

Том I, с. 20–28

УДК: 621.396 + 537.87

АКТУАЛЬНЫЕ НАУЧНЫЕ И ПРИКЛАДНЫЕ ПРОБЛЕМЫ МЕТЕОРНОГО РАСПРОСТРАНЕНИЯ РАДИОВОЛН

А. В. Карпов, А. И. Сулимов, О. Н. Шерстюков

Казанский федеральный университет, 420008, г. Казань, ул. Кремлёвская, 18

E-mail: arkadi.karpov@kpfu.ru, asulimo@gmail.com, oleg.shertyukov@kpfu.ru

Аннотация. В статье кратко описываются основные вехи радиометеорных исследований в Казанском университете от момента организации первых радарных наблюдений радиоотражений от метеорных следов до создания уникальных радиосистем, реализующих сверхточную (наносекундную) синхронизацию стандартов частоты по радиоканалу. Описываются последние достижения в области разработки метеорных систем генерации и распределения секретных ключей шифрования для создания особо защищенных коммуникаций. Рассматриваются актуальные научные и прикладные проблемы по исследованию не взаимности канала связи при метеорном распространении радиоволн.

Ключевые слова: метеорное распространение радиоволн, метеорное радиоотражение, радар, радиосвязь, не взаимный канал, синхронизация, шкала времени, ключ шифрования

MODERN SCIENTIFIC AND APPLIED PROBLEMS OF METEOR SCATTER RADIO PROPAGATION

A. V. Karpov, A. I. Sulimov, O. N. Shertyukov

Abstract. The paper briefly outlines major key points of radio meteor research at Kazan University starting from the first radar observations of meteor radio reflections to development of unique radio systems for high-precision (nanosecond) distant synchronization of time scales. Recent achievements in designing of promising meteor systems for generation and secure distribution of secret encryption keys are considered. Main scientific and applied problems in studying nonreciprocal properties of radio wave propagation in meteor burst communications are discussed.

Keywords: meteor burst communications; meteor radio reflection; radar; nonreciprocal radio wave propagation; synchronization; time scale; encryption key

Введение

Метеорные следы представляют собой естественные ионизации, образующиеся на высотах от 80 до 120 км в результате пролета и сгорания твердых частиц космического происхождения. Их способность отражать радиоволны метрового диапазона на протяжении многих лет использовалась для создания систем радиосвязи, телеметрии и навигации. Несмотря на низкую пропускную способность (не более нескольких килобит в секунду) метеорный радиоканал обладает рядом преимуществ, среди которых можно отметить устойчивость к погодным и ионосферным возмущениям. Это позволяет с успехом использовать метеорные радиосистемы в тех приложениях, где прочие виды радиосвязи не обеспечивают надежного канала (например, в полярных регионах), что поддерживает интерес к исследованию метеорных явлений.

С середины 1950-х годов исследования по метеорному распространению радиоволн активно проводились в США, Канаде, Великобритании, Австралии и Египте. Отечественные исследования метеорных явлений в атмосфере Земли активно проводились на базе Казанского университета, а также Харьковского национального университета радиоэлектроники (г. Харьков, Украина). Практически с самого их основания отличительной особенностью отечественных научных школ являлась ориентация на решение прикладных задач, развитие которых происходило по двум

основным направлениям: радиосвязь и передача точного времени в целях синхронизации сети наземных пунктов связи. В начале XXI века наметилось новое перспективное направление, связанное с использованием стохастических свойств метеорного радиоканала для порождения случайных шифрующих последовательностей.

В данной статье даётся краткий очерк об основных исторических достижениях казанской научной школы радиометеорных исследований. Накопленная база знаний и на сегодняшний день позволяет ставить и успешно решать актуальные научные и прикладные проблемы метеорного распространения радиоволн, связанные с разработкой адаптивных систем синхронизации шкал времени и особо защищенных систем связи.

Основные этапы метеорных исследований в Казанском университете

Первые в России радарные наблюдения метеоров были проведены в Казанском университете ещё в далеком 1956 году. Изначально применялись весьма простые методы наблюдений, обладавшие низкой точностью и информативностью. К 1960 году в Казани был введён в строй первый российский специализированный метеорный радар со сканирующей по азимуту антенной. На основании пяти лет непрерывных радарных наблюдений впервые в мире были построены карты распределения плотности падающего потока метеоров по небесной сфере, которые обеспечили надёжную базу для прогнозирования характеристик систем метеорной связи и для оценки метеорной опасности космических аппаратов.

