«Оптика атмосферы и океана», **33**, № 8 (2020)
DOI: 10.15372/AOO20200802

ОПТИКА СЛУЧАЙНО-НЕОДНОРОДНЫХ СРЕД

УДК 621.373.628.551.510.3

Анализ корреляции интенсивности в приемо-передающих лазерных системах для формирования криптографического ключа

В.П. Аксенов[1], В.В. Дудоров[1], В.В. Колосов[1, 2], Ч.Е. Погуца[1], М.Е. Левицкий[3]*

[1] Институт оптики атмосферы им. В.Е. Зуева СО РАН
634055, г. Томск, пл. Академика Зуева, 1
[2] Томский научный центр СО РАН
634055, г. Томск, пр. Академический, 10/4
[3] Научно-внедренческое предприятие «Топаз»
634055, г. Томск, пр. Академический, 1

Поступила в редакцию 10.12.2019 г.

Исследуются потенциальные возможности и ограничения использования флуктуаций интенсивности лазерных пучков, распространяющихся в турбулентной атмосфере, для генерации случайных данных при формировании криптографических ключей в системе конфиденциальной оптической передачи информации. Метод базируется на теореме взаимности для оптических полей. Выполнено численное моделирование распространения света в системе из двух направленных друг на друга приемо-передатчиков, сигналы от которых искажены атмосферным каналом. Создана экспериментальная установка и проведено экспериментальное исследование формирования коррелированных случайных сигналов в такой системе. Экспериментально установлена необходимость фильтрации низких частот принимаемых сигналов, исследована ее эффективность. На основе численного моделирования установлены зависимости коэффициента корреляции от геометрических параметров системы и турбулентных условий на трассе для различных дистанций, радиусов апертур, значений интенсивности турбулентности. Теоретические результаты хорошо согласуются с результатами лабораторного эксперимента.

Ключевые слова: лазерное излучение, конфиденциальная оптическая связь, криптография, атмосферная турбулентность, флуктуации интенсивности, теорема взаимности; laser radiation, confidential optical communication, cryptography, atmospheric turbulence, intensity fluctuations, reciprocity theorem.

Введение

На сегодняшний день широкое распространение получили способы защиты информации, основанные на методах криптографии с использованием односторонних математических функций. Разработаны симметричные и асимметричные методы распространения криптографических ключей по открытым каналам связи. Принято, что такие методы шифрования практически не поддаются несанкционированной дешифровке. Однако алгоритмическая сложность их дешифровки связана с ограниченными возможностями современных компьютеров и не является абсолютной. К настоящему времени разработаны алгоритмы для квантовых компьютеров, которые с успехом будут справляться с обращением односторонних функций и, следовательно, решать задачи дешифровки таких сообщений. Поэтому остро встает вопрос о разработке методов распределения ключей на новых принципах. Один из подходов к решению этой проблемы заключается в применении метода квантовой криптографии [1–4]. Другой подход, использующий случайность физического процесса, базируется на принципе взаимности распространения электромагнитных волн. Первоначально он был реализован в радиодиапазоне длин волн [5–9]. Здесь используется случайность, вызванная стохастическим многолучевым распространением радиоволн. В качестве наблюдаемой случайной характеристики радиосигнала можно принять, например, задержку по времени распространения или фазу несущей волны.

В оптическом диапазоне используется случайность, вызванная атмосферной турбулентностью. Из принципа взаимности следует, что в качестве наблюдаемой случайной характеристики в этом случае можно взять интенсивности или фазы встречных волн. Однако использование фазовых

* Валерий Петрович Аксенов (avp@iao.ru); Вадим Витальевич Дудоров (dvv@iao.ru); Валерий Викторович Колосов (kvv@iao.ru); Чеслав Евгеньевич Погуца (pce@iao.ru); Михаил Ефимович Левицкий (top@iao.ru).

флуктуаций оправдано только для слабых флуктуаций. В режиме сильных турбулентных флуктуаций, когда фаза изменяется на несколько π, предпочтительнее рассматривать флуктуации интенсивности. В [10–14] приведены результаты экспериментальной реализации указанного принципа, а также выполнены теоретические расчеты для фиксированных дистанций распространения и фиксированных апертур приемо-передающих систем.

В настоящей работе представлены результаты численных расчетов степени когерентности сопряженных сигналов в зависимости от геометрических параметров приемо-передающей системы и турбулентных условий на трассе. Расчеты выполнены для различных дистанций, радиусов апертур, значений структурной характеристики флуктуаций показателя преломления C_n^2. Также приводятся результаты лабораторного эксперимента, находящиеся в хорошем согласии с численными расчетами. При этом в нашей работе не рассматривается сама процедура формирования ключа и не проводится исследование ошибок при его формировании.

