18. *Babu P. C., Prasad A. N., Sudhakar D.* Software Complexity Metrics: A Survey, *International Journal*, 2013, Vol. 3, No. 8.
19. *Stephens R.* Beginning software engineering. John Wiley & Sons, 2015.
20. *Cardoso J.* Quality Metrics for Business Processes. 2011.

Статью рекомендовал к опубликованию к.т.н. П.А. Кокунир.

Чикрин Дмитрий Евгеньевич – Казанский (Приволжский) федеральный университет; e-mail: dmitry.kfu@gmail.com; 420008, Казань, ул. Кремлевская, 18; к.т.н.; доцент.

Егорчев Антон Александрович – e-mail: eanton090@gmail.com; научный сотрудник.

Ермаков Дмитрий Владимирович – e-mail: DVErmakov@kpfu.ru; аспирант.

Chickrin Dmitriy Evgen'evich – Kazan Federal University; e-mail: dmitry.kfu@gmail.com; 18, Kremlyovskaya street, Kazan, 420008, Russia; cand. of eng. sc.; associate professor.

Egorchev Anton Alexandrovich – e-mail: eanton090@gmail.com; researcher.

Ermakov Dmitriy Vladimirovich – e-mail: DVErmakov@kpfu.ru; postgraduate student.

УДК 654.02 DOI 10.18522/2311-3103-2020-2-209-218

А.И. Рыбаков, Р.Е. Кротов, С.А. Кокин

АДАПТАЦИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК К ПОСТОЯННО ИЗМЕНЯЮЩИМСЯ ПАРАМЕТРАМ ИОНОСФЕРНОГО РАСПРОСТРАНЕНИЯ

Целью исследовательской работы явилось изучение и выбор существующих вариантов адаптации по параметрам передачи, для снижения влияния недостатков коротковолновой радиолинии, целесообразно максимально эффективно использовать методы цифровой обработки сигналов. По результатам характеристик аналогово-цифровых преобразователей (АЦП), стало исследования доступных аппаратных средств, для построения протяженных радиолиний, был сделан вывод о том, что с ростом производительности ПЛИС, на которых реализуется цифровая обработка сигналов и технических представляется возможной реализация технологии создания активной антенной решетки (ААР), состоящей из N-го количества независимых антенных модулей, что и является концептуальной задачей в решении вопроса адаптации информационно-технических характеристик к постоянно изменяющимся параметрам ионосферного прохождения, для более энергоэффективного подхода к проектированию системы ионосферной радиосвязи. Повышение производительности радиосистемы путём совершенствования протоколов связи, решение вопроса оптимального по загруженности канала от времени формирования и приема сигналов. Основная идея такой ААР состоит в оцифровке или генерации высокочастотного сигнала в непосредственной близости от антенны, в составе антенных модулей. Указанные результаты позволяют заменить отдельно настраиваемые радиоприемники и трансиверы, построенные по сложной супергетеродинной схеме, на ограниченное число доступных аппаратных блоков, работающих под управлением ПО модели программно-конфигурируемого радиоканала. В следующей работе планируется провести исследования по оценке прохождения сигналов OFDM через многолучевые каналы связи с замираниями Релея и Райса. Получаемая модель позволит оценить помехоустойчивость при различной длине циклического префикса OFDM символа и пронаблюдать за поведением сигнального созвездия при воздействии различных нестабильностей.

Радиотрасса; радиосвязь; декаметровые волны; цифровая обработка сигналов; аналогово-цифровой преобразователь (АЦП); активная антенная решетка (ААР); коротковолновый (КВ) диапозон; уровень сигнала; ионосфера; ионосферное прохождение; модель распространения.

A.I. Rybakov, R.E. Krotov, S.A. Kokin

ADAPTATION OF INFORMATION AND TECHNICAL CHARACTERISTICS TO THE CONSTANTLY CHANGING PARAMETERS OF IONOSPHERIC PROPAGATION

The aim of the research work was to study and select the existing adaptation options for transmission parameters, in order to reduce the influence of shortcomings of the short-wave radio line, it is advisable to use the methods of digital signal processing as efficiently as possible. According to the results of the characteristics of analog-to-digital converters (ADCs), it became a study of the available hardware for constructing extended radio links, it was concluded that with an increase in the performance of FPGAs on which digital signal processing is implemented, it is possible to implement the technology of creating an active antenna array (AAR), consisting of the Nth number of independent antenna modules, which is a conceptual task in solving the issue of adapting information and technical characteristics to constantly changing parameters of ionospheric transmission, for a more energy-efficient approach to designing an ionospheric radio communication system. Improving the performance of the radio system by improving communication protocols, solving the problem of optimal channel load from the time of formation and reception of signals. The main idea of such an AAR is to digitize or generate a high-frequency signal in the immediate vicinity of the antenna, as part of the antenna modules. The indicated results make it possible to replace separately tuned radios and transceivers built according to a complex superheterodyne circuit with a limited number of available hardware units operating under software model of a software-configurable radio channel. In the next work, it is planned to conduct studies to assess the passage of OFDM signals through multipath communication channels with fading of Rayleigh and Rice. The resulting model will allow us to evaluate the noise immunity at different lengths of the cyclic prefix of the OFDM symbol and to observe the behavior of the signal constellation under the influence of various instabilities.

