Современная электроника и беспроводные технологии

Юрий Брауде-Золотарёв (г. Москва)

В статье рассмотрены реализуемые на микросхемах алгоритмы беспроводной связи, осуществляемой сигналами на случайных частотных и временны́х позициях с фазовой модуляцией. Обоснованы преимущества и простота этих алгоритмов, обеспечивающих криптостойкость и защиту от радиопомех, кодами исправления ошибок. Дана критика алгоритмов радиостанций Минобороны РФ, не защищённых от средств радиоэлектронной борьбы, не способных отличить ложные приказы от подлинных.

Введение

Средства электроники давно вторглись в теорию и технику радиосвязи. При этом известными преимуществами аппаратуры на микросхемах по сравнению с приборами, реализуемыми на процессорах, являются высокая надёжность, меньшее энергопотребление и низкая цена. Об этих преимуществах знали ведущие НИИ Минобороны СССР, по заказу которого для космического челнока «Буран» в 1988 г. была разработана микросхема кодека помехозащиты с малой плотностью проверок на чётность (МППЧ) и эффективностью, близкой к пределу Шеннона. Зарубежные фирмы уже более 10 лет реализуют радиосредства сверхширокополосной связи (СШПС) на микросхемах, используя их существенные конкурентные преимущества [1]. Но радиостанции для Минобороны РФ разработчики до сих пор реализуют на процессорах по алгоритмам, которые в 200 раз дороже, сложнее и менее надёжны, чем радиостанции на микросхемах.

Цель настоящей статьи – убедить заказчиков и разработчиков радиоаппаратуры в преимуществах алгоритмов, основанных на критериях микроэлектроники, помочь им отказаться от устаревших алгоритмов и процессоров и, исполняя [2], создать на микросхемах радиоаппаратуру со структурами сигналов, крипто- и помехозащитой, конкурентную на мировом уровне.

Предпочтительное помехоустойчивое кодирование

В микросхеме кодека, разработанной для «Бурана», использован код МППЧ с генераторным полиномом (ГП) на двоичном регистре сдвига (РС) на базе совершенного разностного множества (СРМ) длиной 553 бит с кодовой скоростью $R = 1/2$. Этот кодек работал с жёстким решением лучше, чем значительно более сложный кодек Витерби челнока «Шаттл» с мягким решением и такой же R. Позже по заказу Минобороны РФ для спутникового канала беспилотника была разработана микросхема более короткого кодека [3] на базе СРМ длиной 133 бит, также обладающего $R = 1/2$. Он проще кодека СРМ-553, но не уступает ему по помехоустойчивости благодаря нестационарным ГП на двух ветвях кодирования. Его энергопотребление — около 20 мкДж/бит. Кодек [3] устойчив к большим помехам, хорошо работает с фазовой (ФМ) и частотной (ЧМ) модуляциями, а его синхронизация устойчива даже при действии плотного (до 50%) пакета ошибок длиной до 25 бит. Эти преимущества особо ценны для радиостанций войсковых и охранных сетей, нуждающихся в защите от заградительных помех (ЗП).

В [4] показано, что известные более 25 лет кодеки с алгоритмом МППЧ – наилучшие, а также что кодеки МППЧ-LDPC (low density parity check codes) уже более 5 лет признаны наилучшими и за рубежом. У часто рекламируемых кодеков Рида-Соломона сложны вычисления в многоразрядных полях Галуа, а турбо-кодеки имеют большую длину кода и сложные многоразрядные перемежители. Очевидно, что выбор алгоритма – первый шаг для успешной разработки микросхем, требуемой в [2]. Возможно, что при дальнейшем развитии теории и техники кодирования будут реализованы микросхемы лучших МППЧ кодеков на трёх и более ветвях нестационарности и с мягким решением на базе СРМ-91, СРМ-73 или СРМ-57.

