Метеорная генерация секретных ключей шифрования для защиты открытых каналов связи

А.В. Карпов, В.В. Сидоров, А.И. Сулимов

Аннотация. Задача обеспечения высокой криптостойкости при передаче информации в открытом канале связи решается путем использования для шифрования и дешифрования природного случайного процесса - последовательных измерений случайного времени распространения сигнала на двух концах метеорной радиолинии, на расстояниях до 2000 км. Для разных корреспондентов создаются разные наборы измерений и, соответственно, персональные ключи одноразового использования. Абсолютная криптостойкость обеспечивается тем, что ключевая информация в эфир не излучается.

Введение

Современная криптография, в основном, развивается в своей математической части. Предполагается, что сам канал не может быть абсолютно защищен. В квантовой криптографии [1] впервые к каналу связи подошли с другой позиции - позиции реализации некоторого криптографического алгоритма за счет использования уникальных свойств канала связи. По существу, сам канал связи используется в качестве шифратора и дешифратора. Для засекречивания информации используются квантовые свойства света. Абоненты передают ключ путем измерений на обоих концах линии связи случайной поляризации передаваемого фотона. Криптоаналитик, измерив поляризацию фотона согласно принципу неопределенности Гейзенберга, внесет возмущение в состояние квантово-механической системы - фотона. Это возмущение регистрируется на приемном канале и несанкционированное подключение к каналу связи однозначно идентифицируется.

Цель данной работы показать, как с помощью радиосвязи, можно осуществить другой вариант канальной защиты информации, основанный на использовании уникальных свойств метеорного канала [3], как при организации такой системы обеспечить аутентификацию абонентов и поэтапную проверку достоверности передаваемой информации. Кроме того, представляется важным оценить, насколько вероятен перехват измерительной информации криптоаналитиком по измерениям в непосредственной близости к антеннам участников информационного обмена и указать пути защиты системы от таких действий.

1. Свойства метеорного распространения радиоволн

Прежде чем перейти к рассмотрению метеорной криптографии, кратко опишем метеорный радиоканал. Необходимость такой справки объясняется тем, что метеорная криптография основана на некоторых уникальных свойствах метеорного распространения радиоволн.

Каждую секунду в атмосферу Земли вторгаются миллионы частиц космического происхождения. Частицы имеют наблюдаемую относительно неподвижного наблюдателя скорость в диапазоне от 12 км/с до 72 км/с. Основной диапазон масс частиц, порождающих радиометеоры, составляет 0,0001 – 0,01 г. Более

тяжелые частицы встречаются довольно редко. Метеороид, пролетая с большой скоростью в верхних слоях атмосферы, сталкивается с отдельными атомами и молекулами атмосферы, разогревается и испаряется. Испарившиеся атомы, сталкиваясь с набегающими атомами и молекулами воздуха, ионизируются, поскольку энергия соударений испарившихся атомов метеороида с молекулами и атомами верхней атмосферы достаточна для образования свободных электронов. Ионизированный столб вокруг метеорной частицы создается достаточно быстро. Через 0.001 сек, в результате многочисленных столкновений, скорости испарившихся атомов уменьшаются до значения тепловых скоростей. В среднем электроны следуют за ионами и, в результате, образуется след метеорной ионизации с начальным радиусом около метра и длиной около 10 км. Условия рассеяния радиоволн меняются по длине следа вследствие неравномерности испарения, различной скорости диффузии и разной скорости ветра на разных высотах, однако в первые моменты времени, пока можно пренебречь турбулентным влиянием ветра, происходит зеркальное отражение радиоволн. Факт зеркальности метеорного распространения радиоволн подтвержден экспериментально уже первыми исследователями радиометеоров [4]. На Рис.1 представлено зеркальное распространение радиоволн между двумя пунктами *A* и *B*. Метеорная связь между удаленными пунктами осуществляется на расстоянии до 2000 км. Условие зеркальности приводит к тому, что для другого пункта *C* на следе будет другая точка отражения, другие электродинамические характеристики рассеивающей области на метеорном следе и, соответственно, другое время распространения радиосигнала. Учитывая случайность места появления и ориентации следующего метеорного следа, создающего отражение в B, для отражения в *C* условия зеркальности не будут соблюдаться и в *C* отражения не будет. Но может возникнуть метеорный след, обеспечивающий отражение в *C*, но не обеспечивающий отражение в *B*. Следовательно, каждая радиолиния, такая как *AB* или как *AC,* будет иметь свой персональный набор метеоров, обеспечивающих собственную последовательность радиоотражений.