Накопив значительную научную и экспериментальную базу знаний, казанские специалисты смогли разработать ряд передовых систем связи. Так, в 1967 году была введена в эксплуатацию радиолиния метеорной телеграфной связи Красноярск-Норильск. Впервые в мире была реализована идея пространственной адаптации метеорной системы связи к местам повышенной концентрации метеорных следов. Была введена в строй первая в мире метеорная система связи непрерывного действия (на перекрывающихся метеорных отражениях), много лет эксплуатировавшаяся на радиолинии Салехард-Тюмень. Обе указанные радиосистемы обеспечивали надёжную связь даже в периоды сильных магнитных аномалий. Возможность обеспечения надёжной передачи данных через метеорный канал с заданной регулярностью заложили фундамент для последующей реализации систем передачи точного времени.

Первые работы по дистанционному сличению шкал времени через метеорный радиоканал были выполнены в США [1]. При этом использовались традиционные импульсные методы измерения задержки сигнала в характерной для метеорной связи полосе частот порядка нескольких десятков килогерц. Достигнутая точность синхронизации лежала в диапазоне нескольких микросекунд, вследствие чего дальнейшие исследования в этой области были свернуты и перенесены в область спутниковых систем. Тем не менее, в 1967 году подобные эксперименты были повторены в России. Расширение полосы частот до нескольких мегагерц и увеличение мощности передатчиков позволили снизить погрешность до уровня 0,5 мкс. Дальнейшее развитие систем синхронизации шло по пути внедрения фазовых методов.

Разработанный в Казанском университете многочастотный импульсно-фазовый метод позволил снизить погрешность передачи времени до потенциальной для метеорного радиоканала величины в десятые доли наносекунды. В 1979 году на трассе С.-Петербург–Казань было впервые экспериментально показано, что взаимность условий метеорного распространения радиоволн для значительной части метеорных радиоотражений (МРО) сохраняется с точностью до фазы несущей частоты. Проведенные в 1992 году с использованием водородного стандарта частоты на радиолинии Менделеево-Казань эксперименты позволили достичь субнаносекундной точности сведения шкал времени [2]. Хотя точность сличения по однозначному измерению фазы на единичном метеорном радиоотражении в среднем не превосходила 14–18 нс, дальнейшая оптимальная фильтрация выборки измерений, накопленных на интервале времени до трех часов, позволила снизить погрешность синхронизации до рекордного уровня 0,3 нс, который ограничивался лишь нестабильностью канала вследствие сноса метеорных следов ионосферными ветрами.

Метеорная генерация ключей шифрования

Направленные свойства метеорного радиораспространения традиционно обеспечивали закрытость и высокую устойчивость метеорного канала к внешним радиоизлучениям. На протяжении нескольких десятилетий это обстоятельство с успехом позволяло строить системы специального назначения [3]. Опираясь на достижения в области сверхточной синхронизации двух пунктов связи, исследователи из Казанского университета выдвинули принципиально новую идею о конструктивном использовании стохастических свойств метеорного канала. Непредсказуемость возникновения метеорных вспышек во времени и пространстве, вызывающая прерывистость канала связи и неизбежно усложняющая процедуру организации сеанса, всегда считалась исключительно деструктивным свойством. Однако наличие общей и независимой от внешних источников синхронизации позволило двум корреспондентам A и B с высокой точностью, не доступной иным пунктам связи, отслеживать случайные вариации в канале. После оцифровки таких синхронных наблюдений на обеих сторонах канала создаются две природно-случайные двоичные последовательности K_A и K_B . При этом, в силу приближенной взаимности метеорного канала, можно утверждать, что эти последовательности совпадают: $K_A = K_B$.

Именно так родилась идея использовать природно-случайные вариации характеристик канала связи для порождения на обоих концах радиолинии идентичных случайных последовательностей. Одним из перспективных направлений является использование таких последовательностей в симметричных криптосистемах, например, для зашифрования информации в A с помощью K_A и последующего её расшифрования в B с помощью K_B (либо наоборот). Данное направление, названное «метеорной криптографией» [4–7] (по аналогии с квантовым распределением ключей или «квантовой криптографией» [8]), стимулировало новый виток интереса к физическим особенностям метеорного распространения радиоволн.