На рис. 1 показана принципиальная схема работы систем связи.

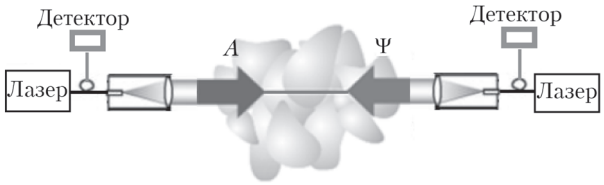

Рис. 1. Принципиальная схема работы систем беспроводной оптической связи через турбулентную атмосферу. Полагаем, что размеры апертур на обоих концах линии связи одинаковы

Работа системы моделировалась в параксиальном приближении на основе численного решения параболического управления для амплитуд встречных пучков A и Ψ с длиной волны $\lambda = 1{,}06$ мкм; турбулентная среда – в виде набора из 10 фазовых экранов, равномерно расположенных на трассе распространения излучения. Развертка сигналов во времени t формировалась путем поперечного смещения фазовых экранов со скоростью ветра v.

Степень корреляции сигналов для различных дистанций и турбулентных условий

Для определения количественной степени совпадения сигналов (значений принимаемой мощности) рассчитывался коэффициент корреляции Пирсона

$$K_{\text{P}} = \frac{\sum \left(P_0 - \langle P_0 \rangle\right)\left(P_Z - \langle P_Z \rangle\right)}{\sqrt{\sum \left(P_0 - \langle P_0 \rangle\right)^2 \sum \left(P_Z - \langle P_Z \rangle\right)^2}}, \qquad (1)$$

где P_0, P_Z – значения мощностей, падающих на апертуры оптических систем (PIB – power-in-the-bucket), расположенных в сопряженных плоскостях $z = 0$ (P_0 = PIBO) и $z = Z$ (P_Z = PIBZ); суммирование и усреднение осуществляется по выборке из 5000 реализаций. Примеры расчетов изменения мощностей, нормированных на начальные, в зависимости от нормированного времени tv/a для различных дистанций L, диаметров апертур d и структурной характеристики C_n^2 приведены на рис. 2–3.

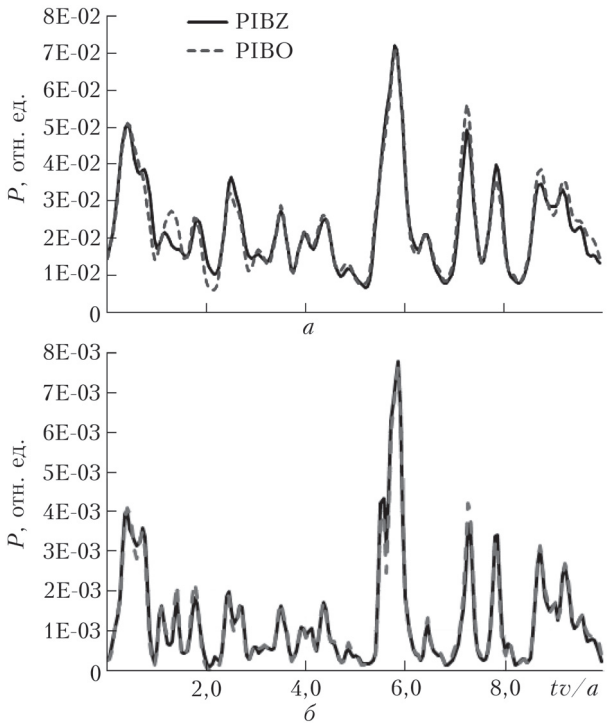

Рис. 2. Зависимость сигналов от времени для дистанции $L = 7$ км и $C_n^2 = 1{,}5 \cdot 10^{-15}$ м$^{-2/3}$: $d = 33$ мм, $K_{\text{P}} = 0{,}9735$ (*а*); $d = 16$ мм, $K_{\text{P}} = 0{,}9924$ (*б*)

На рис. 2, *а* приведены результаты расчетов для параметров трассы и размеров апертур, аналогичных используемым в эксперименте [5]. Расчеты выполнены для $\lambda = 1{,}06$ мкм (в [5] $\lambda = 1{,}53$ мкм). В этой ситуации коэффициент корреляции ($K_{\text{P}} = 0{,}9735$) оказывается меньше 0,99. На рис. 2, *б* показаны расчеты для той же трассы и турбулентных условий, но для апертур, уменьшенных примерно в 2 раза. Видно, что уменьшение размера апертуры существенно увеличивает коэффициент корреляции сигналов ($K_{\text{P}} = 0{,}9924$).