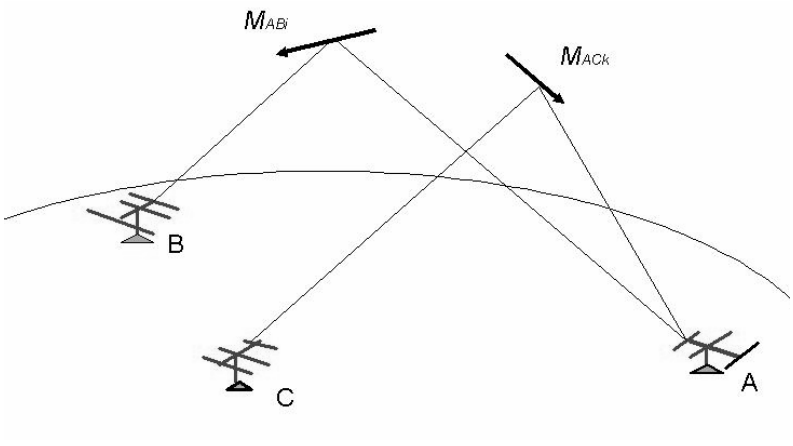

Рис.1. Связь между удаленными пунктами через метеорные следы

2. Описание процедуры выработки ключа в системе метеорной криптографии

В этом разделе описана процедура генерации ключей в системе метеорной криптографии при условии, что абоненты *A* и *B* успешно прошли процедуру аутентификации, а криптоаналитик отсутствует.

Метеорный радиоканал обладает свойствами, не обнаруженными пока в других радиоканалах одновременно [4-9]:

- случайность появления метеорного следа, как во времени, так и в пространстве;
- зеркальное отражение радиоволн: для конкретных пунктов приёма и передачи у каждого метеорного следа будет своя зеркальная точка, положение которой будет случайным в пространстве; вследствие этого будет случайным время распространения по пути *A* (передающий пункт) *M* (зеркальная точка на следе) *B* (приемный пункт);
- большой разброс времени распространения сигнала $\delta\tau$ от метеора к метеору, обусловленный случайными координатами следов метеорной ионизации;

- большой разброс угловых направлений прихода радиоволн, также определяемый случайными координатами точек отражения;

- взаимность - одинаковое с экспериментально доказанной точностью в доли наносекунды время распространения сигнала τ в обоих направлениях в пределах одного метеорного отражения: $(\tau_{AB} \cong \tau_{BA})$;

- одинаковый персональный набор радиоотражений, обеспечивающих радиосвязь абонентов в двух конкретных пунктах, не повторяющийся для других пар абонентов, располагающихся в других пунктах.

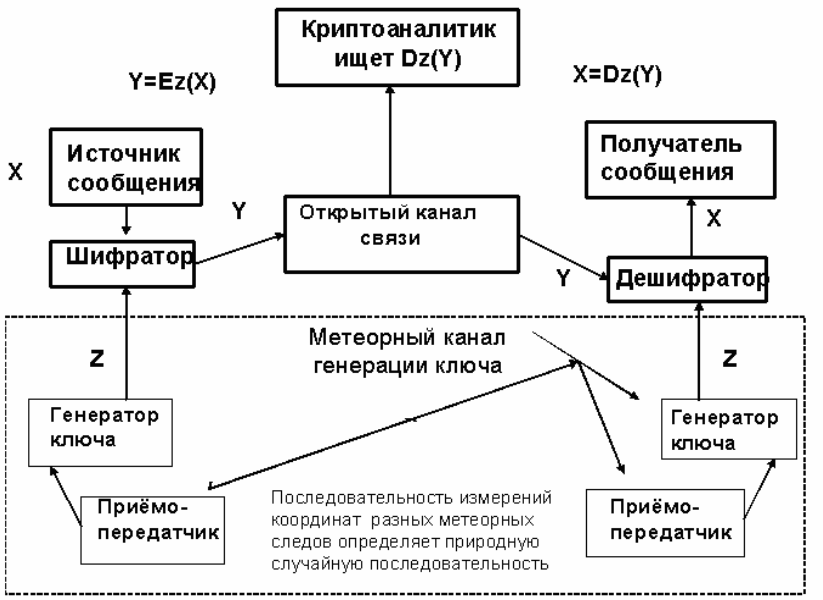

Рис.2. Функциональная схема системы метеорной криптографии

На Рис.2 представлена функциональная схема, иллюстрирующая метеорный способ защиты информации. На функциональной схеме изображены два идентичных комплекта аппаратуры защиты информации, расположенные в пунктах *A* и *B* (Рис1).

Используя высокую стабильность и взаимность условий метеорного радиоканала, можно по метеорному каналу обеспечить высокую синхронность шкал времени [5-9]. Далее, опираясь на единую для участников информационного обмена высокоточную шкалу времени, можно измерить время распространения для конкретного метеора с такой же, как и при синхронизации шкал времени, точностью. Свойство взаимности метеорного канала позволяет такое измерение сделать на обоих концах радиолинии. Эти измерения τ_{AB} и τ_{BA} с точностью до шумовой погрешности будут одинаковыми.

$$\tau_{AB} = \tau^*_{AB} + \Delta_{AB} \qquad (1)$$

$$\tau_{BA} = \tau^*_{AB} + \Delta_{BA} \qquad (2)$$

где: τ^*_{AB} - истинное время распространение на пути *AMB* (на Рис 1),

Δ_{AB} - ошибка измерения времени распространения по пути *AMB*,

Δ_{BA} - ошибка измерения времени распространения во встречном направлении *BMA*.