Дальнейшие исследования показали, что для безопасного распределения ключей шифрования радиоканал должен обладать тремя физическими свойствами: 1) случайностью – для порождения непредсказуемых ключей; 2) взаимностью – для порождения идентичных копий ключа в пунктах A и B ; 3) пространственной избирательностью – резкая пространственная декорреляция метеорных регистраций должна препятствовать созданию третьей копии ключа в любом другом пункте связи C . В связи с этим, зародились четыре новых направления исследований: 1) анализ статистических характеристик МРО; 2) исследование условий и причин нарушения взаимности метеорного канала; 3) исследование пространственной коррелированности характеристик МРО при разнесенном радиоприеме; 4) оценка производительности систем метеорной генерации ключей и разработка способов её повышения. Каждое из указанных направлений ставит новые научные проблемы, решение которых базируется на накопленном в Казанском университете научно-техническом опыте по прикладному использованию радиометеорных явлений.

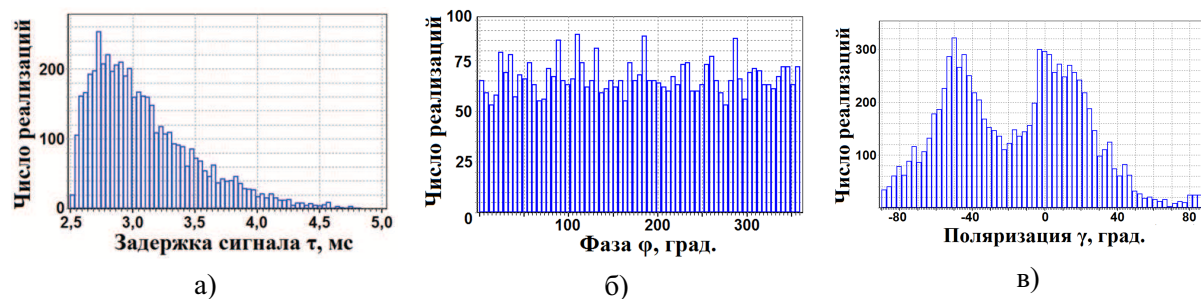


Рис. 1. Типичное распределение вероятностей случайных параметров метеорных радиоотражений: а) задержки сигнала τ ; б) фазы несущей φ ; в) поляризации γ .

В работе [7] была обоснована стохастичность процессов метеорного распространения радиоволн, и в частности, доказана непредсказуемость траектории распространения сигнала. Случайность пути распространения наряду со случайностью процесса рассеяния радиоволн на метеорных следах приводят к принципиальной непредсказуемости временной задержки τ , фазы φ и

поляризации γ [9] принятого сигнала. На рис. 1 представлены характерные гистограммы распределения вероятностей указанных параметров сигнала, полученные путем имитационного моделирования радиолинии Москва-Казань с типичной для метеорной связи протяженностью 720 км. Хотя все три параметра обладают высокой энтропией и обеспечивают удовлетворительную взаимность канала, лишь фаза φ в полной мере обеспечивает выполнение третьего условия, то есть резкую пространственную декорреляцию. Важным преимуществом фазы также является и равномерность распределения, благоприятствующая генерации шифрующих последовательностей. Таким образом, именно фазовые методы были положены в основу формирования симметричных ключей шифрования.

Методика формирования двух экземпляров секретного ключа в пунктах A и B описана в [4] и сводится к обмену серией зондирующих сигналов. Передатчик (например, пункт A) излучает детерминированный радиосигнал с неслучайной фазой φ_0 , а метеорный канал осуществляет её стохастическую модуляцию, придавая регистрируемым при приеме реализациям равномерное распределение на $\varphi_B \in [-\pi; \pi]$. В силу большого интервала корреляции, с каждого МРО снимается лишь одно измерение φ_B . При оцифровке каждому измерению φ_B сопоставляется двоичный код длиной m битов, где m – разрядность кодера измерений. Конкатенация результатов кодирования всей имеющейся выборки измерений позволяет сформировать экземпляр ключа K_B с требуемой битовой длиной. Аналогичные операции выполняются и в пункте A при обработке измерений фазы φ_A – для формирования экземпляра ключа K_A . Однако, в силу инструментальных и шумовых погрешностей, а также неабсолютной взаимности метеорного канала, измерения φ_A и φ_B случайно отклоняются друг от друга, что может порождать асимметричные («ошибочные») биты в экземплярах K_A и K_B . Для их устранения используется аппарат контрольных сумм в виде кодов обнаружения и коррекции битовых ошибок. При сверке экземпляров ошибочные блоки ключевой последовательности отбраковываются, что вызывает некоторые потери в объеме итогового ключа. В общем случае, повышение разрядности кодера m ускоряет генерацию ключевой последовательности, но увеличивает долю ошибочных битов и снижает эффективность η процедуры сверки экземпляров. Анализ показал, что существует оптимальная разрядность кодера m^* , которая одновременно обеспечивает как высокую скорость создания ключевой последовательности, так и приемлемую частоту возникновения ошибочных битов. Использование оптимальной разрядности позволяет достичь максимальной скорости генерации ключа: $R_K \sim \eta m \rightarrow \max$.

