Информационные процессы, Том 8, № 1, 2008, стр. 10–23

О возможности защиты информации на основе использования наносекундной синхронизации шкал времени по метеорным радиоотражениям

В.А. Корнеев, В.В. Сидоров, Л.А. Эпиктетов

Казанский государственный университет
vladimir.sidorov@ksu.ru

Поступила в редколлегию 7.10.2007

Аннотация—Работа посвящена метрологическому обоснованию метеорного метода защиты информации — нового метода дистанционной генерации ключей шифрования, претендующего на совершенную защиту. Метод опирается на высокоточные (фазовые) измерения времени распространения радиоволн, выполняемые в прямом и обратном направлении. Эти измерения возможны при условии наносекундной синхронизации шкал времени. Такую возможность представляет сам метеорный канал. Для преодоления кратковременной нестабильности квантовых стандартов частоты в условиях неравномерности и неравноточности измерений времени в метеорном канале применена модель управления, основанная на использовании метода оптимальной линейной фильтрации и экспериментальной модели-аналога, в качестве которой были использованы результаты эксперимента на радиолинии Менделеево–Казань. Показана возможность организации двойного использования метеорного канала для синхронизации шкал времени и генерации ключей шифрования и дана оценка производительности этой процедуры.

ВВЕДЕНИЕ

Проблема распространения ключей шифрования/дешифрования для реализации методов современной криптографии является одной из актуальных проблем современной науки и техники. Дело в том, что строго криптографических способов, которым можно доверить передачу ключей шифрования на большие расстояния, пока нет. Научно-техническая значимость этой проблемы в том, что на сегодня защита информации при её передаче осуществляется математическими методами криптографии, основанными на использовании псевдослучайных последовательностей и секретных ключей шифрования/дешифрования, однако эти методы в принципе раскрываемы современными методами криптоанализа и суперкомпьютерами, на что нужны только время и деньги. Гарантированно защитить информацию можно только используя частую смену ключей, что делает электронную доставку ключей шифрования важнейшей и нерешённой пока научно технической проблемой. Разрабатываются два способа канальной защиты информации, которым с нашей точки зрения можно доверить распространение ключей шифрования/дешифрования для целей защиты информации современными средствами криптографии: это квантовая криптография [1] и метеорная криптография [2, 3]. Квантовая криптография использует принцип неопределённости Гейзенберга и сейчас активно развивается применительно к оптическим каналам связи. Она основана на том, что факт перехвата информации может быть в таком канале обнаружен. Метеорная криптография использует случайность пространственного расположения метеорного следа, обеспечивающего условия зеркального отражения для конкретной пары участников информационного обмена и условие фазовой взаимности распространения радиоволн в метеорном радиоканале. Этот метод обеспечивает дистанционную генерацию природно-случайных ключей шифрования/дешифрования

исключительно для пары участников информационного обмена в открытом эфире на расстоянии до 2000 км. Метеорная криптография гарантирует совершенную защиту от удалённых криптоаналитиков, поскольку в открытый эфир в такой системе информация о ключах не поступает. Ключи генерируются в антеннах приёмников. Раскрытие ключевой информации в ближней зоне с помощью системы разнесённых приёмников затруднено случайностью углов прихода метеорных эхо-сигналов и, соответственно, случайностью ракурсных различий принимаемых фаз в разнесённых приёмниках. Эти различия могут быть полезны для защиты информации в случае, если шкалы времени участников информационного обмена в метровом диапазоне волн будут сведены с наносекундной точностью.

В настоящее время созданы и постоянно совершенствуются системы передачи времени на большие расстояния, обеспечивающие измерения, погрешность которых не превышает нескольких наносекунд. Можно указать на три основных метода передачи времени: 1) Пассивные спутниковые методы (ГЛОНАСС, GPS — точность/стабильность: 10–40 нс/2–7 нс; GPS Common View: 1–10 нс / 0,1–2 нс) 2) Активные методы, использующие геостационарные спутники (1–5 нс / 0,1–2 нс) [4,5] 3) Фазовые метеорные системы синхронизации (точность 0,3–0,9 нс). Менее всего разработан в техническом и коммерческом плане метеорный метод передачи времени.

На возможность использовать метеорный радиоканал для передачи сигналов точного времени указал Латторе [6] ещё в 1964 году. Однако узкая полоса пропускания использованного им канала, приспособленного для передачи информации, не позволила добиться погрешностей меньших, чем 0,3–0,5 микросекунды. Благодаря усилиям Казанских [7] и Харьковских [8] исследователей к 1980-м годам точность передачи времени через метеорные следы улучшилась до 20–50 нс за счёт применения более широкополосных устройств и автоматического отбора метеорных отражений с требуемыми свойствами.

Метеорный метод передачи времени использует встречную передачу запросных и ответных радиосигналов в канале с высокой степенью взаимности условий распространения. Измерения организованы так, что запросный сигнал привязан к шкале времени, а ответный сигнал несет информацию о сдвиге шкал.

В 1981 году была опубликована работа [9], в которой впервые было показано, что взаимность условий метеорного распространения радиоволн для значительной части метеорных отражений сохраняется с точностью до фазы несущей частоты. Имеющиеся на сегодняшний день теоретические оценки и экспериментальные результаты [10, 11] показывают, что метеорный радиоканал для целей синхронизации является весьма перспективным, при условии, если он опирается на фазовые измерения. Это связано с тем, что потенциальная точность одиночных измерений расхождения времени в метеорном радиоканале по фазе несущей частоты составляет доли наносекунды и эти измерения не требуют затрат времени на накопление результатов, как например в случае GPS/ГЛОНАСС.

В Проблемной радиоастрономической лаборатории Казанского университета были построены многочастотные измерительные комплексы “Кама 5” [10, 11] и “Кама 7”, в которых была реализована наносекундная точность сличения шкал хранителей времени на основе использования условий фазовой взаимности. Наносекундная точность сличения времени по метеорным радиоотражениям была достигнута также в Харьковском национальном университете радиоэлектроники [12].