Radio path; radio communication; decameter waves; digital signal processing; analog-to-digital converter (ADC); active antenna array (AAR); short-wave (HF) range; signal level; ionosphere; ionospheric propagation; propagation model.

Введение. В продолжительном прогнозе, развитие экономики Российский Федерации важную роль отводится на освоение территорий Арктики, Сибири и Дальнего Востока, имеющих огромный ресурсный потенциал.

При этом, важным элементом экономических районов остается инфокоммуникационная инфраструктура [1].

На сегодняшний день крупнейшим оператором магистральных сетей связи является ПАО «Ростелеком», обладающий мощной магистральной сетью связи в стране, по которому можно судить о развитии инфраструктуры в целом.

Рис. 1. Магистральная сеть ПАО «Ростелеком» [2]

По рис. 1 можно оценить масштаб районов страны, не имеющей доступ к волоконно-оптическим линиям операторов связи.

Одним из вариантов обеспечения таких районов цифровой связью является коротковолновая радиосвязь [3].

Описание задачи. Стремительное развитие технических средств позволяет наиболее эффективно использовать радиочастотный спектр и предоставляет возможность реализации относительно высокоскоростной передачи данных на дальние расстояния. Для этого абоненту не потребуется протяженная и требующая постоянного технического обслуживания инфраструктура, как, к примеру, волоконно-оптические линии связи (ВОЛС). [4, 5].

С преимуществами, КВ-радиосвязь имеет и технические недостатки, а именно:

1) нелинейность высокочастотных трактов радиоприёмных (РПУ) и радиопередающих устройств (РПДУ), что может приводить к искажению фазочастотных характеристик высокочастотных (ВЧ) трактов, что наиболее заметно в работе с широкополосным сигналами.

2) неприемлемый алгоритм работы автоматический регулировки усиления старых моделей РПДУ, разработанных для работы с узкополосными аналоговыми сигналами. [6]

3) непостоянство состояния ионосферы и невозможность точного прогнозирования на временной промежуток, в рамках предстоящего сеанса радиосвязи. Перемещающиеся неоднородности электронных концентраций, вместе с изменением концентрации электронов самих слоев, изменяют высоты переотражения электромагнитной волны. Это приводит к флуктуации мощности огибающей и Допплеровским смещениям на приёмной стороне [7].

Задачей проводимого исследования явилось предложение технических решений минимизации недостатков КВ-радиосвязи и проведения адаптации параметров для разработки комплекса связи.

Метод решения. Так, при выборе вариантов адаптации по параметрам передачи и для снижения влияния недостатков коротковолновой радиолинии, целесообразно максимально эффективно использовать методы цифровой обработки сигналов [8].

Рассмотрим структурную схему типового адаптивного комплекса радиосвязи (рис. 2).

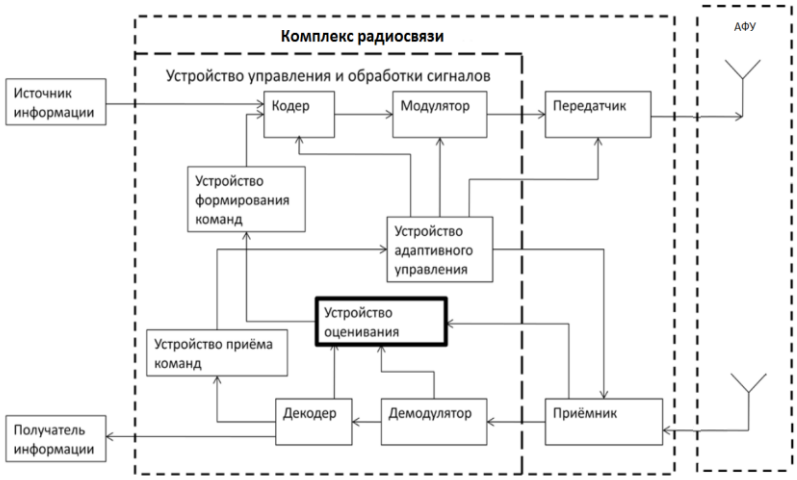

Рис. 2. Структурная схема типового адаптивного комплекса радиосвязи [9]