При оценке скорости генерации ключа предполагалось, что в канале действуют два ограничивающих фактора: неабсолютная взаимность канала и ограниченная численность метеорных регистраций [10]. Имитационное моделирование характеристик регистрируемых МРО выполнялось на основе численного решения строгой задачи дифракции радиоволн на метеорном следе [11]. Учитывался полный комплекс поляризационных явлений при метеорном распространении радиоволн, включая случайную ориентацию метеорного следа в пространстве, вращение плоскости поляризации радиоволн за счёт эффекта Фарадея, а также поляризационные характеристики антенн и электрические свойства подстилающей поверхности. В качестве тестовой использовалась типичная метеорная радиолиния Москва-Казань со следующими параметрами:

- эпоха моделирования: июнь, 6:00 по местному времени;
- несущая частота: $f = 50$ МГц;
- мощность передатчика: $P_T = 2000$ Вт;
- порог регистрации: $U_0 = 0,5$ мкВ (минус 185 дБ);
- тип антенн: пятиэлементный «волновой канал» горизонтальной поляризации;
- требуемое отношение (сигнал/шум): $\text{SNR} = 5$ дБ, 20 дБ и 30 дБ;
- минимальная генерируемая масса метеороидов: $m_0 = 310^{-5}$ г;
- объём выборки: $N = 20000$ метеорных радиоотражений.

На рис. 2 представлены оценки средней скорости генерации ключевой последовательности при различной разрядности кодера измерений m , смоделированные для трёх уровней (сигнал/шум). Средняя численность МРО составила 417 регистраций в час. Высокий уровень взаимности канала ограничил оптимальную разрядность кодирования m^* величиной 2 бит/изм.

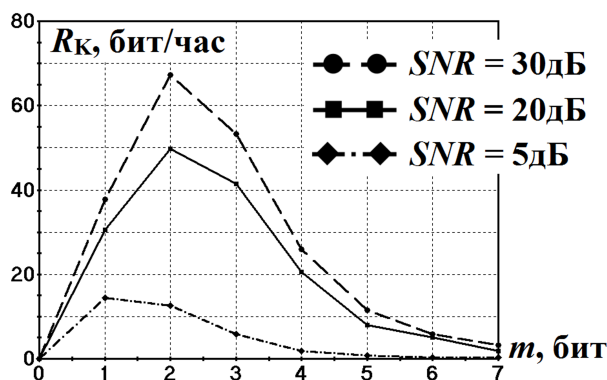


Рис. 2. Скорость генерации ключевой последовательности.

С ростом шумовой погрешности оптимальная разрядность упала до минимально возможного значения 1 бит/изм. Попытка установить более высокую разрядность приводила к росту доли ошибочных битов, что снижало эффективность η сверки симметрии экземпляров K_A и K_B . При оптимальной разрядности доля асимметричных битов составила: 7,9% (при $SNR = 30$ дБ, $m^* = 2$), 8,6% (при $SNR = 20$ дБ, $m^* = 2$) и 8,0% (при $SNR = 5$ дБ, $m^* = 1$). Для устранения ошибочных битов использовались циклические избыточные коды стандарта CRC-16-CCITT. Из-за достаточно большого количества ошибочных битов, достигнутая эффективность сверки η не превысила 10%, а максимальная скорость генерации ключа R_K ограничилась 70 бит/час.