Однако реализация такой высокой точности для решения прикладных задач в реальном времени натолкнулась на проблему хранения соответствующих поправок. Неравномерность и неравноточность измерений в метеорном канале допускает ситуацию, при которой с определённой вероятностью возможны интервалы времени отсутствия достаточно точных измерений, в течение которых шкала времени сместится из-за кратковременной нестабильности квантово-

го стандарта частоты. В данной работе обсуждается проблема автоматического управления вторичной шкалой времени по метеорным отражениям в реальном времени применительно к проблеме защиты информации. Дело в том, что метеорная генерация ключей шифрования опирается на достижения в области наносекундной синхронизации шкал времени с использованием метеорного канала, а также на такую особенность этого канала, как сохранение взаимности условий встречного распространения радиоволн с точностью до фазы несущей [13], при разбросе параметров распространения радиоволн для разных метеорных отражений достигающем 1 мс. Высокая точность синхронизации шкал позволяет измерять случайные составляющие параметров пути распространения радиоволн, изменяющиеся от отражения к отражению и использовать их в качестве элементов ключа в шифре Вернама с обеспечением защищённости в соответствии с теоремой Шеннона [14]. При генерации ключей нельзя использовать те метеоры, по которым сверяются шкалы времени, поскольку при измерении расхождения шкал времени информация о времени распространения содержится в ответном сигнале. Представляется важным вопрос о распределении дефицитного времени существования метеорного канала для успешного решения как задачи синхронизации шкал хранителей времени, так и для генерации природно-случайной последовательности ключа шифрования. Важным представляется определить, как погрешность синхронизации будет влиять на производительность канала генерации ключей шифрования, и оптимизировать в связи с этим распределение времени генерации ключей и синхронизации.

1. ОБОРУДОВАНИЕ И УСЛОВИЯ ЭКСПЕРИМЕНТА

Эксперимент проводился с использованием фазовой аппаратуры метеорной синхронизации и связи “Кама-5”, разработанной в Проблемной радиоастрономической лаборатории Казанского университета [11]. Аппаратура имеет несколько особенностей, отражающих использованный метод метеорной синхронизации:

1) эффективное исключение из результатов измерения времени распространения радиоволн при двухсторонней передаче сигналов;

2) многочастотный фазовый метод передачи времени;

3) порог регистрации метеорных отражений определялся энергетикой канала, а конкретным его выбором задавалось соотношение между численностью регистрируемых метеоров и допустимым числом ошибочных измерений.

Основные параметры аппаратуры и условий эксперимента: длина трассы: 720 км; средняя мощность передатчика: 500 Вт в режиме передачи, 200 Вт в режиме ожидания; полоса частот: 4 канала шириной 25 КГц, с максимальным разносом частот 500 КГц; точность измерения на одном метеорном следе: 14–18 нс по однозначному измерению фазы максимальной разностной частоты, 0.3 нс по неоднозначному измерению фазы несущей; первичный эталон частоты — водородный стандарт частоты, вторичный стандарт — цезиевый, кратковременная нестабильность определялась в основном цезиевым стандартом: стандартное отклонение (интервал 1 сек):

$$\sigma_{\Delta f/f} = 5.6 \cdot 10^{-11}$$

Эксперименты по фазовой метеорной привязке шкал времени проводились в период с 1988 по 1993 годы. Использованный в работе эксперимент выполнялся на трассе Менделеево (Московская обл.)–Казань в 1992 г. Отличительной особенностью экспериментальных данных являлось то, что по ним можно было оценивать шумовую погрешность измерений для большинства зарегистрированных метеорных отражений.

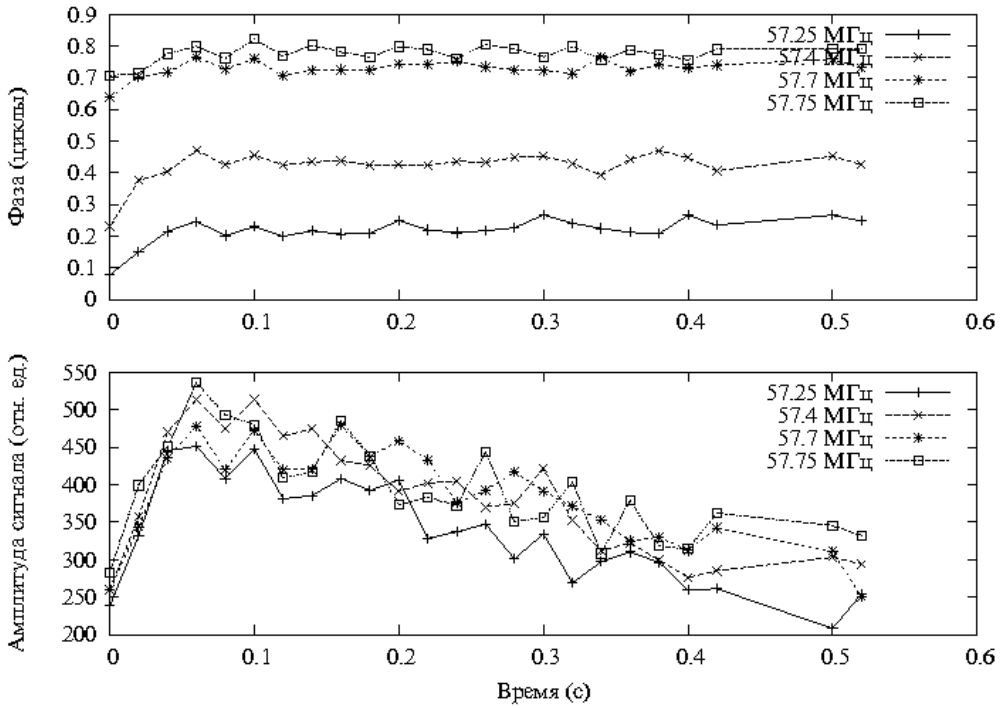

Рис. 1 Пример регистрации изменения во времени фаз сигналов при встречном распространении радиоволн в прямом и обратном направлении на трассе Менделеево–Казань, а также амплитуды метеорного эхо-сигнала на 4-х частотах.