Предпочтительные структуры сигналов

Преимущества случайных частотно-временны́х позиций (СЧВП) (frequency hopping и time hopping – FH и TH) пакетов отмечены в [1, 5–7]. Теория сигналов давно требует отказа от ЧМ. Фирма Atmel в микросхеме AT86RF212, реализующей стандарты IEEE 802.15.4c и IEEE 802.15d, предусмотрела ФМ-4 и ФМ-8, которые в 2–3 раза лучше ЧМ используют ресурсы полосы [1]. В [5–7] на примере охранных радиосетей с СЧВП показано, что переход от ЧМ к офсетной ФМ-4 и к лучшему кодеку помехозащиты повышает помехоустойчивость почти на 10 дБ, и даны рекомендации по эффективному использованию ресурсов канала с кодеками помехозащиты. В офсетной ФМ-4 [7] модулирующие квадратурные компоненты X и Y сдвинуты на половину такта. Это устранило переходы вектора несущей через ноль и улучшило условия обнаружения и синхронизации сигнала. Известно много способов синхронизации сигналов СЧВП.

Ведущие зарубежные фирмы (Motorola, Samsung, Atmel и др.) уже более 10 лет реализуют СШПС с сигналами СЧВП на микросхемах, используя их существенные конкурентные преимущества перед сигнальными процессорами [1]. В РФ также были реализованы СШПС на микросхемах. НИИ полупроводниковых приборов (НИИПП, г. Томск) разработал для СШПС диапазона 3,1–5,1 ГГц комплект монолитных интегральных микросхем по арсенид-галлиевой технологии с проектной нормой (ПН) 0,5 мкм и частотами много выше 30 ГГц. В комплекте есть преобразователи, усилители промежуточной частоты (УПЧ), векторные модуляторы-демодуляторы, частотно-фазовые детекторы и др. Скорость передачи данных – до 100 Мбит/с. Конструкторское бюро опытных разработок (КБОР, г. Москва) разработало «СШПС-ИМПУЛЬС» на программируе-

мых логических интегральных схемах (ПЛИС) и предложило проект нового стандарта IEEE.802.15.4g. Институт радиотехники и электроники РАН (г. Москва) разработал на ПЛИС системы ШПС «РРМ-40» и «РРМ-50» диапазона 3,1–5,1 ГГц с квадратурной ФМ по стандарту IEEE.802.15.4a. Отладку проекта аппаратуры на ПЛИС можно рассматривать как первый шаг, дальнейший переход к проекту микросхемы несложен.

О рекламе устаревших структур сигналов

В [8] приведены примеры взломанных сертифицированных и рекламируемых шифраторов. Эти примеры показывают, что сертификаты не гарантируют защиту информации. Статьи, которые рекомендуют реализацию сложных и неэффективных алгоритмов структур сигналов, криптозащиты и помехоустойчивого кодирования на процессорах, есть во многих журналах. Такие статьи есть и в журнале «Современная электроника» (СоЭл).

В СоЭл № 6, 2010 представлен «новый способ помехоустойчивого кодирования с попарным сложением по модулю 2 состояний всех информационных разрядов», который многократно сложнее кодеков [4].

В СоЭл № 8 и 9, 2010 указано, что «One-Net может быть использован с множеством существующих приёмопередатчиков (трансиверов) и микроконтроллеров». Высокая цена этой универсальности не указана. Средств крипто- и помехозащиты нет, и их необходимость не упомянута.

В СоЭл № 8, 2008 рассмотрены «Беспроводные решения фирмы AeroComm» на процессорах, использующие неэффективную передачу пакетов с ППРЧ без криптозащиты и помехоустойчивого кодирования.

В СоЭл № 6, 2009 и в № 6, 2011 рассмотрен Манчестерский код – кодирование и декодирование на процессоре NM6403 и разработка программ для него. Давно известные низкая помехоустойчивость и избыточные затраты полосы канала этого кода не упомянуты.