Астрономическая природа обуславливает глубокий суточный ход характеристик канала. На рис. 3 представлены результаты моделирования суточных зависимостей, полученные при $SNR = 20$ дБ. На рис. 3а показана суточная зависимость часовой численности метеорных регистраций на тестовой радиолинии, а на рис. 3б – соответствующей скорости генерации ключевой последовательности. Из рис. 3 видно, что скорость генерации R_K в подавляющей степени определяется регистрируемой численностью МРО, то есть энергетическим потенциалом радиолинии. Скорость генерации ключа варьировалась от 22,7 бит/час (для 15 часов по м.в.) до 78,1 бит/час (для 3 часов по м.в.) при среднесуточном значении 46,2 бит/час. Максимальная суточная выработка ключевой последовательности составила 1154 бит/сутки при остаточной (после сверки симметрии) вероятности битовой ошибки не более $2,810^{-6}$.

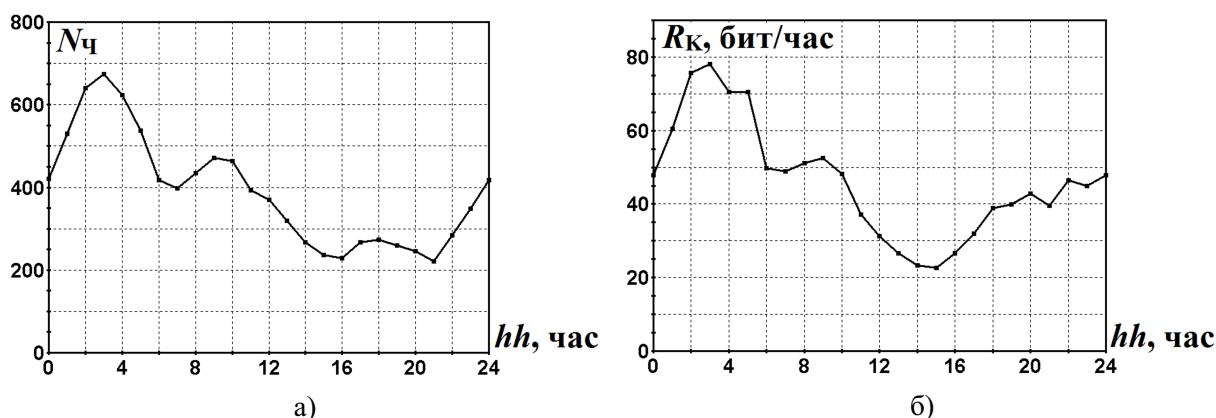


Рис. 3. Суточная зависимость производительности системы метеорной генерации ключей шифрования: а) численность метеорных регистраций; б) скорость генерации ключа.

Исследование пространственной корреляции метеорных радиотражений

Одной из актуальных проблем обоснования безопасности метеорных систем генерации ключей шифрования является исследование пространственной коррелированности МРО при разне-

сенном приеме. Физически, угроза частичного перехвата генерируемых ключей сохраняется до тех пор, пока существует возможность совместного наблюдения МРО в двух разнесенных пунктах приема. Поэтому на первом этапе необходимо оценить размах и конфигурацию области совместного наблюдения МРО, которая индивидуальна для каждой радиолинии и зависит от параметров связной аппаратуры и времени организации сеанса связи.

Вследствие случайности канала, соответствующие экспериментальные исследования являются сложными и дорогостоящими. Известные исследования дают крайне скудные либо противоречивые данные по корреляции условий наблюдения метеоров при разнесениях менее 50 км. По этой причине, предварительные теоретические оценки были выполнены с использованием уточненной модели метеорного радиоканала [11]. Рассматривались две взаимно ортогональные тестовые радиолинии разной протяженности. Первая радиолиния протяженностью 1013 км являлась примером длинной радиотрассы, а вторая радиолиния имела вдвое меньшую длину 466 км и занимала промежуточное положение между метеорными трассами малой и средней протяженности. В пункте A размещался передатчик зондирующих сигналов, а на другой стороне канала размещалась пара разнесенных точек наблюдения радиоотражений – пункты B и C .

Результаты моделирования представлены на рис. 4, где изображен вид сверху на тестовые радиолинии с пунктами A , B и C лежащими в плоскости XOY . Эллиптические контуры ограничивают область пространства в окрестности пункта B , в пределах которой относительная длительность совместной регистрации МРО в пунктах B и C не ниже заданного уровня, отображенного оттенками серого цвета. Эти контуры, по существу, являются контурами равной вероятности для совместного наблюдения метеоров в точках B и C . На рис. 4 показаны только пять таких контуров для относительной доли времени существования совместного канала, равной 5%; 10%; 30%; 50% и 80%, соответственно. Несмотря на быстрый спад вероятности одновременной регистрации МРО в двух разнесенных пунктах, потенциальная область совместного наблюдения имеет сопоставимые с длиной радиолинии L размеры.