На рис. 1 приведён пример регистрации изменения во времени разности фаз сигналов принимаемых в двух пунктах при встречном условии распространения радиоволн в прямом и обратном направлении, а также амплитуды метеорного эхо-сигнала на 4-х частотах.

Видно, что за исключением начального участка, на котором проявляются дифракционные эффекты формирования метеорного следа, разность фаз прямого и обратного сигнала практически не меняется со временем, хотя амплитуда сигнала меняется значительно. Более того, можно показать, что разностная фаза на одной частоте меняется только в связи с изменениями разности фаз используемых стандартов частоты.

Распределение стандартных отклонений шумовых ошибок измерений на отдельных метеорных отражениях показано на рис. 2.

Распределение стандартных отклонений шумовых ошибок измерений на одиночных метеорных отражениях показано на рис. 2. Ошибки оценивались по разбросу результатов измерений внутри отдельных отражений. Видно, что максимум распределения соответствует значению стандартного отклонения 0,012 фазового цикла (0,1 нс). Максимум погрешности 0,5 нс соответствует случаям, когда длительности отражения было недостаточно для оценки погрешности. Этим измерениям приписывалась максимальная погрешность 0,5 нс. На самом деле сюда попадали измерения, выполненные и с большей и с меньшей точностью.

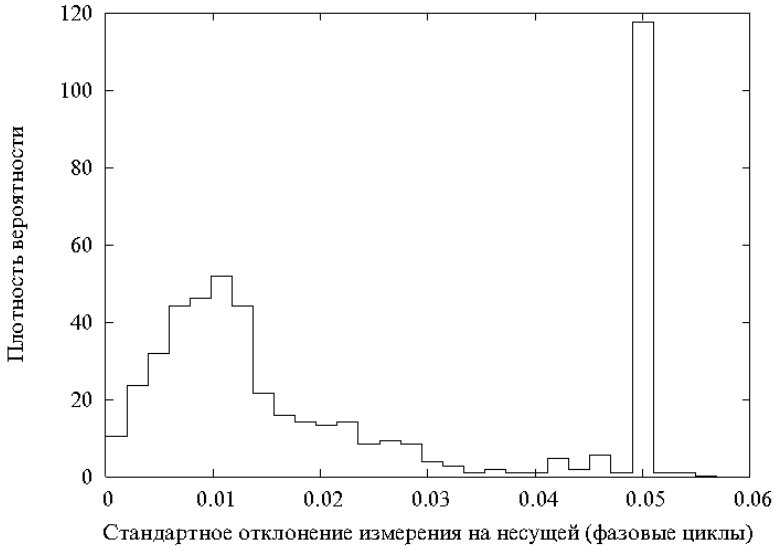

Рис 2. Распределение стандартных отклонений ошибок оценок сдвига шкал времени (для случая 120 регистрируемых метеорных отражений в час).

Данные эксперимента содержат информацию о фазовых измерениях на нескольких несущих, что можно использовать при пересчете величин ошибок измерений для других вариантов разнесения частот.

Кратковременная нестабильность цезиевых стандартов хорошо описывается белым частотным шумом на всем интересующем нас интервале от единиц секунд до нескольких часов. Таким образом, двухвыборочная дисперсия (Аллена) может быть использована как дисперсия относительного отклонения частоты от номинала, как при фильтрации экспериментальных данных, так и в модели, использующей экспериментально полученное распределение ошибок измерений.

2. МОДЕЛЬ УПРАВЛЕНИЯ ШКАЛОЙ ВРЕМЕНИ

При создании модели управления нужно описать модель измерения [15, 18]. Фазовое измерение сдвига шкал на текущем метеорном следе описывается следующим образом. Измерение содержит два типа ошибок: шумовую ошибку и ошибку невзаимности канала на текущем пути распространения сигналов. Шумовая ошибка может быть различна для всех используемых несущих. Неустранимая, на момент проведения эксперимента, остаточная ошибка невзаимности связана главным образом с ветровым смещением метеорного следа. Такая ошибка одинаково проявляется на всех несущих частотах и практически не изменяется в течение существования метеорного следа, однако может различаться для разных отражений.

Измерение фазы удвоенного (особенность двухсторонней передачи сигналов) сдвига шкал запишется следующим образом:

$$\phi_k^j = \|2f_j[\tau_k + \epsilon_k] + \theta_j(\sigma_k)\|,$$

где τ_k — сдвиг шкал в момент появления k-го метеорного отражения, f_j — j-я несущая частота, $\theta_j(\sigma_k)$ — ошибка текущего измерения по фазе несущей, ϵ_k — ошибка невзаимности канала для текущего измерения. $\|\cdot\|$ означает отбрасывание целой части: $\|a\| = a - \lfloor a \rfloor$.

Уход шкал вследствие нестабильности стандарта частоты будет записан как:

$$\tau(t) = \tau_0 + \frac{\Delta f}{f_0} t + \int_0^t \rho dt,$$

где $\rho(t)$ — случайный процесс, описывающий частотный шум стандарта частоты, τ_0 — сдвиг шкал в начальный момент времени, f_0 — номинальная частота стандарта, Δf_0 — систематическая составляющая сдвига частоты стандарта от номинальной. Для использования в уравнениях дискретной фильтрации удобнее представить относительный уход шкал в виде

$$\tau_k = \left(\gamma_{k-1} + \frac{\Delta f}{f_0}\right)(t_k - t_{k-1}) + \tau_{k-1},$$

где τ_k — сдвиг шкал на момент t_k текущего измерения, γ_{k-1} — случайная величина, представляющая шумовой сдвиг шкал накопленный с момента t_{k-1} до момента t_k. Дисперсия случайной величины γ_k может быть представлена либо с использованием величины дисперсии Аллена $\sigma^2_{\frac{\Delta f}{f}}(dt_k)$ (паспортная характеристика), либо представлена в виде $N_0/2dt_k$, где спектральная плотность мощности частотного шума $N_0/2$ вычисляется по величине $\sigma^2_{\frac{\Delta f}{f}}(1)$.