На рис. 3 представлены результаты расчета сигналов для $L = 2$ км и $C_n^2 = 2{,}3 \cdot 10^{-14}$ м$^{-2/3}$. Для $d = 16$ мм уменьшение дистанции привело к снижению K_{P} от 0,9924 (для $L = 7$ км) до 0,9656. Если для указанной дистанции уменьшить размер апертуры до $d = 10$ мм, то $K_{\text{P}} = 0{,}9984$.

Эти результаты – следствие того факта, что принцип взаимности сформулирован для точечных

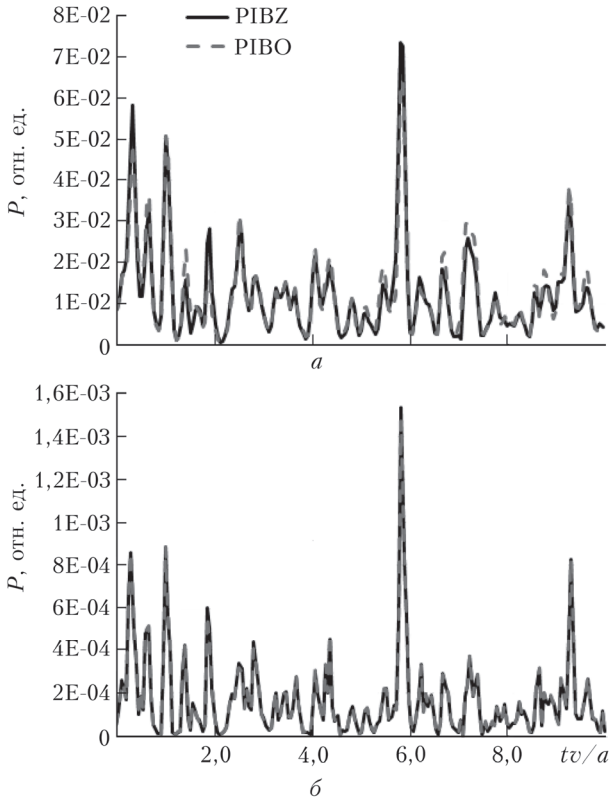

Рис. 3. Зависимость сигналов от времени для дистанции $L = 2$ км и $C_n^2 = 2{,}3 \cdot 10^{-14}$ м$^{-2/3}$: $d = 16$ мм, $K_\text{Р} = 0{,}9656$ (*а*); $d = 10$ мм, $K_\text{Р} = 0{,}9984$ (*б*)

источников. Коэффициент корреляции сигналов должен стремиться к единице при стремлении размера апертуры к нулю.

Зависимость степени корреляции от размера апертур

Результаты расчетов степени корреляции сигналов (1) для различных условий приводятся ниже. Расчеты выполнены для широкого диапазона параметров приемо-передающей системы и турбулентных условий. Дистанция L изменялась в диапазоне от 0,1 до 7 км; диаметр приемо-передающих апертур d — от 5 до 35 мм; параметр C_n^2 — от $5{,}0 \times \times 10^{-17}$ до $5{,}0 \cdot 10^{-13}$ м$^{-2/3}$. В качестве параметра, характеризующего, насколько размер апертуры приближается к точечному источнику, выступает параметр дифракции $\Omega = \dfrac{kd^2}{8L}$ (k — волновое число). Предельное значение параметра дифракции, равное нулю, соответствует точечному источнику.

Для более наглядного представления результатов введем коэффициент декорреляции $\Delta = (1 - K_\text{Р}) \cdot 100\%$. Турбулентные условия на трассе характеризуются безразмерным параметром $D_0 = d/r_0$, где r_0 — радиус Фрида:

$$r_0 = 1{,}68\left(k^2 L C_n^2\right)^{-3/5}.$$

Расчет производился на сетке размером 1024×1024 точек, а турбулентные неоднородности моделировались посредством 10 фазовых экранов. Усреднение проводилось по 5000 статистически независимым реализациям турбулентности (наборам фазовых экранов).

Из результатов расчетов, показанных на рис. 4, следует, что степень декорреляции сигналов значительно снижается при уменьшении дифракционного параметра. Для фиксированного значения дифракционного параметра меньшие значения декорреляции наблюдаются для бóльших дистанций. С усилением турбулентных флуктуаций показателя преломления возрастает степень декорреляции. Расчеты указывают, что для $\Omega < 0{,}05$ достигается уровень декорреляции $\Delta < 1\%$ во всем диапазоне рассмотренных параметров.