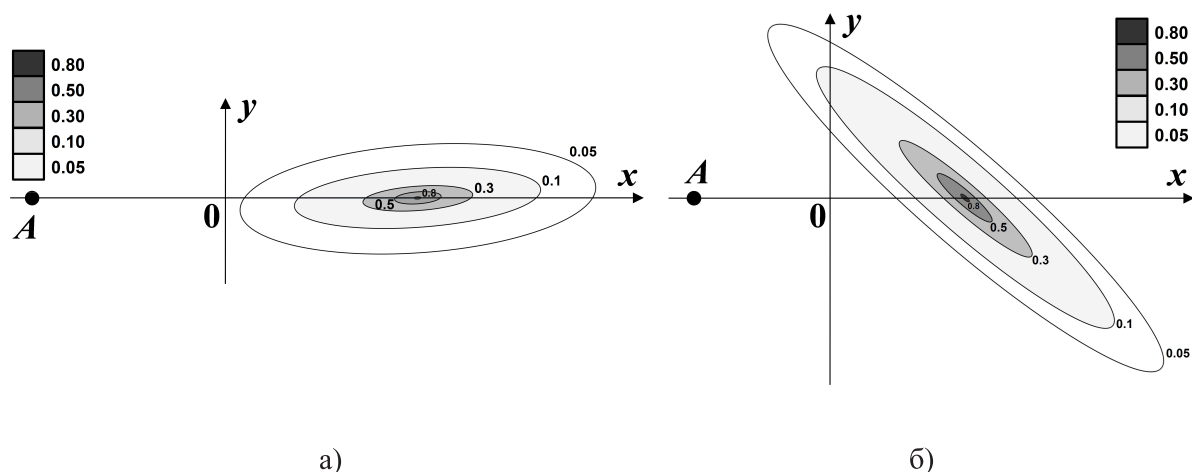


Рис. 4. Области совместного наблюдения метеоров на тестовых радиолиниях: а) радиотрасса длиной 1013 км; б) радиотрасса длиной 466 км.

Ориентация областей совместного наблюдения МРО определяется текущей локализацией «горячих зон» повышенной концентрации регистрируемых метеорных следов на заданной радиолинии. В соответствии с этим, конфигурация этих областей подвержена значительной суточно-сезонной изменчивости, определяемой закономерностью изменения локализации «горячих зон». Для длинной радиолинии главная ось области совместного наблюдения была почти сонаправлена с осью радиолинии, отклоняясь от неё всего на 4° . Однако, для более короткой радиолинии отклонение составило 41° , что значительно меняет традиционную геометрию разнесенного приема. Представленные на рис. 4 результаты моделирования хорошо согласуются с экспериментальными данными [12], особенно в случае «поперечного» разнесения точек регистрации.

Несмотря на полученный размах областей совместного наблюдения метеоров (см. рис. 4), фаза радиосигнала проявляет быстрые пространственные осцилляции, обусловленные, в том числе, дифракционными эффектами рассеяния радиоволн на метеорных следах. Это должно значительно ускорить спад корреляции измерений при разнесении приемных пунктов *B* и *C*. Синтез профилей пространственной корреляции фазы МРО для радиолиний различной протяженности является предметом будущих исследований.

Анализ не взаимных свойств метеорного радиоканала

Благодаря низкой высоте отражения радиосигнала от метеорных следов (80-120 км) анизотропными свойствами ионосферы обычно пренебрегают и считают канал взаимным. Хотя такое упрощение оправдано при решении большинства традиционных задач радиосвязи, оно оказывается несостоятельным при разработке более продвинутых систем, предназначенных для наносекундной синхронизации шкал времени и, в особенности, для генерации ключей шифрования, так как последнее требует взаимности канала не в среднем, а в частности и для каждого метеора. В указанных системах проблема неабсолютной взаимности канала выходит на первый план, приобретая статус одного из принципиальных факторов, ограничивающих производительность. Таким образом, исследование причин и факторов проявления не взаимных свойств метеорного канала является крайне важным направлением, позволяющим разработать надежные методы оперативной идентификации и отбраковки регистраций с неприемлемо высокой не взаимностью.