Для адекватного описания и учета случайных процессов, оказывающих влияние на результирующую точность управления шкалой, требуется построить модель управления, учитывающую неравномерность и неравноточность измерений в условиях нестабильности исследуемого процесса. Для учета этих процессов хорошо подходит использование оптимальной линейной фильтрации для случая систем с дискретными измерениями. Этот подход удобен по ряду причин: 1) исследуемый случайный процесс (уход шкал) оценивается по дискретным измерениям в моменты появления регистрируемых метеорных отражений, 2) ошибки измерений можно полагать гауссовскими, причем необходимые значения параметров распределения для каждого измерения, как на несущей, так и на максимальной разностной частотах, легко находятся из экспериментальных данных по измерениям на несущих частотах, 3) допустимым является предположение о независимости измерений, что обусловлено пространственным разделением метеорных следов и случайностью их положения, 4) нестабильность используемого цезиевого КСЧ хорошо описывается частотным белым гауссовским шумом, значение которого берется из описания стандарта частоты и легко вносится в уравнение фильтра.

При решении данной задачи необходимо принять во внимание проблему, не решаемую оптимальной линейной фильтрацией: неоднозначность фазовых измерений на несущей частоте. Необходимо связать процедуру оптимальной линейной фильтрации доступных однозначных измерений с проблемой перехода к фазе несущей и обеспечения, таким образом, максимально возможной точности измерений.

Оптимальная линейная фильтрация предполагает представление рассматриваемого процесса в виде системы матричных уравнений:

$$\begin{aligned} x(k+1) &= F(k+1,k)x(k) + G(k+1,k)w(k) \\ z(k+1) &= H(k+1)x(k+1) + v(k+1), \end{aligned}$$

где x — n-вектор состояния; w — p-вектор возмущения; z — m-вектор измерения; v — m-вектор ошибки измерения; $k = 0, 1 \ldots$–дискретное время; F — переходная матрица состояния размера $n \times n$; G — переходная матрица возмущения размера $n \times p$; H — матрица измерения размера $m \times n$.

Вектором состояния в нашей системе будет:

$$\begin{pmatrix} \tau \\ \frac{\Delta f}{f_0} \end{pmatrix}_{k+1} = \begin{pmatrix} 1 & dt_k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \tau \\ \frac{\Delta f}{f_0} \end{pmatrix}_k + \begin{pmatrix} 0 & dt_k \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ \gamma \end{pmatrix}_k,$$

где τ — величина текущего сдвига шкал, $\frac{\Delta f}{f_0}$ — постоянное отклонение частоты стандарта от номинала.

Вектор измерения (в нашем случае скаляр) запишется как

$$Z_{k+1} = (2\,0) \cdot \begin{pmatrix} \tau \\ \frac{\Delta f}{f} \end{pmatrix}_{k+1} + V_{k+1},$$

где V_{k+1} — ошибка текущего измерения удвоенного сдвига шкал времени.

При использовании модели в численном эксперименте последовательно генерируются следующие величины:

1) сдвиг шкал

$$\tau_{k+1} = \tau_k + \frac{\Delta f}{f_0} dt_k + \gamma_k,$$

где γ_k — случайная величина с гауссовским распределением, нулевым средним и дисперсией $N_0/(2dt_k)$;

2) ошибка невзаимности текущего измерения ϵ_k, как нормально распределенная случайная величина со стандартным отклонением 0,3 нс (данную ошибку считаем одинаковой для каждой несущей частоты, хотя это некоторое упрощение реальной ситуации);

3) стандартное отклонение текущего измерения удвоенного сдвига шкал по фазе несущей σ_k, генерируется по распределению, полученному в эксперименте (рис. 2);

4) фазовые различия удвоенного сдвига шкал ϕ_k^0 и ϕ_k^1, соответствующие максимально разнесенным частотам f_0 и f_1;

5) сдвиги шкал по фазе максимальной разностной частоты вычисляются как

$$M_\tau^d = \frac{\phi_1 - \phi_0}{f_1 - f_0},$$

причем к величине M_τ^d добавляется необходимое количество периодов однозначности, что имитирует процедуру последовательного разрешения неоднозначности фаз разностных частот.

Предполагается, что наиболее уязвимым для ошибок является переход от фазы максимальной разностной частоты к фазе несущей, что обусловлено возможностью выбора соотношения несущих частот [16]. Достижение однозначной фазы максимальной разностной частоты считаем в модели осуществимым и безошибочным. Управление шкалой времени вторичного стандарта в рамках работы осуществляется путем введения поправок непосредственно в шкалу времени в виде ее смещения. Поправка вычисляется на основании результатов оптимальной линейной фильтрации измерений и вводится мгновенно, по принятии решения об ее необходимости. Таким образом, величина ошибки управления определяется величиной ошибки оптимальной оценки на момент принятия этого решения. Поправка по частоте на длительных интервалах не вычисляется и в модель не вводится, хотя есть все данные для её определения. Дело в том, что долговременная нестабильность квантовых стандартов много меньше кратковременной, уточняется усреднением и её не трудно корректировать. Поэтому полагаем, что для модели средние частоты совпадают, а текущие отклонения корректируются системой управления.

3. ПОТЕНЦИАЛЬНАЯ ТОЧНОСТЬ ПОДДЕРЖАНИЯ СИНХРОННОСТИ ШКАЛ ВРЕМЕНИ

Под потенциальной точностью будем иметь ввиду точность, которую можно достичь, используя для управления все зарегистрированные метеоры на аппаратуре заданного энергети-

ческого потенциала. В первую очередь рассмотрен вопрос о потенциальной точности управления шкалой времени на аппаратуре метеорной синхронизации, использующей технические решения на основе фазовой аппаратуры "Кама". Здесь требуется ответить на вопрос, каким может быть расхождение шкал в случайный момент времени после начала работы аппаратуры синхронизации, независимо от наличия или отсутствия в этот момент метеорного следа. При этом предполагается, что время передается при наличии метеорного следа с точностью, обеспечиваемой измерением фазы несущей частоты, а отслеживание и разрешение неоднозначности измерений на несущей частоте происходит безошибочно. Главной исследуемой характеристикой является ошибка фильтрации, как текущая, так и интервальная. Ошибкой управления будет ошибка прогноза ухода шкал, а остаточная ошибка, в тех случаях, где можно отложить принятие решений об управлении, — ошибка задержанной во времени интервальной оценки. Точность управления в случайный момент времени удобно представить в виде распределения ошибок оптимальной линейной оценки.

