«Неуправляемые» боевые роботы и беспилотники

Светлой памяти зам. Главного Конструктора АО «Камов» Николая Николаевича Емельянова, ставшего жертвой COVID-19

Алексей Галицын (a.a.galitsyn@gmail.com)

В статье рассмотрены основные требования, предъявляемые к радиочастотным (RF) технологиям для военных применений. Приведено описание российской C-UWB RF-технологии, обладающей такими качествами, как развед- и помехозащищённость, возможность использования RF-спектра на вторичной основе, принципиальная недоступность для кибератак, невосприимчивость к эффекту Доплера и эффекту «замирания радиосигнала» – технологии, перспективной для систем мобильной военной радиосвязи, систем дистанционного управления боевыми роботами, боевыми и разведывательными беспилотниками.

Статья публикуется в авторской редакции. Мнение редакции не всегда совпадает с позицией автора. Но редакция открыта для диалога и предоставляет специалистам возможность донести свои идеи до аудитории журнала. Специализированный журнал – это информационная площадка, на которой порой встречаются самые невероятные проявления творческой мысли. Орфография и пунктуация автора сохранены.

Введение

Россия – страна гигантских природных ресурсов, потерявшая свою полупроводниковую индустрию, спасти которую теперь может только чудо [1]. В ожидании этого чуда в России финансируются циклопические государственные проекты («Цифровая экономика», «Космонавтика» и т.п.) не имеющие под собой собственной реальной технологической основы в виде полупроводниковой элементной базы. При этом деньги на науку, исследования и разработки, в части полупроводниковой элементной базы, выделяются по остаточному принципу [2, 3]. Но даже эти скудные бюджетные средства зачастую вкладываются в создание оружия, смертоносного для собственной армии – например, в создание боевых радиокомплексов и систем без развед-, помехо-, крипто- и киберзащищённости.

Именно этой щекотливой теме, на примере очередного проекта, из серии «бесперспективных» [4, 5, 6, 7], уничтоженных Департаментом радиоэлектронной промышленности минпромторга РФ и посвящена настоящая статья.

Основные требования к боевым радиосистемам

Автор не берётся, не имеет права и не хочет давать оценку состоянию современных российских вооружений в плане их разведзащищённости (определения см. далее), возможности эффективного противостояния зарубежным средствам радиоэлектронной борьбы (РЭБ) и в плане защиты информации. Но одно только то, что «величайшим российским достижением» за 2019 год [8] является оснащение системой крипто-кодирования речи истребителя СУ-57, известного своей готовностью к «ярким» (в смысле его радио-яркости и очевидного отсутствия стелс-технологий) боевым полётам (в Индии), говорит о многом...

Специфика военной техники предъявляет жёсткие требования к радиоэлектронному оборудованию [9] в плане разведзащищённости, защиты информации и устойчивости против подавления каналов связи средствами РЭБ.

Теоретически расшифровать и подавить в эфире можно всё. Однако, для того чтобы подавить, надо знать, что, где, в каком диапазоне, когда и как подавлять. Эту информацию обеспечивает радиоразведка. Противостоять радиоразведке позволяет скрытность (разведзащищённость) радиоканала. Противостоять собственно подавлению радиосигнала позволяет помехоустойчивость радиосистемы.

Скрытность – способность канала сохранять в тайне факт передачи и смысл передаваемой информации. Скрытность определяется двумя факторами: разведзащищённостью и имитостойкостью.

Разведзащищённость – это энергетическая скрытность и скрытность структуры радиосигнала (факта работы канала), т.е. это скрытность радиосигнала по энергетике, частоте, времени, пространству.

Имитостойкость – это кодовая защита собственно передаваемой информации, обеспечивающая невозможность «прочитать» информацию даже после записи её на носитель.

Информация является информацией, а не «мусором» только тогда и только для того, для кого она обладает актуальностью. Однако в боевых условиях актуальность зависит от времени предоставления информации. В связи с этим, важной характеристикой имитостойкости является уровень её криптостойкости.

Криптостойкость определяется минимальным временем, которое необходимо для расшифровки передаваемой информации любыми доступными способами.

Помехоустойчивость – это способность радиосистемы обеспечивать передачу информации с заданным качеством в условиях воздействия преднамеренных помех всех видов, т.е. способность противостоять всем мерам подавления.

Двумя этими категориями (скрытность + помехоустойчивость) определяется такое более общее понятие, как *помехозащищённость*.

Таким образом, можно сделать следующий вывод: если отсутствует либо скрытность, либо помехоустойчивость, то речи о помехозащищённости не может быть априори. Такая аппаратура подавляется средствами РЭБ или огневыми средствами. Типичным примером является система «военной» радиосвязи «АЗАРТ», разработанная по заказу министерства обороны РФ зеленоградским предприятием «Ангстрем» за 1,1 млрд рублей, но впоследствии так и не принятая на вооружение.

Специфика военной радиосвязи

Независимо от способа реализации широкополосной радиосистемы её предельные скорости передачи опре-

деляются следствием из теоремы Найквиста-Шеннона-Котельникова и зависят от ширины используемого спектра радиочастот и соотношения сигнал/шум в демодуляторе (или корреляторе), согласно известной формуле:

$$C = W \log_2 (1 + P_c/P_ш),$$

где C – пропускная способность (б/с), W – ширина полосы канала (1/с), $P_c/P_ш$ – соотношение «сигнал-шум».

С точки зрения возможности применения в военной технике принципиальное значение скорее имеют изначально присущие радиочастотной технологии (т.е. способам модуляции, демодуляции и передачи радиосигнала) особые уникальные качества: помехоустойчивость, разведзащищённость, невосприимчивость к эффекту Доплера, к эффекту «замиранию» сигналов и т.п. При этом количественные показатели (в пределах теоремы Котельникова) обычно могут размениваться один на другой. Особенностью военной техники является то, что именно перечисленные ниже качественные характеристики радиочастотных технологий являются для неё более важными, чем количественные в силу следующих факторов:

- возможность интегральной реализации (это одновременно и себестоимость, и надёжность, и массогабаритные, и энергетические показатели);
- разведзащищённость (обуславливает возможность обнаружения и подавления противником в военных применениях);
- помехозащищённость (необходима для того, чтобы сама система не была выведена из строя внешними воздействиями);
- имитостойкость (важна, чтобы информация не была перехвачена);
- возможность работы на вторичной основе (это возможность работы в частотном диапазоне, уже используемом радиосистемами противника);
- возможность изменения диапазона (т.к. разные диапазоны имеют разные свойства и качество прохождения радиосигнала, разный уровень помех);
- невосприимчивость к эффекту Доплера (это важно для гиперзвуковых, аэрокосмических объектов и СВЧ-систем);
- невосприимчивость к эффекту «замирания сигнала» (важна для ослабления эффекта интерференции радиосигналов, переотражённых от плоских морских и наземных поверхностей);
- термостабильность эксплуатационных параметров (традиционное требование к военной технике);
- возможность, благодаря разведзащищённости, создания военных систем принципиально нового типа с новыми свойствами и новыми возможностями (это подавляющее преимущество в боевых действиях);
- технологичность, т.е. простота и дешевизна (что позволит устранить преступное дублирование радиокомплексов и систем в боевых изделиях).