В пяти выпусках журнала (№ 4–6 за 2009 г. и № 2–3 за 2010 г.) рассмотрены «Самосинхронизирующиеся коды и их преобразователи (СКП)». Все они ориентированы на алгоритмы с плохой помехоустойчивостью и неэффективным использованием пропускной способности радиоканала. В частности, в пятой части описаны «схемотехнические решения кодирующих и декодирующих устройств самосинхронизирующегося фазоманипулированного кода» с помехоустойчивым кодированием по алгоритмам Витерби, Рида-Соломона и турбокодов, которые сложнее и слабее кодеков МППЧ-LDPC [4], что видно из патента РФ авторов СКП № 2303376.

Микроэлектронные критерии сложности алгоритмов

Микросхемы – матричные БИС (МБИС) помехоустойчивого кодирования [3] и генератора случайных чисел (ГСЧ) Н1515ХМ1-888 [9] разработаны по критериям микроэлектроники и на практике доказали преимущества теории. Этот ГСЧ – абсолютно криптостойкий шифратор (АКШ) в смысле критериев К. Шеннона. Лучших аппаратных АКШ нет до сих пор. Оценки сложности алгоритмов по количеству вычислительных операций были отклонены как непригодные, дающие при оценках аппаратной сложности ошибки в 10–100 раз. Сложность МБИС определяют объём и структура трассировок, соединяющих элементы, а также количество условных вентилей (УВ) с комплементарными парами полевых транзисторов с p- и n-каналами. Они затрачивают энергию только при переключениях собственной и нагрузочной ёмкости. Один УВ содержит 4 транзистора. Выбор ширины трасс – компромисс. В трассе высокая плотность тока вызывает быстрое старение. Более тонкие участки испаряются и осаждаются на более толстых. Отказы возникают или от замыкания толстых участков, или от разрыва тонкого. Снижение плотности тока расширением трасс увеличивает нагрузочную ёмкость и расходы площади кристалла, что нецелесообразно. Преимущества алгоритмов с малыми затратами энергии очевидны, так как затрачиваемая энергия – мера старения БИС.

После завершения функционально-логического проекта (ФЛП) и топологического проекта (ТП) этого ГСЧ [9] на САПР, его ТП был откорректирован вручную заменой «плохих» участков ТП, где у МБИС серии 1515 велика вероятность замыканий и обрывов, такими, где такие вероятности малы. В проектах без коррекции ТП для выхода годных МБИС не ниже 10% используют не больше 50% вентилей МБИС. Очевидно, что для МБИС, содержащей два ГСЧ – шифратор и дешифратор, имеющий каждый около 1,4 тыс. УВ, – ожидаемый выход годных без коррекций ТП даже при коротких трассах ГСЧ был бы чуть выше 1%. Выпускать такие МБИС по установленной фиксированной цене изготовитель бы не захотел. После устранения «плохих» участков ТП (близких параллельных нагруженных трасс, переходов связей в другой слой вблизи соседней трассы и т.п.) был

получен реальный выход годных МБИС около 10–12%. Этот рекорд удивил даже специалистов Ангстрема – консультантов коррекций, но потребовал небольших корректировок ФЛП. У «заказных» микросхем ФЛП и ТП проектируют вместе, и коррекции ТП не нужны.

Преимущества аппаратных алгоритмов на двоичных регистрах сдвига

В теории информации и электронике давно доказано, что наиболее простые вычисления и в криптографии, и в помехоустойчивом кодировании осуществляют «автоматы», содержащие двоичные регистры сдвига (РС) с короткими трассами. Математическое описание обратных связей автомата дают генераторные полиномы (ГП). Если ГП реализуют только сумматоры по модулю 2 (XOR), то автомат – «линейный» (LFSR), при других связях – автомат «нелинейный» (NLFSR). В автоматах на двоичных РС [3, 4, 9–14] вычисления значительно проще суммирований и умножений многоразрядных чисел по модулю, которые расходуют много энергии в длинных трассах при перемешивании массивов в нескольких циклах обработки (раундах). Критика таких шифраторов, включая стандарты AES (США) и ARIA (Ю. Корея) дана в [10]. Эти шифраторы требуют около 100 тыс. УВ и потребляют в 30–100 раз больше энергии на бит информации, чем ГСЧ-АКШ [9], и соответственно, менее надёжны. По заказу Минобороны СССР (в.ч. 11232) для защиты непрерывно работающих войсковых радиостанций (ВРС) от средств радиоборьбы (СРБ) был разработан ГСЧ [9]. Необходимость разработки заказчик обосновал большим энергопотреблением и низкой надёжностью шифратора ГОСТ-28147-89.

