Ошибки в новых войсковых радиостанциях

Реклама войсковых радиостанций «Аргон», «Созвездие-М» и «Азарт» создает опасные иллюзии того, что маскирование аналоговой речи и псевдослучайная перестройка рабочей частоты линейной обратной связью регистров защищает их от средств радиоборьбы. Цель данного материала — дополнить изложенную в предыдущей статье (см. БТ № 4'2012) критику метода Software-Defined Radio (SDR); обосновать необходимость использования надежных и абсолютно криптостойких алгоритмов для защиты от радиоразведки, заградительных помех, ложных приказов и других угроз радиоборьбы; побудить заказчиков и разработчиков войсковых радиостанций проводить сравнение алгоритмов, чтобы сделать невозможными дальнейшие ошибки. Приводятся доказательства того, что предпочтение следует отдавать алгоритмам, работающим на двоичных регистрах сдвига с нелинейными и нестационарными функциями обратной связи.

Юрий Брауде-Золотарев
braude-zolotarev@mail.ru

Введение

В статьях [1–4] показаны ошибки разработчиков и заказчиков войсковых радиостанций (ВРС), из-за которых более 20 лет в Вооруженных силах нет оборудования, защищенного от средств радиоборьбы (СРБ), и предложены алгоритмы защиты ВРС от СРБ для их реализации на российских компонентах. В настоящее время ведущие фирмы уже более 13 лет реализуют на микросхемах собственной разработки сверхширокополосные сигналы, устанавливаемые на случайных частотно-временных позициях, определяемых шифраторами AES. В 2010 г. Янчевский И. В. указал [5], что из-за «недееспособности авторов» существующие ВРС «через несколько минут работы могут быть заблокированы», что они «не защищены от информационного вторжения» и поэтому «пригодны только в мирное время». Чтобы предотвратить выпуск ВРС шестого поколения, не защищенных от СРБ, автор неоднократно высылал статьи [1, 2] в Минобороны, Минпромторг и «Созвездие» и предлагал экспертизу описанных в этих материалах и других алгоритмов, чтобы выбрать наилучшие для реализации на микросхемах ВРС, защищенных от СРБ. В ответ были получены заверения, что для ВРС-6 по теме ЕСУ ТЗ выбраны реализуемые на процессорах алгоритмы SDR, которые лучше предложенных автором, и последовали отказы от экспертизы. Выполнить требования [6] к разработке аппаратуры, конкурентной на мировом уровне, представители указанных организаций, по-видимому, не хотят. Описанные в [7] войсковые испытания показали, что новые ВРС-6 «Созвездие-М» с SDR не защищены от СРБ. Как отмечает Д. Кандауров, их алгоритмы выбраны из-за «карманных интересов больших начальников» — с целью завышения цены разработок (8 млрд руб. за 1700 шт. для войсковой бригады). В [8, 9] дана опасная реклама алгоритмов SDR, но структурные схемы ВРС-6 с SDR не описаны.

Основные рекомендации криптографов

Главной причиной незащищенности ВРС от СРБ [9] являются ошибки разработчиков, не знакомых с серьезной литературой по криптографии. По-видимому, им неизвестно, что псевдослучайные последовательности на базе линейных генераторных полиномов (ГП) нестойки и что для их вскрытия даже при неизвестной структуре ГП достаточно принять 2n реализаций псевдослучайных последовательностей, где n — максимальная степень генераторного полинома. Кроме того, разработчики недооценивают необходимость использования для защиты от СРБ действительно случайных последовательностей (True Random Number Sequence, TRNS), эквивалентных рекомендованному Шенноном шифрблокноту с однократным использованием «страниц». Для TRNS в генераторах случайных чисел (ГСЧ) рекомендовано изменять случайным образом ГП и ключ — содержимое регистров сдвига. В криптографии рассмотрены пути реализации таких ГСЧ и отмечено, что автоматы на двоичных регистрах сдвига наилучшим образом подходят для реализации TRNS и что их применению препятствует отсутствие необходимой теории. Поэтому для первых абсолютно криптостойких ГСЧ около 20 лет TRNS подбирали вручную. Специалисты в области криптографии отмечают целесообразность создания стандарта для ГСЧ с TRNS. В [4] приведены примеры взлома 12 шифраторов с сертификатами и лицензиями (Wi-Fi и др). Среди них — шифраторы GMR-1 и GMR-2 спутниковой мобильной радиосвязи