Можно отметить, что процедуры адаптации по рабочей частоте, мощности РПДУ, выбору сигнально-кодовой конструкции не представляют из себя ничего нового и описаны в зарубежных стандартах связи, таких, как MIL-STD-188-110(A,B,C), MIL-STD-188- 141C(A,B,C), HFDL (ARINC 635), STANAG 4538. В частности, реализованы они на таком оборудовании, как: Rohde & Schwarz M3SR Series4100, Codan 3012, 3112, 3212, RM50e HF Data modems, Rockwell Collins MDM Q9604, Harris Corp. RF-5800H-MP, RF-7800H-MP, AN/PRC-150(C), Rapid Mobile RM6, RM6-A, RM8, ТС4.

В Российской Федерации единых стандартов адаптивных линий связи нет, среди отечественных разработок можно выделить следующие адаптивные комплексы радиосвязи: ААКТС «Пирс» (ПАО «РИМР»), «МКТС-1» (АО ОНИИП), «КТС ААРС» (ФГУП НИИР), «Ангара-5М» (АО «Егоршинский радиозавод»), «Нептун» (АО НИИ АСиКС «Нептун»), «Антей» (АО «Концерн «Созвездие»). [10]

По результатам исследования доступных аппаратных средств, для построения протяженных радиолиний, можно сделать вывод, что с ростом производительности ПЛИС, на которых реализуется цифровая обработка сигналов и технических характеристик аналогово-цифровых преобразователей (АЦП), представляется возможным реализация технологии создания активной антенной решетки (ААР), состоящей из N-го количества независимых антенных модулей, что и является концептуальной задачей в решении вопроса адаптации информационно-технических характеристик к постоянно изменяющимся параметрам ионосферного прохождения.

Основная идея такой ААР состоит в оцифровке или генерации высокочастотного сигнала в непосредственной близости от антенны, в составе антенных модулей.

Приёмный сегмент комплекса радиосвязи представляется следующим образом (рис. 3):

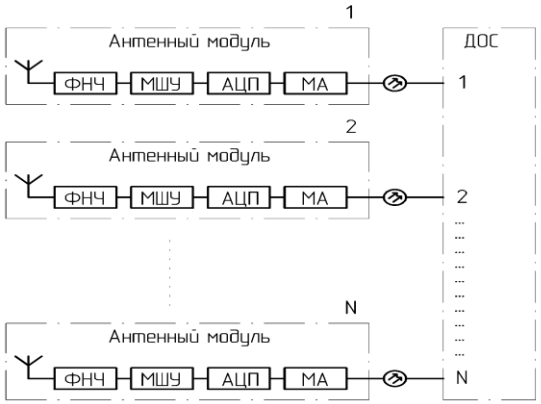

Рис. 3. Приёмный сегмент комплекса радиосвязи

Получается, ВЧ сигнал, поступающий с антенны, фильтруется ФНЧ от бытовых помех и мощных вещательных станций, находящихся на частоте менее 1,5 МГц.

Малошумящий усилитель (МШУ) усиливает сигнал, наведенный на антенну.

Блок АЦП оцифровывает всю полосу от 1,5 МГц до 30 МГц. [11].

После чего, оцифрованный сигнал, при помощи медиаконвертера (МА), преобразуется в оптический и по ВОЛС передается в диаграмма-образующую систему (ДОС), основным вычислительным средством которого является ПЛИС [12].

Поскольку оцифрованный ВЧ сигнал передается по независимым каналам, математический аппарат позволяет сдвигать фазу сигнала, поступающего с каждого антенного элемента, тем самым, формировать диаграмму направленности всей антенной решетки.

При таком решении задачи, мы получим следующие возможности:

1) реализацию антенной системы с многолепестковой диаграммой направленности [13];

2) использование разнесенного по частотам и пространству приёма [14, 15] ;

3) оцифровывая весь КВ диапазон, возможно оперативно оценить качество радиолинии по ряду доступных частот [16];

4) реализацию приёма по всему запасу доступных частот, для значительного повышения скорости приёма данных;

5) исключает потери в аналоговых трактах, коммутаторах и разъемных соединителях, минимизирует регламентные работы по поддержанию открытых электрических соединений;

6) минимизация воздействия электромагнитных помех на весь аналоговый приёмный тракт [17];

7) в случае выхода из строя части элементов сети, программными методами возможно адаптировать АР под новые условия и приёмный комплекс останется в работоспособном состоянии;

8) в случае реализации антенных с двумя поляризациями, возможно добиться снижения вероятности битовой ошибки (Е) за счет поляризационного разнесения, тем самым, снизив влияние рэлеевских замираний. На рис. 4 представлена вероятность битовой ошибки, в зависимости от отношения сигнал\шум (ОСШ). [18–20].

