ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 621.316.97

Печатается в порядке обсуждения

АЛГОРИТМЫ НАДЕЖНОЙ ЗАЩИТЫ РАДИОСТАНЦИЙ ОТ СРЕДСТВ РАДИОБОРЬБЫ

Ю. М. Брауде-Золотарев, к.т.н.; braude-zolotarev@mail.ru

Ключевые слова: *радиоэлектронная борьба, криптостойкость, имитостойкость, защита от заградительных радиопомех, генератор случайных чисел, обновление ключа, помехоустойчивое кодирование, оптимальное синдромное декодирование, случайные частотные и временные позиции радиосигналов, реализация алгоритмов на микросхемах.*

Введение. Описанные в [1] войсковые радиостанции («Акведук» и др.) не защищены от средств радиоборьбы (СРБ): радиоразведки, заградительных помех [2] и ложных сообщений [3]. Используемые в них маскирование и псевдослучайную перестройку рабочей частоты (ППРЧ) противник легко вскроет радиоразведкой, а значит, сможет прослушивать все переговоры радиостанций и передавать им ложные донесения и приказы, не отличимые от истинных. Это обусловлено реализацией рекомендаций, приведенных в работах [4, 5], и самая угрожающая из них — использование ППРЧ, управляемой псевдослучайными последовательностями (ПСП) с линейными неприводимыми генераторными полиномами (ГП), непригодность которых известна давно [6].

Описания [1] создают опасную иллюзию защищенности ПСП от СРБ и не учитывают предостережений [3] о ложном приказе, заставившем в 1967 г. отступить Египетскую танковую армию, или о группе авиаудара США, которая теперь сопровождается не 6—8 самолетами, как раньше, а в три раза большей группой СРБ — из 20—25 самолетов. Разнообразными СРБ обладают также вооруженные силы Англии и других стран.

Необходимость применения для защиты от СРБ криптостойких генераторов случайных чисел обоснована в [7—10], где используется опыт защиты радиосетей технических средств охраны (ТСО) Росатома. Все параметры радиостанций [1] много хуже, чем могли быть при современном уровне науки и техники. Они излучают сигналы с избыточной энергией бита и малой помехоустойчивостью, потребляют излишнюю энергию, имеют малую надежность, слишком сложны и дороги. Результаты поиска надежных и простых алгоритмов защиты от СРБ описаны в [11—24].

Цель данной статьи — рекомендовать разработчикам комплекс эффективных и простых алгоритмов защиты радиостанций и радиосетей от угроз СРБ. Комплекс реализует (с малым энергопотреблением и высокой надежностью!) криптостойкие генераторы случайных чисел (ГСЧ), эффективное помехоустойчивое кодирование и случайную расстановку частотно-временных позиций (ЧВП) сигналов. Вместе алгоритмы обеспечивают имито- и криптостойкость, защиту от радиоразведки, заградительных помех, ложных донесений и приказов.

Приведем **перечень неполных и ошибочных рекомендаций** [4, 5]:

- Не отмечена непригодность ППРЧ, управляемой псевдослучайными последовательностями, которые радиоразведка сделает предсказуемыми; при этом радиосвязь станет уязвимой для помех и ложных приказов.
- Не указана необходимость управления частотными и временны́ми позициями сигналов криптостойкой последовательностью случайных чисел.
- Отсутствует перечень криптостойких алгоритмов, а первый простой криптостойкий ГСЧ, давно разработанный для войсковых радиостанций [11], даже не упомянут.
- Рекомендованы «плохие» (создающие короткие циклы, снижающие стойкость и усложняющие выбор ключей) коды БЧХ, Голея и коды с многократным дублированием, а коды, лучше работающие в больших шумах и при заградительных помехах, более эффективно использующие ресурсы канала, проигнорированы.
- Не рассмотрены преимущества перехода от частотной модуляции (ЧМ) к фазовой.
- Не освещены вопросы сложности реализации алгоритмов, снижения энергопотребления, повышения надежности и помехоустойчивости радиостанций.