Отсутствие у радиочастотной технологии хотя бы одного из этих качеств делает военную технику потенциально уязвимой, а саму технологию – принципиально непригодной для создания военной техники, тем более, если речь идёт о дорогостоящей интегральной реализации такой радиочастотной технологии.

Тем не менее, сплошь и рядом, разработчики стараются использовать свой гражданский опыт, а Заказчики, в определённых ситуациях – не обращать внимания на подобные «мелочи» даже при наличии альтернатив, отвечающих реальным боевым требованиям. Например, пресловутые радиосредства «Азарт», использующие метод быстрой перестройки рабочей частоты (ППРЧ), нельзя признать разведзащищёнными, что делает их в прямом смысле смертоносным для собственной Армии оружием и непригодными для создания новых современных систем вооружений, принципиальным требованием к которым (в эпоху высокоточного оружия) становится разведзащищённость.

В самом деле, для приёма «быстрой ППРЧ», используемой в системе «Азарт», сигналы в точке приёма на каждой из используемых частот должны иметь уровень радиосигнала принципиально выше уровня радио-фона местности. Это полностью демаскирует не только постоянно «светящуюся» базовую станцию, превращающуюся в идеальную мишень, но и каждый радиопередатчик, которому смертельно опасно работать постоянно, тогда как повышение активности работы передатчиков – это предвестник начала боевой операции. Принимая эти сигналы двумя узконаправленными антеннами, ориентированными в одном и том же направлении, а затем перемножая их, т.е. фактически в каждый конкретный момент времени умножая «скачущий» узкополосный радиосигнал сам на себя (только для совпадающих по частоте сигналов этих двух каналов!) и, тем самым перенося результат перемножения совпадающих в данный момент по частоте сигналов в область нулевых частот и накапливая результат на нулевой частоте, мы будем видеть и пеленговать «быструю ППРЧ» каждого такого передатчика на поле боя не хуже, чем это делали в кино немецкие пеленгаторы времён Великой Отечественной Войны.

Кроме того, попытки повышать помехоустойчивость в системе «Азарт», передавая каждый бит информации последовательно на нескольких разных частотах – занятие само по себе неблагодарное: чем больше частот - тем ниже, причём кратно, скорость передачи информации.

Ну а такая, принципиально присущая этой системе связи уязвимость, как её полное поражение элементарной сканирующей помехой, делает эту систему связи принципиально непригодной для боевых применений. Впрочем, польза от этой радиосистемы очевидна – в свободное от боев время бойцы могут с её помощью слушать передачи Центрального телевидения, рискуя жизнью.

С учётом вышеизложенного, нам хотелось бы рассказать широкой публике о российской C-UWB (Controlled Ultra Wide Band) RF-технологии беспроводной связи [10, 11, 12]. В аббревиатуре C-UWB буква «C» – от слова controlled, т.е. управляемый (полоса, диапазон, скорость), а UWB (Ultra Wide Band) – сверхширокополосный. Термин «сверхширокополосный» здесь применён по чисто историческим причинам, поскольку в момент создания технологии, т.е. ещё до «изобретения» американцами соответствующей классификации, в России все технологии с нестационарной несущей относились к категории сверхширокополосных, т.е. к UWB.

C-UWB RF-технология отвечает всем, перечисленным выше, военным требованиям и вполне могла бы стать базовой технологией для создания развед- и помехозащищённых, недоступных для кибератак, сетей радиосвязи, систем дистанционного управления российскими боевыми роботами и беспилотниками, а также стать основой для других боевых систем принципиально нового типа.

Краткое описание и особенности C-UWB RF-технологии

C-UWB RF-технология использует радиочастотный ресурс на вторичной основе, обеспечивает высочайшую

развед- и помехозащищённость, а также отсутствие необходимости централизованного частотного планирования радио-пространства (какое может быть частотное планирование среди вражеских радиосистем?), не требует организации жёсткой централизованной синхронизации при создании и работе радиосистем массового обслуживания. C-UWB RF-технология представляет собой развитие широкополосных шумоподобных технологий в соответствии с современными требованиями технологичности производства, интегральной реализации, минимизации себестоимости, существенного улучшения технических характеристик и конкурентоспособности.

Идея технологии заключается в нетрадиционном переходе от традиционных для широкополосных (с кодовым разделением каналов) систем связи, методов модуляции, основанных на изменении (в различных сочетаниях) амплитуды, частоты и фазы высокочастотного сигнала к некогерентной (энергетической) обработке широкополосных шумоподобных радиосигналов [4, 7, 10, 11, 12], которая допускает нелинейную обработку сигналов (новая, нелинейная радиотехника). То есть, если в традиционных широкополосных системах для расширения спектра используется модуляция амплитуды, фазы или частоты, либо и того, и другого, и третьего, вместе взятых, то в технологии C-UWB передача информации основана на модуляции мощности сложного шумоподобного сигнала и переходе к его некогерентной обработке. Это позволяет избавиться от промежуточных частот и гетеродинирования в классическом понимании этих терминов, а вместе с этим и от всех проблем, присущих супергетеродинным системам (зеркальный канал, интермодуляция, фликкер-эффект, утечка сигнала, фазовые шумы гетеродина, необходимость высокой линейности радио-тракта) и соответствующих элементов, которые весьма трудно интегрировать на кристалле.

Всё это позволяет качественно расширить динамический диапазон обрабатываемых сигналов, кардинально снижает требования к линейности и схемотехнике радиочастотного тракта, технологическим процессам производства, позволяет резко сократить аппаратурные затраты на его реализацию. Предлагаемый подход позволяет добиться предельного упрощения аналоговой части, а вопросы корреляционной обработки радиосигнала перенести на «низкую частоту», вследствие чего кардинально упрощается построение радиосистем на кристалле, причём открывается возможность создания на кристалле широкополосных цифровых приёмников даже без использования сложных, дорогостоящих и медленных цифровых сигнальных процессоров.