9) в режиме работы приёмных антенных модулей, в качестве самостоятельных антенн, реализуема система разнесенного приёма. На рис. 5 представлена вероятность битовой ошибки (Е), в зависимости от ОСШ, для количества ветвей разнесения (М) 1…8. [21, 22].

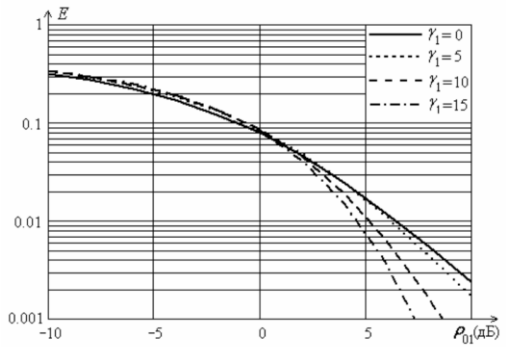

Рис. 4. Вероятность битовой ошибки (Е), в зависимости от ОСШ (ρ_{01})

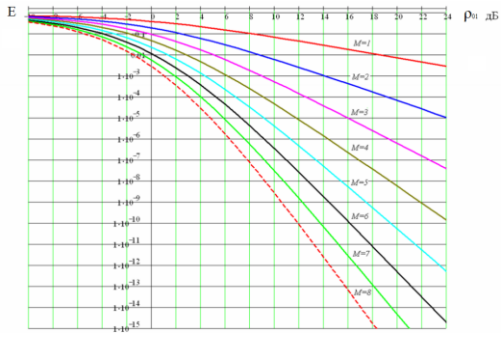

Рис. 5. Соотношения вероятностей

Передающий сегмент радиоцентра:

Передающая антенная решетка реализуется методом прямого цифрового синтеза с формированием высокочастотного сигнала, непосредственно, в каждом передающем антенном модуле. Передающие антенные модули строятся по схеме, представленной на рис. 6:

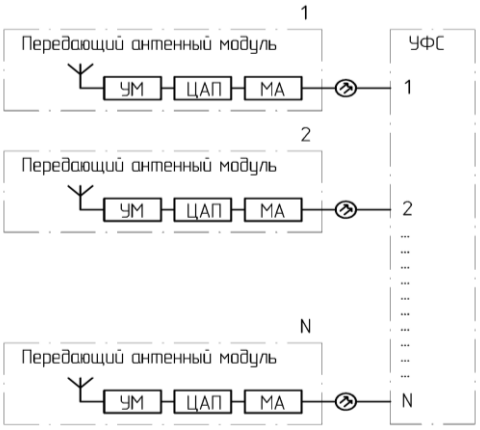

Рис. 6. Передающий сегмент радиоцентра

Для каждого передающего антенного модуля сигнал формируется устройстве формирования сигналов (УФС) индивидуально, с заданной фазой, и передается по ВОЛС. В медиаконвертере (МА) оптический сигнал преобразуется в цифровой и передается блок ЦАП. Блок ЦАП формирует аналоговый высокочастотный сигнал, усиливаемый усилителем мощности (УМ), подается непосредственно на антенну [23].

При формировании высокочастотного сигнала, непосредственно, в каждом антенном модуле, предоставляются следующие преимущества:

1) исключение потерь ВЧ сигнала на протяженных фидерных линиях [24];

2) с экономической точки зрения, освобождает от необходимости постройки дорогостоящих мощных фидерных трактов;

3) передающие антенные модули могут использовать усилители малой мощности и «набирать» мощность, в направлении корреспондента, путем пространственного сложения мощностей [25];

4) формирование нескольких каналов связи с разными рабочими частотами и направлениями излучения [26].

Заключение. Экономическая целесообразность выражается в достаточной реализации комплексов связи, в масштабах, требуемых для решения задач обеспечения цифровой связью конкретного региона. Количество приёмных и передающих антенных элементов выбирается, исходя из основных требуемых параметров радиоцентра [27].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Гурлев И.В.* Развитие волоконно-оптических линий связи как средства управления и обеспечения национальной безопасности // Вестник Евразийской науки. – 2018. – № 4 (10). – С. 42.
2. *Воробьев О.В., Рыбаков А.И.* Вариант реализации двунаправленной связи в СМС (системе метеорной связи). Описание программно-аппаратного комплекса СМС // Матер. VII Международную научно-технической и научно-методической конференции «Актуальные проблемы инфокоммуникаций в науке и образовании». – 2017. – С. 128-136.