(сети GSM и Inmarsat), сертифицированные ETSI и имеющие лицензию ФСБ, выданную в августе 2010 г., которые были взломаны в январе 2012 г. Специалисты постоянно указывают на необходимость открытой публикации криптоалгоритма, ибо неопубликованные алгоритмы надо считать нестойкими, а «обещания производителей лишь создают иллюзию защищенности». В настоящее время в Интернете можно найти довольно много литературы по криптографии. Особо надо отметить книгу [14], где большое внимание уделено совершенным шифрам, формируемым абсолютно криптостойкими шифраторами, рассмотренным в [1, 2, 4] и далее.

Ошибки в рекламных публикациях по SDR

Сначала технология SDR была реализована на отечественной ПЭВМ «Багет». Из-за огромной сложности SDR позже перешли на ПЭВМ ЕС1866 с импортными микросхемами, что противоречит требованиям [6]. Реклама SDR в [8, 9] игнорирует содержание [1–4], требования [6] и испытания [7]. В [4] отмечено, что SDR выбрали из-за выполнения многих функций (связь с сетями Wi-Fi, WiMAX, Mech, связь с сотовыми телефонами и др.), эффектных для некомпетентных чиновников Минобороны и Минпромторога, но ненужных для ВРС тактического звена и существенно усложнивших ВРС-6. Метод SDR был предложен еще в 1984 г. в лаборатории E Systems (ныне Raytheon). После испытаний макетов по программе SpeakEasy в 1970 г. от использования SDR в войсках США отказались, указав на трудности с обеспечением криптостойкости сигналов и необходимость доработок. Работы по развитию и улучшению SDR в военной программе США Military's Joint Tactical Radio System (JTRS) прекратили из-за огромных затрат на доработку и выпуск ($6,8 млрд для 180 тыс. ВРС). Поэтому фирме Raytheon заказали поставки других ВРС, разработанных в 2004 г. Серьезные неприятности процессорной реализации SDR побудили фирму IMEC создать микросхему трансивера SCALDIO с функциями SDR в диапазоне от 154 МГц до 6 ГГц. Но ни одна фирма (кроме Promwad) не применила SDR из-за огромной цены, энергопотребления, сложности и невысокой надежности.

В [8] описан опыт компании Promwad проектирования «открытой SDR-платформы» на базе сложного четырехъядерного процессора TMS320C6674, использованного ранее в макетах SpeakEasy. Мультистандартность платформы, существенно ее усложняющая, необоснованно отмечена как достоинство. Ошибочно указана пригодность платформы для передачи конфиденциальной информации, поскольку нет данных по криптозащите сигналов. Правильно, как и в [1, 2, 4], рекомендован кодек помехозащиты с малой плотностью проверок на четность (LDPC), лучший из известных, но не даны ссылки на его реализацию. Ошибочно рекомендован код Рида–Соломона с очень сложными вычислениями в многоразрядных полях Галуа.

В [9] рекламируется комплекс ВРС-6 «Азарт» с SDR и утверждается, что разработка велась «совместно со специалистами Министерства обороны РФ». Вероятно, отсутствие конкретных имен связано с тем, что авторы знают о показанной в [7] незащищенности ВРС-6 от СРБ. Тем не менее в статье утверждается, что «комплекс осуществляет криптографически защищенную одновременную передачу голоса и данных». Выбранные структуры радиосигналов, кодов цифровой речи, помехо- и криптозащиты не указаны, таким образом, данной рекламе верить нельзя. Надлежащих войсковых испытаний комплекса «Азарт» не было и, по-видимому, не будет. Тем временем Минобороны уже приобретает «Азарт» (2500 шт. в 2012 г.).

