УДК 621.396.96 DOI 10.18522/2311-3103-2022-4-63-77

К.Е. Румянцев, П.Д. Миронова, Шакир Хайдер Хуссейн

ОЦЕНКА ВЛИЯНИЯ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ НА ПАРАМЕТРЫ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ОСНОВЕ ПРОТОКОЛА B92

Исследовано влияние параметров функциональных элементов на энергетические, временные и вероятностные характеристики системы квантового распределения ключа (КРК) на основе протокола B92. Построены зависимости вероятности записи правильного и ошибочного битов в сырую квантовую ключевую последовательность от длины волоконно-оптической линии связи (ВОЛС) и использовании 4-х типов лазеров (EML, DFB, VCSEL, FP) и фотоприёмных модулей (id201; id210; id220; id230). Установлено, что, изменения вероятности записи правильного бита в сырую квантовую ключевую последовательность значительно более весомы, чем изменения вероятности записи ошибочного бита (50,9 раза против 3,3 раза при ширине спектра лазера 80 пм и изменении протяжённости ВОЛС с 10 до 100 км). Это связано с тем, что с ростом протяжённости ВОЛС резко растёт вероятность отсутствия регистрации на приёмной станции фотонов или импульсов темнового тока (ИТТ). Числовой материал указывает на прямую пропорциональную зависимость вероятности записи ошибочного бита от частоты генерации шумовых импульсов однофотонных лавинных фотодиодов (ОЛФД). Так, при увеличении частоты появления ИТТ в 60 раз (с 100 до 6000 Гц) вероятность записи ошибочного бита также увеличивается в 60 раз (например, при длине ВОЛС 100 км – 6,39 против 383,3). Установлено, что среднеквадратичное отклонение (СКО) времени задержки фотона прямо пропорционально длине ВОЛС и ширине спектра лазера. При ширине спектра лазера 10 пм и увеличении длины ВОЛС с 10 до 100 км (в 10 раз) среднеквадратичное отклонение времени задержки фотона также увеличивается в 10 раз (с 4,16 до 41,6 пс). Для достижения наилучших характеристик системы КРК в целом целесообразно использование лазера с минимальной шириной спектра излучения, например, EML-лазера. Однако EML-лазеры считаются самыми сложными и дорогостоящими из рассмотренных типов лазеров, поэтому использование EML-лазеров значительно повышает стоимость всей системы КРК.

Квантовое распределение ключей; протокол B92; энергетические характеристики; временные характеристики; вероятностные характеристики.

K.E. Rumyantsev, P.D. Mironova, Shakir Hayder Hussein

EVALUATION OF THE FUNCTIONAL ELEMENTS INFLUENCE ON THE PARAMETERS OF THE QKD SYSTEM BASED ON B92 PROTOCOL

The influence of the parameters of functional elements on the energy, time and probabilistic characteristics of the quantum key distribution system (QKD) based on the B92 protocol is studied. The dependences of the probability of writing correct and erroneous bits into a raw quantum key sequence are plotted for various lengths of a fiber-optic communication line (FOCL) and the use of various lasers (EML-laser; DFB-laser; VCSEL-laser and FP-laser) and photodetector modules (id201; id210; id220; id230). Thus, changes in the probability of writing a correct bit into a raw quantum key sequence are much more significant than changes in the probability of writing an erroneous bit (50.9 times versus 3.3 times with FWHM=80 pm and a change in the length of the FOCL from 10 to 100 km). This is due to the fact that with an increase in the length of the FOCL, the probability of the absence of registration at the receiving station of photons or dark current pulses (DCP) sharply increases. Numerical material indicates a direct proportional dependence of the probability of writing an erroneous bit on the frequency of generation of noise pulses of single-photon avalanche photodiodes (SAPD). So, with an increase in the frequency of occurrence of DCP by 60 times (from 100 to 6000 Hz), the probability of recording an erroneous bit also increases by 60 times (for example, with a FOCL length of 100 km – 6.39 versus 383.3). It has been established that the root-mean-square deviation of the photon delay time is directly

proportional to the length of the FOCL and the width of the laser spectrum. With a spectrum width of FWHM=10 pm and an increase in the FOCL length from 10 to 100 km (by a factor of 10), the standard deviation of the photon delay time also increases by a factor of 10 (from 4.16 to 41.6 ps). To achieve the best performance of the QKD system as a whole, it is advisable to use a laser with a minimum width of the radiation spectrum, for example, an EML-laser. However, EML-lasers are considered the most complex and expensive of all the considered types of lasers, so the use of EML-lasers significantly increases the cost of the entire QKD system.