3. *Bilitza D., Altadill D., Zhang Y., Mertens Ch., Truhlik V., Richards Ph., McKinnell L-A., Reinisch B.* The International Reference Ionosphere 2012 – a model of international collaboration // Journal of Space Weather and Space Climate. – 2014. – Vol. 4. A07. – P. 1-12.
4. *Березин Ю.В., Вылегжанин И.С.* Декаметровые ионосферные линии радиосвязи с высокой пропускной способностью // Радиотехника. –2005. – № 1. – С. 6-12.
5. *Иванов В.С., Никитин Б.К., Пирмагомедов Р.Я.* Строительство ВОЛС. // Современные технологии и организация. Ч. 1. – СПб.: СПбГУТ им. М.А. Бонч-Бруевича, 2015. – 71 с.
6. *Богданов [и др.]*. Современное состояние и перспективы развития радиопередающих устройств и радиомодемов профессиональной ДКМВ радиосвязи в ОНИИП // Успехи современной радиоэлектроники. – 2011. – № 11. – С. 24-31.
7. *Браницкий А.В., Ким В.Ю., Полиматиди В.П., Пучков В.А.* Методика измерения доплеровского смещения частоты многолучевого сигнала // Матер. VI Международную научно-технической и научно-методической конференции «Актуальные проблемы инфокоммуникаций в науке и образовании». – 2016. – С. 126-132.
8. *Климов И.З., Копысов А.Н., Чувашов А.М*. Исследование вариантов построения широкополосных систем связи // Цифровая обработка сигналов и ее применение - DSPA-2012: Тр. Российского научно-технического общества радиотехники, электроники и связи им. А.С. Попова. Доклады 14-й Международной конференции. – 2012. – С. 435-439.
9. *Смаль М.С.* Бестестовые способы оценивания состояния коротковолнового радиоканала в адаптивных радиолиниях: дисс. … канд. техн. наук: 05.12.13; Место защиты: ГУАП. – СПб., 2018. – 147 с.
10. *Березин Ю.В., Вылегжанин И.С., Якушева М.А.* Адаптивная по поляризации сеть коротковолновой ионосферной радиосвязи с селективным возбуждением электромагнитных волн в ионосфере // Тр. X Всероссийской школы-семинара «Физика и применение микроволн». – 2005. – С. 29-31.
11. The Art of Electronics [Horowitz, Paul, Hill, Winfield]. – 2015. – P. 900-910.
12. *Никитин М.Л.* Особенности построения широкополосного программно-определяемого радиомодема с использованием аппаратных возможностей ПЛИС // Интеллектуальные системы в производстве. – 2015. – № 3 (27). – С. 59-62.
13. *Лучин Д.В., Плотников А.М., Трофимов А.П., Юдин В.В.* Компактные приемные антенны для поляризационно-избирательного приема в составе систем радиомониторинга // Электросвязь. – 2015. – № 8.
14. *Ермолаев В.Т., Маврычев Е.А Флаксман А.Г.* Эффективность систем связи с антенными решетками в условиях рассеивающей среды // Успехи современной радиоэлектроники. – 2003. – № 3. – С. 41-48.
15. *Luchin D., Plotnikov A., Trofimov D., Filippov D.* Problems of implementation of ground biorthogonal and triorthogonal antenna systems // XI Междунар. IEEE Сибирская конф. по управлению и связи (SIBCON-2015). – Омск, 2015.
16. *Флаксман А.Г.* Адаптивная пространственная обработка сигналов в многоканальных информационных системах: дисс. … д-ра наук. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2004.
17. *Simon K., Alouini M.-S.* Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. – N. Y.: John Wiley&Sons, 2000. – 544 p.
18. *Ступницкий М.М., Лучин Д.В.* Потенциал КВ-радиосвязи - для создания цифровой экосистемы России // Электросвязь. – 2018. – С. 49-54.
19. *Ермолаев В.Т., Маврычев Е.А. Флаксман А.Г.* Уменьшение вероятности битовой ошибки при параллельной передаче информации в MIMO системе // Известия Вузов. Радиофизика. – 2003. – Т. 46, № 3. – С. 251-260.
20. *Savischenko Nikolay V.* Special Integral Functions Used in Wireless Communications Theory. – Singapore: World Scientific Publishing Company, 2014.
21. *Савищенко Н.В. и др.* Расчет вероятности битовой и символьной ошибок для канала связи, при приеме сигнальных конструкций стандарта DVB-S2 Н. В. // Информация и Космос. – 2015. – № 1. – С. 9-15.
22. Digital Communications: Fundamentals and Applications. – 2nd ed. [Bernard Sklar]. – P. 961-975.