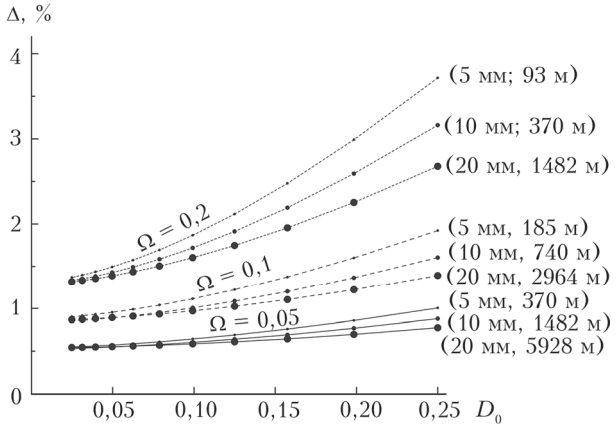

Рис. 4. Зависимость коэффициента декорреляции Δ от параметра D_0 для различных значений Ω; справа от кривых указаны пары значений (d, L)

Результаты, приведенные на рис. 4, могут быть аппроксимированы эмпирической формулой

$$\Delta \approx 3{,}9\Omega^{2/3} + 14\Omega^{6/5}\left(1\text{м}/d\right)^{9/20} D_0^{8/5}. \qquad (2)$$

Значения коэффициента декорреляции, вычисленные по формуле (2), совпадают с результатами численного моделирования на рис. 4 с погрешностью, не превышающей 5–10%.

Энергетические параметры системы. Мощность, перехваченная приемной апертурой

Выше было показано, что для увеличения степени корреляции сигналов необходимо уменьшать значение параметра дифракции, то есть диаметр приемной апертуры. Но это приводит к снижению принимаемой мощности. При организации работы систем связи по открытым атмосферным каналам вопрос о выборе мощности является комплексным. С одной стороны, мощность должна быть достаточно высокой для надежного приема сигнала в конце

трассы. С другой стороны, она не должна превышать некоторый критический уровень, гарантирующий безопасность для людей, животных и объектов, которые могут оказаться в области воздействия излучения.

На рис. 5 приведены расчеты доли мощности, перехватываемой приемной апертурой, в зависимости от безразмерного параметра турбулентности D_0 для различных значений Ω. Расчеты были выполнены при тех же условиях, что и на рис. 4.

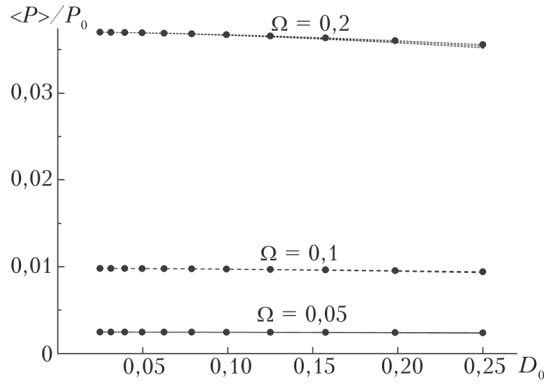

Рис. 5. Средняя мощность, принимаемая на другом конце трассы, нормированная на мощность источника (т.е. доля принимаемой мощности), в зависимости от D_0 для различных значений Ω

Доля принимаемой мощности практически однозначно определяется значением дифракционного параметра Ω и не зависит от дистанции. Для $\Omega < 0{,}1$ доля принимаемой мощности практически не зависит от турбулентных условий, так как для этих параметров дифракционная расходимость пучка многократно превышает турбулентную расходимость. Для $\Omega = 0{,}1$ доля принимаемой мощности составляет ~ 1%, и с дальнейшим уменьшением указанного параметра квадратично уменьшается. С увеличением дифракционного параметра доля мощности возрастает. Для $\Omega = 0{,}15$ она составляет ~ 2%. Но увеличение мощности сопряжено с уменьшением степени корреляции сигналов.

Относительная дисперсия флуктуаций сигнала

Следует отметить, что в рассматриваемой постановке задачи случайные флуктуации мощности являются не шумом, а полезным (информативным) сигналом. Поэтому с увеличением дисперсии сигнала растет измеряемая степень корреляции. При уменьшении дисперсии принимаемой мощности (полезного сигнала) дисперсия полезного сигнала может сравняться с дисперсией шума приемо-передающего тракта, который при наложении на полезный сигнал может существенно понизить корреляцию сигналов.

На рис. 6 приведена относительная дисперсия случайного (турбулентного) сигнала, рассчитанная при тех же параметрах, что и на рис. 4 и 5.