Параметры автоматов ГСЧ с общей длиной 256 бит приведены в таблице.

Кроссинговер Cr1 = 1 переносит секцию «20» из A8 в A9, а секцию «28» – из A9 в A8. Кроссинговер Cr2 = 1 переносит секцию «17» из A10 в A11, а секцию «30» – из A11 в A10.

Автоматы A1 и A2 управляют неравномерной синхронизацией и реверсом в A3–A5. Автоматы A3–A7 управляют кроссинговером и реверсом в A8–A11. Автоматы A12 и A13 собирают неавтономными входами сигналы от автоматов A1–A11.

Реверс R и кроссинговер Cr изменяют содержимое (ключ) и аппаратную структуру автоматов. Кроссинговер Cr использует четыре трассы и четыре УВ, а R – две трассы и четыре УВ. Все цепи рандомизации используют меньше 70 УВ, а два ГСЧ на МБИС – около 2,8 тыс. УВ. Энергопотребление ГСЧ всего 0,015 мкДж/бит. Малое энергопотребление (около 0,01 от ГОСТ) указывает на высокую надёжность ГСЧ-АКШ. Это особенно ценно для датчиков технических средств охраны (ТСО) и для радиостанций войсковых и охранных сетей. При переходе от проектной нормы ПН 5 мкм к новой ПН 0,25 мкм, уже освоенной в Зеленограде, потребление ГСЧ-АКШ будет уменьшено ещё – более чем в 10 раз.

Криптоаналитиков НИИ Минобороны и КГБ СССР обрадовали малые ресурсы топологии и УВ, обеспечившие абсолютную криптостойкость и высокую надёжность ГСЧ [9] благодаря кроссинговеру. Остальные средства рандомизации ГСЧ (реверс, неравномерное движение автоматов, неавтономные воздействия и др.) они сочли излишними. Но заменить ГОСТ-28147-89 этим ГСЧ они не могли, указав на сложность программной реализации кроссинговера в средствах, использующих ГОСТ. Они надеялись для нового ГОСТ найти за 2–3 года программно простые алгоритмы без кроссинговера.

Таблица. Параметры автоматов ГСЧ с общей длиной 256 бит

Номер автомата	Длина РС автомата	Параметры*	Номера управляемых автоматов, выбранных с учётом снижения длины трасс ТП
A1	4	NA, NL	2– 4, 8–10, 12
A2	8	NA, L	3–9, 11
A3	9	A, L, R1	6, 7, 9
A4	7	A, L, R2	6, 7, 10
A5	6	A, L, R3	6, 11
A6	3	A, NL	8, 9, 12
A7	5	A, NL	9, 10, 12
A8	25 + 20	Cr1, NA, L, R	13
A9	31 + 28	Cr1, NA, L, R	13
A10	15 + 17	Cr2, NA, L	13
A11	34 + 30	Cr2, NA, L, R	13
A12	4	NA	13
A13	10	NA, L, R	Выход

Примечания: A – автономный автомат, NA – неавтономный, L – линейный, NL – нелинейный; Cr – «кроссинговер» – новый термин, обозначающий обмен секциями РС автоматов; R – реверс ГП, осуществляемый «зеркальным» изменением ГП-автомата

Разработки простых в программной и аппаратной реализации АКШ

Для разработки абсолютно криптостойких шифраторов без кроссинговера, простых не только при аппаратной, но и при программной реализации, потребовалось более 10 лет [11–14]. Исследования выполняли для ТСО совместно СНПО «Элерон» Росатома и ООО «Альтоника». Они опирались на идеи Шеннона, доказавшего, что абсолютную криптостойкость обеспечивают последовательности случайных чисел (ПСЧ) шифрблокнота при однократном использовании его «страниц». В этих ГСЧ для создания действительно случайных ПСЧ – true random number sequence – случайно, как и в ГСЧ [9], но без кроссинговера изменяли нестационарные генераторные полиномы (ГП) и содержимое РС (ключ).