На рис. 3 приведены распределения стандартных отклонений ошибок оценок хода шкал σ_τ для системы автоматического управления шкалой времени, полученное на описанной выше модели с использованием экспериментальных данных модели-аналога "Кама 5" для двух случаев: для текущего времени (наиболее вероятное $\sigma_\tau = 0,25$ нс, максимальное $\sigma_\tau = 0,5$ нс) и по задержанной, интервальной оценке (наиболее вероятное $\sigma_\tau = 0,2$ нс, максимальное $\sigma_\tau = 0,4$ нс).

Отметим, что для аппаратуры с другим энергетическим потенциалом, обеспечивающим другую регистрируемую численность, будут другие оценки, однако для всех рассмотренных нами случаев они не превышали 1 нс.

4. МЕТЕОРНАЯ КРИПТОГРАФИЯ И ТРЕБОВАНИЯ К ТОЧНОСТИ СИНХРОНИЗАЦИИ ШКАЛ ХРАНИТЕЛЕЙ ВРЕМЕНИ

Как уже отмечалось выше, идея метеорной криптографии заключается в том, что в эфир излучается информация только о координатах пунктов связи и временной шкале. Ключи шифрования генерируются персонально для двух участников информационного обмена на основе измерения фаз встречно распространяющихся сигналов, отражённых от случайно расположенных во времени и в пространстве метеорных следов. Такие ключи являются персональными для участников информационного обмена, используются однократно, их нельзя заранее узнать, украсть или купить. Однако такое применение метеорного канала предполагает использование метеорного канала в двух режимах: синхронизации и генерации ключей.

Для оценки производительности метеорного канала генерации ключей шифрования сначала рассмотрим наиболее простую задачу получения максимально доступного количества бит ключа путем измерения полного времени распространения сигнала при отсутствии необходимости разрешать неоднозначность фазовых измерений на несущей частоте. Производительность канала генерации ключей шифрования определяется здесь только свойствами метеорных отражений, неопределенностью времени распространения волн по текущему пути и точностью синхронизации. Решение о переходе от режима передачи времени в режим измерения времени распространения сигналов и наоборот принимается по пороговому значению ошибки текущей оценки сдвига шкал. Если ошибка оценки текущего сдвига шкал возрастает в отсутствие синхронизационных измерений и выходит за пределы порогового уровня, аппаратура переходит в режим синхронизации. В остальных случаях передается сигнал, позволяющий определить случайную составляющую текущей длины трассы, причем количество получаемых бит ключа зависит от текущей ошибки оценки сдвига шкал. Использование порогового уровня величины ошибки текущей оценки позволяет сделать распределение синхронизационных измерений более равномерным, что положительно сказывается на равномерности поведения ошибки оценки, т.к. интервалы между измерениям становятся приблизительно одинаковой длительности. Ко-

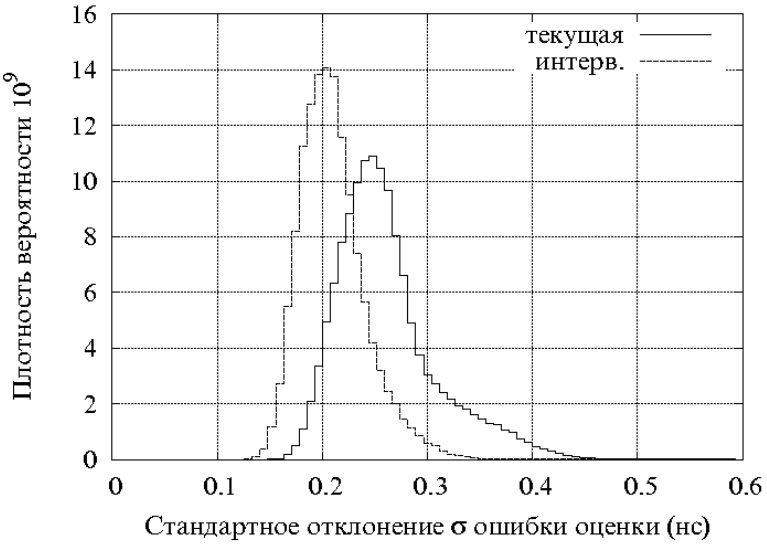

Рис 3. Распределение стандартных отклонений ошибок текущих оценок сдвига шкал времени (для случая 120 регистрируемых метеорных отражений в час)

личество бит, передаваемых на одном следе в режиме передачи данных, есть логарифмическая функция текущей ошибки оценки сдвига шкал. Возможность использования интервальной (задержанной во времени) оценки сдвига шкал определяется наличием в метеорной аппаратуре системы переспроса, позволяющей ведомому пункту по прошествии необходимого времени накопления уведомить ведущий о новом, более точном значении ошибки сдвига шкал на момент генерации ключа.

Предел измерения точности сдвига шкал в метеорном радиоканале определяется остаточной фазовой невзаимностью канала (0,3 нс). Мы можем использовать следующую функцию количества передаваемых бит на одном следе N от стандартного отклонения ошибки σ оценки сдвига шкал:

$$N(\sigma) = \lfloor \log_2 \frac{\tilde{T}}{a\sigma} \rfloor,$$

где, $\tilde{T}$ — величина разброса случайной составляющей времени распространения сигнала (в данном случае 500 мкс), а коэффициент a соответствует требуемой вероятности ошибки передачи ключа. Например, величина $a = 6$ соответствует вероятности получения ошибочного младшего бита ключа 0,003, что для максимально возможной точности сверки шкал (ошибка 0,3 нс) дает 18 бит ключа.