Особенностью C-UWB-технологии являются способы формирования сигнала в передатчике и его обработки в приёмнике. Рассмотрим основные принципы реализации C-UWB-системы.

Формирование радиосигнала

В качестве широкополосной несущей в рамках C-UWB RF-технологии может быть использован шумоподобный сигнал любого уровня сложности, любого вида и происхождения. Это может быть любой шум: «белый», «бледно-розовый», хаотический, «шум эфира» и т.п., то есть любой высокочастотный широкополосный шумовой сигнал. Выбором именно шумовой формы сигнала несущей, при соответствующих способах модуляции и синхронизации, обеспечивается главное – разведзащищённость радиосигнала в эфире и, соответственно, двойное назначение технологии.

В простейшем случае, можно взять случайный дискретно-частотно-модулированный сигнал (без «перескока» фаз) или линейно-частотно-модулированный (ЛЧМ) сигнал, имеющий полосовой спектр и перемножить его на высокочастотную псевдослучайную кодовую последовательность (ПСП) с периодом повторения в несколько лет, спектр которой имеет вид $(\sin(x)/x)^2$, что дополнительно расширяет полосу частот результирующего радиосигнала. В итоге будет сформирован результирующий сигнал, спектр которого, являясь результатом перемножения полосового спектра и спектра вида $(\sin(x)/x)^2$, теряет характерный колоколообразный вид и принимает более равномерную, практически прямоугольную форму.

Таким образом структура C-UWB-сигнала полностью скрывается, представляя собой совершенно случайный (шумовой) сигнал с плоской формой спектра и без периодического повторения мощности на любой конкретной частоте, как в основной полосе, так и на кратных гармониках (в отличие от систем CDMA – используемой в системе «Акведук»). В системах CDMA (и аналогичных) сигнал синхронизации, а также чётные гармоники широкополосного информационного сигнала являются узкополосными. Импульсы синхронизации полностью демаскируют CDMA-изделия. Пропустив CDMA-сигнал через нелинейный элемент и усилитель-ограничитель, легко выделить вторую гармонику и получить собственно информацию, «зашифрованную» известными методами. Основной спектр CDMA – линейчатый, что позволяет констатировать наличие факта передачи цифровой информации даже на слух и подавить его средствами РЭБ или огневыми средствами.

Передача информации в рамках предлагаемой технологии может быть реализована как на основе стационарной, так и на основе нестационарной несущей (это программируемая функция).

В случае *стационарной несущей* высокочастотный широкополосный шумовой сигнал модулируют в соответствии с передаваемой информацией,

используя в качестве модулируемого параметра мощность радиочастотного сигнала, а в качестве модулирующего параметра – частотный параметр с частотой модуляции мощности $F_{mod} << (F_1-F_0)$, где (F_1-F_0) – частотная полоса приёмопередачи. Полученный сигнал *умножают аналоговым способом* на обеспечивающие кодовое разделение каналов псевдослучайные кодовые последовательности, формируемые идентичными в передатчике и приёмнике комплементарной пары, генераторами псевдослучайных кодовых последовательностей с использованием принципа кодового разделения каналов и принципа самосинхронизации.

Для *нестационарной несущей* широкополосный высокочастотный шумовой сигнал аналоговым способом, но по правилам логического умножения – посредством аналогового ключа, умножают на обеспечивающую кодовое разделение каналов псевдослучайную последовательность импульсов, которую генерируют генераторами псевдослучайных кодовых последовательностей и модулируют данные сигналы по мощности с частотой

модуляции мощности $F_{mod} << (F_1-F_0)$, где (F_1-F_0) – частотная полоса приёмопередачи. В качестве модулирующих параметров используются позиционный или временной параметры изменения положения (или, соответственно, длительности) передаваемых импульсов относительно моментов их изменения, ожидаемых в отсутствие модуляции.

При этом в приёмниках демодуляцию промодулированного по мощности полезного сигнала, полученного после выделения огибающей, для получения собственно информации, осуществляют анализируя корреляционным способом уровень рассогласования модулирующих параметров принимаемых импульсов и аналогичных параметров немодулированных последовательностей импульсов, специально для этого синхронно генерируемых в приёмнике.

Обработка радиосигнала. Синхронизация

Общая структурная схема C-UWB приёмника достаточно подробно описана в [4, 7, 10, 11]. При использовании в военных целях, её наиболее существенным отличием будет программируемая многорежимная система синхронизации, которая будет обеспечивать целый ряд как более простых (примитивных), так и более сложных (вплоть до крипто-функций) способов синхронизации помимо базового.

Базовый процесс синхронизации заключается в умножении широкополосной несущей (в зависимости от её типа – см. ранее) на обеспечивающие кодовое разделение каналов циклические псевдослучайные кодовые последовательности (ПСП), формируемые идентичными в передатчике и приёмнике, генераторами ПСП, стартующими с идентичных стартовых адресов (кодов, известных только взаимодействующим передатчику и приёмнику) для формирования, на основе этих кодов, каналов связи с использованием общеизвестного принципа *кодового разделения каналов* и принципа *самосинхронизации*.

Принцип самосинхронизации основан на сдвиге в каждом новом цикле на такт во времени, формируемых на основе этих адресов, циклически повторяющихся адресных псевдослучайных кодовых последовательностей ограниченной длины в приёмнике, до, констатируемого корреляционным методом, момента совпадения во времени этих циклических последовательностей с точно такими же, циклически повторяющимися, адресными ПСП передатчика и запуска с этого момента системы автоподстройки частоты синхронизации приёмника. Тем самым обеспечивается идентичность и синхронность генерации ПСП в передатчике и приёмнике взаимодействующих корреспондентов, необходимые для обеспечения кодового разделения каналов и осуществления демодуляции.

Обеспечение помехозащищённости и других важных для военной техники качеств C-UWB RF-технологии

В плане обеспечения помехозащищённости C-UWB RF-технология обеспечивает 4 уровня защиты радиоканала со следующими особенностями.