23. *Ступницкий М.М., Лучин Д.В.* Потенциал КВ-радиосвязи - для создания цифровой экосистемы России // Электросвязь. – 2018. – С. 49-54.
24. *Богданов А.В. [и др.].* Об оптимизации требований к передающим комплексам радиолиний высокоскоростной передачи данных диапазона ДКМВ // Успехи современной радиоэлектроники. – 2011. – № 7. – С. 10-16.
25. *Жидяев А.В., Копысов А.Н., Богданов А.А., Савельев А.В., Никитин М.Л.* Исследование энергетических характеристик сигналов, применяемых для передачи данных по декаметровому каналу // Вестник ИжГТУ им. М.Т. Калашникова. – 2015. – № 3 (67). – С. 85-88.
26. *Bridger Wray W., Ruiz Mark D.* Advisors: Aruna Apte, James B. Greene. Naval Postgraduate School Monterey, California "Total Ownership Cost Reduction Case Study: AEGIS Radar Phase Shifters" December 2006.
27. *Ступницкий М.М., Харитонов Н.И., Девяткин Е.Е.* Инфокоммуникационная инфраструктура цифровой экономики: задачи отраслевого института // Электросвязь. – 2018. – № 4. – С. 70-76.

REFERENCES

1. *Gurlev I.V.* Razvitie volokonno-opticheskikh liniy svyazi kak sredstva upravleniya i obespecheniya natsional'noy bezopasnosti [Development of fiber-optic communication lines as a means of managing and ensuring national security], *Vestnik Evraziyskoy nauki* [Bulletin of Eurasian science], 2018, No. 4 (10), pp. 42.
2. *Vorob'ev O.V., Rybakov A.I.* Variant realizatsii dvunapravlennoy svyazi v SMS (sisteme meteornoy svyazi). Opisanie programmno-apparatnogo kompleksa sms [A variant of implementing bidirectional communication in SMS (meteor communication system). Description of the SMS software and hardware complex], *Mater. VII Mezhdunarodnuyu nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii «Aktual'nye problemy infokommunikatsiy v nauke i obrazovanii»* [Materials of the VII International scientific-technical and scientific-methodical conference "Actual problems of Infocommunications in science and education"], 2017, pp. 128-136.
3. *Bilitza D., Altadill D., Zhang Y., Mertens Ch., Truhlik V., Richards Ph., McKinnell L-A., Reinisch B.* The International Reference Ionosphere 2012 – a model of international collaboration, *Journal of Space Weather and Space Climate*, 2014, Vol. 4. A07, pp. 1-12.
4. *Berezin Yu.V., Vylegzhanin I.S.* Dekametrovye ionosfernye linii radiosvyazi s vysokoy propusknoy sposobnost'yu [Decameter ionospheric radio communication lines with high throughput], *Radiotekhnika* [Radiotechnics], 2005, No. 1, pp. 6-12.
5. *Ivanov V.S., Nikitin B.K., Pirmagomedov R.Ya.* Stroitel'stvo VOLS [Construction of VOLS], Sovremennye tekhnologii i organizatsiya [Modern technologies and organization]. Part 1. Saint Petersburg: SPbGUT im. M.A. Bonch-Bruevicha, 2015, 71 p.
6. *Bogdanov [i dr.].* Sovremennoe sostoyanie i perspektivy razvitiya radioperedayushchikh ustroystv i radiomodemov professional'noy DKMV radiosvyazi v ONIIP [Current state and prospects of development of radio transmitting devices and radio modems of professional dcmv radio communication in onip], *Uspekhi sovremennoy radioelektroniki* [Success of modern radio electronics], 2011, No. 11, pp. 24-31.
7. *Branitskiy A.V., Kim V.Yu., Polimatidi V.P., Puchkov V.A.* Metodika izmereniya doplerovskogo smeshcheniya chastoty mnogoluchevogo signala [Method for measuring the Doppler frequency offset of a multipath signal], *Mater. VI Mezhdunarodnuyu nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii «Aktual'nye problemy infokommunikatsiy v nauke i obrazovanii»* [Materials of the VI International scientific-technical and scientific-methodical conference "Actual problems of Infocommunications in science and education"], 2016, pp. 126-132.
8. *Klimov I.Z., Kopysov A.N., Chuvashov A.M.* Issledovanie variantov postroeniya shirokopolosnykh sistem svyazi [Research of variants of construction of wide-band communication systems], *Tsifrovaya obrabotka signalov i ee primenenie - DSPA-2012: Tr. Rossiyskogo nauchno-tekhnicheskogo obshchestva radiotekhniki, elektroniki i svyazi im. A.S. Popova. Doklady 14-y Mezhdunarodnoy konferentsii* [Digital signal processing and its application-DSPA-2012: Proceedings of the Russian scientific and technical society of radio engineering, electronics and communications named after A. S. Popov. Reports of the 14th International conference], 2012, pp. 435-439.