Quantum key distribution; B92 protocol; energy characteristics; time characteristics; probabilistic characteristics.

Введение. Обеспечение безопасности данных при передаче между легитимными пользователями является актуальной задачей. Существует множество классических систем и способов шифрования и передачи информации, которые с развитием вычислительной техники не обеспечивают секретность передаваемых данных.

В отличие от классических систем, применение систем квантового распределения ключа (КРК) обеспечивает абсолютную безопасность данных и контроль несанкционированного доступа (НСД) злоумышленниками [1–14], что достигается благодаря принципу неопределённости Гейзенберга: попытка измерения в квантовой системе искажает её состояние, а полученная в результате такого измерения информация не полностью соответствует состоянию системы до начала измерений.

Анализируемая система КРК состоит из приёмопередающей и кодирующей станций, связанных посредством волоконно-оптической линии связи (ВОЛС). Используя методику расчёта параметров как системы КРК в целом, так и отдельных функциональных модулей [15], разработано программное обеспечение для анализа влияния отдельных характеристик функциональных элементов на энергетические, временные и вероятностные параметры системы.

Оценка влияния протяжённости направляющей линии коммуникации на параметры системы КРК. Проводим моделирование работы системы КРК по протоколу B92 для оценки вероятностных, временных и энергетических характеристик системы КРК при протяжённости ВОЛС в диапазоне 10…100 км для ряда значений ширины спектра лазера FWHM. Диапазон изменений значений параметра FWHM 10…100 пм характерен для электроабсорбционных модулированных лазеров (EML − Electroabsorptive Modulated Laser). Особенностью EML-лазеров является присутствие в спектре излучения одной ярко выраженной моды.

Центральная длина волны лазерного излучения равна λ_s=1550 нм, а среднее число регистрируемых фотонов за длительность квантового импульса на выходе однофотонного источника $\overline{N_{FA}}$=0,2. Длительность импульса лазера принята равной τ_s=300 пс. При моделировании исключается нестабильность генерации лазерных импульсов ΔT_s=0.

Погонное затухание одномодового оптического волокна SMF-28 ULL, используемого в ВОЛС, составляет α_{SMF}=0,18 дБ/км, а эффективный показатель преломления в сердечнике $n_{SMF} = 1{,}4682$.

Погонное затухание одномодового оптического волокна Panda, сохраняющего состояние поляризации и применяемого внутри передающей и приёмной станций, составляет α_{PMF}=1 дБ/км, а эффективный показатель преломления в сердцевине n_{PMF}=1,468.

При моделировании исключается нестабильность генерации импульсов стробирования ΔT_{strob}=0.

Частота генерации импульсов темнового тока в однофотонном лавинном фотодиоде (ОЛФД) f_b= 100 Гц.

На рис. 1 представлена зависимость вероятности записи правильного бита в сырую квантовую ключевую последовательность от длины ВОЛС. По оси OY используется логарифмический масштаб.

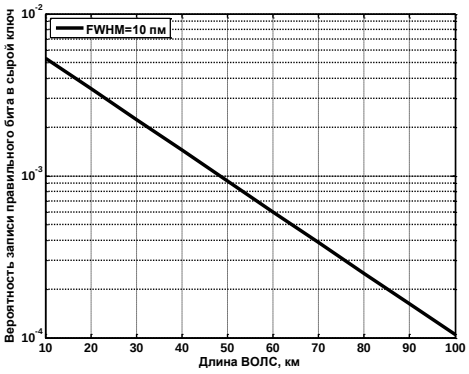

Рис. 1. Вероятность записи правильного бита в сырую квантовую ключевую последовательность при различных значениях длины ВОЛС

Необходимо отметить значительное снижение вероятности записи правильного бита при увеличении длины ВОЛС. При увеличении длины ВОЛС в 5 раз с 10 до 50 км вероятность записи правильного бита снижается в 5,7 раза, а с 10 до 100 км (в 10 раз) – уже в 48,5 раз. Причём, при каждом увеличении длины ВОЛС на 10 км вероятность записи правильного бита падает в 1,55 раза (на ~2 дБ).