Цифровые эквиваленты DE_{AB} времени распространения τ_{AB} и DE_{BA} времени распространения τ_{BA} используются в качестве ключа, который измеряется одновременно в *A* и *B* при появлении подходящего метеорного следа. Основной проблемой является необходимость гарантированного выполнения равенства $DE_{AB} = DE_{BA}$. Это равенство с очень высокой вероятностью обеспечивает двухступенчатая система отбраковки ошибочных измерений. Первая ступень будет описана в конце этого раздела, а вторая ступень в разделе 3. Последовательность таких измерений создаст на двух концах метеорной радиолинии два одинаковых ряда случайных чисел.

Для измерения времени распространения τ_i в принципе может быть использован любой способ измерения временного положения сигнала в радиоканале [10,11], в частности, одиночные импульсы малой длительности или широкополосные сигналы с большой базой. Точность определения τ_i при согласованной фильтрации в этом случае будет определяться шириной полосы пропускания радиоканала *($\Delta\tau \sim 1/\Delta f$)*. Однако использование полосы частот более 200 кГц в метеорном канале затруднено из-за резкого падения численности регистрируемых отражений, а получающаяся в этом

случае погрешность измерения времени 1-5 мкс (в зависимости от отношения сигнал/шум) слишком велика для целей настоящей работы. В то же время, высокая фазовая стабильность и взаимность метеорного канала позволяют использовать для измерения τ фазовый метод. Этот метод даем возможность при ограниченной полосе пропускания значительно уменьшить ошибки измерения времени $(\Delta\tau \sim 1/f)$, однако эти измерения являются неоднозначными, причём период неоднозначности для сверки шкал времени равен $1/2f$, а для измерения времени распространения - $1/f$. Для снятия неоднозначности применяется известный метод, опирающийся на неоднозначные фазовые измерения на нескольких частотах [9]. Использование этого метода для привязки шкал времени по метеорному каналу позволяет обеспечить синхронизацию шкал хранителей времени с погрешностью менее *1 нс*. *С* погрешностью менее 1 *нс* можно измерить и время распространения, если использовать несколько частот.

Процедура выработки ключа (Рис 3) сводится к следующему: навстречу друг другу абоненты на одной частоте передают сигналы, содержащие собственный адрес, и сигналы, несущие информацию об отметках времени, привязанных к единой для абонентов шкале времени. Эти сигналы принимает (1) на обоих концах трассы, а (2) измеряет времена распространения τ_i. В пределах времени существования метеорного отражения стороны информируют друг друга только о том, что процедура измерения времени распространения выполнена. Коды результатов измерения времени распространения τ_i, выполненных на последовательных метеорных отражениях и привязанных к временной шкале, заносятся на обоих пунктах в регистры ключа (5). Выделим старшие разряды этого кода τ_{ic} и младшие разряды $\tau_{iм}$. Учтём, что от ошибок измерения страдают в первую очередь младшие разряды, поэтому отделим младшие разряды для целей аутентификации. По предыдущим измерениям из кодов старших разрядов в регистре (4) построим в регистре (5) случайную временную последовательность $\psi_{i-k-1} = (\tau_{i-k,c}, \tau_{i-k+1,c}, \ldots. \tau_{i-2,c}, \tau_{i-1,c})$. Последовательности кодов измерений в обоих регистрах будут одинаковыми, случайными и непрерывно пополняемыми, поэтому они могут быть ис-

Рис 3. Функциональная схема формирования ключа, его проверки и аутентификации абонентов в системе МК

пользованы в качестве шифрующей последовательности для одного абонента и в качестве дешифрующей последовательности для другого. Эти последовательности и будут искомым ключом K_{i-k-1}, синхронная генерация которого является целью системы метеорной криптографии. По мере использования ключ будет изыматься из регистра (5), поэтому индекс i-k-1 будет определяться размером ещё не использованной последовательности. Само сообщение может быть послано по любому открытому каналу связи. Для его дешифрования достаточно предпослать сообщению координаты отрезка шифрующей последовательности. Может быть использован любой достаточно эффективный способ шифрования. Для обеспечения гарантированной защиты может быть выбран, например, шифр Вернама [14] в симметричной схеме шифрования.

Производительность передачи защищенной информации (ключей) системы метеорной криптографии Q будет определяться частотой появления метеоров N и производительностью системы Q_0 на одном метеорном следе. Частота появления метеоров может быть определена из экспериментальных наблюдений или на компьютерной модели метеорного радиоканала [13].