9. *Smal' M.S.* Bestestovye sposoby otsenivaniya sostoyaniya korotkovolnovogo radiokanala v adaptivnykh radioliniyakh: disc. … kand. tekhn. nauk: 05.12.13 [Best-selling methods for evaluating the state of a short-wave radio channel in adaptive radio lines: cand. of eng. dc. diss.]; Place of protection: GUAP. Saint Petersburg, 2018, 147 p.
10. *Berezin Yu.V., Vylegzhanin I.S., Yakusheva M.A.* Adaptivnaya po polyarizatsii set' korotkovolnovoy ionosfernoy radiosvyazi s selektivnym vozbuzhdeniem elektromagnitnykh voln v ionosfere [Adaptive polarization network of short-wave ionospheric radio communication with selective excitation of electromagnetic waves in the ionosphere], *Tr. X Vserossiyskoy shkoly-seminara «Fizika i primenenie mikrovoln»* [Proceedings of the X all-Russian school-seminar "Physics and application of microwaves"], 2005, pp. 29-31.
11. The Art of Electronics, Horowitz, Paul, Hill, Winfield, 2015, pp. 900-910.
12. *Nikitin M.L.* Osobennosti postroeniya shirokopolosnogo programmno-opredelyaemogo radiomodema s ispol'zovaniem apparatnykh vozmozhnostey PLIS [Features of building a broadband software-defined radio modem using hardware capabilities of the FPGA], *Intellektual'nye sistemy v proizvodstve* [Intelligent systems in production], 2015, No. 3 (27), pp. 59-62.
13. *Luchin D.V., Plotnikov A.M., Trofimov A.P., Yudin V.V.* Kompaktnye priemnye antenny dlya polyarizatsionno-izbiratel'nogo priema v sostave sistem radiomonitoringa [Compact receiving antennas for polarizing selective reception as part of radio monitoring systems], *Elektrosvyaz'* [Telecommunications], 2015, No. 8.
14. *Ermolaev V.T., Mavrychev E.A Flaksman A.G.* Effektivnost' sistem svyazi s antennymi reshetkami v usloviyakh rasseivayushchey sredy [Efficiency of communication systems with antenna arrays in a scattering medium], *Uspekhi sovremennoy radioelektroniki* [Success of modern Radioelectronics], 2003, No. 3, pp. 41-48.
15. *Luchin D., Plotnikov A., Trofimov D., Filippov D.* Problems of implementation of ground biorthogonal and triorthogonal antenna systems, X*I Mezhdunar. IEEE Sibirskaya konf. po upravleniyu i svyazi (SIBCON-2015)* [XI international IEEE Siberian conference. management and communications (SIBCON-2015)]. Omsk, 2015.
16. *Flaksman A.G.* Adaptivnaya prostranstvennaya obrabotka signalov v mnogokanal'nykh informatsionnykh sistemakh: diss. … d-ra nauk [Adaptive spatial signal processing in multi-channel information systems: dr. of sc. diss.]. Nizhniy Novgorod: Nizhegorodskiy gos-universitet im. N.I. Lobachevskogo, 2004.
17. *Simon K., Alouini M.-S.* Digital Communication over Fading Channels: A Unified Approach to Performance Analysis. N. Y.: John Wiley&Sons, 2000, 544 p.
18. *Stupnitskiy M.M., Luchin D.V.* Potentsial KV-radiosvyazi - dlya sozdaniya tsifrovoy ekosistemy Rossii [Potential of KV-Radiocommunication-for creating a digital ecosystem in Russia], *Elektrosvyaz'* [Telecommunications], 2018, pp. 49-54.
19. *Ermolaev V.T., Mavrychev E.A. Flaksman A.G*. Umen'shenie veroyatnosti bitovoy oshibki pri parallel'noy peredache informatsii v MIMO sisteme [Reducing the probability of bit error when transmitting information in parallel in the MIMO system], *Izvestiya Vuzov. Radiofizika* [Proceedings of Universities. Radiophysics], 2003, Vol. 46, No. 3, pp. 251-260.
20. *Savischenko Nikolay V.* Special Integral Functions Used in Wireless Communications Theory. Singapore: World Scientific Publishing Company, 2014.
21. *Savishchenko N.V. i dr.* Raschet veroyatnosti bitovoy i simvol'noy oshibok dlya kanala svyazi, pri prieme signal'nykh konstruktsiy standarta DVB-S2 N. V. [Calculation of the probability of bit and character errors for the communication channel, when receiving signal structures of the DVB-S2 standard N. V.], *Informatsiya i Kosmos* [Information and Space], 2015, No. 1, pp. 9-15.
22. Digital Communications: Fundamentals and Applications. 2nd ed. Bernard Sklar, pp. 961-975.
23. *Stupnitskiy M.M., Luchin D.V.* Potentsial KV-radiosvyazi - dlya sozdaniya tsifrovoy ekosistemy Rossii [Potential of KV-Radiocommunication-for creating a digital ecosystem in Russia], *Elektrosvyaz'* [Telecommunications], 2018, pp. 49-54.
24. *Bogdanov A.V. [i dr.]*. Ob optimizatsii trebovaniy k peredayushchim kompleksam radioliniy vysokoskorostnoy peredachi dannykh diapazona DKMV [About optimization of requirements for transmitting complexes of high-speed data transmission lines in the dcmv range], *Uspekhi sovremennoy radioelektroniki* [Success of modern radio electronics], 2011, No. 7, pp. 10-16.