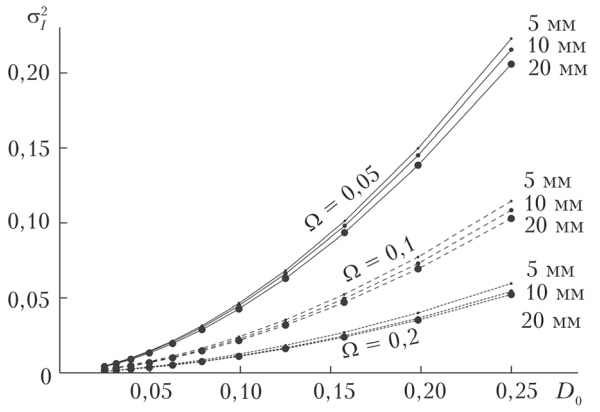

Рис. 6. Относительная дисперсия случайного (турбулентного) сигнала в зависимости от D_0 для различных значений Ω; справа от кривых указан диаметр апертуры

Видно, что с уменьшением турбулентности очень быстро уменьшается и дисперсия полезного сигнала. Для меньших значений параметра дифракции дисперсия имеет более высокие значения. Уменьшение дисперсии с ростом Ω связано с эффектом усредняющего действия апертуры.

Экспериментальная установка

Для исследования характеристик оптического излучения и атмосферного канала, определяющих характер криптографического ключа в лабораторных условиях, использовалась экспериментальная установка, схема которой приведена на рис. 7.

В качестве источника излучения использовался одномодовый полупроводниковый лазер *1* с распределенными брэгговскими решетками и волоконным выводом излучения, генерирующий линейно-поляризованное излучение с центральной длиной волны $\lambda = 1064$ нм и выходной мощностью до 150 мВт. Излучение лазера разделялось на два канала, равных по мощности, с помощью волоконного разветвителя (каплера) *2*. В каждом канале был установлен волоконно-оптический циркулятор *3*, *4*, разделяющий каналы передачи и приема излучения. Циркуляторы сопряжены с волоконными коллиматорами *8*, *9*, которые используются как для передачи, так и для приема излучения. Принимаемое излучение регистрировалось фотодетекторами *5* и *6*. Волоконные коллиматоры *8* и *9* были идентичными с фокусным расстоянием 6,12 мм и формировали гауссовы пучки излучения с диаметром на выходе 1,33 мм на уровне интенсивности e^{-2} и расходимостью, близкой к дифракционному пределу.

Коллимированное излучение распространялось на заданную (переменную) дистанцию, отражалось от плоского зеркала *13* и частично (вследствие большой расходимости) попадало на приемную апертуру коллиматора *9*, затем отводилось с помощью циркулятора *4* на фотодетектор *6*. В свою очередь, выходное волокно циркулятора *4* соединялось с коллиматором *9*, и далее коллимированное излучение

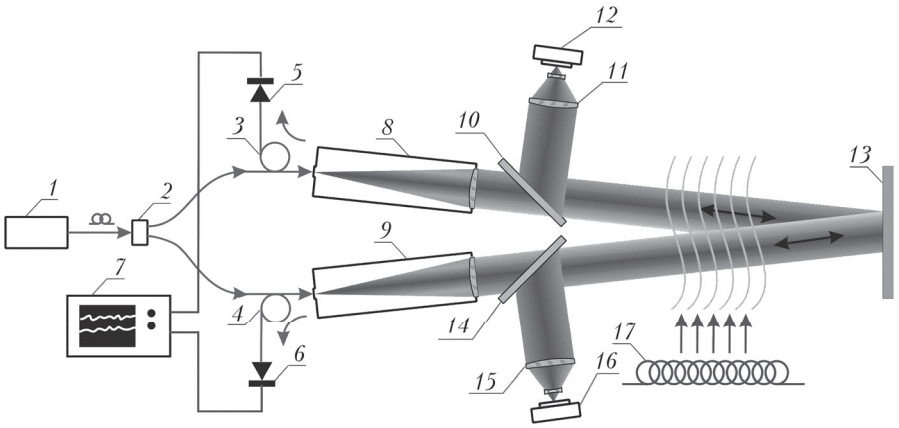

Рис. 7. Схема экспериментальной установки: *1* – одномодовый лазер; *2* – волоконный разветвитель; *3* и *4* – волоконные циркуляторы; *5* и *6* – фотодетекторы; *7* – осциллограф; *8* и *9* – коллиматоры; *10* и *14* – светоделительные пластины; *11* и *15* – обратные коллиматоры; *12* – измеритель пространственных характеристик пучка; *16* – датчик Шака–Гартмана; *13* – плоское зеркало; *17* – нагреватель

распространялось на ту же (переменную) дистанцию, отражалось от плоского зеркала *13* и частично попадало на приемную апертуру коллиматора *8*, а затем отводилось с помощью циркулятора *3* на фотодетектор *5*. Сигналы с фотодетекторов регистрировались двухлучевым осциллографом.