Оценки сложности алгоритмов. Для выбора алгоритмов защиты радиостанций от СРБ необходимы корректные оценки сложности их реализации по критериям микроэлектроники — количеству условных вентилей (УВ) и площади трассировок [11—16]. Оценки по объему вычислительных операций программ давно устарели и непригодны, ведь процессор также реализован на микросхеме. Один УВ — это четыре КМОП-транзистора. В трассах обычно очень высока плотность тока — основная причина старения и отказов. Узкие участки испаряются и оседают на широких. Ширину трассы и зазора выбирают из условия равной вероятности обрыва узкой трассы и замыкания широкой. Увеличение ширины и длины трасс ведет к увеличению их емкости и энергопотребления, а снижение ширины снижает надежность — важнейший параметр радиостанций. Поэтому длинные трассы, транслирующие многоразрядные числа, существенно усложняют алгоритм и снижают его надежность.

В [15] показано, что шифраторы, работающие с многоразрядными числами, в том числе те, что используются в стандартах США и Южной Кореи, чрезмерно сложны, не соответствуют современному уровню науки и много хуже шифраторов [11—14]. При отсутствии сведений по трассировкам сложность оценивают снизу — количеством УВ. Разработки алгоритмов [11—20] опирались на микроэлектронные критерии сложности.

Алгоритм, реализованный программно на процессоре, наиболее сложный, энергозатратный и ненадежный, он пригоден только на начальном этапе отладки. Программируемая логическая интегральная схема (ПЛИС) экономнее по энергопотреблению в 3—10 раз, работает быстрее, надежнее и проще почти в 10 раз. Во столько же раз возрастают эти преимущества при переходе от ПЛИС к «полузаказной» микросхеме — матричной

БИС (МБИС). Преимущества алгоритмов криптозащиты на двоичных регистрах сдвига (РС) перед многоразрядными алгоритмами известны давно — из сравнения БИС ГОСТ28147—89 и МБИС Н1515ХМ1-888 криптостойкого ГСЧ [11] с одинаковыми ключами 256 бит и проектными нормами (ПН) 5 мкм того же изготовителя («Ангстрем», Зеленоград). МБИС содержит два ГСЧ — шифратор и дешифратор, каждый около 1,5 тыс. УВ. БИС ГОСТ содержит один шифратор и около 100 тыс. УВ. Максимальная скорость БИС ГОСТ меньше на два порядка, чем у ГСЧ. Затраты энергии на один шифруемый бит у ГСЧ всего $1{,}5 \cdot 10^{-8}$ Дж, что на два порядка меньше, чем у БИС ГОСТ. Малое энергопотребление указывает на высокую надежность ГСЧ, так как мерой старения БИС является потребленная энергия. Это особенно ценно для войсковых радиостанций и радиостанций ТСО. Использованию МБИС ГСЧ вместо БИС ГОСТ препятствовала сложность программной реализации [11], нужной для замены программных средств, использующих ГОСТ.

Рекомендуемые криптостойкие алгоритмы. Преимущества ГСЧ с двоичными РС и нелинейными и нестационарными случайными функциями обратной связи (*NLFSR и Random FSR*) с двумя состояниями — пары генераторных полиномов — видны из [6 и 11]. Сначала были найдены алгоритмы ГСЧ с короткими ключами, не требующими согласований для замены использованного в ГСЧ [11] сложного в программной реализации «кроссинговера», простые и в микроэлектронной, и в программной реализации. Основной трудностью был поиск вручную «хороших» пар ГП с двумя циклами и длиной не ниже 50 бит.