Численным экспериментом по описанной выше методике получена зависимость скорости передачи ключа от порогового уровня в оценке текущей ошибки для перевода системы в режим синхронизации (рис. 4).

Видно, что скорость передачи ключа составляет приблизительно 1 бит за 2 секунды по текущей оценке и незначительно увеличивается при использовании интервальной оценки.

Порог, при котором скорость передачи близка к оптимальной, соответствует относительно нечастым синхронизационным измерениям. На каждое отражение, использованное для синхронизации, приходится в среднем 15–20 передач ключа.

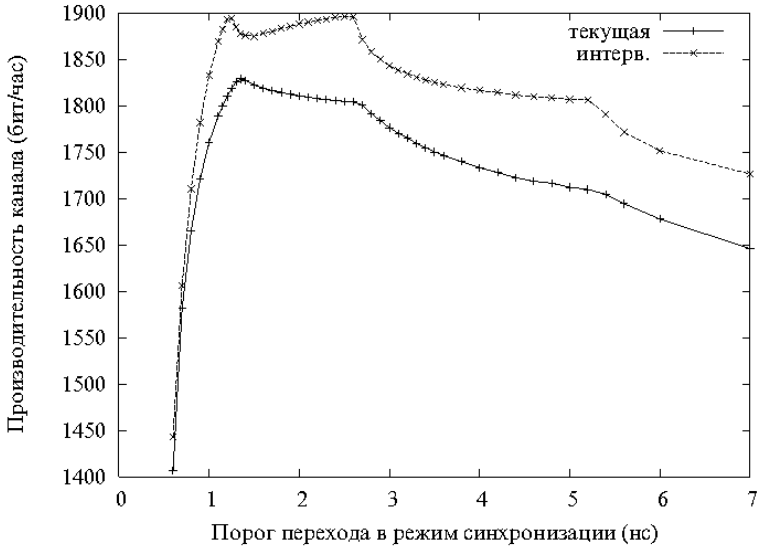

Рис. 4. Средняя скорость передачи ключа на один частотный канал в зависимости от порога перехода системы в режим синхронизации

Измерение полного времени распространения сигналов на текущем метеорном следе является нежелательной процедурой по причине того, что условия возможности его осуществления (последовательное разрешение неоднозначности фаз разностных частот) совпадают с условиями успешного перехвата информации криптоаналитиком в зоне, находящейся вблизи пунктов приема. Максимальное уменьшение зоны возможного прослушивания защищенного канала требует использования несущих частот, выбранных таким образом, чтобы обеспечивать независимость фазовых измерений времени распространения. Количество бит ключа, получаемого при этом по неоднозначному измерению на одной частоте, определяется величиной ее периода, точностью ее измерения и величиной ошибки текущей синхронизации. В дальнейшем предполагаем, что ошибка измерения фазы несущей несущественна в режиме передачи ключа, так как она, по крайней мере, не должна быть меньше ошибки, получаемой при измерении времени. Учитывая, что передача ключей происходит как раз в моменты отсутствия синхронизационных измерений, понятно, что основной вклад в ошибку вносит расхождение шкал времени. В выражении для количества передаваемых бит на одном следе N от стандартного отклонения ошибки σ оценки сдвига шкал величина $\tilde{T}$ будет равняться периоду несущей частоты. Использование k рабочих частот позволяет увеличить количество переданных бит ключа в k раз. Отказ же от процедуры последовательного разрешения неоднозначности фаз разностных частот позволяет уменьшить зону возможного пассивного прослушивания канала до 100–150 метров. В то же время, каждая дополнительная несущая приближает общее количество бит, переданных на одном следе к величине 18–19 бит, обеспечиваемой неоднозначностью длины текущего пути распространения волн, измеренного с суб-наносекундной точностью.

На рис. 5 показаны зависимости производительности канала передачи ключа при использовании во встречном режиме одной несущей частоты от величины порога принятия решения о переходе в режим синхронизации. Графики приведены для различных величин количества регистрируемых отражений в час. На рис 5 также также показаны значения производительности канала, получаемые при использовании текущей оценки. Видно, что использование ин-

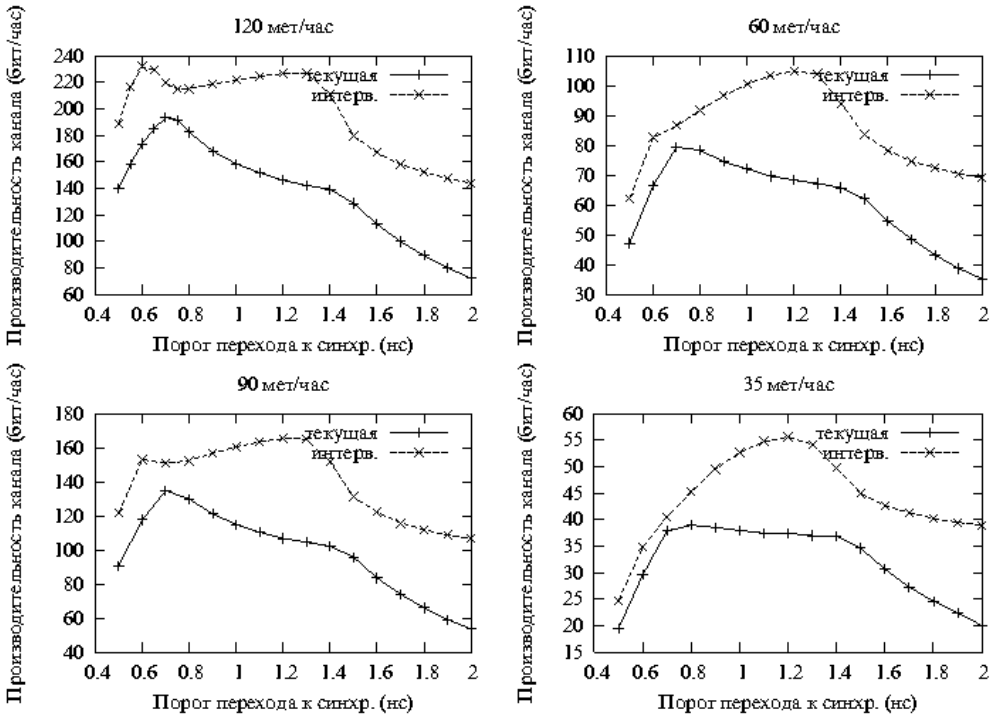

Рис. 5 Производительность канала передачи ключей, использующий всего одну несущую, для различных значений среднего количества отражений в час.

