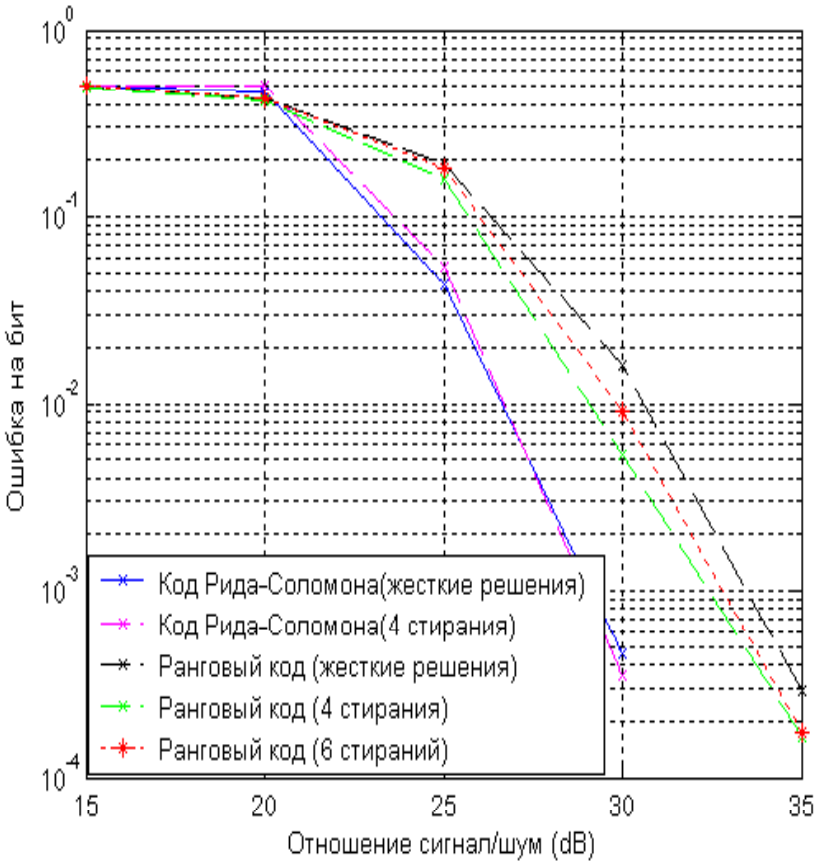




Кафедра радиотехники МФТИ

Декодирование при модуляции 256-QAM



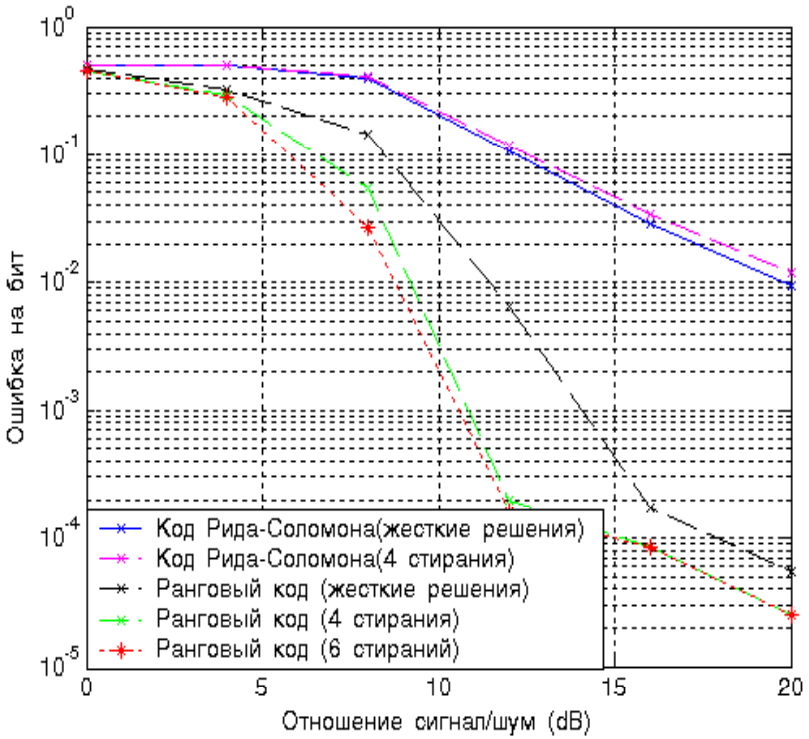


Сравнительная эффективность кодов

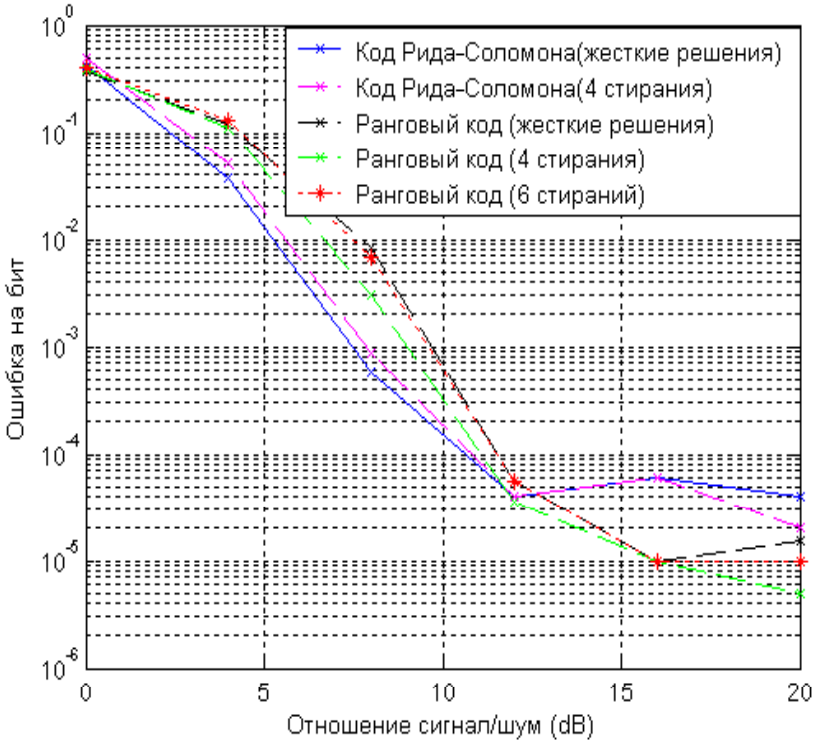
2-PSK	Ранговые коды значительно эффективнее практически во всех случаях
4-PSK	Ранговые коды значительно эффективнее, если не используется перемежение. При использовании перемежения эффективность сравнима в диапазоне 0-7 дБ, затем ранговые коды эффективнее.
16-QAM	Ранговые коды сравнимы по эффективности, либо значительно эффективнее, если не используется перемежение. При использовании перемежения ранговые коды сравнимы по эффективности при SNR<15 дБ, затем ранговые коды эффективнее.
64-QAM	Ранговые коды сравнимы по эффективности при SNR<20 дБ, либо эффективнее, если не используется перемежение. При использовании перемежения ранговые коды эффективнее при SNR>20дБ.
256-QAM	Недостаточный объем статистики для количественных оценок. Качественно -- ранговые коды эффективнее, если не используется перемежение и SNR>30дБ.