Исследования вариантов ГП показали преимущества байтовых ГП с простейшей нелинейностью на двухвходовых элементах «И» и «ИЛИ». В отличие от использованного в кодеке [17] внешнего нелинейного управления для ГСЧ было выбрано внутреннее нелинейное управление от того же РС. Сначала «хорошие» пары ГП для ГСЧ с ключами 32, 39, 40, 48, 56, 64 и 128 бит [12, 13] подбирались вручную. В [13] описан не требующий лицензирования криптостойкий ГСЧ с ключом 39 бит на пяти РС ($8 \times 4 + 7$). Позже полный перебор группой ПЭВМ дал 164 пары «хороших» ГП для байтовых и восемь — для 7-разрядных РС [14], использованных в [15, 16].

Для простых и криптостойких ГСЧ в [16] рекомендованы:

1. Двоичные РС длиной от 2 до 6 байт (16—48 разрядов) с нелинейными нестационарными случайными ГП — функциями обратной связи.

2. Обновление ключа сложением по модулю 2 обновляющего бита с выбираемым разрядом РС, эквивалентное полной смене ключа.

3. Малоразрядные простые векторы управления и векторы обновления, выбирающие не более восьми адресов обновления ключа и восьми пар нестационарных ГП.

4. Интервалы обновления, много меньшие интервала единственности.

5. Неравномерное движение РС в сочетании с этими средствами.

Потоковые ГСЧ с этими алгоритмами можно использовать в качестве блоковых, что удобно для пакетной радиосвязи ТСО, подобной [22].

В [11—16] описаны алгоритмы, позволяющие получать абсолютно криптостойкие («в смысле Шеннона») ГСЧ длиной от 2 до 8 байт. Эти описания доступны для проверки и критики, так как отсутствие описания алгоритма является признаком его нестойкости [6]. Простейший из них — это ГСЧ-24 сложностью около 1,2 тыс. УВ с тремя байтовыми РС, каждый с четырьмя парами нелинейных нестационарных ГП [16]. ГСЧ-16 [15] немного сложнее, так как уменьшение длины РС требует увеличения количества выбираемых пар нелинейных нестационарных ГП.

Рекомендуемые алгоритмы помехоустойчивого кодирования. Для защиты радиоканалов от СРБ были разработаны кодеры и декодеры (кодеки) [17—21] на двоичных РС. У них лучше помехоустойчивость в области больших шумов, и они значительно проще известных, работающих с многоразрядными числами.

Для Минобороны была разработана МБИС 5503ХМ7-158 [17] с ПН 1,5 мкм (МИЭТ, Зеленоград, совместно с компанией «Вигстар»). Это рекуррентный (сверточный) высокоскоростной (до 15 Мбит/с) кодек на базе совершенного разностного множества (СРМ-133), укороченного до 99, с кодовой скоростью $R = 1/2$, с двумя ветвями кода на паре нестационарных ГП. Его сложность — 5,0 тыс. УВ, энергопотребление — около 20 мкДж/бит. Кодек устойчив к большим помехам, а его синхронизация устойчива даже при действии плотного (до 50%) пакета ошибок длиной до 25 бит. Это преимущество кодека представляет особую ценность для защиты от заградительных помех СРБ.

Для радиосетей ТСО совместно с компанией «Альтоника» были разработаны, реализованы программно и испытаны в радиоканале два коротких кодека. Первый — блоковый биортогональный код (16, 4) [18, 19] — для замены кода «Манчестер 2», часто используемого в радиосвязи с ЧМ, и второй — блоковый код (16, 8) с оптимальным синдромным декодированием (ОСД) [20, 21], работающий лучше других кодеков при негауссовских помехах, заградительных помехах СРБ и конфликтах от случайных наложений пакетов радиостанций сети. Энергетический выигрыш кодирования (ЭВК) в гауссовском канале у биортогонального кодека — около 3 дБ, у ОСД — около 4 дБ. В радиоканалах с негауссовскими помехами их ЭВК был почти 10 дБ. Кодек ОСД (16, 8) — лучший для ТСО и войсковых радиостанций.