Вычисление Q_0 рассмотрим на примере метеорной системы синхронизации, практически реализуемой на данный момент, которая обеспечивает точность синхронизации 10^{-9} с с вероятностью $p=0,98$. С такой же точностью может быть измерено и время распространения Δt (первая ступень отбраковки ошибочных измерений). Последнее означает, что равенство $DE_{AB} = DE_{BA}$ выполняется с вероятностью $p=0.98$.

При точности измерения времени распространения Δt, весь диапазон изменения времени распространения $\Delta\tau = \tau_{\max} - \tau_{\min}$ (в случае, если τ распределено равномерно) даст $K_0 = \Delta\tau / \Delta t$ реализаций случайного процесса. Таким образом, каждому измерению может быть приписано случайное двоичное число с числом разрядов, равным $m=log_2(K_0-1)$.

Для метеорной радиолинии длиной 1200 км разброс времени распространения составляет $\Delta\tau = 10^{-3}$с. Таким образом, в данном случае $Q_0 = 19$ бит.

3. Аутентификация абонентов и проверка правильности текущей работы системы МК

Проблема аутентификации абонентов, строго говоря, является самостоятельной проблемой и может решаться известными приёмами, например, блочного кодирования адресной информации, которой обмениваются абоненты в открытом эфире. Однако наличие постоянно генерируемой случайной последовательности на обоих пунктах даёт надежду и аутентификацию осуществить с гарантированной надёжностью. На Рис 3 представлена функциональная схема одного из вариантов процедуры аутентификации абонентов в системе метеорной криптографии. По предыдущим измерениям из кодов младших разрядов в регистре (4) построим в регистре (7) случайную временную последовательность $\zeta_{i-k-1} = (\tau_{i-k,м}, \tau_{i-k+1,м}, \ldots. \tau_{i-2,M}, \tau_{i-1,м})$. Глубина памяти k может быть ограниченной, а может быть определена моментом пуска и начальной сертификации системы. Перед моментом t_i над последовательностью ζ_{i-k-1} выполним легко осуществимое одностороннее МАС преобразование $Y_i = f(\zeta_{i-k-1})$, где Y_i – функция необратимого сжатия массива ζ_{i-k-1} (хеш-функция). Особенность этой функции состоит в том, что ее входной массив может иметь неограниченный размер, а хеш-функция – фиксированный. Это своего рода контрольная сумма массива ζ_{i-k-1}. Для данной задачи важно, что функция $Y_i = f(\zeta_{i-k-1})$ чувствительна к любому изменению в последовательности ζ_{i-k-1}. Поскольку функция ζ_{i-k-1} природно-случайная, природно-случайной будет и хеш-функция Y_i. Заметим, что код измерения τ_i и функция Y_i не коррелированны, поскольку τ_i определяется последним измерением, а Y_i - младшими разрядами всех предыдущих измерений. Некоррелированными будут и соседние по номеру i значения функции Y_i, поскольку преобразование f применено к массивам с постоянно меняющимся размером. Теперь добавим к функции Y_i открытый номер абонента и сформируем код запроса $K(\tau_{iм}, Y_i, t_i)$ очередного i-го измерения. Таким образом,

в *i*-й момент времени код запроса $K(\tau_{iм}, Y_i, t_i)$ будет своего рода паспортом двух взаимодействующих абонентов, причём этот паспорт в каждый *i*-й этап измерения будет разным, но одинаковым в обоих пунктах. Паспортом он является потому, что он находится в зависимости от начальных данных, установленных в пункте *B* при его запуске, и от персональной истории генерации им ключей в течение всего периода его жизни до *i*-1 -го момента времени. Кроме того, код запроса *i-го* измерения будет и кодом проверки правильности *i*-1 измерения, поскольку, если это измерение окажется неверным, изменится и код запроса. Функция $K(\tau_{iм}, Y_i, t_i)$ зависит от наиболее уязвимой части измерения ($\tau_{iм}$), так как всегда есть вероятность возникновения ошибки измерения в младших разрядах как по физическим особенностям радиоотражений, так и по особенностям пороговых ситуаций. Правильность измерения младших разрядов *i*-1 измерения проявится в том, что запрос $K_B(\tau_{iм}, Y_i, t_i)$ будет узнан в пункте *A* $(K_B(\tau_{iм}, Y_i, t_i) = K_A(\tau_{iм}, Y_i, t_i))$ и пункт *A* пришлёт подтверждение. Если код не будет узнан $(K_B(\tau_{iм}, Y_i, t_i) \neq K_A(\tau_{iм}, Y_i, t_i))$, то пункт *A* пришлёт отказ, который станет одновременно и указанием возврата к *i*-1 измерению. Все предыдущие измерения были верными, иначе система не добралась бы до *i-го* измерения. Отметим, что накопление в памяти системы МК информации о младших разрядах измерения не открывает ключевой информации, даже если криптоаналитик знает все запросы $K_B(\tau_{iм}, Y_i, t_i)$ постольку, поскольку они выходят в открытый эфир. Дело в том, что регистры (5) и (7) используют независимые источники информации $\tau_{i\,м}$ и $\tau_{i\,с}$. Значение младшего разряда и граница между младшими и старшими разрядами определяют два порога: первый с заданной вероятностью гарантирует правильность работы измерителя (2), а второй гарантирует конечный результат повтором измерений до тех пор, пока адрес пункта *B* не будет опознан пунктом *A*.