В том же источнике Беккиев А. Ю. (новый генеральный директор «Созвездия») повествует о многофункциональности ВРС-6 с SDR под названием «Созвездие-М», разработанных по ЕСУ ТЗ, но уже не уверяет в их защищенности от СРБ, а рекламирует комплекс «Аргон» без архитектуры SDR. Он утверждает, что один членкорр. РАН, 23 д. т. н. и 146 к. т. н., работающие в «Созвездии», используют «практически все современные телекоммуникационные решения», но при этом избегает сравнения предлагаемых ими алгоритмов с алгоритмами, описанными в [1, 2]. Трудно поверить, что он не нашел среди этих 170 человек хотя бы одного специалиста, знакомого с современным состоянием науки в теории сигналов, криптографии и помехоустойчивом кодировании и способного сравнить алгоритмы.

В [4] отмечено, что алгоритмы ВРС-6 ЕСУ ТЗ с SDR по криптозащите, имитозащите, энергопотреблению, помехоустойчивости и надежности непригодны ни для тактического звена, ни для гражданской радиосвязи с передачей ценной научной, технологической и коммерческой информации. Чтобы скрыть эту непригодность, исчерпывающих сведений о выбранных алгоритмах не приводится. Но в Интернете можно найти хотя бы неполные данные.

Незащищенность комплекса «Аргон»

Комплекс радиостанций «Аргон» без SDR был представлен на XVI Международном форуме «Технологии безопасности» (15–18.02.2011). Перечень его недостатков был передан руководителям «Созвездия» через их представителей на этом форуме и по электронной почте. «Аргон» использует псевдослучайную перестройку рабочей частоты (256 частот при 240 скачках/с) в диапазоне 146–174 МГц с шагом сетки частот 12,5 кГц и регулярным интервалом между скачками 4,17 мс. Возможны только 100 рабочих каналов с частотной модуляцией, не защищенных от прицельных заградительных помех (ЗП). Общий ресурс 28-МГц радиоканала позволяет реализовать с модуляцией ФМ-4 общую скорость 44800 кбит/с и количество позиций $V = 44800/S$, где S — скорость цифровой речи (кбит/с). С упомянутыми в [1, 2, 4] стандартами MELP со скоростями $S = 2{,}4$, 1,2 и 0,6 кбит/с защита от ЗП при случайных частотно-временных позициях будет равна $V = 18{,}7$, 37,4 и 74,7 тыс. (подавление ЗП 43, 46, 49 дБ соответственно), так как для нарушения связи ЗП должна перекрыть все позиции. Количество защищенных от СРБ каналов при этом 900, 1800 и 3700. При помехоустойчивом кодировании с кодовой скоростью $R = 1/2$ с кодами LDPC, рекомендованными в [1, 2, 4], существенно выше помехоустойчивость, но количество возможных каналов меньше: 450, 900 и 1850 соответственно, но это намного больше, чем 100 незащищенных каналов комплекса «Аргон».

«Аргон» использует маскируемую аналоговую речь, которая при любой длине ключа будет вскрыта за несколько минут средствами, основанными на статистической избыточности речи. Необходимость криптозащищенной цифровой речи обоснована в [1, 4]. Поэтому ВРС «Аргон», как и предыдущие ВРС, более 20 лет поставляемые «Созвездием» в Минобороны, не защищены от ложных приказов и передаваемых на предсказуемых позициях прицельных ЗП, которые подавят связь при мощности, равной мощности пакета (подавление ЗП 0 дБ). Очевидно, что все параметры комплекса «Аргон» много хуже возможных при современном уровне науки и техники. Радиосеть, использующая рекомендованные в [1, 2, 4] помехоустойчивое кодирование на базе кодов LDPC, фазовую модуляцию, абсолютно криптостойкие шифраторы, цифровую речь и устанавливаемые случайно Frequency и Time Hopping (FH и TH), создаст в этом диапазоне значительно больше каналов, будет защищена от ЗП и ложных сообщений.