Рекомендации по защите радиосетей ТСО. Основной угрозой для сети ТСО является имитация ложных контрольных сообщений на участке нарушения и тревожных — в удаленном месте, для отвлечения туда сил охраны. Криптостойкое кодирование сообщений в ТСО обычно не требуется, ведь смысл передаваемых в ТСО сообщений известен: до нарушения это контрольные сообщения, а после нарушения — тревожные. А вот криптостойкие ГСЧ необходимы — для установки в выделенном широкополосном канале случайных непредсказуемых частотно-временных позиций (ЧВП) сигналов. Сигналы с такими ЧВП подобны сигналам с ППРЧ, отнесенным в [4, 5, 22, 23] к широкополосным сигналам (ШПС).

В [22, 23] описана защищенная от СРБ и использующая такие ШПС радиосеть, в которой объекты охраны передают в центр охраны на случайных ЧВП короткие узкополосные (50 Гц) контрольные пакеты ЧМ-сигналов, кодированные кодом Голея (24, 12) длиной не выше 87 бит. В каждом объекте охраны 15 разрядов ГСЧ выбирают ЧВП пакетов независимо от других объектов охраны. Количество возможных ЧВП — около 30 тыс.: 32 позиции во времени при среднем интервале 3 мин и около 1000 частотных позиций в полосе частот 48 кГц. Коэффициент защиты от помех (КЗП — отношение объема выделенного пространства ШПС к объему пакета) равен 30 тыс. В сравнении с сигналами обычных ШПС сигналы с ЧВП имеют наивысшую помехоустойчи-

вость при наименьшей энергии бита и надежно защищены от СРБ. В центре охраны сигналы всей полосы рабочих частот принимают быстрым преобразованием Фурье (БПФ) двумя параллельно работающими процессорами, каждый на 500 точек в полосе 24 кГц. Возможна работа и в меньшей полосе частот. Несмотря на большую частотную нестабильность передаваемых сигналов (±4 кГц), прием каждого пакета осуществлен с незначительной избыточностью в шумовой полосе около 100 Гц. Для настройки узкой полосы приема в центре охраны работают ведомые ГСЧ и узлы определения и хранения информации о расхождениях по частоте и времени этих ГСЧ относительно ГСЧ всех объектов охраны. Расхождения обновляют по принимаемым контрольным пакетам объектов охраны.

Малая шумовая полоса обеспечивает устойчивую связь до 23 км прямой видимости при излучаемой мощности 1 мВт и энергии излучения всего 20 мкДж/бит. Мощная (50 Вт) заградительная помеха СРБ с полосой 10 кГц, перекрывавшая используемую пакетами часть общей полосы, не нарушала прием в центре охраны, если источник помех был не ближе 5 м от него [21]. Передатчик пакетов объектов охраны с мощностью 10 мВ был удален от центра охраны на 20 м. Мощность помехи превышала мощность сигнала на 50 дБ, и КЗП был близок к 100 тыс. Простота ГСЧ и других узлов передатчиков объектов охраны обеспечивает их работу без замены аккумулятора в течение года. Сложный узел БПФ работает только в центре охраны.

Независимая работа ГСЧ всех абонентов сети [21] создает опасность потери информации при наложениях пакетов объектов охраны со случайными ЧВП. Вероятность E такой потери можно оценить выражением $E = 1 - (1 - w/V)N$, где w — коэффициент влияния (от 2 до 9), зависящий от качества помехозащиты; V — возможное количество ЧВП в канале ШПС; N — количество передатчиков ТСО. Требование ТСО, чтобы вероятность задержки регистрации тревоги свыше 15 с не превышала 10^{-6}, эта сеть выполняет, если $N < 800$. При увеличении N необходимо или соответственно увеличивать интервалы передачи контрольных пакетов, или снижать их длину.