В книгах по криптографии нет предложений по АКШ и описаний шифраторов, реализуемых на базе современной электроники. Стандарты шифраторов мобильной радиосвязи, разработанные криптографами США (ORIX) и Европы (GSM-A5), были вскрыты через год после публикации, и появились бесплатные программы прослушивания секретных переговоров. Были вскрыты и многие другие рекламируемые шифраторы [8]. В [11] были выбраны алгоритмы на двоичных РС с нелинейными и нестационарными ГП-функциями обратной связи (NLFSR + Random FSR). Исследования показали преимущества ГП на РС длиной 8 бит с простейшей нелинейностью на двухвходовых элементах «И» и «ИЛИ». У более длинных РС меньше количество автоматов при избыточном количестве ГП. Для РС короче 8 бит хороших ГП очень мало. Большинство нестационарных ГП с двумя состояниями создают короткие циклы, усложняющие выбор ключей.

Отсутствие теории требовало сначала поиска вручную «хороших» пар нестационарных ГП, не создающих коротких циклов. На таких ГП разработан не требующий лицензирования ГСЧ-39 на пяти РС ($8 \times 4 + 7$). Он эквивалентен шифрблокноту объёмом 2^{39} бит [12]. Его сложность – около 0,8 тыс. УВ. Можно увеличить объём шифрблокнота ГСЧ-39 до 2^{73} вводом дополнительных цепей рандомизации (16 разрядов вектора управления структурой и 18 разрядов вектора обновления ключа). Его сложность – около 1,2 тыс. УВ. Теперь поиск хороших пар ГП не нужен. В [13] опубликованы 164 пары хороших ГП для АКШ на байтовых РС и 8 пар для 7-разрядных РС. Они получены полным перебором на группе ПЭВМ.

ГСЧ-24 с тремя байтовыми РС, имеющий каждый по четыре пары нелинейных нестационарных ГП, обладает сложностью около 1,2 тыс. УВ. В [14] описаны абсолютно криптостойкие ГСЧ-16-1 и ГСЧ-16-2 с длиной ключа 16 бит на двух байтовых РС с двумя цепями управления. Эквивалентный объём шифрблокнота у ГСЧ-16-1 при интервале обновления 1 байт, который много меньше «интервала единственности», достигает 2^{41} байт. Этого объёма достаточно для непрерывной работы войсковой радиостанции (ВРС) со скоростью 16 кбит/с в течение 30 лет, а охранных радиостанций ТСО – более 100 лет. Его сложность – около 1,4 тыс. УВ, что больше, чем у ГСЧ-24 и ГСЧ-39. У ГСЧ-16-2 объём шифрблокнота 2^{54} бит, но его сложность из-за очень большого количества выбираемых пар возросла до 8,0 тыс. УВ. Очевидно, что предпочтительнее увеличивать объём шифрблокнота путём увеличения количества РС и длины ключа байтовыми ступенями 32-40-48-64-128 бит и т.д., а увеличение количества выбираемых пар нестационарных ГП нецелесообразно. Испытания ГСЧ-39 и ГСЧ-16 показали, что замена пар ГП и обновление разряда РС переносят состояние ГСЧ скачком в новую «точку» полного цикла. Это соответствует вводу в ГСЧ нового ключа. Величины скачков распределены по полным циклам автоматов хаотически, и последовательности состояний байтовых РС после обновлений эргодичны.