Абсолютно криптостойкие шифраторы на двоичных регистрах сдвига

В [1, 2, 4] были даны ссылки на простейший ГСЧ — абсолютно криптостойкий шифратор (АКШ) на двоичном регистре сдвига (РС) [10]. Он входил в комплект, заказанный Минобороны СССР, и впервые на практике на микросхеме Н1515 ХМ1-888 доказал преимущества АКШ на двоичных РС.

В ГСЧ автоматы на РС общей длиной 256 бит образуют группы управления (А1–А7), рандомизации (А8–А11) и сборки (А12, А13). Их параметры приведены в таблице 1.

Таблица 1. Параметры групп управления, рандомизации и сборки автоматов на РС длиной 256 бит

An	N	Параметры	Ag
A1	4	NA, NL	4, 8–10
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, R	13
A11	34+30	Cr2, NA, L, R	13
A12	4	NA	13
A13	10	NA, L, R	Выход

Примечание: An — номер автомата; N — количество разрядов в двоичных РС автомата; A — автономный; NA — неавтономный; L — линейный; NL — нелинейный; Cr — кроссинговер (обмен секций РС автоматов); R — реверс («зеркальное» изменение) ГП автомата; Ag — номера управляемых автоматов.

При Cr1 = 1 кроссинговер переносит 20 разрядов из A8 в A9 и 28 разрядов из A9 в A8. Кроссинговер Cr2 = 1 переносит 17 разрядов из A10 в A11 и 30 разрядов из A11 в A10. Автоматы A1 и A2 управляют неравномерным движением и реверсом в A3–A11. Автоматы A3–A7 управляют кроссинговером и реверсом в A8–A11. Неавтономные входы автоматов A12, A13 собирают сигналы от автоматов A1–A11. Кроссинговер Cr и реверс R изменяют аппаратную структуру автоматов, используя: Cr — четыре трассы и четыре условных вентиля (каждый из которых содержит четыре транзистора), а R — две трассы и четыре условных вентиля. По таблице видно, что все средства нелинейности и нестационарности вместе с другими цепями управления требуют меньше 200 условных вентилей, из-за которых ГСЧ сложнее нестойкого LFSR той же длины менее чем на 1,4%.

Генштаб и НИИ заказчика требовали снизить энергопотребление и повысить надежность микросхемы, удовлетворяющей всем требованиям ГОСТ 28147-89, не менее чем в 10 раз, указав на ее непригодность для защиты ВРС от СРБ. Сравнение микросхем ГСЧ и удовлетворяющих ГОСТу одного и того же изготовителя с одинаковой проектной нормой 5 мкм показало, что энергопотребление БИС ГСЧ составляет около 0,01 относительно потребления БИС ГОСТ при равных скоростях шифрования. Надежность ГСЧ выше почти в 100 раз, так как мерой старения является потребленная энергия. Это особенно ценно для ВРС. К тому же ГСЧ проще почти в 100 раз, а его скорость выше на два порядка. Воронежский НИИ связи (ныне «Созвездие») и другие заводы знают о ГСЧ более 20 лет и могли его использовать для надежной защиты от СРБ вместо нестойких LFSR и псевдослучайных перестроек рабочей частоты.

Криптоаналитики НИИ Минобороны, КГБ СССР и ФАПСИ РФ отметили, что АКШ пригоден для защиты ВРС, но при этом указали, что заменить им ГОСТ нельзя из-за сложности реализации кроссинговера на имеющихся программных средствах, использующих ГОСТ, и что необходимы алгоритмы ГСЧ, простые и аппаратно, и программно. В [4] отмечено, что уже разработаны простые программно АКШ с длинами ключей от 16 до 256; их испытания показали эргодичность состояний байтовых РС после обновлений ключа с шагом 1 байт. У самого короткого АКШ с ключом 16 бит длина цикла (объем шифрблокнота) достигает 2^{41} байт. Этого достаточно для непрерывной работы со скоростью 16 кбит/с в течение 30 лет. Но для ВРС, по-видимому, предпочтения заслуживают АКШ с длиной РС в 24–64 бита.