Кафедра радиотехники МФТИ

Ранговые коды в системе OFDM при 32 несущих



Без перемежения



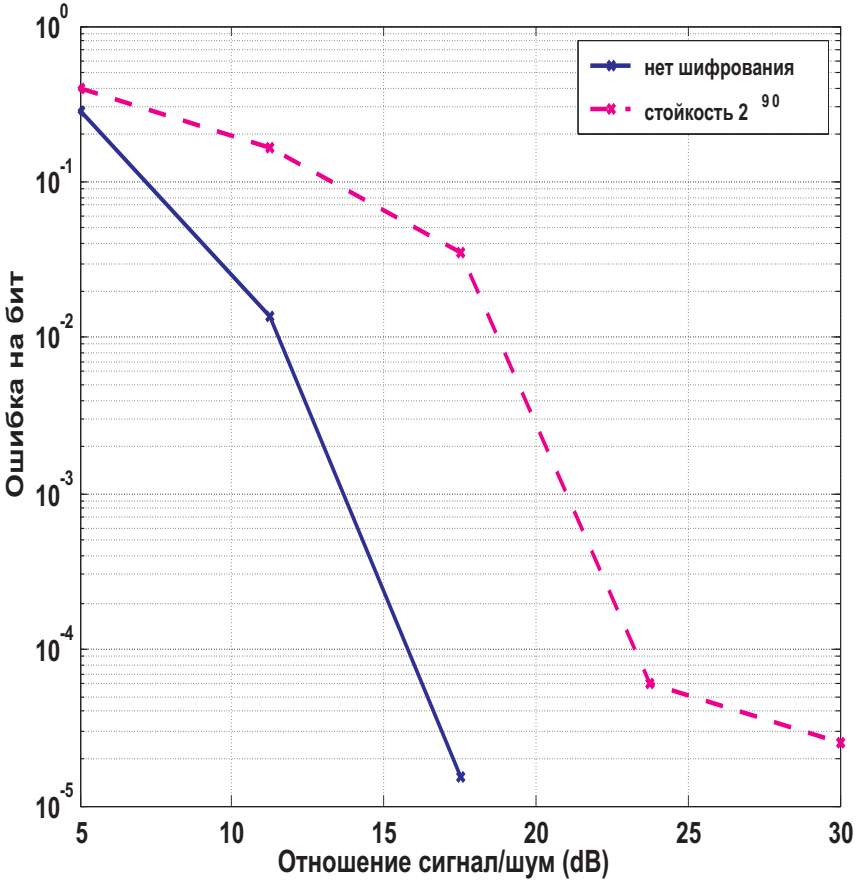
С перемежением

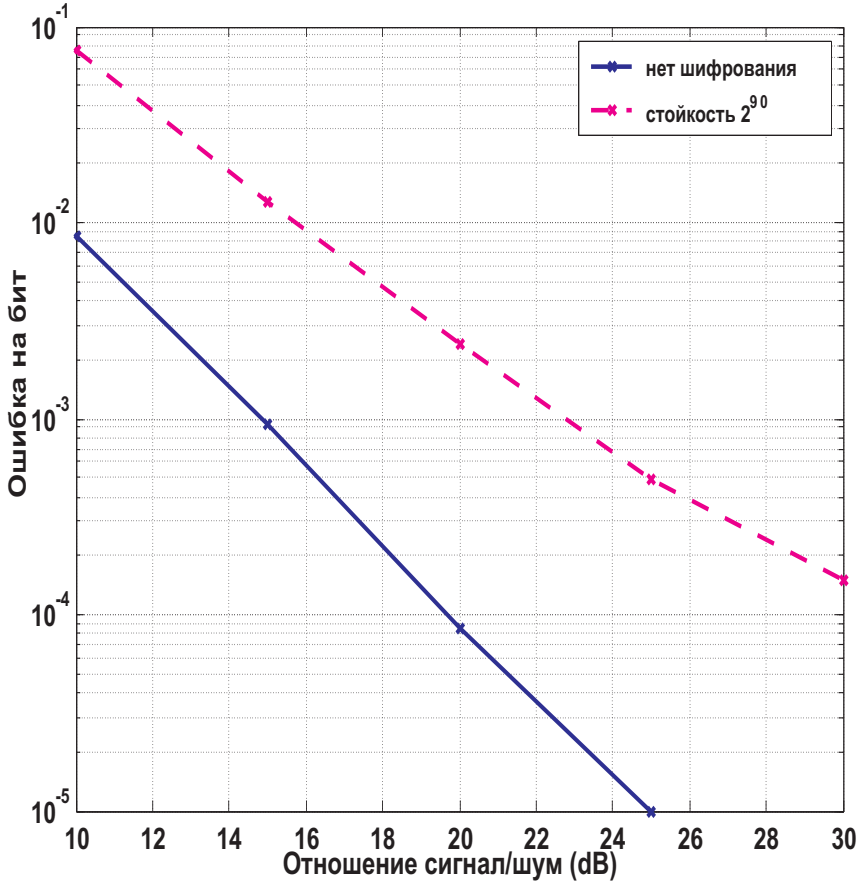
Сравнительная эффективность криптосистем на ранговых кодах