Радиосеть, рассмотренная в [22], наиболее устойчива к СРБ среди имеющихся — но она не оптимальна. В [23] была отмечена возможность ее улучшения переходом от ЧМ к более помехоустойчивой фазовой модуляции (ФМ). Способы реализации приема ФМ средствами БПФ при большой частотной нестабильности сигналов уже известны [24], но ФМ еще не реализована. Улучшить радиосеть можно увеличением скорости передачи, ослабляющим влияние нестабильности частот, а также заменой расширенного кода Голея (24, 12) более простым кодом ОСД (16, 8) с лучшей помехоустойчивостью [20, 21]. Уменьшение количества частотных позиций и увеличение количества позиций во времени не изменят КЗП. Переход к ФМ и кодеку ОСД повысят помехоустойчивость почти на 10 дБ, сократят избыточность шумовой полосы и позволят снизить энергию передачи до 2—3 мкДж/бит.

Рекомендации по защите войсковых радиостанций. Случайные ЧВП полезны и в войсковых сетях. В них, в отличие от сетей ТСО, необходима криптостойкая связь каждого абонента сети с другими, а также использование цифровой передачи речи. Поэтому для устранения влияния взаимной нестабильности частот ГСЧ всех радиостанций должны работать в едином масштабе частот и времени. Это выполняется по контрольным сигналам одной из станций сети, как в ТСО [22], или по сигналам времени навигационных систем ГЛОНАСС либо GPS, имеющим точность не хуже ±0,1 мкс. Можно также использовать таблицы ключей, а адрес формировать по номеру абонента, сеанса связи и текущему времени. Эти вопросы заслуживают особого разговора.

Возможно, в некоторых радиосетях понадобятся радиостанции с приемом всей полосы средствами БПФ. Для всех радиостанций нужны кодеки с наименьшей скоростью цифровой речи. На низких скоростях качество речи хуже, но возрастет количество ЧВП и защищенность от СРБ, что позволит при сохранении дальности связи существенно снизить излучаемые мощности. Многие кодеки речи имеют внутреннее помехоустойчивое кодирование. Интересны стандарты США MELP (Mixed Excitation Linear Prediction) на скорости 2,4; 1,2 и 0,6 кбит/с и с качеством 3,45; 3,1 и 2,7 баллов соответственно. Кодек MELP-0,6 [25] обеспечивает приемлемое качество речи при высокой защищенности от СРБ. При тех же скоростях и качестве речи возможны более простые кодеки речи, чем кодеки MELP, но их алгоритмы требуют отдельного рассмотрения.

Реализация алгоритмов на микросхемах позволит создать защищенные от СРБ простые и недорогие радиостанции. Преимущества микроэлектронных критериев сложности описаны в [11—16]. Другие варианты морально устарели, а реализация на зарубежных процессорах — опасна. Необходимые МБИС могут изготовить НПК «Технологический центр МИЭТ» (ТЦ МИЭТ), «Ангстрем» и «Микрон» (Зеленоград).

Удобный для заказчика САПР «Ковчег» и маршрут проектирования имеет ТЦ МИЭТ (*www.asic.ru*) для серий 5503 и 5507 с ПН 1,5 мкм и серии 5509 с ПН 1,0 мкм, введенных в Перечень МОП 44001.02. Библиотеки элементов этих серий содержат обширный набор цифровых элементов, а также аналоговые узлы для операционных усилителей, генераторов с управляемой частотой, смесителей, преобразователей частоты, компараторов, фазовых детекторов и других узлов тракта приема и передачи радиостанций в диапазоне до 200 МГц. Узлы с более высокой частотой могут быть внешними. Для четырех вариантов базовых матричных кристаллов (БМК) серии 5503, давно освоенной в ТЦ МИЭТ, количество УВ и информационных контактов в корпусах следующее: (576, 26), (1296, 40), (3720, 62), (5478, 60). На этих БМК можно поместить ГСЧ [15, 16], кодек помехозащиты ОСД [20, 21] вместе с их вспомогательными узлами. Возможная скорость кодирования — до 50 Мбайт/с — многократно превышает необходимую для радиостанций с цифровой передачей речи. Это позволит передавать в широкополосном канале очень короткие высокоскоростные пакеты. У серий 5503 и 5507 время задержки D-триггера менее 5,5 нс, XOR менее 3 нс. У БМК серии 5509 максимальные скорость и объем — 200 Мбайт/с и 30 тыс. УВ. Этот объем и скорости достаточны для АЦП и приемника БПФ — наиболее сложных узлов радиостанции.