Такое поведение вероятности следует из роста потерь оптического излучения непосредственно в одномодовом волокне на 1,8 дБ при изменении протяжённости ВОЛС на 10 км. Незначительный дополнительный рост потерь на 0,01 дБ при каждом приросте протяжённости ВОЛС на 10 км связан с потерями на сварных соединениях.

Если при длине ВОЛС в 10 км вероятность записи правильного бита в сырую квантовую ключевую последовательность составляет порядка 0,005, то при длине ВОЛС в 100 км не превышает 0,0001. Следовательно, только 1 бит из 10 000 сгенерированных будет правильно записан в сырую ключевую последовательность.

Как и следовало ожидать, ширина спектра лазера FWHM не влияет на вероятность записи правильного бита в сырую квантовую ключевую последовательность при оптимальном выборе длительности импульса стробирования в соответствии с формулой $\tau_{strob} = \tau_s + 2 \cdot \Delta\tau_{TF} + 2 \cdot \Delta T_{strob}$.

На рис. 2 представлена зависимость вероятности записи ошибочного бита в сырую квантовую ключевую последовательность от длины ВОЛС. По оси OY здесь также использован логарифмический масштаб.

При изменении протяжённости ВОЛС с 10 до 100 км при FWHM=80 пм вероятность записи ошибочного бита в сырую квантовую ключевую последовательность увеличивается в 4,6 раза (на 6,6 дБ) с $2{,}5 \cdot 10^{-8}$ до $11{,}7 \cdot 10^{-8}$. При увеличении длины ВОЛС с 10 до 20 км вероятность записи ошибочного бита увеличивается в 1,4 раза, при увеличении с 20 до 30 км – в 1,3 раза, а при увеличении с 90 до 100 км – всего в 1,10 раза. Напомним, что вероятность записи правильного бита изменяется в 1,55 раза при любом изменении длины ВОЛС на 10 км.

Сравнение с данными на рис. 1 показывает, что изменения вероятности записи правильного бита в сырую квантовую ключевую последовательность значительно более весомы, чем изменения вероятности записи ошибочного бита (50,9 раза против 3,3 раза при FWHM=80 пм и изменении протяжённости ВОЛС с

10 до 100 км). Это связано с тем, что с ростом протяжённости ВОЛС резко растёт вероятность отсутствия регистрации на приёмной станции фотонов или импульсов темнового тока (ИТТ).

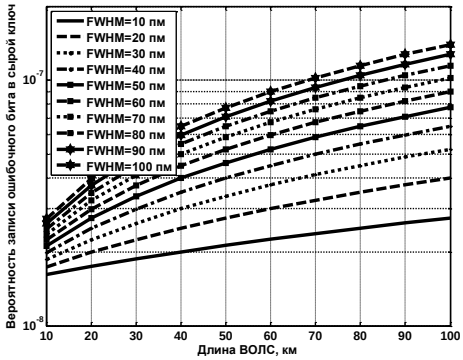

Рис. 2. Вероятность записи ошибочного бита в сырую квантовую ключевую последовательность при различных значениях длины ВОЛС

В процессе моделирования установлено, что влиянием поляризационной модовой дисперсии в одномодовом оптическом волокне можно пренебрегать. Действительно, даже при минимальной ширине спектра лазера FWHM=10 пм и минимальной протяжённости ВОЛС в 10 км среднеквадратичное отклонение (СКО) времени задержки фотона после распространения через ВОЛС из-за хроматической дисперсии равно 4,16 пс, в то время как СКО из-за поляризационной модовой дисперсии – 0,13 пс. Различие превышает 32 раза (15 дБ). Причём различие растёт с расширением спектра лазера и превышает 320 раз при FWHM=100 пм (на верхней границе для электроабсорбционных модулированных лазеров).

На рис. 3 представлены результирующие зависимости среднеквадратичного отклонения задержки фотона после распространения через ВОЛС, которые совпадают с зависимостями СКО задержки фотона после распространения через ВОЛС из-за хроматической дисперсии.