Разведзащищённость (*1-й уровень защиты радиоканала*). Источник C-UWB радиоизлучения (абонентский комплект) излучает широкополосный спектр радиосигнала с очень низкой радио-яркостью благодаря обеспечению низкой спектральной плотности мощности формируемого радиосигнала, который на расстоянии 100 м от передатчика имеет уровень ниже уровня радио-фона местности. Структура радиочастотного сигнала, используемого в рамках предлагаемой технологии достаточно подробно описана выше. Посылки радиоимпульсов, используемые в предлагаемой C-UWB RF-технологии имеют контролируемую ширину и прецизионное, формируемое электронными схемами, наполнение спектра шумоподобного сигнала (сложный сигнал), обеспечивая абсолютную управляемость параметрами сигнала: диапазон, ширина полосы и любую, наперёд заданную (вплоть до криптографического уровня), сложность структуры сигнала. При плоской форме спектра и полном отсутствии периодического повторения мощности как на любой конкретной частоте в полосе приёма, так и на кратных гармониках, это обеспечивает идеальную разведзащищённость создаваемых на её основе радиосистем.

Помехоустойчивость (*2-й уровень защиты радиоканала*). Если сравнивать помехоустойчивость предлагаемой C-UWB RF-технологии с помехоустойчивостью существующих «шумоподобных» военных систем, таких, как, например система «Акведук», то описываемая технология при сравнимых показателях по помехоустойчивости в отношении широкополосных (полосовых) помех, будет иметь как минимум ещё и реальную разведзащищённость, и на два порядка более высокую помехозащищённость в отношении мощных узкополосных помех (включая сканирующие помехи), являющихся наиболее вероятными и наиболее опасными для систем радиосвязи подобного типа. Достигается это благодаря запатентованным способам помехоподавления, практически не применимым для других радиочастотных технологий.

Классические шумоподобные системы за счёт базы радиосигнала обеспечивают наивысшую помехозащищённость по сравнению с любыми другими классами систем радиосвязи. Тем не менее, попадание помех любого вида в приёмный радиотракт не только существенно ухудшает соотношение сигнал/шум и соответственно ухудшает все количественные характеристики систем шумоподобной радиосвязи (в соответствии с теоремой Шеннона-Котельникова), но легко может привести к превышению предельного соотношения сигнал/шум и полному выводу из строя даже шумоподобной системы связи. Поскольку широкополосные шумоподобные системы по своей природе (в этом суть механизма корреляции) восприимчивы не ко всем широкополосным помехам, а лишь к помехам с очень сходной структурой сигнала, да ещё и синхронизированным с работой приёмника, то такие специальные помехи действительно большой мощности, в большой полосе и на большом пространстве – исключительная редкость, даже в военное время. Наиболее реальный и опасный тип помех, критически влияющий на работоспособность систем широкополосной связи, это случайные мощные помехи от близко расположенных мощных узкополосных станций и преднамеренные сканирующие помехи, попавшие в полосу пропускания приёмника.

Для борьбы с мощными узкополосными помехами нами предложен ряд новых способов помехоподавления [12, 13]. Фантастическая простота, и деше-

визна этих способов заключается в удалении мощных узкополосных помех (включая сканирующие) из широкополосного спектра сигнала посредством обычной фильтрации. Причём, фильтрация осуществляется без применения сложнейших алгоритмов, да и вообще методов цифровой обработки сигналов (бессильных, кстати, в отношении сканирующих помех), или каких-либо сложных адаптивных или режекторных фильтров (тем более бессильных по отношению к сканирующим помехам) – что, казалось бы, невозможно.

Поясним как это осуществляется. На вход принимающего устройства поступает сигнал, равный векторной сумме напряжений полезного сигнала $U_{сиг}$ и узкополосной помехи $U_{узк}$. Этот смешанный сигнал поступает на вход полосового фильтра с полосой пропускания частот приёмника (F_1,F_2). Затем отфильтрованный сигнал, предварительно усиленный малошумящим усилителем, разделяют на два сигнала. При этом первый сигнал получают после усиления отфильтрованного в указанной полосе частот сигнала и ограничения его по амплитуде в усилителе-ограничителе. При прохождении сигнала с помехой через усилитель-ограничитель помеха подавит полезный сигнал и на его выходе остаётся лишь сигнал помехи нормированной величины $U_{узк}/|U_{узк}|$. В качестве второго сигнала используют упомянутый отфильтрованный сигнал или отфильтрованный сигнал, усиленный линейным усилителем. Полученные два сигнала подают на соответствующие входы блока умножения, который перемножает их. При этом в умножителе сигнал нормированной величины $U_{узк}/|U_{узк}|$, поступающий из канала с ограничением начинает играть роль сигнала гетеродина для широкополосного сигнала в линейном канале В результате такого перемножения сигнала помехи «самого на себя» на выходе умножителя сигнал помехи переносится в область нулевых частот и вырезается обычным низкочастотным фильтром, а спектр полезного информационного сигнала при этом автоматически конвертируется в область низких частот и используется для последующей «энергетической» корреляционной обработки на видеочастоте. При этом, имея в одном из каналов усиление-ограничение, мы не умножаем милливольты одного канала на милливольты другого и не получаем в результате микровольты, а обеспечиваем нормальную (без потери усиления) работу умножителя и вполне приемлемый по амплитуде сигнал на выходе. То есть в данной системе отсутствуют потери усиления на преобразованиях радиочастотного сигнала, что существенно повышает качество, упрощает схемотехнику и улучшает стабильность работы радиосистемы в целом.

Главным в этом методе является то, что информация закладывается в изменение мощности сигнала и передаётся во всей полосе частот передачи (F_1, F_2), а при переносе спектра во время обработки в приёмнике переносится вместе со спектром. Определяющим фактором для данного способа подавления узкополосной помехи является частотная полоса спектра изменения мощности помехи, а не частотная полоса, занимаемая помехой в эфире. Это позволяет, не зная реального месторасположения помехи в спектре сигнала, «вырезать» из принимаемого широкополосного сигнала даже сканирующие (с любой скоростью и в пределах всей полосы пропускания приёмника) мощнейшие узкополосные помехи (с собственной шириной полосы до 20% от полосы пропускания приёмника). Причём (что уже действительно парадоксально), чем мощней (опасней) помеха, тем стабильнее работает система, а мощные узкополосные помехи, у которых модуляция мощности отсутствует вообще, не будут являться помехами для данной системы радиосвязи.

Как показали испытания, проведённые в ряде ведущих российских научных институтов, рассмотренные выше способы обеспечивают практически «бесплатное» повышение помехозащищённости широкополосной шумоподобной системы радиосвязи более чем на два порядка по сравнению с уровнем помехоподавления в системах CDMA («Акведук»), ZigBee и т.п.