4. Защищенность системы МК от криптоаналитика

Поскольку ключевая информация ни в каком виде в эфир не поступает, для криптоаналитика в дальней зоне - в космосе, на самолёте или на земле, за пределами 25 километровой зоны вокруг пункта приёма - система не раскрываема. Вся информация, которую может получить криптоаналитик, заключается в возможности «угадать» параметры сигнала, принимаемого абонентом, располагая свои приёмники поблизости от его антенны. При использовании фазовых методов определения времени распространения следует учесть не только факт одновременного приёма метеорных отражений в разнесённых пунктах от одного метеорного следа, но и различие физических условий рассеяния радиоволн от различных участков метеорного следа, а также неопределенность фазы сигнала, определяемую деталями подстилающей поверхности реальных антенн, в условиях разброса углов прихода отражённых сигналов. Кроме того, для косвенного измерения фазы сигнала, принимаемого в пункте связи (например, пункте В) с помощью разнесённых наблюдателей, располагающихся вокруг *B*, в условиях изменений от метеора к метеору углов прихода сигналов, необходимо учитывать многозначность определения абсолютных фазовых различий при измерениях разности фаз, а именно, измерительная аппаратура фиксирует лишь значения фазы волны в пределах всего одного периода ($\leq 2\pi$), в то время как абсолютный набег фазы радиоволны до следящей антенны относительно антенны корреспондента может быть существенно большим 2π. На Рис. 4 приведена зависимость количества областей однозначности фазы **N** от расстояния **ρ** (в длинах волны) между антенной абонента и антенной криптоаналитика.

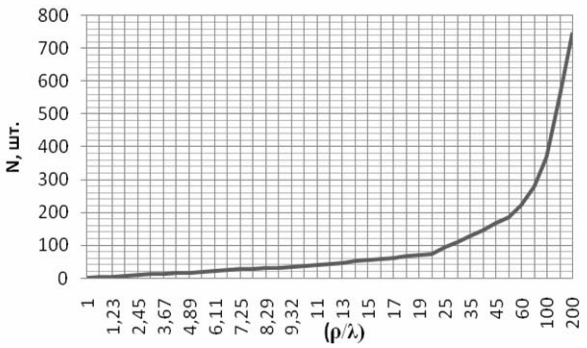

Рис. 4. Количество N областей однозначности фазы в зависимости от удаления **ρ** от абонента (**ρ/λ**)

Например, при разносе, равном 10 λ, число периодов однозначности, которые надо разрешить, равно 36, а при разносе порядка 100 λ их количество уже около 370. Наличие погрешностей фазовых измерений существенно усложняет процесс косвенного определения фазы, а при некотором предельном соотношении расстояния **(ρ/λ)** и величины ошибок **δφ** вероятность косвенного определения фазы сводится к нулю. На Рис 5 приведена зависимость оценочного предельного расстояния **(ρ/λ)** от величины ошибок фазовых измерений **δφ**. Под ошибкой измерения фазы имеем ввиду сумму погрешностей за счёт шума, неточности сведения шкал времени, неточности оценки фазовых центров антенн из-за различия подстилающих поверхностей и условий многолучёвости. Из Рис 5 видно, что при уровне ошибок **δφ** = 10° вероятность косвенного определения фазы обращается в ноль на расстоянии порядка **ρ** = 32 λ. Практически область вероятного «угадывания» фазы сигнала, принимаемого приёмником корреспондента, может быть сделана менее 100 метров, так что криптоаналитик может рассчитывать на перехват только незначительной части кода, характеризующего время распространения радиоволн. Можно показать, что частично перехваченные коды результатов измерений или их фрагменты при определённых правилах организации системы метеорной криптографии (раздел 5) не решают проблему её раскрытия криптоаналитиком.