Проявление не взаимных свойств канала в метеорных системах связи зафиксировано в ряде экспериментов [13], но недостаточная точность аппаратуры и малый объём качественных данных затруднили количественную оценку данного эффекта. Возможности теоретических исследований долгое время ограничивались приближенным характером классической теории отражения радиоволн от метеорных следов, основанной на рассмотрении двух предельных частных случаев взаимодействия радиоволн с метеорными следами низкой и высокой ионизации. При этом распространение сигнала описывалось как симметричное в обе стороны зеркальное отражение от следа, без учета поляризации падающей радиоволны и дополнительного скачка фазы при рассеянии. Иными словами, классическая модель не предоставляла инструментов для моделирования не взаимности канала.

Для исследования не взаимных свойств канала была разработана уточненная модель распространения сигнала [11], основанная на строгом численном решении задачи дифракции радиоволн на метеорном следе. Уже первые результаты показали, что хорошее согласие классической и уточненной моделей наблюдается только в диапазоне невысоких ионизаций, примерно в середине области недоуплотнённых следов (линейная электронная плотность $\alpha \sim 5 \cdot 10^{13}$ эл/м). По мере разрушения следа его электронная плотность убывает, и сходимость обеих моделей друг к другу улучшается. Большие отличия возможны в области высоких электронных плотностей ($\alpha > 7.5 \cdot 10^{14}$ эл/м), где классическая модель переуплотнённого следа обычно завышает амплитуду радиоотражения. Как правило, в начале существования метеорного следа в нём происходят активные динамические процессы (такие как плазменный резонанс и расширение), которые приводят к высокой не стабильности характеристик следа и сопровождаются высокой не взаимностью канала. К окончанию радиоотражений динамические процессы в метеорном следе прекращаются, его рассеивающие характеристики стабилизируются, и уровень не взаимности канала обычно снижается [14].

Работа [11] явилась первым систематическим исследованием не взаимности канала в системах метеорной связи, в которой представлены её количественные оценки для конкретных тестовых радиолиний. Моделировались четыре радиолинии протяженностью от 434 км до 1464 км, все пункты связи которых имели близкие широты в окрестности $66,5^\circ$ с.ш. Столь высокие широты были выбраны специально, чтобы проследить влияние ионосферных возмущений на степень не взаимности метеорного канала. Тем не менее, результаты моделирования показали, что характерные для полярных широт аномальные возмущения ионосферы влияют на уровень не взаимности метеорного канала в гораздо меньшей степени, чем регулярный суточный ход его

характеристик. Это в очередной раз подтвердило тезис об устойчивости систем метеорной связи к ионосферным возмущениям [3].

Дальнейшие результаты выявили существование группы радиоотражений, проявляющих крайне высокий уровень фазовой невязимности канала $\Delta\varphi(t)$ в течение всей регистрации. Такие МРО были условно названы «невязимными», поскольку средняя за время их регистрации абсолютная фазовая невязимность не опускалась ниже 90° . В зависимости от параметров радиолинии и аппаратуры, доля невязимных МРО может изменяться от 0% до 50%, а средний уровень фазовой невязимности при этом может варьироваться от 1° до 88° .

Установлено, что наиболее значимым фактором невязимности канала является высотное распределение метеоров, поскольку оно напрямую определяет суммарное электронное содержание атмосферы на пути сигнала из пункта связи до отражающей точки метеора, то есть степень проявления поляризационной асимметрии канала вследствие эффекта Фарадея. Почти столь же значимым оказался частотный фактор. Повышение частоты с 30 МГц до 70 МГц более чем в 7 уменьшило долю невязимных радиоотражений и почти в 4 раза снизило уровень фазовой невязимности канала. Негативным эффектом явилось почти 20-кратное снижение рабочего цикла радиолинии (с 3,24% до 0,18%). Следовательно, выигрыш в качестве канала связи влечет за собой значительные потери в длительности его существования.

Проведённые исследования показали, что невязимность метеорного канала является комплексным явлением, имеющим сложную многофакторную природу. Некорректный выбор параметров связной аппаратуры может привести к многократному повышению уровня невязимности канала. Однако объяснение всех закономерностей и прогнозирование уровня невязимности канала является сложной задачей, требующей учета большого количества астрономических, физических и технических факторов.