Таким образом была сформирована двухсторонняя линия связи, в которой передающие и приемные каналы сопряжены. Часть излучения из каждого канала отводилась с помощью светоделительных пластин *10* и *14* и посредством обратных коллиматоров *11* и *15*, сжимающих пучки в 4 раза, поступала на измеритель пространственных характеристик пучка *12*, расположенный в одном из каналов, либо на датчик Шака–Гартмана, расположенный в другом канале.

В эксперименте были реализованы трассы протяженностью $L = 7$; 14; 23 и 35 м. На трассе распространения излучения была предусмотрена возможность расположения протяженного (1 м длиной) нагревателя *17*, создающего тепловой поток для моделирования условий атмосферной турбулентности. Температура нагревателя изменялась путем регулировки напряжения. Вид сигнала в зависимости от напряжения показан на рис. 8.

Видно, что с уменьшением напряжения нагревателя (т.е. с уменьшением силы турбулентности) степень корреляции сигналов падает. Как отмечалось выше, это могло быть связано с возрастанием доли некоррелированной шумовой составляющей в сигнале. Для проверки этого факта была использована частотная фильтрация сигналов. Результаты расчета коэффициента декорреляции сигналов от частоты среза фильтров приведены на рис. 9.

Проведенный анализ показал, что для частоты среза менее 200 Гц наблюдается искажение полезного сигнала. Фильтрация с частотой среза 300 Гц дает оптимальный результат, при котором полезный сигнал очищается от высокочастотного некоррелированного шума, не испытывая заметных искажений.

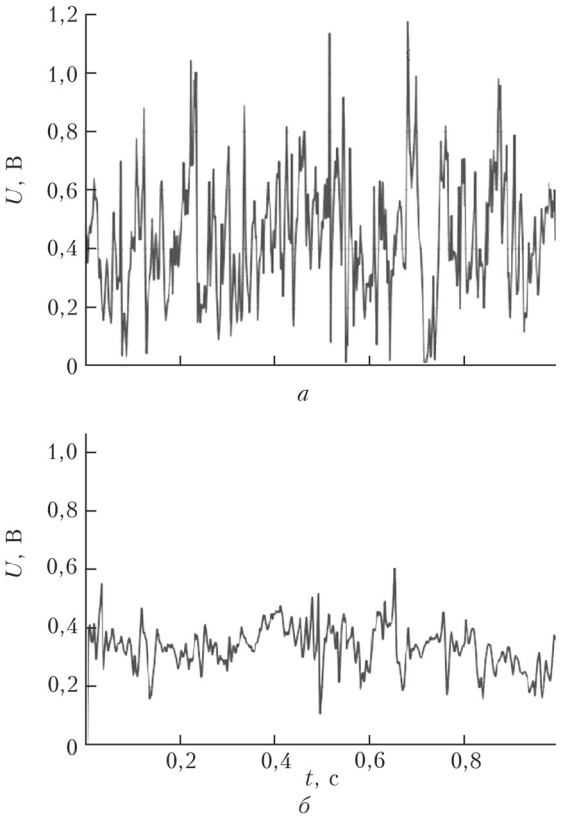

Рис. 8. Развертка сигналов для напряжения нагревателя $U = 220$ (*а*) и 70 В (*б*)

Сравнить сигналы до и после фильтрации можно на рис. 10.

Отметим, что после фильтрации вид сигнала становится подобным виду сигнала, полученному в численном моделировании (см. рис. 2).

Результаты определения коэффициента декорреляции после фильтрации сигнала для $L = 7$; 14; 23 и 35 м приведены на рис. 11, где каждая точка построена после усреднения по 10 сериям измерений для каждой дистанции.