Следует заметить, что описанные выше методы повышения помехозащищённости применимы только для систем на основе широкополосных радиосигналов, передача информации у которых построена на модуляции мощности широкополосного сигнала, и могут осуществляться процессорными методами цифровой обработки сигналов. Но, как говорится, «если не видно разницы – зачем платить больше»?

Криптозащита структуры радиосигнала (3-й, нетрадиционный, уровень защиты радиоканала). C-UWB RF-технология представляет собой классическую криптографическую систему, но впервые реализованную не на уровне передачи информации, а на уровне формирования структуры радиочастотного сигнала [14], в которой генерация и корреляционная обработка сложных шумоподобных радиочастотных сигналов осуществляется на основе обмена между вступающими в контакт корреспондентами открытой ключевой информацией. Ключевая информация формируется с использованием любых криптографических алгоритмов (например, метода Диффи-Хелмана), обеспечивающих практически любую их криптографическую стойкость. Весь вопрос уровня криптозащиты созданного выделенного виртуального радиоканала между изделиями будет заключаться в следующем:

- какого типа шифроблок (алгоритм) будет использоваться для перекодирования открытой ключевой информации и получения идентичных закрытых кодов, необходимых для работы генераторов псевдослучайных кодовых последовательностей подсистемы каналообразования;
- на основе обмена какой открытой ключевой информацией этим шифроблоком будет формироваться закрытая ключевая информация (сеансовые ключи) и в каком порядке, или по каким признакам (динамически) она будет синхронно изменяться в приёмнике и передатчике в процессе сеанса связи;
- какие именно методы генерации псевдослучайных кодовых последовательностей будут использоваться.

Такая система обеспечивает абсолютную информационную безопасность создаваемых беспроводных решений, поскольку вместо открытой (широковещательной) среды в эфире для каждого соединения создаётся по сути выделенный канал связи, представляющий собой криптосистему реального времени (подключение к которому и физическое прослушивании которого попросту невозможно). Это делает принципиально невозможным не только считывание, запись и последующую расшифровку информации, но и традиционные атаки, основанные на анализе и изменении сетевого трафика, являющиеся наиболее массовым видом атак в широковещательных сетях.

Для того чтобы обеспечить качество и эффективность процесса кодирова-

ния было развито новейшее революционное направление криптографии – теория дискретной стохастической криптографии. Данная теория позволяет создавать динамические цифровые системы, называемые стохастическими системами дискретного времени. Оборудование, создаваемое на основе методов предложенной дискретной стохастической криптографии, обеспечивает при той же криптографической стойкости десятикратное уменьшение аппаратных затрат и, соответственно, стоимости, что чрезвычайно важно в интегральных радиочастотных системах. Обе инновации (стохастическая криптография и новый радиочастотный канал) находятся вне конкуренции на рынке специальной аппаратуры связи. Аппаратная реализация этих методов обеспечит уникальные характеристики создаваемого оборудования и позволит решить неразрешённые в настоящее время задачи, касающиеся безопасного беспроводного доступа и передачи конфиденциальной информации.

Криптозащита собственно информации (4-й традиционный уровень защиты). При построении более развитой системы связи с выходом в глобальные сети, безопасность информации уже будет зависеть не только от уровня защищённости самого радиоканала, но и от угроз, действующих во внешней сети. Однако, в этом случае решение задачи обеспечения криптографической защиты собственно информации, которая будет циркулировать в такой гибридной системе, по чисто экономическим причинам, ни по своей постановке, ни по способам решения, ничем не должна отличаться от решений, используемых в существующих военных и гражданских телекоммуникационных сетях (по крайней мере до «точки входа» в радиоканал). Классическим способом решения этой проблемы является организация VPN-соединения.

Эффект Доплера

Большинство RF-систем дальнего радиуса действия, относящихся к военному сектору применений, предполагают работу с мобильными объектами, поэтому, помимо высокого уровня разведзащищённости, информационной безопасности и помехозащищённости требуют некоторых весьма специфических качеств, связанных с мобильностью объектов. Это, в первую очередь – требование невосприимчивости к воздействию эффекта Доплера, характерного для высокоскоростных (гиперзвуковых) мобильных объектов и сверхвысокочастотных каналов передачи. Сокращение влияния эффекта Доплера на несколько порядков по сравнению с любыми другими технологиями, в рамках C-UWB технологии осуществляется благодаря использованию некогерентной (энергетической) обработки шумоподобных сигналов и отказа от частотно-фазовых методов модуляции. Действительно, в предлагаемой C-UWB технологии весь приём и вся обработка высокочастотного сигнала, включая помехоподавление и переход на низкую частоту (для демодуляции) осуществляется без использования сигналов и каких-либо конкретных частот, вырабатываемых внутренними схемами приёмника (как, например, это имеет место в супергетеродинной аппаратуре). Потому каких-либо смещений фаз и изменения частот принимаемого высокочастотного сигнала, рассогласования фильтров, обусловленного доплеровским смещением частоты принимаемого сверхвысокочастотного сигнала, оборудованием C-UWB-приёмника наблюдаться не будет. Следовательно, при обработке высокочастотного сигнала не будет необходимости ни в специальной автоподстройке прецизионных внутренних генераторов частот и в подстройке фильтров, необходимых для компенсации воздействия эффекта Доплера на сам радиочастотный тракт. Процесс демодуляции (т.е. непосредственно процесс выделения информационной составляющей сигнала) осуществляется корреляционным способом уже на низкой частоте, без использования каких-либо свойств фазы и частоты самого высокочастотного сигнала. Вполне очевидно, что проявление влияния эффекта Доплера на низкочастотный сигнал, при его демодуляции, на несколько порядков слабее, чем его влияние на фазу и частоту высокочастотного радиосигнала. К тому же сам радиочастотный сигнал является широкополосным, а каждый бит передаётся сразу во всей полосе частот. Поэтому смещение всего сигнала из-за эффекта Доплера по полосе не окажет серьёзного влияния на информационную компоненту (определяемую модуляцией мощности на видеочастоте) и даже не потребует подстройки грубых полосовых фильтров, которыми задаётся полоса пропускании приёмника. Эти особенности C-UWB-технологии действительно позволят избавиться от всей той сложнейшей техники, которая традиционно используется в узкополосных радиочастотных супергетеродинных системах для компенсации эффекта Доплера и которую весьма трудно интегрировать на кристалле. Всё это позволяет на порядки ослабить влияние эффекта Доплера на C-UWB-радиосистемы и кардинально упрощает интегральную реализацию высокоскоростных (гиперзвуковых) и сверхвысокочастотных мобильных военных систем, наиболее критичных к данному эффекту. В связи с этим можно утверждать, что C-UWB-технология ещё скажет своё слово в создании авиационных, спутниковых, гиперзвуковых ракетных и, связанных с ними, наземных комплексов и систем.