Таблица нестационарных и нелинейных ГП с двумя циклами

Приведем таблицу (таблица 2) с нестационарными и нелинейными ГП из [11]. При поиске были программно исключены пары ГП с циклами короче 58. Для автоматов с РС-8 были найдены полным перебором более 200 хороших пар, для РС-7 — восемь пар. Чтобы облегчить разработки АКШ для простых ВРС, надежно защищенных от СРБ, приведем пары таких ГП для РС-8.

Таблица 2. Пары нестационарных и нелинейных ГП для автоматов с РС-8

Длины циклов	Пары ГП
136+120, всего 35 ГП	07-04, 07-37, 0B-3B, 0D-0E, 0E-0D, 0E-3E, 13-10, 13-23, 16-26, 19-1A, 19-29, 1A-19, 1C-1F, 1C-2C, 23-13, 23-20, 25-15, 26-16, 26-25, 29-19, 29-2A, 2C-1C, 2F-1F, 2F-2C, 31-01, 31-32, 32-02, 32-31, 34-37, 37-07, 38-08, 38-3B, 3B-38, 3D-0D, 3D-3E
120+136, всего 28 ГП	01-02, 01-31, 02-01, 02-32, 04-07, 04-34, 08-0B, 08-38, 0B-08, 0D-3D, 10-13, 10-20, 5-16, 15-25, 16-15, 1A-2A, 1F-1C, 1F-2F, 20-10, 20-23, 2A-1A, 2A-29, 2C-2F, 34-04, 37-34, 3B-0B, 3E-0E, 3E-3D
179+77, всего 12 ГП	41-58, 42-5B, 44-5D, 44-62, 47-61, 48-6E, 4B-52, 4B-6D, 4D-54, 4E-57, 4E-68, 50-76
77+179, всего 6 ГП	41-67, 42-64, 47-5E, 48-51, 4D-6B, 50-49
180+76, всего 14 ГП	40-5B, 40-76, 43-58, 43-75, 45-5E, 45-73, 46-5D, 49-52, 49-7F, 4A-51, 4A-7C, 4C-7A, 4F-54, 4F-79
76+180, всего 4 ГП	46-70, 4C-57, 51-4A, 51-67
198+58, всего 41 ГП	01-08, 01-25, 02-0B, 02-26, 04-0D, 04-20, 08-01, 08-2C, 0B-2F, 0D-04, 10-19, 10-34, 13-1A, 13-37, 15-1C, 15-31, 16-32, 19-10, 19-3D, 1A-13, 20-04, 20-29, 23-07, 23-2A, 25-01, 26-02, 26-2F, 2A-0E, 2A-23, 2C-08, 2F-26, 31-15, 31-38, 32-16, 32-3B, 34-3D, 37-13, 37-3E, 3B-1F, 3B-32, 3D-19
58+198, всего 22 ГП	07-0E, 07-23, 0B-02, 0D-29, 0E-07, 0E-2A, 16-1F, 1A-3E, 1C-15, 1C-38, 1F-16, 1F-3B, 25-2C, 29-0B, 2C-25, 2F-0B, 34-10, 38-1C, 38-31, 3D-34, 3E-1A, 3E-37

Примечание: У всех пар опущен индекс Ox. Первый цикл содержит 00.

Из-за отказа от кроссинговера и реверса аппаратная реализация этих АКШ сложнее. Например, АКШ с ключом 256 бит сложнее АКШ [10] почти в два раза, но проще микросхемы ГОСТ в 50 раз и быстрее ее более чем в 100 раз [1]. Все вычисления в АКШ с ГП на базе этой таблицы значительно проще суммирований и умножений многоразрядных чисел по модулю, используемых в криптостандартах AES, ARIA, ГОСТ и др., которые расходуют много энергии в длинных трассах и при перемешивании многоразрядных массивов в нескольких циклах обработки. Поэтому они потребляют в 30–100 раз больше энергии и, соответственно, менее надежны, чем АКШ [1, 2, 4].