Рассмотрим работу криптоаналитика в активном режиме. Криптоаналитик в ближней зоне может работать на передачу и посылать сигналы, двух типов: мешающие сигналы и имитирующие сигналы. Мешающие сигналы могут выбить из последовательности некоторые или все измерения, уменьшив тем самым производительность генерации ключа (в зависимости от степени корреляции), но не более. Все открытые каналы можно заглушить помехами, но борьба с помехами - проблема вообще всех видов радиосвязи, а не только метеорных. В этом смысле у метеорных каналов есть некоторые преимущества. Большой динамический диапазон амплитуд метеорных отражений позволяет выбором высоких порогов использовать только те метеорные отражения, которые

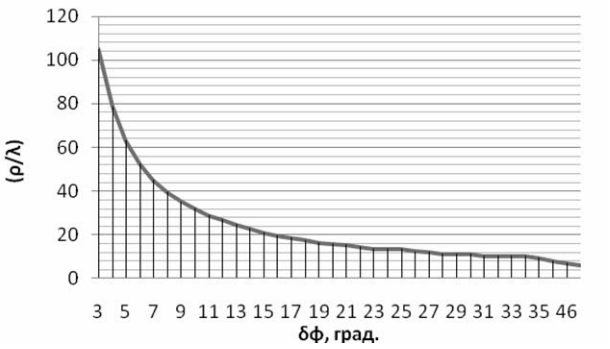

Рис 5. Зависимость предельного расстояния косвенного измерения от уровня ошибок фазовых измерений**δφ** (в градусах)

имеют требуемое отношение сигнал/помеха. В этом случае помехи уменьшат производительность системы, но не прекратят синхронную генерацию ключей полностью. Схожая ситуация складывается при описании метода квантовой криптографии [1] - авторы показали только, что могут определить наличие криптоаналитика, но не могут передавать в это время ключ.

По поводу имитирующих сигналов мы предполагаем, что криптоаналитик может разместить в *C* аппаратуру, аналогичную *B*. Если криптоаналитик в *C* сумеет выдать себя за абонента B, то имеется возможность перехвата части передаваемых ключей. Эффективная аутентификация корреспондентов, о которой шла речь выше, позволяет пункту *A* не входить во взаимодействие с пунктом *C*. Если имитирующий пункт *C* располагается в зоне прямой видимости от *B*, то одновременная работа на одной частоте может восприниматься как взаимная помеха, влекущая за собой прекращение сеанса связи.

5. Защита от потерь при частично перехваченных измерениях

Метеорная криптография не гарантирует защиты от перехвата части измерений криптоаналитиком в непосредственной близости от антенны абонента. Однако если речь идет о частично перехваченных измерениях, то можно сделать как угодно малой их эффективность, поставить формирование ключа в зависимость не от набора текущих измерений, а от трансформированной совокупности большой части,

или даже всего набора измерений выполненного системой. Более того, комбинируя метод МК с современными методами создания псевдослучайных последовательностей, например, используя его для регулярного внесения энтропии в такую последовательность на обоих пунктах, можно не только защититься от случаев частичного перехвата измерений, но и увеличить производительность генерации ключа. На Рис 6 продемонстрирован пример возможной организации синхронной генерации ключей в системе МК, обеспечивающей такую защиту.

Так же, как и на Рис 3, здесь в регистре последовательности измерений (5) накапливается i-k-1 результатов измерений $\theta_{i-k-1} = (\tau_{i-k,c}, \tau_{i-k+1,c}, ... \tau_{i-2,c}, \tau_{i-1,c})$. Однако эти результаты не используются в качестве ключа, а преобразуются с помощью одностороннего MAC преобразования в хеш-код *G(i-k-1)* (6), характеризующий всю совокупность данных, накопленных в регистре (5). Индекс *k* в данном случае ограничивает накопление данных некоторым размером, который должен быть достаточно большим, чтобы перехваченные фрагменты ключа составляли небольшую его долю. В то же время этот размер должен быть ограничен требованием, чтобы информация, доставляемая очередным измерением и добавленная в регистр (5), существенно меняла энтропию в системе (5) – (6). В этом случае последовательность хеш-кодов G_{i-k-1} (7), соответствующих последовательности измерений, будет представлять собой природно-случайную последовательность, составленную из фрагментов (8) последовательностей, определяемых каждым текущим i-k-1 содержанием данных в регистре (5). Из этой последовательности можно сформировать последовательность кодов (9) генерируемого ключа $K_{i-n-1} = (G_{i-n}, G_{i-n+1}, G_{i-n+2} ....G_{i-1})$. Индекс n характеризует размер не использованной на настоящий момент ключевой последовательности.

Размер сформированного таким образом ключа может быть значительно больше, чем сумма размеров кодов очередных измерений, впрочем, безопасность такого способа увеличения производительности генерации ключа требует дополнительного исследования.

Что касается частично перехваченных измерений, то они будут бесполезными до тех пор, пока не будут перехвачены все измерения на глубине памяти *i-k-1*. В этом варианте защиты данные, накопленные в регистре (5), не должны быть доступны криптоаналитику, также, как и данные, накопленные в регистре ключевой информации (9).