Эффект «замирания» сигнала

Одним из важных достоинств широкополосных и сверхширокополосных радиосистем, основанных на корреляционных принципах обработки радиосигнала, является снижение влияния эффекта интерференции прямо распространяющегося сигнала с сигналами, отражёнными от плоских морских и наземных поверхностей. Переотражения и последующая интерференция радиоволн – это бич всех систем радиосвязи, за исключением широкополосных и сверхширокополосных шумоподобных, в которых явление «замирания» выражено не так сильно. Это связано с тем, что получить сложение прямого и отражённого сигналов строго в противофазе, причём сразу на всех конкретных частотах (имеющих разную длину волны, частоту и периоды колебаний) в пределах всей полосы пропускания приёмника – дело столь же непростое, как и получить отражённый сигнал, строго синхронный работе коррелятора по основному сигналу. В большинстве шумоподобных систем отражённый сигнал просто поступает в коррелятор с запозданием и воспринимается им как случайная помеха, никак не воздействующая на демодуляцию прямого сигнала. Поэтому сверхширокополосные шумоподобные системы весьма слабо подвержены воздействию эффекта «замирания» сигнала, что было практически подтверждено нами во время реальных испытаний C-UWB RF-технологии на море, с уча-

стием институтов ВМФ МО РФ Санкт-Петербурга.

Вместе с тем, в широкополосных системах с корреляционной обработкой шумоподобного радиосигнала, наоборот, существует возможность использовать переотражённые сигналы для повышения достоверности принимаемого сигнала, т.е. повышения качества радиосвязи. Для этого используется структура, называемая Rake-приёмник, в котором, помимо приёма прямого сигнала, параллельно работают ещё несколько настроенных на приём отражённых сигналов каналов приёма с собственными корреляторами. Результирующая информация берётся либо с приёмника, принимающего самый мощный сигнал, либо с нескольких каналов на мажоритарной основе в пределах одного или нескольких информационных пакетов. Конечно, это уже более сложная техника, которая, кстати, может быть эффективно реализована с использованием C-UWB RF-технологии.

Термостабильность

C-UWB RF-технология обеспечивает на порядок более высокую термостабильность изделий, т.к. температурные изменения характеристик радиоэлементов оказывают на порядок меньшее воздействие на энергетические компоненты сигнала (основной информационный параметр предлагаемых C-UWB радиосистем) по сравнению с их воздействием на традиционные фазу и частоту. Кроме того, C-UWB RF-технология являет собой тот редкий образец радиосистемы, в которой отсутствуют и потери амплитуды при переносе (преобразовании) полосы спектра полезного широкополосного сигнала в процессе его обработки. Это делает радиосистему чрезвычайно устойчивой не только в плане изменения уровня и условий прохождения радиосигнала, но и в плане термостабильности её рабочих характеристик.

Дополнительным фактором, повышающим термостабильность системы, является полное отсутствие взаимодействия высокочастотного полезного сигнала в процессе его обработки (на фазовом уровне) с ВЧ-сигналами, формируемыми собственными схемами приёмника (такими, например, как сигнал гетеродина и т.п.) вплоть до стадии демодуляции, которая осуществляется корреляционным способом на низкой частоте. Таким образом, помимо дополнительного повышения термостабильности, достигается на порядок меньшая чувствительность ВЧ-тракта приёмника и к эффекту Доплера.

Связь, беспилотники, боевые роботы и компьютерные войны

Для обеспечения эффективного управления войсками на современном театре военных действий, управления подразделениями, беспилотниками и боевыми роботами, осуществления опознавания и целеуказания в ходе реальных боевых действий, необходима не трансляция (с губительной радиояркостью) гигабайт «потрясающего вида баталий», и, соответственно, не гигабитные скорости передачи информации, а наличие всего трёх эффективно действующих компонент:

1. разведзащищённой, помехозащищённой, не восприимчивой к эффектам Доплера и «замирания сигнала» (для работы на аэромобильных гиперзвуковых объектах) и термостабильной радиосвязи;
2. знания точного расположения и динамики перемещений подразделений и отдельных мобильных объектов на местности – отслеживания всеми доступными средствами карты их расположения на местности в реальном масштабе времени;
3. эффективного решения задачи опознавания «свой/чужой» и сопряжения результатов с системами управления боем (выдача азимутов боевым единицам и целеуказания системам наведения их поражающих средств) в динамике боя, на уровне и с использованием в процессе ведения боя, систем искусственного интеллекта.

Беспилотники

Для российской C-UWB RF-технологии беспроводной связи организовать разведзащищённую, помехоустойчивую и, впервые, принципиально недоступную для кибератак систему радиосвязи для дистанционного управления боевыми ударными и разведывательными беспилотниками, или, например, боевыми роботами – самая тривиальная задача, которая могла бы быть решена ещё 20 лет тому назад. Вместе с тем, именно эта задача для страны сейчас оказалась нерешённой, первоочередной и наиболее жизненно-важной, даже по сравнению со всеми теми «глобальными» системами, описание которых приведено ниже. Ведь ослеплять и расстреливать беспилотники, даже гиперзвуковые (на встречном курсе) [5], на основании излучаемого ими радиосигнала, это самое простое дело для любого, даже самого слабого, противника. С традиционными средствами связи в системах дистанционного управления, целое поколение российских беспилотников может оказаться стаей «белых ворон-камикадзе».

Кроме того, для новых типов беспилотных летательных аппаратов (БПЛА), например, при создании БПЛА для ВМФ, возникают совершенно новые проблемы, которые требуется решать:

- возможность вертикального взлёта-посадки;
- автономное позиционирование относительно посадочной платформы;
- вмешательство систем позиционирования и посадки в контур управления и их непосредственного воздействия на специальные элементы управления летательным аппаратом;
- обеспечение прецизионного локального позиционирования (в условиях качки);
- обеспечение гарантированной надёжности работы каналов радиосвязи дистанционного управления во всех режимах («взлёт» – «полёт» – «посадка»), т.е. обеспечение все той же развед- и помехозащищённости, невозможности перехвата управления, невосприимчивости к эффекту Доплера, эффекту «замирания» радиосигнала и т.п.