Выбор помехоустойчивого кодирования

В [4] были отмечены преимущества кодов LDPC и недостатки турбокодов и кодов Рида–Соломона, выбранных для ВРС с SDR, но не были упомянуты коды стандартов цифрового телевидения. В стандарте DVB использовали внутренние турбокоды и коды Рида–Соломона. Турбокоды, близкие к пределу Шеннона, имеют длину 131072, кроме того, необходим перемежитель на 65536 бит, приближающий код к случайному. Более простые турбокоды, успешно используемые в телеметрии, имеют длинный код 1784 и большой перемежитель. У кодов Рида–Соломона очень сложны вычисления в многоразрядных полях Галуа. Энергопотребление и надежность у кодеков турбокодов и кодов Рида–Соломона хуже, чем у кодеков [1, 2, 4], более чем в 100 раз, а помехозащита не лучше. Поэтому в стандарте DVB-T2 их заменили: внутренний турбокод на LDPC, внешний Рида–Соломона — на коды Боуза–Чоудхури–Хоквингхема (БЧХ). Код с оптимальным синдромным декодированием (ОСД) лучше, чем БЧХ. Непонятно, почему в ВРС-6 с SDR выбраны кодеки турбокодов и кода Рида–Соломона с худшей помехоустойчивостью и в 100 раз более сложные, чем кодеки LDPC.

Выбор структур сигналов

Преимущества сигналов ФМ-4 на случайных частотно-временных позициях (СЧВП) в сравнении с частотной модуляцией и псевдослучайной перестройкой рабочей частоты, используемых в SDR, игнорируются авторами статей [8, 9]. В [4] кратко описана СЧВП радиосети технических средств охраны (ТСО). Детальное описание используемых СЧВП дано в [12, 13]. Первая радиосеть сверхширокополосных сигналов (UWB) на микросхемах с Times Hopping описана в [12]. После этого уже 10 лет преимущества СЧВП и микросхем успешно используют многие радиосети, описанные в [13]. Из них семь стандартизованы, а остальные — внелицензионные. Ведущие фирмы отмечают конкурентные преимущества микросхем: меньшую цену, энергопотребление и лучшую надежность, чем с сигнальными процессорами. На преимущества микросхем на 11 лет ранее указал заказчик ГСЧ [10]. Наиболее распространенный стандарт WiMedia UWB разработала группа фирм WiMedia Alliance (Intel, Texas Instrument, Nokia, Microsoft, Hewlett-Packard и др.). Он работает в диапазоне 3,1–10,6 ГГц, скорость — 480 Мбит/с. Предусмотрена возможность применения ФМ, ВИМ (TH) и алгоритмов принятого в 2006 г. Европейского стандарта ETSI TS 102455. В 2007 г. ECMA International признала WiMedia международным стандартом ISO/IEC 2690. Он используется во многих странах и работает также в диапазонах 314–787 МГц (Китай) и 950–956 МГц (Япония) со скоростями 20–250 кбит/с, обеспечивая подавление ЗП до 40 дБ. Стандарты UWB ECMA-368 и ECMA-369 диапазона 3,1–10,6 ГГц приняты в декабре 2007 г. Возможен выбор разных вариантов сигналов СЧВП (FH и TH) для ВРС и ТСО [4]. В России три фирмы разработали сеть сверхширокополосных сигналов без процессоров [3, 4]. В московском Конструкторском бюро опытных разработок была создана «СШПС-ИМПУЛЬС» и предложен проект нового стандарта IEEE.802.15.4g. Этот опыт игнорируют разработчики ВРС с SDR [8, 9].