Заключение

Метеорное распространение радиоволн остается важным направлением исследований, позволяющим решать актуальные научно-технические проблемы. Системы метеорной синхронизации шкал времени позволяют организовать независимый от спутников резервный канал передачи точного времени, успешно работающий даже в труднодоступных (малонаселенных) регионах, где малоэффективны иные виды радиосвязи. Изучение причин и факторов проявления невязимных свойств канала позволяет разработать новые методы оперативной отбраковки низкокачественных регистраций для повышения точности синхронизации. В начале XXI века наметилось новое перспективное направление исследований, сопряженное с использованием стохастических свойств метеорного радиоканала для порождения секретных ключей шифрования. В результате, был предложен принципиально новый подход к организации систем передачи информации с особо высокой защищенностью, работающий при разнесении пунктов связи на расстояния до 1800 км.

Благодарности

Работа выполнена при поддержке Программы Повышения Конкурентоспособности Казанского Федерального Университета.

Список литературы

1. Latorre V. R. Utilization of the Phase Stability of Meteor Trails for Accurate Synchronization // IEEE Int. Conf. Res. — 1965. — pt. 2. — P. 121–129.
2. Epictetov L. A. Application of Meteor Burst Equipment for High Precision Comparisons of Time and Frequency Standards // Proc. of 7th European Frequency and Time Forum (EFTF). — 1993. — P. 413–416.
3. Oetting J. D. An analysis of meteor burst communications for military applications // IEEE Trans. on comm. — 1980. — Vol. COM-28. No. 9. — P. 1591–1601.
4. Сулимов А. И., Карпов А. В., Сидоров В. В., Шерстюков О. Н. Генерация и распределение ключей симметричного шифрования на основе физических свойств радиометеорного распростра-

- нения // Сб. докл. XXIII Всеросс. научн. конф. «Распространение радиоволн». — 2011. — Т. 1. — С. 421–425.
5. Сидоров В. В., Карпов А. В., Сулимов А. И. Метеорная генерация секретных ключей шифрования для защиты открытых каналов связи // Информационные технологии и вычислительные системы. — 2008. — № 3. — С. 45–54.
 6. Сулимов А. И., Карпов А. В., Шерстюков О. Н., Сидоров В. В., Хузяшев Р. Г. Моделирование синхронной генерации криптографических ключей в метеорном радиоканале // Уч. Зап. Казанского ун-та. Сер. Физ.-мат. науки. — 2011. — Т. 153, кн. 4. — С. 167–175.
 7. Sulimov A., Karpov A. Secure key distribution based on meteor burst communications // Proc. of the 11th Int. Conf. on Security and Cryptography (SECRYPT-2014). — 2014. — P. 445–450.
 8. Bennett C. H., Brassard G. Quantum Cryptography: Public key distribution and coin tossing // Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing. — 1984. — P. 175–179.
 9. Sulimov A. I. On possibility of using of measurements of random polarization of radio reflections from meteor trails for generating shared encryption keys // Proc. 2017 Int. Conf. on Radiation and Scattering of Electromagn. Waves (RSEMW-2017). — 2017. — P. 146–149.
 10. Sulimov A. I., Karpov A. V. Performance evaluation of meteor key distribution // Proc. of the 12th Int. Conf. on Security and Cryptography (SECRYPT-2015). — 2015. — P. 392–397.
 11. Sulimov A. I., Karpov A. V., Lapshina I. R., Khuzyashev R. G. Analysis and Simulation of Channel Nonreciprocity in Meteor-Burst Communications // IEEE Trans. on Antennas and Propagation. — 2017. — Vol. 65. Iss. 4. — P. 2009–2019.
 12. Villard O. G. Some properties of oblique radio reflections from meteor ionization trails // Jour. of Geophys. Research. — 1956. — Vol. 61. No. 2. — P. 233–249.
 13. Bazlov A. E. Experimental study of nonreciprocity of a meteor radio channel // Radiophys. and Quantum Electron. — 1992. — Vol. 35. No. 1. — P. 66–67.
 14. Safiullina A. R., Sulimov A. I., Karpov A. V. On the dynamics of nonreciprocal properties of radio reflections from ionized meteor trails // Proc. Int. Conf. Radiation and Scattering of Electromagn. Waves (RSEMW). — 2017. — P. 138–141.