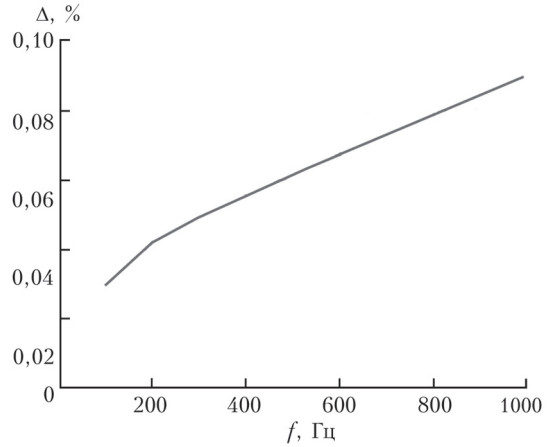

Рис. 9. Зависимость коэффициента декорреляции Δ от частоты среза фильтра

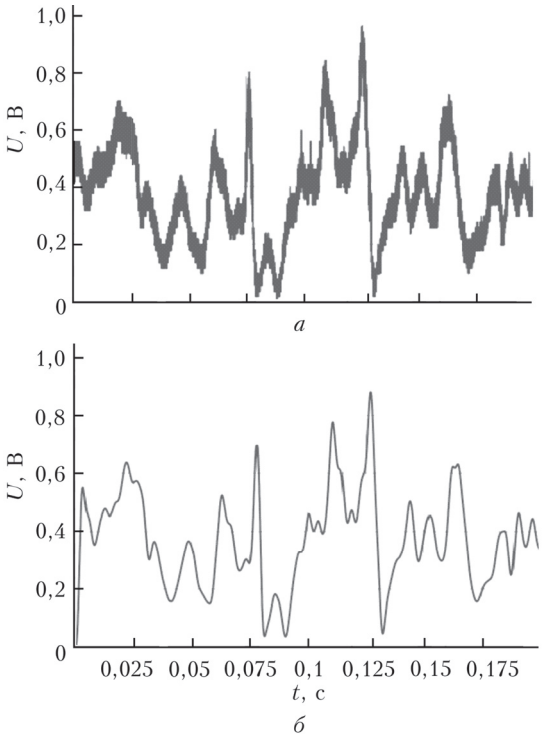

Рис. 10. Начальный участок сигнала ($\Delta t = 0{,}2$ с): *а* – до фильтрации с частотой среза 300 Гц; *б* – после фильтрации

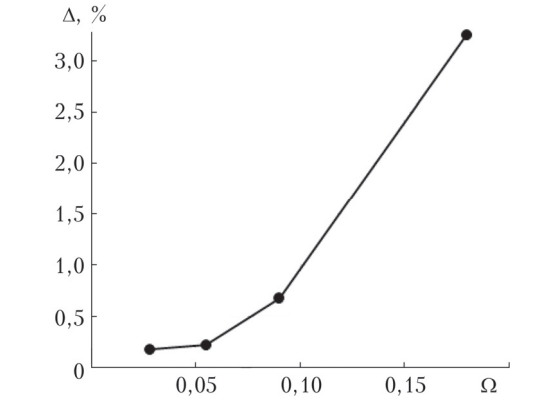

Рис. 11. Экспериментальная зависимость коэффициента декорреляции Δ от дифракционного параметра Ω (L = 7; 14; 23 и 35 м)

Видно, что результаты эксперимента достаточно хорошо согласуются с результатами численных расчетов. Для дифракционного параметра $\Omega \cong 0{,}1$ степень декорреляции принимает значения порядка 1%.

Заключение

Выполнено численное моделирование распространения двух сопряженных (направленных друг на друга) пучков приемо-передающих систем на основе измерений быстро меняющихся характеристик оптических полей, искаженных атмосферным каналом распространения. Создана экспериментальная установка и проведено экспериментальное исследование формирования коррелированных случайных сигналов в приемо-передающих лазерных системах. Установлена необходимость использования и исследована эффективность фильтрации низких частот принимаемых сигналов.

На основе численного моделирования получены зависимости коэффициента корреляции от геометрических параметров системы и турбулентных условий на трассе для различных дистанций (0,1–7 км), радиусов апертур (5–35 мм), значений структурной характеристики флуктуаций показателя преломления ($5{,}0 \cdot 10^{-17} - 5{,}0 \cdot 10^{-13}$ м$^{-2/3}$). Теоретически показано, что для $\Omega < 0{,}05$ достигается уровень корреляции сигналов > 99% во всем диапазоне исследуемых параметров. Этот результат хорошо согласуется с результатами лабораторного эксперимента.

Работа в части теоретических и экспериментальных исследований возможностей использования принципа взаимности на линии оптической связи в турбулентной среде финансово поддержана РНФ (проект № 18-19-00437), исследования статистики флуктуаций энергетических параметров пучков выполнены при частичной поддержке РФФИ (проект № 18-29-20115\18), разработка методов и программ численного моделирования распространения лазерных пучков в атмосфере выполнена по проекту фундаментальных исследований РАН № АААА-А17-117021310143-2.