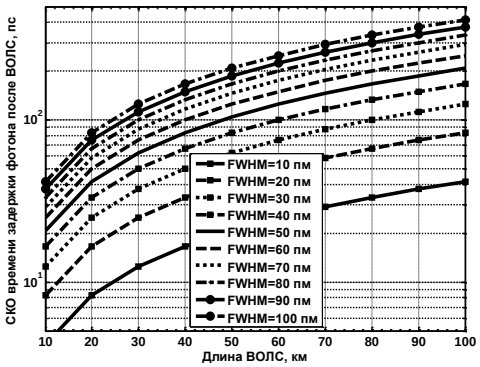

Рис. 3. Среднеквадратичное отклонение времени распространения фотона через ВОЛС

Среднеквадратичное отклонение времени задержки фотона прямо пропорционально длине ВОЛС и ширине спектра лазера. При увеличении длины ВОЛС с 10 до 100 км (в 10 раз) среднеквадратичное отклонение времени задержки фотона

также увеличивается в 10 раз (с 4,16 до 41,6 пс). Причём при каждом увеличении длины ВОЛС на 10 км при FWHM=10 пм СКО времени задержки фотона увеличивается на 4,16 пс.

Из графиков видно, что уже при протяжённости ВОЛС в 100 км среднеквадратичное отклонение времени задержки фотона превышает длительность импульса лазера τ_s=300 пс при значениях FWHM более 75 пм.

Графики на рис. 4 отражают зависимость длительности импульса стробирования от длины ВОЛС. Учитывая то, что нестабильность генерации импульсов стробирования исключена при моделировании, длительность импульса стробирования зависит только от временного разброса времени задержки фотона после распространения через ВОЛС и длительности импульса лазера, которая фиксирована.

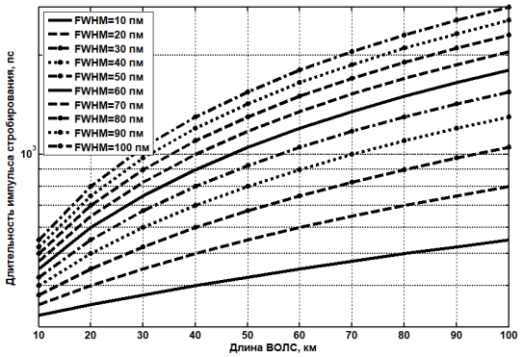

Рис. 4. Зависимости длительности импульса стробирования от длины линии коммуникации

В целом при увеличении длины ВОЛС с 10 до 100 км длительность импульса стробирования увеличивается в 1,69 раза при ширине спектра FWHM=10 пм, в 3,64 раза при FWHM=50 пм и уже в 5,09 раза при FWHM=100 пм. Различие при каждом увеличении длины ВОЛС на 10 км между предыдущим и текущим значением длительности импульса стробирования сокращается. Например, при FWHM=100 пм при увеличении длины ВОЛС с 10 до 20 км значение длительности импульса стробирования увеличивается в 1,45 раза, с 20 до 30 км – в 1,31 раза, а с 90 до 100 км – всего в 1,1 раза.

При каждом увеличении длины ВОЛС на 10 км длительность импульса стробирования возрастает. Причём если при ширине спектра FWHM=100 пм увеличение длины ВОЛС с 10 до 20 км требует увеличения длительности импульса стробирования на 45 %, то с 90 до 100 км – уже только на 10%.

Важно, что требуемая длительность импульса стробирования во много раз может превышать длительность импульса лазера. Действительно, при наименьшей ширине спектра FWHM=10 пм для группы электроабсорбционных модулированных EML-лазеров изменение длины ВОЛС с 10 до 100 км потребует выбор длительностей импульса стробирования на 8…83 % больше длительности импульса лазера. Однако при худших параметрах лазера длительность импульса стробирования будет уже в десять раз превышать длительность импульса лазера. Естественно, что последнее негативно сказывается на параметрах системы КРК, увеличивая вероятность записи ошибочного бита.

На рис. 5 представлена зависимость максимальной требуемой частоты следования оптических импульсов от длины ВОЛС.