Ошибки разработчиков радиостанций

В [15] показана неспособность войсковых радиостанций (ВРС), поставляемых более 23 лет концерном «Созвездие» в Минобороны РФ, отличать ложные приказы от подлинных. Причина этого – ППРЧ, управляемые нестойкими ПСП, формируемыми линейными ГП–LFSR. Для вскрытия такой ПСП достаточно принять 2n реализаций ППРЧ, где n – максимальная степень ГП этой ПСП. Содержание [15] было направлено в «Созвездие» до её опубликования. Затем была выслана и сама статья [15] с предложением реализовать совместно на микросхемах новые ВРС с наилучшими алгоритмами. Полученные ответы заставили усомниться в том, что алгоритмы [15] и требования [2] о расширении экспорта конкурентной на мировом уровне высокотехнологичной аппаратуры на базе отечественных микросхем были поняты. В ответном письме было чётко сформулировано, что специалисты «Созвездия» считают для ВРС 6-го поколения (ВРС-6) наилучшим алгоритм SDR (SoftwareDefined Radio – «программно определяемое радио»). Чиновники Минобороны и Минпромторга в отказах от экспертизы алгоритмов [15] также подтвердили, что уже выбрали SDR из-за многофункциональности, эффектной для них, но ненужной для тактического звена и существенно усложнившей ВРС-6. Войсковые испытания показали, что ВРС-6 «Созвездие-М» с SDR не защищены от СРБ [16]. Причин много: отказ от АКШ, использование ППРЧ и процессоров, ненужная в тактическом звене многофункциональность (связь с мобильными телефонами 4G, с сетями Wi-Fi, Wi-MAX, связь с сотовыми телефонами и пр.), сложные и неэффективные алгоритмы помехоустойчивого кодирования.

Технологию SDR предложила в 1984 г. компания E-Systems. После испытаний макетов по программе SpeakEasy в 1990 г. использование ВРС с SDR в войсках США отменили. На E-Systems наложили штраф $4,6 млн. По программе Military's Join Tactical Radio System (JTRS) были начаты доработки SDR, но они были прекращены из-за огромных затрат и дороговизны ВРС с SDR – $37,8 тыс. за одну единицу оборудования ($6,8 млрд за 180 тыс. ВРС для тактического звена). Проблемы с процессорной реализацией SDR побудили фирму IMEC создать микросхему трансивера SCALDIO с функциями SDR. Для ПЭВМ радиолюбителей Promwad создала на сложном четырёхъядерном процессоре TMS320C6674, использованном ранее в макетах SpeakEasy, «открытую SDR-платформу».

В России SDR сначала реализовали на отечественной ПЭВМ «Багет». Но по причине чрезвычайной сложности перешли на ещё более сложную ПЭВМ ЕС1866 с импортными микросхемами, что противоречит требованиям [2]. В [17, С. 182] Ангстрем (автор не назван) рекламирует незащищённые ВРС-6 «Азарт» с SDR и, оправдывая их сложность и незащищённость, уверяет, что разработка велась «совместно со специалистами Министерства обороны РФ», имена которых также оказались «за кадром». Этой рекламе верить нельзя. Надлежащих войсковых испытаний комплекса «Азарт» не было и, учитывая [16], не будет. Выбранные структуры радиосигналов, кодов цифровой речи, помехозащиты и криптозащиты не указаны. Однако Минобороны уже приобрел в 2012 г. 2500 шт. «Азарт» и заказал поставку еще 23 тыс. штук в 2013 г. (по данным интернет-ресурсов). В [17, С. 220] А.Ю. Беккиев, новый гендиректор «Созвездия», уже не уверяет в защищённости от СРБ ВРС-6 «Созвездие-М» с SDR, но заявляет, что 1 член-корр. РАН, 23 д.т.н. и 146 к.т.н., работающие в «Созвездии», используют практически все современные телекоммуникационные решения. Сравнения предлагаемых ими алгоритмов с алгоритмами [15] он избегает.

Очевидно, что алгоритмы ВРС-6 с SDR из-за маскирования аналоговой речи, а также по криптозащите, имитозащите, энергопотреблению, помехоустойчивости, сложности и низкой надёжности непригодны ни для тактического звена, ни для гражданской радиосвязи с передачей ценной научной, технологической и коммерческой информации.