Параметры	Криптосистема 1	Криптосистема 2	Криптосистема 3
N	29	41	53
n	58	82	106
k	30	50	62
t	7	8	11
Ранг ошибки	2	3	6
Длина ключа, Кбит	50	168	348
Скорость	0.52	0.61	0.58
Стойкость	2^{90}	2^{133}	2^{200}

Кафедра радиотехники МФТИ

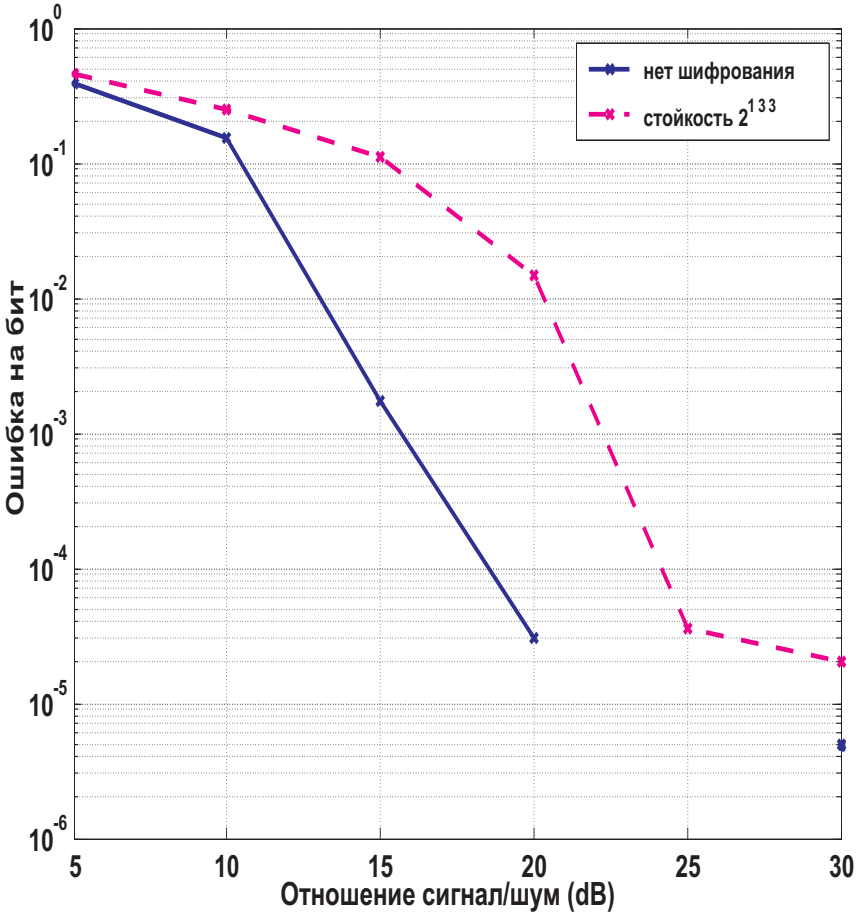
Криптосистема 1

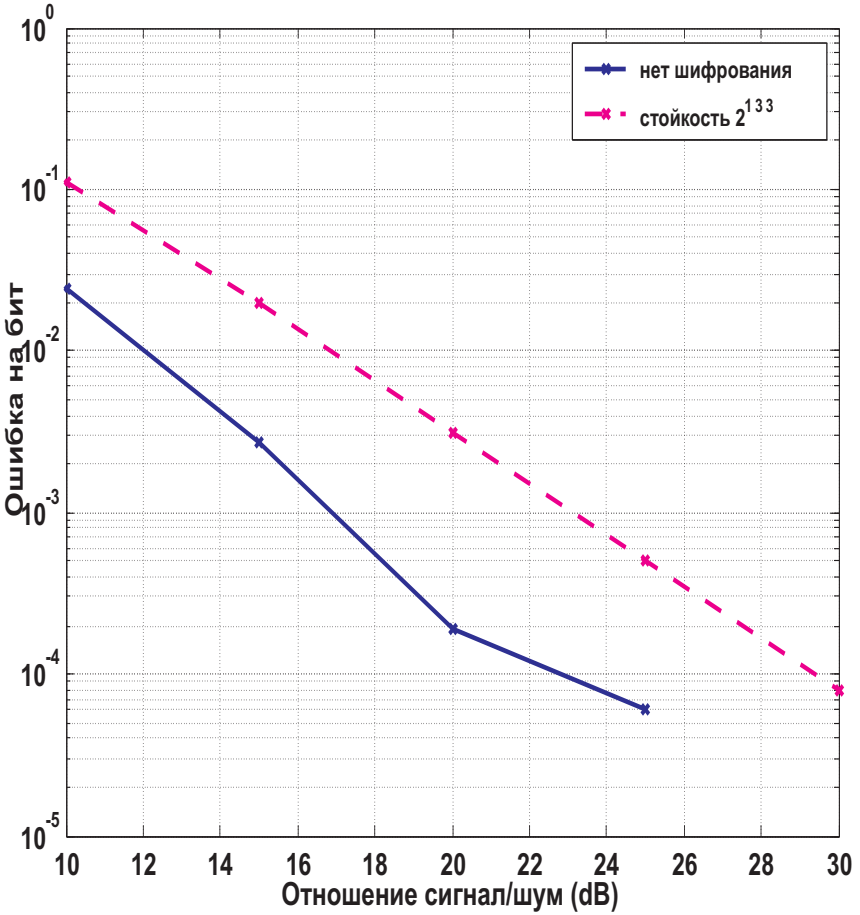




Кафедра радиотехники МФТИ

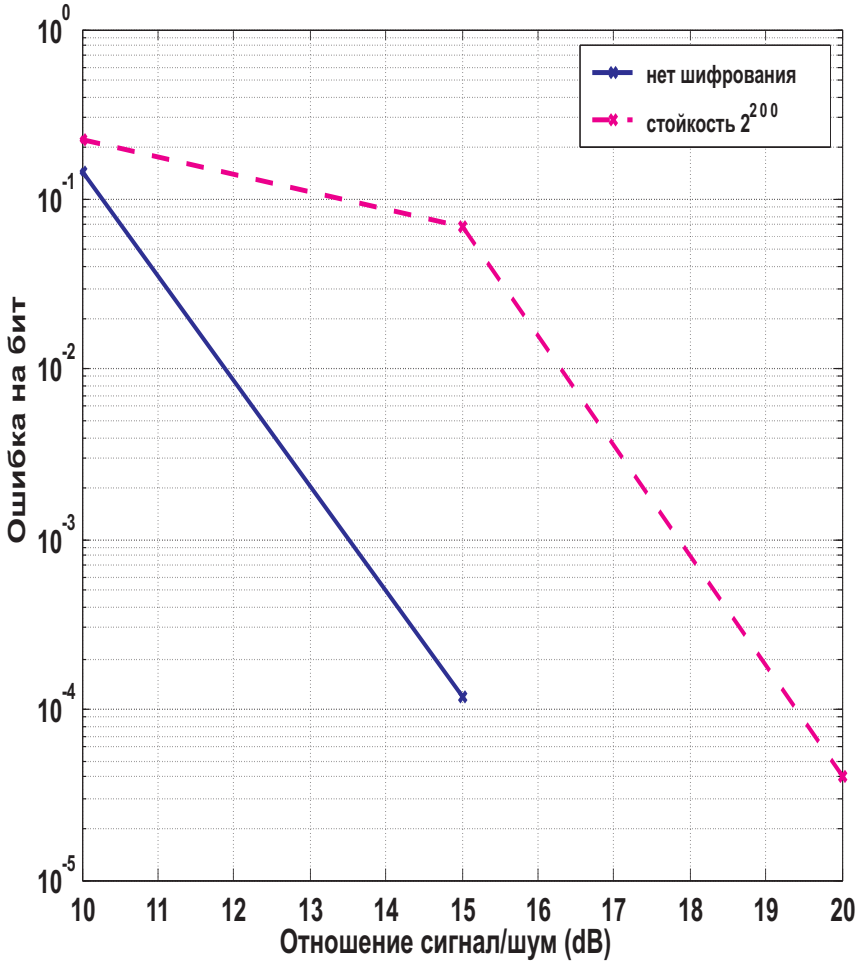
Криптосистема 2

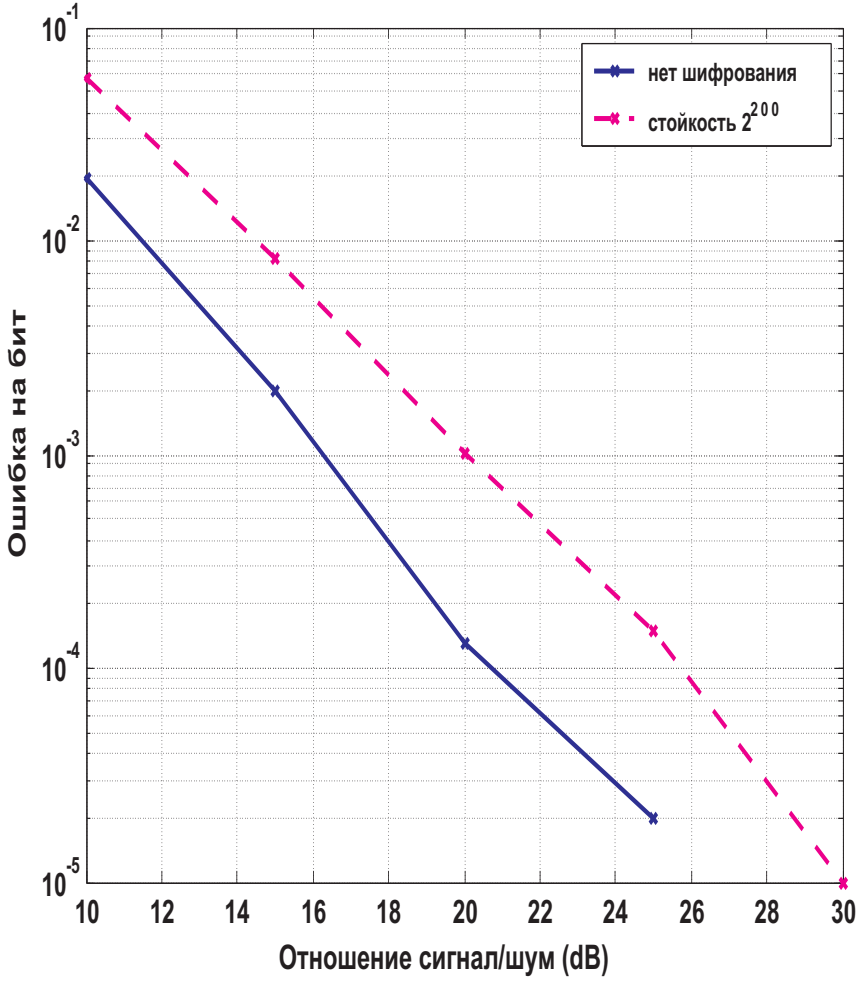




Кафедра радиотехники МФТИ

Криптосистема 3





Кафедра радиотехники МФТИ

Рекомендации по применению полученных результатов

- Использовать ранговые коды с разработанными здесь улучшенными алгоритмами кодирования и декодирования в многоканальных системах передачи информации при наличии в канале мощных организованных помех.