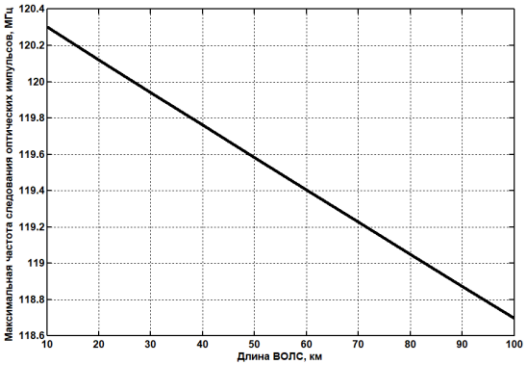

Рис. 5. Максимальная требуемая частота следования оптических импульсов при различных значениях длины ВОЛС

При каждом увеличении длины ВОЛС на 10 км максимальная частота следования оптических импульсов уменьшается на 170…180 кГц. Например, при длине ВОЛС 10 км максимальная частота следования оптических импульсов составляет 120,3 МГц, при длине ВОЛС 20 км – 120,12 МГц, при длине ВОЛС 100 км – 118,7 МГц. В целом при увеличении длины ВОЛС в 10 раз (с 10 до 100 км) максимальная требуемая частота следования оптических импульсов уменьшается на 1,6 МГц (120,3 МГц против 118,7 МГц).

Оценка влияния типов лазеров на параметры системы КРК. В системах КРК применяются различные типы лазеров. Выбор последнего зависит от необходимых характеристик реализуемой системы, например ширина спектра излучения, скорость передачи данных, стоимость и другие. Приведённые выше результаты характерны для электроабсорбционных модулированных лазеров (EML − Electroabsorptive Modulated Laser), отличительной особенностью которых является присутствие в спектре излучения одной ярко выраженной моды.

Специфика применения различных типов лазеров в системах КРК рассмотрена в [16]. Показано, что кроме EML-лазеров в системах КРК используют ещё три типа лазеров:

♦ простейшие излучатели Фабри-Перо, используемые в одномодовых и многомодовых передатчиках;

♦ поверхностно-излучающие лазеры с вертикальным резонатором (VCSEL-лазеры), получившие распространение в многомодовых системах на коротких расстояниях и отличающиеся высокой температурной стабильностью, малой потребляемой мощностью и минимальной стоимостью производства передатчиков на их основе;

♦ лазеры с распределённой обратной связью (DFB-лазеры), обеспечивающие высокую мощность излучения при сохранении узкой ширины спектра излучения. Также лазеры DFB обладают высокой температурной стабильностью и возможностью подстройки длины волны.

Характеристики указанных типов лазеров сведены в табл. 1 [17–19].

Таблица 1

Характеристики различных типов лазеров

Параметр лазера	FP	VCSEL	DFB	EML
Длина волны излучения, нм	1310/1550 850/1300	850	850 1550	1550
Скорость передачи данных, не более, Гбит/с	1	25	1 до 150 км 10 до 40 км	100
Ширина спектра излучения, нм	3…5	0,5…1	0,1…0,5	0,01…0,08
Типовая длительность оптического импульса, пс	300		300	
Стоимость, USD	25…500	5…100	100…3000	

Проведён вычислительный эксперимент для сравнительного анализа вероятностных, временных и энергетических характеристик рассмотренных типов лазеров при изменении протяжённости направляющей ВОЛС в диапазоне 10…100 км для крайних (минимального и максимального) значений ширины спектра излучения лазеров FWHM (для FP-лазера – 3 и 5 нм, для VCSEL-лазера – 0,5 и 1 нм, для DFB-лазера – 0,1 и 0,5 нм, для EML-лазера – 0,01 и 0,08 нм).

Использование лазеров с большой шириной спектра излучения значительно сказывается на разбросе времени распространения фотонов в ВОЛС. Так, при ширине спектра излучения лазера 5 нм при использовании FP-лазера СКО времени распространения фотона достигает 20,8 нс при протяжённости ВОЛС 100 км, что в 62,5 раза больше СКО времени распространения при использовании EML-лазера с шириной спектра излучения 80 пм. Различие результирующего СКО времени распространения фотона в ВОЛС при максимальном и минимальном значениях ширины спектра излучения прямо пропорционально изменению ширины спектра излучения и составляет 8 (332,80 пс против 41,60 пс); 5 (2079,98 пс против 416,00 пс); 2 (4159,96 пс против 2079,98 пс) и 1,67 раза (20799,80 пс против 12479,88 пс) при использовании EML-лазера, DFB-лазера, VCSEL-лазера и FP-лазера соответственно.