Обычная радиосвязь здесь, к сожалению, не подходит. Со всеми этими задачами C-UWB RF-технология может справиться блестяще, совершенно бесплатно обеспечивая при этом ещё и автономное локальное позиционирование летательных аппаратов относительно корабля.

Результаты наших исследований показывают, что в качестве БПЛА ВМФ РФ должны быть созданы совершенно новые [15] летательные аппараты, например, для незаметной для радаров маловысотной доставки торпед «Шквал» непосредственно к цели. Ведь подводных лодок в акватории может и не быть, надводный корабль на торпедный выстрел, авианосец к себе не подпустит, а реально потопить его можно только из-под воды, пробив ему борт ниже ватерлинии. Совершенно другие БПЛА [16] нужны для ретрансляции сигналов загоризонтного управления беспилотниками, а также для превращения обычных малогабаритных РЛС в РЛС загоризонтного обнаружения. По корабельным мало-

габаритным загоризонтным РЛС мы уже отстаём даже от Китая. При этом элементы физического управления такими беспилотниками, обязательно, в процессе разработки самого беспилотника и комплекса «корабль – беспилотник», должны быть интегрированы непосредственно с системами локального позиционирования и посадки. Аппаратура выполнения полётного задания может быть независимой и автономной, в пределах ТТХ БПЛА.

Наземная связь

В наземных войсках, на основе C-UWB RF-технологии могли бы быть созданы разведзащищённые сети наземной радиосвязи повышенной живучести. Причём живучесть сетей радиосвязи, создаваемых на основе C-UWB RF-технологии, будет обеспечиваться не только и не столько за счёт развед- и помехозащищённости, сколько благодаря принципиально новой архитектуре этой сети связи [17], обеспечивающей возможность организации автоматической динамической маршрутизации радиотрафика и работы множества дешёвых ($100–500) ретрансляторов сети в режиме динамического «горячего» резерва (вместо легкоуязвимой и дорогостоящей сети центральных базовых станций). В отличие от традиционных радиосистем с централизованной синхронизацией, в радиосети нового поколения предлагается асинхронное взаимодействие абонентов. Это взаимодействие будет осуществляться как непосредственно между собой (на микро-мощностях), так и через простейшие ретрансляторы с интегральной конвертацией радиочастотного спектра, что оказывается возможным благодаря запатентованному способу устранения из спектра широкополосного сигнала мощных узкополосных помех [12, 13] и многократного расширения динамического диапазона ретрансляторов.

Архитектура новой сети предполагает (избыточное) оснащение дешёвыми ($500) собственными ретрансляторами каждого воинского подразделения и независимую работу всех ретрансляторов в режиме динамического горячего резерва, что делает каждое подразделение ответственным за «свою» связь и связь «с соседями». Такие системы связи также гарантируют разведзащищённое соединение каждому бойцу в любое время и в любых условиях, т.к. разделение каналов будет осуществляться исключительно по кодовому принципу на физически предельно-возможном уровне обработки радиосигналов. Такой подход исключает как массовые отказы в соединении, возникающие в сотовых сетях из-за ограниченности числа каналов, так и катастрофические отказы сети, из-за вывода из строя или подавления дорогостоящих и легко уязвимых, традиционных базовых станций, работающих на принципах централизованной организации синхронного взаимодействия абонентов. Новая архитектура позволяет кардинально повысить живучесть мобильной военной радиосети в целом. Выбор маршрута связного трафика между корреспондентами осуществляется аппаратурой самих корреспондентов, причём автоматически, корреляционным способом, посредством выбора на физическом уровне обработки сигнала наилучшего из радиосигналов, приходящих через разные ретрансляторы. Это может быть любой один (или даже пара разных: для канала приёма и канала передачи) из множества параллельно работающих ретрансляторов, наиболее подходящих, с точки зрения условий прохождения радиосигнала и даже напрямую, без участия последних.

Бортовые радиокомплексы

С появлением развед- и помехозащищённой C-UWB RF-технологии у России могли бы открыться возможности для создания высокоэффективных тактических систем наземных и аэрокосмических вооружений не только в плане их «механической части», но и в части их электронной и информационной составляющей, т.е. создания нового «интеллектуального» тактического оружия высочайшей эффективности и качества, способного противостоять ушедшему на экспорт «механическому». Такое оружие, созданное на основе C-UWB RTLS-систем (Real-time Locating System – систем локального позиционирования в реальном масштабе времени) будет использовать уже существующие, причём весьма эффективные боевые радары и системы наведения поражающих средств и при этом обеспечит отказ от использования абсолютных координат (и, соответственно, глобальной спутниковой навигации). Это позволит оружию работать в собственной, «боевой» системе координат, предельно удобной для визуального восприятия и оценки реальной обстановки пилотом или оператором и приемлемой для систем наведения различного рода вооружений. При этом система обеспечит и решение задач целеуказания и проблемы «свой-чужой» [18] в естественном для операторов визуальном (графическом) режиме, независимо от времени суток. Причём эти возможности доступны не только непосредственно на наземном поле боя, но и в рамках систем «земля-воздух», «воздух-земля», а также систем «воздух-воздух» (особенно гиперзвуковых), т.к. C-UWB-технология невосприимчива к эффекту Доплера.

Такая система может быть организована следующим образом. Разведзащищённая мобильная RTLS-радиосеть, выполненная на базе C-UWB-технологии и размещённая, например, на танках, вертолётах, самолётах, беспилотниках или боевых роботах, позволяет автоматически определять их расстояния друг до друга. Затем триангуляционным методом рассчитываются координаты, в реальном времени формируется карта расположения танков на местности (самолётов в пространстве). Полученная картина передаётся на звено истребителей, где бортовые компьютеры автоматически её масштабируют, сверят с реальной картиной расположения объектов на местности, полученной бортовым радаром или даже видеокамерой, отделят «своих» от «чужих» и распределят цели. После этого пилотам (или операторам беспилотников) останется только выводить машины на оптимально отобранные каждому бортовым компьютером цели и запускать ракеты. Такой боевой искусственный интеллект обеспечит подавляющее преимущество в боевых действиях, особенно в современной «войне без фронтов» и в стратегических сражениях, где будут задействованы тысячи единиц техники, внешне практически неотличимой для всех противоборствующих сторон. До появления радиосвязи, обладающей таким качеством, как разведзащищённость, подобного рода системы не могли быть созданы принципиально, поскольку открытый радиосигнал, не требуя никаких радаров, выдавал бы их «с головой».