- Использовать разработанную интегрированную криптосистему для совместной помехозащиты и криптозащиты, что позволит экономить энергоресурсы системы.

Рекомендации для дальнейших исследований

- Анализ предложенных новых систем криптозащиты и помехозащиты, основанных на ранговых и других нехэмминговых метриках.
- Усовершенствование алгоритмов кодирования и декодирования помехоустойчивых кодов.

Кафедра радиотехники МФТИ

Справка о выполнении индикатора И3 по проекту № 3969

Фамилия И. О. защитившего диссертацию	Ученая степень	Название диссертации	Дата защиты	№ диссертационного совета
Булыгин Ю. С.	Кандидат технических наук	Построение эффективных методов криптографической защиты программ от компьютерных вирусов	14.02.2006	К 212.156.04
Кшевецкий А.С.	Кандидат физико-математических наук	Разработка новых кодов в ранговой метрике и криптосистем с открытым ключом	14.05.2007	Д.002.077.01

Справка о выполнении программных и дополнительных индикаторов

№ инд	Название индикатора	Выполненов 2006 г.	Выполнено в 2007 г.	Всего
И 1	Количество публикаций в ведущих научных журналах, содержащих результаты исследований научного коллектива по проекту (в единицах)	8	6	14
	Количество публикаций, изданных в 2005 году, в ведущих научных журналах, содержащих результаты исследований, полученных этим коллективом до выполнения проекта (в единицах)			6
	Отношение количества публикаций в ведущих научных журналах, содержащих результаты исследований научного коллектива по проекту, к количеству публикаций, изданных в 2005 году, в ведущих научных журналах, содержащих результаты исследований, полученных этим коллективом до выполнения проекта (в процентах)	133%	100%	233%
И 2	Число модернизированных и разработанных новых учебных программ высшего и послевузовского профессионального образования (в единицах)	1	1	2
И 3	Количество диссертаций на соискание ученой степени кандидата наук, защищенных в рамках выполнения проекта (е единицах)	1	1	2
	Количество диссертаций на соискание ученой степени доктора наук, защищенных в рамках выполнения проекта (е единицах)			
Д 1	Количество подготовленных (изданных) монографий (в единицах)		2	2
Д 2	Количество подготовленных (изданных) учебников, учебных пособий и других учебно-методических изданий (в единицах)		2	2
Д 3	Количество планов учебников, учебных пособий и других учебно-методических изданий (в единицах)		2	2