«Микрон», где уже работает оборудование для изготовления МБИС с ПН 0,18 мкм и объемом до 1 млн УВ, достаточным для реализации всех узлов радиостанций, имеет международный стандартизованный маршрут VHDL, доступный, как показал опыт, грамотным инженерам и программистам. «Ангстрем» ведет отладку оборудования для выпуска МБИС с ПН до 0,13 мкм и также имеет удобный маршрут проектирования, использованный при разработке МБИС [11]. Пакет программ [26] для быстрого перехода от ПЛИС к МБИС доступен всем. Ожидаемые объемы МБИС «Микрона» и «Ангстрема» многократно превышают объемы, необходимые для всех цифровых и аналоговых узлов радиостанций,

защищенных от СРБ, кроме усилителя мощности передатчика. Опыт разработок МБИС [11, 17] показывает, что цена и энергопотребление защищенных от СРБ радиостанций будет по меньшей мере на порядок ниже, чем у описанных в [1], а надежность — на порядок выше. Поэтому главное препятствие для разработок современных радиостанций сегодня не в малых ПН, а в низкой квалификации разработчиков, неспособных работать с МБИС. Структурные схемы аналоговых узлов радиостанций на упомянутых МБИС заслуживают отдельного рассмотрения.

Заключение. Показаны надежные и простые алгоритмы защиты радиостанций и радиосетей от средств радиоборьбы, позволяющие реализовать с малой энергией бита, малым энергопотреблением и высокой надежностью криптостойкие генераторы случайных чисел, эффективное помехоустойчивое кодирование и случайную расстановку позиций сигналов по частоте (Frequency Hoping, FH) и времени (Time Hoping, TH), что в совокупности обеспечит крипто- и имитостойкость, защиту от радиоразведки, заградительных помех, ложных донесений и приказов. Эти алгоритмы предпочтительнее всех известных для программной и микроэлектронной реализации на отечественных микросхемах с проектными нормами 0,18 и 0,13 мкм. Ожидаемая сложность, а также цена, энергопотребление и надежность радиостанций с этими алгоритмами будут на два порядка ниже, чем у не защищенных от СРБ радиостанций, выпускаемых в настоящее время [1].