Федеральная целевая программа перехода к микросхемам

На реализацию этой программы направлено Постановление Правительства (ПП) [2], требующее разработок конкурентной на мировом уровне аппаратуры на базе микросхем с новыми технологиями с проектной нормой от 0,25 и 0,18 мкм в 2012 г. и с ПН до 90 нм и 45 нм в 2015 г.

На НИР и ОКР в разделе IV ПП «Ресурсное обеспечение» выделены 66 000 млн руб. Приложение 2 к ПП поручает ряду предприятий Минпромторга, включая концерн «Созвездие», создание базовых проектных центров для разработок аппаратуры на микросхемах.

В [15] показано, что в библиотеках элементов освоенных серий базовых матричных кристаллов (БМК) есть цифровые и аналоговые элементы для тракта приёма и передачи радиостанций в диапазоне до 200 МГц. БМК серии 5529, выпускаемые с 2012 г., обеспечивают диапазон до 1 ГГц. Эти БМК с ПН 0,25 мкм, питанием от 3,3 В, ёмкостями 50, 150, 409, 800 тыс. и 1,5 млн УВ имеют скорость триггера в счётном режиме 350 МГц. На БМК с 1,5 млн УВ можно поместить ГСЧ-АКШ [9–12], кодеки помехозащиты [3, 4], кодек речи и все вспомогательные узлы ВРС. Скорости этих БМК уже превышают значения, необходимые для цифровой обработки речи кодека MP MLQ, в кодеках речи по ОКР «Ц-2010-08-7.3» [18] и в других. Это позволит передавать в ВРС на этих БМК очень короткие высокоскоростные пакеты с цифровой речью и с СЧВП. В 2015 г. частотный диапазон увеличат до 6 ГГц и выше, а ёмкость БМК увеличат до 10 млн УВ.

Опыт разработок МБИС [3, 10] показал, что цена и энергопотребление защищённых от СРБ радиостанций будут по меньшей мере в 200 раз ниже, чем у радиостанций «Созвездие-М» и «Азарт» [17], а надёжность, соответственно, выше. На базе описанных в [3, 10] реализованных на микросхемах алгоритмов можно создать конкурентные на мировом уровне радиостанции, защищённые от СРБ, и реализовать требования ПП [2]. Необходимые МБИС можно разрабатывать в НПК «Технологический центр МИЭТ» (ТЦ МИЭТ) на БМК серий 5529 с ПН 0,25 мкм и 5521 с ПН 0,18 мкм. ТЦ МИЭТ имеет систему проектирования цифро-аналоговых микросхем «Ковчег 2.2», успешно использованную ранее [3]. Есть международный стандарт IEEE «VHDL», утверждённый в 1987 г. и откорректированный в 1998 г., для описания микросхем на вентильном и регистровом уровнях. Возможен переход от БИС на БМК к разработкам аналогово-цифровых заказных БИС. Рекомендовать САПР «Авокад» (СоЭл № 9, 2010) нет оснований.

Заключение

Ведущие НИИ СССР более 25 лет назад рекомендовали разработку аппаратуры на микросхемах и отказ от процессоров ввиду их низкой надёжности и сложности. Более 10 лет ведущие зарубежные фирмы разрабатывают аппаратуру сверхширокополосной радиосвязи на собственных микросхемах типа «система на кристалле». Но в РФ до сих пор разрабатывают коммерчески выгодную аппаратуру на процессорах по неэффективным алгоритмам, которая почти в 200 раз дороже, сложнее и менее надёжна, чем аппаратура на алгоритмах, ориентированных на микросхемную реализацию. Главные препятствия разработкам радиостанций, защищённых от средств радиоборьбы и конкурентных на мировом уровне, создают Главное управление связи Минобороны (заказчик) и Департамент радиоэлектронной промышленности Минпромторга с концерном «Созвездие» (изготовители). Более 23 лет они поощряют разработки незащищённых от СРБ, ненадёжных и дорогих войсковых радиостанций. Это противоречит требованиям Постановления Правительства № 809 от 26.11.07 разработать на базе отечественной микроэлектроники конкурентные на мировом уровне радиостанции с малой

энергией бита, малым энергопотреблением, высокой надёжностью, защищённые от радиоразведки, заградительных помех, ложных донесений и приказов. Обсуждение описанных здесь алгоритмов может помочь «Созвездию» и другим разработчикам реализовать на микросхемах радиостанции, защищённые от СРБ.