Помимо кратного увеличения количества каналов связи, одновременно работающих на поле боя (необходимого для реализации принципа «всегда на связи») и ограничиваемого только физикой Шеннона-Котельникова,

предлагаемая технология позволит решить проблему оперативно-тактического взаимодействия разных родов войск (благодаря использованию для всех родов войск общей или специально выделенной для межвидового взаимодействия частотной полосы и разделения родов не по частотному, а по кодовому принципу). Поэтому данная технология (при полной унификации технических средств!) может послужить инструментом для организации эффективного ситуационного межвидового взаимодействия всех боевых подразделений, участвующих в конкретной операции (в т.ч. взаимодействия подразделений непосредственно с вооружением, т.е. с вертолётами огневой поддержки, корабельными системами, артиллерией, ракетными, танковыми подразделениями и т.п.), что в условиях современного боя является жизненно необходимым.

Историческая справка

Во времена предыдущих руководителей отрасли описанные в статье системы не могли быть созданы принципиально, поскольку не существовало [11, 12, 19] соответствующей радиочастотной технологии. Технологии, которая обеспечила бы одновременно и помехозащищённость, т.е. эффективное функционирование всей системы в зонах активных преднамеренных радиопомех, и полную информационную безопасность, и, что самое главное – разведзащищённость, чтобы сами мобильные объекты не стали отличными мишенями и идеальным источником информации для радиопеленгационного оборудования и систем наведения поражающих средств противника. Не существовало технологии, которая при этом была бы ещё и невосприимчивой к эффекту Доплера (работала на гиперзвуке), эффекту «замирания» радиосигнала и обеспечивала бы высочайший уровень термостабильности. Не существовало технологии, которая, благодаря использованию, описанных выше, методов группового управления и опознавания целей, позволяла бы реализовать решение всех этих трёх задач (связь, опознавание, целеуказание) в едином радиочастотном и процессорном блоках и избавиться от многократного и бессмысленного дублирования радиоаппаратуры в боевых комплексах и системах.

Заключение

Создание описанных в статье систем связи, навигации, авиаразведки и боевого управления давно могло бы качественно повысить боеспособность Российской Армии и сократить стоимость её переоснащения современным оружием. Но, как показывает многолетняя практика, не аффилированным компаниям, инновационные оборонные проекты реализовывать в стране было просто невозможно [19, 20].

К счастью, теперь все эти вопросы полностью находятся в зоне персональной ответственности первого вице-премьера – настоящего специалиста в области электроники, Героя России, доктора технических наук, профессора Юрия Ивановича Борисова. Поэтому нет сомнений, что теперь «чудо», наконец-то, произойдёт [21]: страна возродит полупроводниковую индустрию и столь важная для государства задача, как безопасная военная радиосвязь, безопасное управление боевыми роботами, боевыми разведывательными и ударными беспилотниками, будет успешно решена.

Литература

1. Википедия – чудо. Режим доступа: https://ru.wikipedia.org/wiki/%D0%A7%D1%83%D0%B4%D0%BE.
2. Борисов назвал Россию отставшей от США по инвестициям в радиоэлектронику. РБК 2020: https://www.rbc.ru/society/15/04/2020/5e9741bc9a79477045117a32.
3. *Пешкова И.* Российская микроэлектроника требует 800 миллиардов. CNEWS. 2019: https://www.cnews.ru/news/top/2020-09-07_rossijskaya_mikroelektronika.
4. *Галицын А. А.* IoT-радиопроцессор с криптокодированием структуры радиосигнала. Современная электроника. 2019. №7.
5. *Галицын А. А., Рождественский А. Е., Рождественский Д. Б.* Системы управления с «предвидением». Современная электроника. 2019. №9.
6. *Егоров Е. В., Егоров В. К., Галицын А. А.* Явление и последствия волноводно-резонансного распространения и взаимодействия радиационных потоков. Современная электроника. 2019. №10.
7. *Галицын А.А.* Туманный интернет вещей. Современная электроника. 2020.№3.
8. На Су-57 испытывается новейшая криптозащищённая система связи. ТАСС. 2019: https://tass.ru/armiya-i-opk/6897150.
9. *Алексенко А. Г., Галицын А. А., Иванников А. Д.* Проектирование радиоэлектронной аппаратуры на микропроцессорах. Радио и связь. 1984.
10. *Галицын А. А.* Интегральный радиопроцессор – перспективная техническая основа Интернета вещей. Датчики и Системы. 2015. №1.
11. *Галицын А. А.* Технология C-UWB – основа для информационно-телекоммуникационных систем нового поколения. Электроника: наука, технология, бизнес. 2008. №5.
12. *Бобков М. Н., Галицын А. А., Калугин В. В.* Патент на изобретение №2232464 RU. Способ подавления узкополосной помехи в системе широкополосной связи. 2002.
13. *Bobkov M., Galitsyn A., Kalugin V.* US Patent № 7.250.541 B2. Method for suppressing narrowband noise in a wideband communication system. 2002.
14. *Галицына О. И.* Патент на изобретение №2557451 RU «Способ динамической адресации корреспондентов мобильной радиосети и устройство для его реализации». 2012.
15. В. Путин и С. Шойгу в Севастополе. Россия -1. Вести. 2020: https://www.ontvtime.ru/index.php?option=com_content&task=view_record&id=1450&start_record=2020-01-12-22-50.
16. Автожир. Википедия: https://ru.wikipedia.org/wiki/Автожир.
17. *Галицын А. А.* Патент на изобретение № 2463736 RU «Способ групповой обработки сигналов внутризоновых корреспондентов базовых станций радиотелефонной сети с кодовым разделением каналов и устройство для его реализации». 2009.
18. *Галицын А. А.* Патент на изобретение №2507538 «Способ группового опознавания объектов («свой-чужой») и обеспечения целеуказания на основе беспроводной системы позиционирования в реальном масштабе времени и интеллектуальных радаров». 2009.
19. *Галицын А. А.* Технология широкополосной высокозащищённой радиосвязи (C-UWB): что лежит «под сукном» у российских чиновников. Техносфера. 2008. №1.
20. *Степанов Д.* Заместитель главы департамента радиоэлектронной промышленности Минпромторга Антон Исаев задержан по подозрению в мошенничестве. CNEWS.2020: https://www.cnews.ru/news/top/2020-09-11_siloviki_zaderzhali_zamglavy.
21. *Николаев А.* Кадры, которые не решают ничего. Интернет-журнал «Интересант». 2020: https://www.interessant.ru/politics/kadry-kotoryie-nie-rieshai-1.