1. *Fürst H., Weier H., Nauerth S., Marangon D.G., Kurtsiefer C., Weinfurter H.* High speed optical quantum random number generation // Opt. Express. 2010. V. 18, N 12. P. 13029–13037. DOI: 10.1364/OE.18.013029.
2. *Fiorentino M., Santori C., Spillane S.M., Beausoleil R.G., Munro W.J.* Secure selfcalibrating quantum random-bit generator // Phys. Rev. 2007. V. 75, N 3. DOI: 10.1103/PhysRevA.75.032334.
3. *Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U.L., Marquardt C., Leuchs G.* A generator for unique quantum random numbers based on vacuum states // Nat. Photon. 2010. V. 4, N 10. P. 711–715. DOI: 10.1038/NPHOTON.2010.197.
4. *Bennett C.H., Brassard G.* Quantum cryptography: public key distribution and coin tossing // Theor. Comput. Sci. 2014. V. 560, N 1. P. 7–11. DOI: 10.1016/j.tcs.2014.05.025.
5. *Сидоров В.В., Карпов А.В., Сулимов А.И.* Метеорная генерация секретных ключей шифрования для защиты открытых каналов связи // Информ. технол. и вычислительные системы. 2008. № 3. С. 45–54.

6. *Sulimov A.I., Galiev A.A., Karpov A.V., Markelov V.V.* Verification of wireless key generation using software defined radio // Proc. Intern. Siberian Conf. on Control and Commun. (SIBCON). Tomsk, Russia. 2019. P. 1–6. DOI: 10.1109/SIBCON.2019.8729607.
7. *Sulimov A.I., Karpov A.V.* Performance evaluation of meteor key distribution // Proc. the 12th Intern. Conf. on Security and Cryptography (SECRYPT-2015). Colmar, France. 2015. P. 392–397.
8. *Premnath S.N., Jana S., Croft J., Gowda P.L., Clark M., Kasera S.K., Patwari N., Krishnamurthy S.V.* Secret key extraction from wireless signal strength in real environments // IEEE Trans. Mobile Comput. 2013. V. 12, N 5. P. 917–930.
9. *Wallace J.W., Sharma R.K.* Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis // IEEE Trans. Inf. Forensics Security 2010. V. 5, N 3. P. 381–392.
10. *Minet J., Vorontsov M.A., Polnau E., Dolfi D.* Enhanced correlation of received power-signal fluctuations in bidirectional optical links // J. Opt. 2013. V. 15, N 2. P. 022401.
11. *Drake M.D., Bas C.F., Gervais D.R., Renda P.F., Townsend D., Rushanan J.J., Francoeur J., Donnangelo N.C., Stenner M.D.* Optical key distribution system using atmospheric turbulence as the randomness generating function: Classical optical protocol for information assurance // Opt. Eng. 2013. V. 52, N 5. P. 055008.
12. *Wang N., Song X., Cheng J., Leung V.C.* Enhancing the security of free-space optical communications with secret sharing and key agreement // J. Opt. Commun. Netw. 2014. V. 6, N 12. P. 1072–1081.
13. *Shapiro J.H., Puryear A.L.* Reciprocity-enhanced optical communication through atmospheric turbulence — Part I: Reciprocity proofs and far-field power transfer optimization // J. Opt. Commun. Netw. 2012. V. 4, N 12. P. 947–954.
14. *Bornman N., Forbes A., Kempf A.* Random number generation & distribution out of thin (or thick) air // J. Opt. 2020. V. 22, N 7. P. 075705. DOI: 10.1088/2040-8986/ab9513.

V.P. Aksenov, V.V. Dudorov, V.V. Kolosov, Ch.E. Pogutsa, M.E. Levitskii. **The analysis of intensity correlation in laser transceiving systems for keying.**

The potentials for and limitations to the use of intensity fluctuations of laser beams propagating through a turbulent atmosphere for generating random data when keying in confidential optical communication systems are analyzed. The technique is based on the reciprocity theorem for optical fields. Light propagation in a system of two transceivers directed at each other, the signals from which are distorted by an atmospheric channel, is numerically simulated. An experimental setup is created; the generation of random correlated signals in such a system is experimentally studied. A need for low-pass filtering of signals received is experimentally ascertained. The efficiency of this filtration is estimated. The dependences of the correlation coefficient on the geometrical parameters of the system and turbulent conditions along the propagation path are derived from the numerical simulation in a wide range of distances, aperture radii, and values of turbulence intensity. Theoretical results are shown to be in a good agreement with the results of laboratory experiments.