25. *Zhidyaev A.V., Kopysov A.N., Bogdanov A.A., Savel'ev A.V., Nikitin M.L*. Issledovanie energeticheskikh kharakteristik signalov, primenyaemykh dlya peredachi dannykh po dekametrovomu kanalu [Investigation of energy characteristics of signals used for data transmission over a decameter channel], *Vestnik IzhGTU im. M.T. Kalashnikova* [Bulletin of Kalashnikov ISTU], 2015, No. 3 (67), pp. 85-88.
26. *Bridger Wray W., Ruiz Mark D.* Advisors: Aruna Apte, James B. Greene. Naval Postgraduate School Monterey, California "Total Ownership Cost Reduction Case Study: AEGIS Radar Phase Shifters" December 2006.
27. *Stupnitskiy M.M., KHaritonov N.I., Devyatkin E.E*. Infokommunikatsionnaya infrastruktura tsifrovoy ekonomiki: zadachi otraslevogo instituta [Information and communication infrastructure of the digital economy: challenges for industry Institute], *Elektrosvyaz'* [Telecommunications], 2018, No. 4, pp. 70-76.

Статью рекомендовал к опубликованию к.т.н., профессор О.В. Воробьев.

Рыбаков Алексей Игоревич – Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича; e-mail: lexeus.r1@gmail.com; 193232, Санкт-Петербург, пр. Большевиков, 22; кафедра радиопередающих устройств и средств подвижной связи; аспирант.

Кротов Роман Евгеньевич – e-mail: ub1cag@yandex.ru; кафедра радиопередающих устройств и средств подвижной связи; аспирант.

Кокин СергейАлексеевич – e-mail: sergeikokins@gmail.com; кафедра радиопередающих устройств и средств подвижной связи; магистр.

Rybakov Aleksei Igorevich – St. Petersburg state University of telecommunications. prof. M.A. Bonch-Bruevich; e-mail: lexeus.r1@gmail.com; 22 Bolshevikov Ave., Saint Petersburg, 193232, Russia; the department of radio transmitting devices and means of mobile communication; post-graduate student.

Krotov Roman Evgen'evich – e-mail: ub1cag@yandex.ru; the department of radio transmitting devices and means of mobile communication; post-graduate student.

Kokin Sergey Alexandrovich – e-mail: sergeikokins@gmail.com; the department of radio transmitting devices and means of mobile communication; master.

УДК 004.422 DOI 10.18522/2311-3103-2020-2-218-227

Л.К. Бабенко, И.Д. Русаловский

БИБЛИОТЕКА ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ ЦЕЛЫХ ЧИСЕЛ

Рассматривается одно из новых направлений криптографии – гомоморфная криптография. Его отличительной особенностью является то, что данный вид криптографии позволяет обрабатывать зашифрованные данные без их предварительной расшифровки таким образом, что результат операций над зашифрованными данными эквивалентен после расшифровки результату операции над открытыми данными. В работе приведены основные области применения гомоморфного шифрования. Выполнен анализ существующих разработок в области гомоморфного шифрования. Анализ показал, что существующие реализации библиотек позволяют обрабатывать только биты или массивы бит и не поддерживают операцию деления. Однако для решения прикладных задач необходима поддержка выполнения целочисленных операций. В результате анализа была выявлена необходимость реализация операции гомоморфного деления, а также актуальность разработки собственной реализации библиотеки гомоморфного шифрования над целыми числами. Возможность выполнения четырех операций (сложение, разность, умножение и деление) над зашифрованными данными позволит расширить области прикладного использования го-