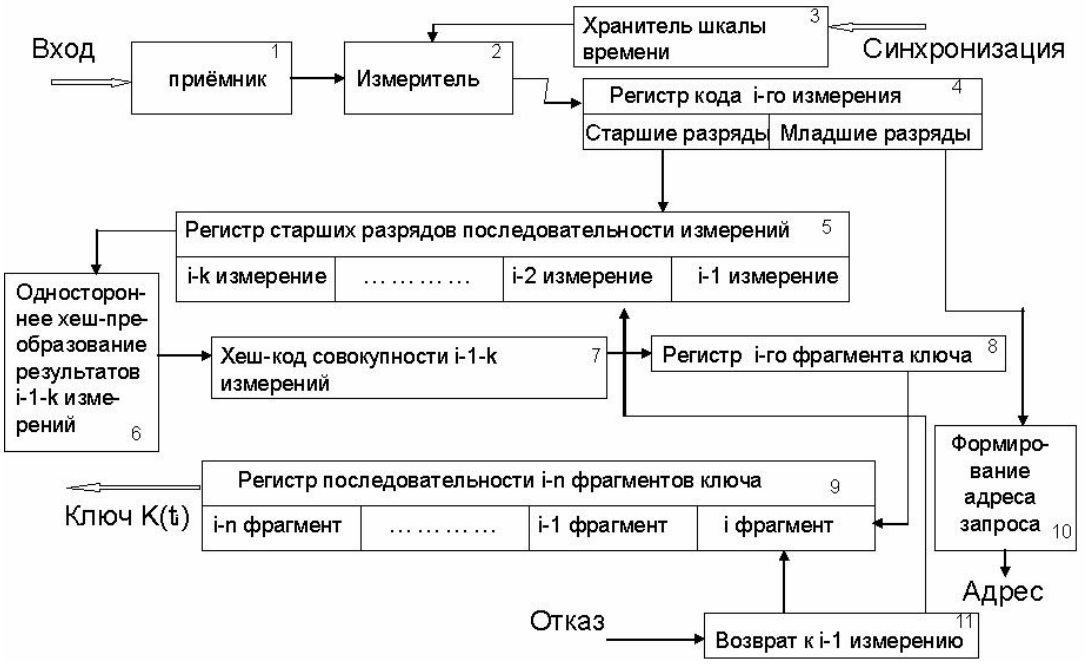

Рис 6. Функциональная схема процедуры выработки ключа с защитой от частично перехваченных измерений

6. Экспериментальная проверка идеи метеорной криптографии

Для проверки метода метеорной криптографии был использован эксперимент по фазовой синхронизации шкал времени на радиолинии Менделеево – Казань [8]. В этом эксперименте фазовые времена распространения радиоволн измерялись на обоих концах трассы и вычитались одно из другого. Проверялись условия фазовой взаимности на нескольких частотах.

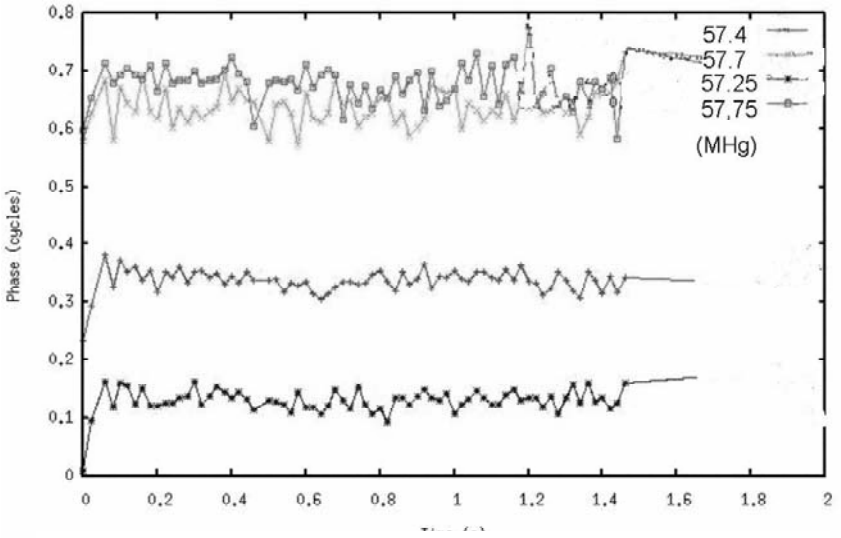

Рис. 7. Пример сохранения условий фазовой взаимности при прямом и обратном распространении радиоволн в течение одного длительного метеорного отражения

На Рис. 7 показан пример сохранения условий фазовой взаимности во время одного длительного метеорного отражения, во время которого измеряемые фазы менялись на несколько периодов за счёт ветрового сноса метеорного следа. Видно, что на всех частотах условия взаимности не сохраняются только в самом начале отражения, когда метеорный след только формируется. В остальное время различия времени распространения радиоволн в прямом и обратном направлениях сохраняются в пределах шумовых погрешностей приёмников. Наблюдаемые различия фазового смещения на разных частотах определяются смещением временных шкал, так что имеется возможность не только измерить времена распространения в прямом и обратном направлениях, но и проверить результат повторными измерениями.