ЛИТЕРАТУРА

1. Связь в Вооруженных Силах Российской Федерации.— М.: Информост, 2009 (*www.army.informost.ru*).
2. **Палий А.И.** Радиоэлектронная борьба.— М.: Воениздат, 1974.
3. **Палий А.И.** Радиоэлектронная борьба.— М.: Воениздат, 1989.
4. **Борисов В.И., Зинчук А.Е., Лимарев А.Е.** и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты.— М.: Радио и связь, 2000.
5. **Борисов В.И.** Помехозащищенность систем радиосвязи. Основы теории и принципы реализации.— М.: Наука, 2009.
6. **Шнайер Б.** Прикладная криптография/Пер. с англ.— М.: Триумф, 2002.
7. **Мишин Е.Т.** и др. Как защитить каналы связи//Мир связи.— 1998.— № 10.
8. **Шемигон Н.Н.** и др. Использование средств криптографической защиты информации в сетях связи систем физической защиты ядерно-опасных объектов//Связь и автоматизация МВД России: сб. ст.— М., Информационный мост, 2004.
9. **Давыдов Ю.Л.** и др. Имитостойкие радиоканалы технических средств охраны//Транспортная безопасность и технологии.— 2007.— № 4 (33).
10. **Брауде-Золотарев Ю.М., Максимов С.А., Руднев А.Н., Соколов Е.Е.** Защита каналов технических средств охраны//Системы безопасности.— 2002.— № 5 (47).
11. **Брауде-Золотарев Ю.М.** и др. Генератор случайных чисел с высокой степенью рандомизации: науч. тр. НИИ радио, 1997.
12. **Брауде-Золотарев Ю.М.** Перспективные пути построения шифраторов//Электросвязь.— 2004.— № 3.
13. **Брауде-Золотарев Ю.М.** Потоковый шифратор с ключом 39 бит//Электросвязь.— 2004.— № 12.
14. **Брауде-Золотарев Ю.М., Давыдов Ю.Л., Качер И.Л.** Программы, генерирующие случайные числа: сб. науч. тр./ФГУП СНПО «Элерон».— М., 2008.
15. **Брауде-Золотарев Ю.М.** Возможно ли криптостойкое шифрование с ключом 16 бит?//Электросвязь.— 2009.— № 4.
16. **Брауде-Золотарев Ю.М.** Абсолютно криптостойкие и самые простые шифраторы//Электросвязь.— 2010.— № 3.
17. **Брауде-Золотарев Ю.М., Брауде-Золотарев М.Ю., Каблучкова А.А.** и др. Микросхема помехоустойчивого кодирования канала//Электросвязь.— 2002.— № 10.
18. **Брауде-Золотарев Ю.М., Грибань С.В.** Способ помехоустойчивого кодирования и декодирования//Патент РФ № 2213416, 30.12.2002.
19. **Брауде-Золотарев Ю.М., Грибань С.В., Косарев С.А.** Радиоканал с ЧМ и помехоустойчивым кодированием//Электросвязь.— 2003.— № 12.
20. **Брауде-Золотарев Ю.М., Лаврентьев М.А.** Способ помехоустойчивого кодирования и декодирования//Патент РФ № 2214678, 05.01.2003.
21. **Брауде-Золотарев Ю.М., Лаврентьев М.А.** Помехоустойчивое кодирование радиоканалов с частотной модуляцией//Радиотехника.— 2004.— № 6.
22. **Брауде-Золотарев Ю.М., Давыдов Ю.Л., Косарев С.А., Шептовецкий А.Ю.** Помехоустойчивость радиосетей технических средств охраны: матер. IV науч.-техн. конф. «Фундаментальные проблемы радиоэлектронного приборостроения» Intermatic-2005 (Москва, МИРЭА, МТУСИ, 25—28 окт. 2005 г.).
23. **Брауде-Золотарев Ю.М., Давыдов Ю.Л.** Перспективное направление развития техники связи: матер. конф. МТУСИ (февр. 2006 г.).
24. **Брауде-Золотарев Ю.М., Давыдов Ю.Л., Шептовецкий А.Ю., Косарев С.А.** Способ радиосвязи//Патент РФ № 2342785, 24.05.2008.
25. **Chamberlain M.W.** A 600 bps MELP vocoder for use on HF channels.— IEEE MILCOM, 2001.
26. **Артемов С.А.** Пакет программ для перевода проекта схемы ПЛИС в базис БМК//Современная электроника.— 2007.— № 5.

Получено 25.05.10

Не забудьте подписаться на журнал «Электросвязь»

- во всех почтовых отделениях по каталогам:
  «Агентства «Роспечать», индекс — 71107;
  «Пресса России», индекс — 41411;
  «Почта России», индекс — 61854;
- через альтернативные агентства:
  «Интер-Почта 2003», тел. (495) 788-0060;
  «Урал-Пресс», тел. (495) 789-8636;
  «Артос-Гал», тел. (495) 981-0324;
  «Глобал Пресс Логистик», тел. (499) 269-0900;
  «Орикон-М», тел. (495) 937-4959;
- в редакции журнала «Электросвязь»,
  тел. (495) 625-8436, e-mail: tim@elsv.ru;
  www.elsv.ru