тервальной оценки повышает производительность и уменьшает требования к порогу перехода к режиму синхронизации.

Наиболее сложным случаем является генерация ключей при ограниченном максимальном частотном разносе, что не позволяет разрешать неоднозначность измерений на несущей частоте непосредственно в течение существования одного метеорного отражения.

В этом случае задачу можно представить как распределение метеорных отражений для трех целей: 1) передача времени для уточнения шкалы времени, 2) передача времени с целью поддержания однозначности (и высокой точности) измерений времени, 3) передача ключей. Алгоритм, предложенный для решения этой задачи предполагает использование двух фильтров для фильтрации соответственно фазовых измерений по максимальной разностной частоте, и фазовых измерений на несущей. Окончательное решение о возможности перехода к фазе несущей и точности результирующих измерений времени распространения (бит ключа) определяется по величине ошибки интервальной оценки фильтра разностных измерений. Производительность канала для случая максимального разнесения частот 2,5 МГц приведена на рис 6. В результирующую производительность включена также величина ошибочных бит ключа, полученных из-за неправильного определения номера периода однозначности несущей. Отдельно на графиках приведен также вклад таких ошибочных измерений, из чего видно, что он достаточно мал и начинает проявляться уже после превышения оптимального значения порогом перехода в режим передачи времени.

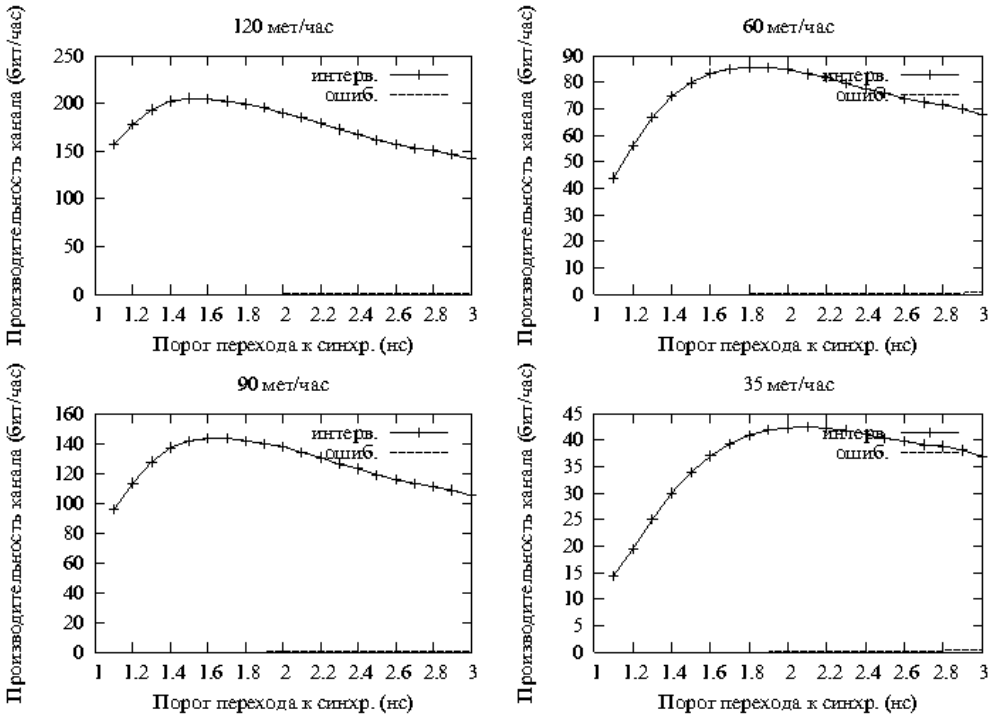

Рис. 6. Производительность канала передачи ключей, приходящаяся на одну несущую частоту, для различных значений среднего количества метеорных отражений в час в зависимости от порога принятия решения о синхронизации при максимальном частотном разносе 2,5 МГц.

Видно, что при использовании интервальной оценки лучшая производительность достигается при порогах принятия решений о переходе к режиму синхронизации от 1,5 нс при численности метеоров 120 в час до 2,1 нс при численности метеоров 35 в час. Однако, при малой численности и пороге выше 2,5 нс, обнаруживаются ненулевые ошибки, которые при генерации ключей нежелательны.

Эти исследования демонстрируют высокую степень зависимости эффективности метеорной криптографии от возможности реализации субнаносекундного уровня управления шкалой времени по метеорному каналу.

ЗАКЛЮЧЕНИЕ

Возможность использования метеорного канала для целей метеорной криптографии — претендующего на совершенство метода генерации одинаковых для участников информационного обмена ключей шифрования/дешифрования конфиденциальной информации — определяется соотношением разброса изменений времени метеорного распространения радиоволн и погрешностями синхронности используемых для измерений шкал времени.

Практическое использование наносекундной точности привязки шкал разнесённых хранителей времени по метеорным радиоотражениям затруднено из-за наличия кратковременной нестабильности квантовых стандартов частоты.

Поддержать шкалы времени синхронными можно методами автоматического управления, работу которых осложняет проблема неравноточности и неравномерности измерений, доставляемых метеорными отражениями. Показано, что, комбинируя в численном эксперименте приёмы оптимальной линейной фильтрации (Калман), и данные прямого эксперимента на действующей метеорной радиолинии в качестве модели аналога, можно оценить и оптимизировать эффективность управления вторичной шкалой времени для разной регистрируемой численности метеорных отражений, обеспечивая синхронность шкал времени на субнаносекундном уровне.