7. О правовом режиме использования МК

Метеорная криптозащита представляет собой канальную защиту информации и не использует стандартных математических методов шифрования сообщений. Это просто прибор для одновременной генерации секретных ключей одноразового использования для двух или более удалённых абонентов. В дальнейшем эти ключи можно использовать в любых лицензированных способах шифрования сообщений, в том числе определяемых Государственными стандартами.

Заключение

Показано, что специфические свойства метеорного распространения радиоволн позволяют реализовать систему метеорной криптозащиты, которая:

- защищает передаваемую информацию по открытым радиоканалам на расстояния до 1500-2000 км, обеспечивая при этом абсолютную криптостойкость для криптоаналитика с наблюдателями в космосе, на самолёте или на земле в дальней от абонентов зоне;
- решает проблему взаимной аутентификации абонентов;
- решает проблему проверки правильности одинаковой генерации ключей на двух концах радиолинии;
- обеспечивает защиту от редких или неточных случаев косвенного дистанционного определения фазы сигнала в приёмнике абонента наблюдателями криптоаналитика.

Предложенный способ метеорной криптографии решает проблему распространения ключей по открытому эфиру на расстояния до 2000 км. Размер ключевой информации неограничен,

а производительность её генерации определяется точностью синхронизации и численностью регистрируемых метеорных отражений.

Ключ при метеорной криптографии является природно-случайным. До окончания процедуры аутентификации ключ неизвестен, используется однократно, автоматически уничтожается после использования. Его нельзя украсть или продать.

Литература

1. C.Bennett, F.Bessette, G.Brassard, L.Salvail, J.Smolin Experimental quantum cryptography // Journal of cryptology, 1992, V.5, N1, p.3-28
2. Shannon C.E. Communication theory of secrecy systems. Bell Syst. Tech. J., V.28, 1949, P. 656-715.
3. Карпов А.В., Сидоров В.В. Способ защиты информации в метеорном радиоканале путем шифрования случайным природным процессом. Патент РФ № 2265957.- МПК[6] H 04 B 7/22, H 04 L. Бюл. №34 от 10.12.2005.
4. Villard O.G., Peterson A.M., Manning L.A., Eshleman V.R. Some properties of oblique radio reflections from meteor ionization trails // J.Geophys.Res.- 1956.- V.61.- P.233-249.
5. 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.- N1.- С. 94-96.
6. Дудник Б.С., Кащеев Б.Л., Коваль Ю.А. Новый комплекс аппаратуры сличений эталонов времени и частоты по радиометеорному каналу // Измерительная техника, 1986, N 4, С.15-16.
7. Кащеев Б.Л., Коваль Ю.А., Кундюков С.Г. Фазовая радиометеорная аппаратура сличения шкал времени // Измерительная техника, 1998. -№5 –С.27-30.
8. Epictetov L.A., Merzakreev R.R., Sidorov V.V. 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, pp. 413-416.
9. 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 ВУЗ-ов, Радиофизика, Том 47, № 12, 2003, С. 933-939.
10. Леонов А.И., Фомичёв К.И.., Моноимпульсная радиолокация // Издательство «Советское радио», Москва, 1970.
11. Казаринов Ю.М. и др. Радиотехнические системы // Издательство «Советское радио», Москва, 1968.
12 Чепура В.Ф., Кащеев Б.Л., Бондарь Б.Г. Исследование направленных свойств рассеяния УКВ радиосигналов метеорными следами // Электросвязь.- 1962.- №11.- С.3-10.
13. Карпов А.В. Компьютерная модель метеорного радиоканала // Изв. Вузов. Сер. Радиофизика.- 1995.- т.38 с.- №12.- С.1177-1186.
14 G.S.Vernam “Cipher printing telegraph systems for secret wire and radio telegraphic communications” J. Amer. Inst. Elec. Eng. Vol.55, p.p.109-115, 1926.

Сидоров В.В. Доктор физико-математических наук, профессор кафедры радиофизики Казанского университета, научный руководитель Проблемной радиоастрономической лаборатории, заслуженный профессор Казанского университета, заслуженный деятель науки республики Татарстан и России. Область научных интересов – радарные исследования метеорных явлений и поиск путей их эффективного прикладного использования для радиосвязи, службы времени и защиты информации.

Карпов А.В. Доктор физико-математических наук, профессор кафедры радиофизики Казанского университета. Область научных интересов – имитационное компьютерное моделирование условий работы систем радиосвязи.

Сулимов А.И. Студент КГУ, выпускник магистратуры по направлению «Информационные процессы и информационные системы», исследует корреляцию фазовых измерений на местности.