Кафедра радиотехники МФТИ

Справка о выполнении индикаторов И1, И2, Д3

Индикатор И1: Публикации до начала проекта

1. **Gabidulin E.M., Shorin V.V**.Научная статья“Unimodular Perfect Sequences of Length p^s”. // *IEEE Trans. Inform. Theory*, Vol.51, No. 3, P. 1163- 1166, March 2005.
2. **Габидулин Э. М., Пилипчук Н. И.**Научная статья“Симметричные ранговые коды”, // *Проблемы передачи информации*, 2004 . Т. 40. №2. С. 3-17.
3. **Gabidulin E .M., Pilipchuk N. I.**Научная статья``Symmetric matrices and codes correcting rank errors beyond the (d-1)/2 - bound," *Discrete Applied Mathematics”.* Available online 29 September 2005. 154 (2006), P. 305-312.
4. **Габидулин Э. М., Пилипчук Н. И.**Научная статья“Корректирующая способность ранговых кодов за пределами теоретической границы”. // В Сб. научных трудов «*Некоторые проблемы фундаментальной и прикладной математики и их приложениях в задачах физики*», сс. 40-52. М.: МФТИ, 2005.
5. **Габидулин Э. М., Кшевецкий А.С.** Научная статья“Декодирование ранговых кодов новой конструкии”. // В Сб. научных трудов «*Некоторые проблемы фундаментальной и прикладной математики и их приложениях в задачах физики*», сс. 53-61. М.: МФТИ, 2005.
6. **Габидулин Э. М., Обернихин В. А.**Научная статья“ Коды в F-метрике Вандермонда и их приложения”. *Проблемы передачи информации*, 2003 . Т. 39. №2. С. 3-14.

Справка о выполнении индикаторов И1, И2, Д3 -- 2

Индикатор И1: Публикации 2007

1. **Gabidulin E .M., Pilipchuk N. I.** “Erasure Correcting Algorithms for Rank Codes.” *Designs, codes and cryptography.* (2007).
2. **Gabidulin E. M.,** Martínez C., Beivide R. “Perfect Codes for Metrics Induced by Circulant Graphs.” IEEE Transactions on Information Theory, Vol. 53, No. 9, September 2007. P. 3042-3052..
3. **Габидулин Э. М.,** Мартинес К., Стаффорд Э., Байвиде Р. «Представление гексагональных созвездий с помощью графов Эйзенштейна—Якоби».*Проблемы передачи информации.* Т. 44. № 1. 2008 (принято к печати).
4. **Pilipchuk N. I., Gabidulin E. M.** “On Codes Correcting Symmetric Rank Errors”. In: “Coding and Cryptography”. LNCS 3969. 2007. P. 14-22.
5. **Gabidulin E .M** “Attacks and Counter-attacks on the GPT Cryptosystem.” *Designs, codes and cryptography.* (2007).
6. **Gabidulin E.M**., Martínez C., Stafford E., Beivide R. “Perfect Codes over 4D Lattices Based on Lipschitz Integers”. IEEE Transactions on Information Theory, Vol. 53 (to be published)

Индикатор И2: Учебные программы, связанные с проектом

1. **Габидулин Э. М., Пилипчук Н.И.** Программа и Задания по курсу «Теория информации»
2. **Габидулин Э. М.,** Программа и Задания по курсу «Защита информации»

Индикатор Д3: планы учебных пособий

1. **Воронов Е.В.** «Цепи с распределенными параметрами». Учебное пособие. – М.: МФТИ, 2007.
2. **Ларин А.Л.** «Аналоговая электроника». Учебное пособие. – М.: МФТИ, 2007.

Кафедра радиотехники МФТИ

Приложение к справке о выполнении индикаторов Д1, Д2

Индикатор Д1: монографии

Gabidulin E .M.Коллективная монография“Metrics in Coding Theory”. In E. Biglieri, L. Györfi (Eds), “Multiple Access Channels. Theory and practice.” IOS Press, 2007. P. 327-349200723IOS Press

Габидулин Э. М.Коллективная монография“Линейные коды в криптографии“. В коллективной моногрфии “Криптографические методы защиты информации” (ред. Е. М. Сухарев). 2007, 304 с. С. 82—106.200724М.: Радиотехника.

Индикатор Д2: учебные пособия

Озерский Ю. П. «Радиотехнические цепи и сигналы». Уч. пособие. 192с. М.: МФТИ (ГУ), 2007.

Габидулин Э. М., Пилипчук Н. И.
«Лекции по теории информации». Уч. пособие. 214с.
М.: МФТИ (ГУ) 2007.