Литература

1. *Брауде-Золотарёв Ю.М.* Алгоритмы и технологии сверхширокополосных сигналов. Радиотехника. № 9. 2011.
2. Постановление Правительства РФ № 809 от 26.11.07. «Развитие электронной компонентной базы и радиоэлектроники на 2008–2015 годы».
3. *Брауде-Золотарёв Ю.М., Брауде-Золотарёв М.Ю., Каблучкова А.А., Писаренко В.Т., Фомин Ю.П.* Микросхема помехоустойчивого кодирования канала. Электросвязь. № 10. 2002.
4. *Брауде-Золотарёв Ю.М.* О наилучших алгоритмах помехоустойчивого кодирования. Беспроводные технологии. № 1. 2013.
5. *Брауде-Золотарёв Ю.М., Давыдов Ю.Л., Косарев С.А., Шептовецкий А.Ю.* Помехоустойчивость радиосетей технических средств охраны. Материалы IV науч.-техн. конф. «Фундаментальные проблемы радиоэлектронного приборостроения». Intermatic-2005 (Москва, МИРЭА, МТУСИ, 25–28 октября 2005 г.).
6. *Брауде-Золотарёв Ю.М., Давыдов Ю.Л.* Перспективное направление развития техники связи. Материалы конференции МТУСИ (февраль 2006 г.).
7. *Брауде-Золотарёв Ю.М., Давыдов Ю.Л.* Офсетная фазовая модуляция в радиоканалах систем охраны. Сборник научных трудов «Состояние и развитие систем физической защиты». ФГУП «СНПО „Элерон“». Москва. 2010.
8. *Асфандияров А., Брауде-Золотарёв Ю.М.* О банковской информационной безопасности. Мир безопасности. № 4. 2013.
9. *Брауде-Золотарёв Ю.М.* и др. Генератор случайных чисел с высокой степенью рандомизации. Научные труды НИИ радио. 1997.
10. *Брауде-Золотарёв Ю.М.* Абсолютно криптостойкие и самые простые шифраторы. Электросвязь. № 3. 2010.
11. *Брауде-Золотарёв Ю.М.* Перспективные пути построения шифраторов. Электросвязь. № 3. 2004.
12. *Брауде-Золотарёв Ю.М.* Потоковый шифратор с ключом 39 бит. Электросвязь. № 12. 2004.
13. *Брауде-Золотарёв Ю.М., Давыдов Ю.Л., Качер И.Л.* Программы, генерирующие случайные числа. Сборник научных трудов ФГУП «СНПО „Элерон“». 2008.
14. *Брауде-Золотарёв Ю.М.* Возможно ли криптостойкое шифрование с ключом 16 бит? Электросвязь. № 4. 2009.
15. *Брауде-Золотарёв Ю.М.* Алгоритмы надёжной защиты радиостанций от средств радиоборьбы. Электросвязь. № 11. 2010.
16. *Кандауров Д.* Комплекс ЕСУ ТЗ: желаемое и действительное. Армейский вестник. 23.11.2011.
17. Связь в Вооруженных силах Российской Федерации. М.: Информост. 2010. www.army.informost. ru.
18. Техническое задание на ОКР «Разработка перспективного радиомодема, обеспечивающего помехоустойчивое кодирование и передачу речевых сигналов по каналам связи с ограниченной пропускной способностью». Шифр «Ц-2010-08-7.3», в/ч 35533, в/ч 43753-Р, в/ч 68240.