Показана принципиальная возможность совмещения процедур автоматического поддержания шкал времени и генерации ключей шифрования для целей метеорной криптографии в одном метеорном радиоканале.

Предложена процедура принятия решений о переходе метеорной системы генерации ключей шифрования в режим передачи времени в условиях ограниченного максимального частотного разноса, которая предполагает опору на текущую оценку фильтрации разностных измерений. Имеется возможность, как увеличения информационной значимости, так и отбрасывания переданных ранее ключей шифрования посредством системы переспроса по результатам запаздывающей интервальной оценки. Показано, что для энергетического потенциала аппаратуры модели-аналога “Кама 5”, производительность метеорной системы генерации ключей шифрования для различных вариантов максимального частотного разноса может меняться от 300 до 1200 бит в час.

Учитывая, что ключи шифрования можно накапливать неограниченно во времени, можно полагать, что такая аппаратура может решать проблему распространения ключей шифрования, а разработанный метод является значимым шагом в реализации права человека и сообщества на защиту конфиденциальной информации.

СПИСОК ЛИТЕРАТУРЫ

1. Bennett C., Bessette F., Brassard G., Salvail L., Smolin J. Experimental quantum cryptography. *Journal of cryptology,* 1992, V.5, №1, p. 3–28.

2. Карпов А.В., Сидоров В.В. Способ защиты информации в метеорном радиоканале путем шифрования случайным природным процессом *Патент Федеральной службы по интеллектуальной собственности и товарным знакам №2265957*, МПК6 H 04 B 7/22, H 04 L. Бюллетень изобретений №34 за декабрь 2005.

3. Sidorov V.V., Karpov A.V., Korneev V.A., Nasyrov A.F. Meteor Time Transfer and Meteor Cryptography *Proceed. of* 21^{st} *European Frequency and Time Forum* (TimeNav'07), Geneva, 29 May–1 June 2007. http://ieeexplore.ieee.org/iel5/4318993/4318994/04319088.pdf

4. Медведев Ю.Н., Порошков В.В. Методы улучшения синхронизации шкал времени при использовании СРНС ГЛОНАСС *Труды 5 Российского симпозиума “Метрология времени и пространства”* (МВП'94), 11–13 октября 1994 г., Менделеево, с. 388–395.

5. Parker T.E. Introduction to time and frequency transfer. *Tutorial at the Joint Meeting of* 17^{th} *European Frequency and Time Forum and the 2003 IEEE Frequency Control Symposium and PDA Exhibition* May 4, 2003

6. Lattore V., Jonson G. Time synchronization techniques *IEEE International conference.* Rec. 1964. Part 6. P. 422–428.

7. Сидоров В.В. Управление шкалами времени при измерениях по метеорным радиоотражениям *Метеорное распространение радиоволн,* Казань: Изд-во КГУ, 1979. Вып. 14, с. 89–105.

8. Дудник Б.С., Кащеев Б.Л., Коваль Ю.А., Семёнов С.Ф. Новый комплекс аппаратуры для сличения эталонов времени и частоты по радиометеорному каналу *Измерительная техника,* 1986, №4, с. 15–16.

9. Курганов А.Р., Сидоров В.В., Овчинников В.В., Плеухов А.Н., Хузяшев Р.Г. Экспериментальные исследования фазовой нестабильности и относительной фазовой невзаимности при метеорном и Es распространении радиоволн *Метеорное распространение радиоволн* Изд-во КГУ, Казань, 1981. Вып. 17, С 30–39.

10. Базлов А.Е. Казакова Т.В., Курганов А.Р., Мерзакреев Р.Р., Сидоров В.В. Хузяшев Р.Г., Эпиктетов Л.А Экспериментальные исследования невзаимности метеорного радиоканала *Изв. вузов., Радиофизика*, 1992. Т. 35 №1 с. 94–96.

11. Sidorov V.V., 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'93), Neuchatel, 16–18 March 1993, p. 413–416.

12. Коваль Ю.А., Кащеев Б.Л., Кундюков С.Г. Фазовая радиометеорная аппаратура сличения шкал времени *Измерительная техника*, 1998, №5, с. 27–30.

13. Desourdis R.I.Jr. Wojtaszek J.H., Sidorov V.V., Huziashev R.G., Kurganov A.R., Merzakreev R.R. and Epictetov L.A. Nonreciprocity of Meteor Scatter Radio Links *Proc. Of Ionospheric Effects Symposium (IES'93)*, 4–6 May 1993, pp. 165–173.

14. Shannon C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.*, V. 28, 1949, p. 656–715.

15. Korneyev V.A., Epictetov L.A., Sidorov V.V. Time & Frequency coordination using unsteady, variable-precision measurements in meteor burst channel, *Proc. of 17th European Frequency and Time Forum,* Tampa, USA, May 4–7 2003 — p. 186.

    http://www.ieee-uffc.org/archive/fc/proceed/2003/proceed/s0310285.pdf

16. Корнеев В.А., Сидоров В.В., Эпиктетов Л.А. Исследование времени однозначного перехода к фазе несущей при автоматическом управлении шкалой времени по измерениям в метеорном радиоканале. *Известия вузов. Радиофизика.* — 2003 — Том XLVI №12 с. 1044–1050.

17. Korneev V.A., Sidorov V.V. Optimization of concurrent data and high-precision time transfer modes in meteor burst synchronization equipment — *Proc. of* 21st *European Frequency and Time Forum (Time-Nav'07),* Geneva, 29 May–1 June 2007. http://ieeexplore.ieee.org/iel5/4318993/4318994/04319214.pdf

18. Корнеев В.А. Наносекундная синхронизация шкал времени по метеорным радиоотражениям и ее приложение к защите информации. *Автореферат кандидатской диссертации,* Казань: Казанский государственный университет им. В.И. Ульянова-Ленина, 2007.