О завышенных ценах на радиостанции с SDR

Работы по ЕСУ ТЗ были начаты в ноябре 2001 г. О затратах на них сведений нет, но цены на ВРС позволяют предположить, что они фантастически велики. Так, известна цена 8 млрд руб. за 1700 шт. ВРС «Созвездие-М» для войсковой бригады. Это близко к 4,7 млн руб. за одну ВРС, что дороже аналогичной ВРС США с SDR более чем в четыре раза, поскольку в США приводится цена $6,8 млрд за 180 тыс. ВРС (около $38 тыс./шт.), что близко к 1,2 млн руб. Причем такая стоимость признана в Америке чрезмерной. Чиновники «Созвездия» уже ведут разговоры о модернизации ВРС с SDR, но переход к алгоритмам, рекомендованным в [1, 2, 4,] для защиты от СРБ и удешевление ВРС в 100 раз им невыгодны. Какое решение по модернизации принято — неизвестно.

Заключение

Главные причины разработок не защищенных от средств радиоборьбы войсковых радиостанций с архитектурой SDR, которая сделала войска тактического звена небоеспособными, — либо некомпетентность заказчиков и разработчиков ВРС, либо указанные в [7] «карманные интересы больших начальников». Более 20 лет они поощряют выпуск негодных ВРС с неэффективными алгоритмами и избегают обсуждений технических заданий со специалистами, которые могли бы им помочь в выборе эффективных алгоритмов. Их отказы от экспертизы создали опасность продолжения выпуска не защищенных от СРБ и очень дорогих ВРС. Эффективные алгоритмы, позволяющие реализовать с малым энергопотреблением и высокой надежностью криптостойкие генераторы случайных чисел, случайную расстановку позиций сигналов по частоте и времени, ФМ-4, помехоустойчивое кодирование и цифровую речь, например MP MLQ, известны давно. Эти алгоритмы могут обеспечить защиту ВРС от всех средств радиоборьбы — радиоразведки, заградительных помех, ложных донесений и приказов. Автор надеется, что обсуждение приведенных в статье доводов поможет исполнить требования [6] и создать на базе отечественной микроэлектроники защищенные от СРБ и конкурентные на мировом уровне радиостанции. Ожидаемая сложность, энергопотребление и цена таких устройств будут на два порядка ниже, чем у выпускаемых в настоящее время не защищенных от СРБ ВРС, а надежность — на два порядка выше. ■

Литература

1. Брауде-Золотарев Ю. М. Абсолютно криптостойкие и самые простые шифраторы // Электросвязь. 2010. № 3.
2. Брауде-Золотарев Ю. М. Алгоритмы надежной защиты радиостанций от средств радиоборьбы // Электросвязь. 2010. № 11.
3. Брауде-Золотарев Ю. М. Алгоритмы и технологии СШПС — сверхширокополосных сигналов // Радиотехника. 2011. № 9.
4. Брауде-Золотарев Ю. М. Защита информации в беспроводных технологиях // Беспроводные технологии. 2012. № 4.
5. Янчевский И. В. Связь в Вооруженных силах Российской Федерации. М.: Информост. 2010.
6. Постановление Правительства РФ № 809 от 26.11.07 «Развитие электронной компонентной базы и радиоэлектроники на 2008–2015 гг.».
7. Кандауров Д. Комплекс ЕСУ ТЗ: желаемое и действительное // Армейский вестник. 23.11.2011.
8. Кондратьев А. Технология SDR: опыт проектирования универсальной платформы // Беспроводные технологии. 2012. № 4.
9. Радиостанции с SDR. Связь в Вооруженных силах Российской Федерации. М.: Информост. 2012.
10. Брауде-Золотарев Ю. М. и др. Генератор случайных чисел с высокой степенью рандомизации // Науч. труды НИИ радио. 1997.
11. Брауде-Золотарев Ю. М., Давыдов Ю. Л., Качер И. Л. Программы, генерирующие случайные числа // Сб. науч. тр. ФГУП СНПО «Элерон». 2008.
12. Win M. Z., Scholtz R. A. Ultra-Wide Bandwidth time-hopping spread spectrum impulse radio for wireless multiple-access communications // IEEE Trans. on Commun. V.48. № 4. 2000.
13. Косичкина Т. П., Сидорова Т. В., Сперанский В. С. Сверхширокополосные системы коммуникаций. М. Инсвязьиздат. 2008.
14. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ. 2005.