Расчёты показывают, что результирующее среднеквадратичное отклонение времени распространения фотона в ВОЛС определяется только хроматической дисперсией. Влиянием поляризационной модовой дисперсии в одномодовом оптическом волокне можно пренебрегать при протяжённости ВОЛС менее 100 км. Это справедливо и для EML-лазеров, где могут генерироваться импульсы существенно меньшей длительности.

На рис. 6 представлена зависимость требуемой длительности импульса стробирования однофотонных фотодетекторов от длины ВОЛС. Поскольку длительность импульсов применяемых в системах КРК лазеров не превышает 300 пс, то из графиков видно значительное превышение их значений длительностями импульсов стробирования. Так в диапазоне возможных значений ширины спектра излучения для FP-лазера (см. табл. 1) длительность импульса стробирования составляет 75,2…125,1 нс при протяжённости ВОЛС в 100 км. Длительности импульсов стробирования для лазеров VCSEL, DFB и EML лежат в диапазонах 12,8…25,3 нс, 2,8…12,8 нс и 0,55…2,3 нс соответственно.

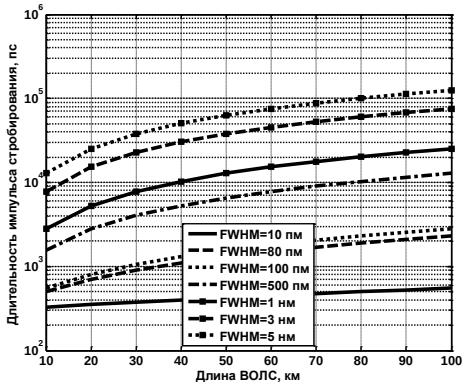

Рис. 6. Зависимость длительности импульса стробирования от длины ВОЛС

С учётом данных табл. 1 различия в длительностях импульсов лазера и стробирования превышают 250,6…417 раз для FP-лазера, 42,6…84,2 для VCSEL-лазера, 9,32…42,6 для DFB-лазера, и 1,83…7,66 раз для EML-лазера при протяжённости ВОЛС 100 км.

Многократное превышение длительности импульса лазера длительностью импульса стробирования увеличивает вероятность записи ошибочного бита.

На рис. 7 представлена зависимость вероятности записи ошибочного бита в сырую квантовую ключевую последовательность от длины ВОЛС при различных значениях ширины спектра излучения, соответствующих различным типам лазеров. По оси OY использован логарифмический масштаб.

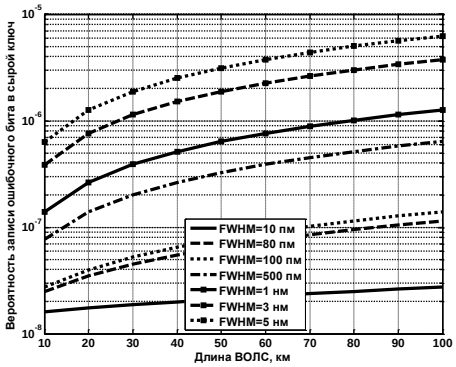

Рис. 7. Вероятность записи ошибочного бита в сырую квантовую ключевую последовательность при различных значениях длины ВОЛС

При протяжённости ВОЛС 100 км максимальное значение вероятности записи ошибочного бита в сырой ключ при использовании FP-лазера в 54 раза больше значения вероятности при использовании EML-лазера ($62{,}54 \cdot 10^{-7}$ при ширине спектра излучения 5 нм против $1{,}15 \cdot 10^{-7}$ при ширине спектра излучения 80 пм). При использовании VCSEL-лазера и DFB-лазера различие максимальных вероятностей значительно сокращается и составляет 11 и 5,6 раза соответственно, по сравнению со значением вероятности записи ошибочного бита при использовании EML-лазера ($1{,}15 \cdot 10^{-7}$ при ширине спектра излучения 80 пм). Следовательно, для достижения минимальной вероятности записи ошибочного бита целесообразно использование EML-лазера с шириной спектра излучения 10…80 пм.

Анализируя рассмотренные зависимости, отметим целесообразность использования лазера с минимальной шириной спектра излучения, например, EML-лазера, для достижения наилучших характеристик системы КРК в целом. Однако EML-лазеры считаются самыми сложными и дорогостоящими из всех рассмотренных типов лазеров [20], поэтому использование EML-лазеров значительно повышает стоимость всей системы КРК.

Влияние параметров фотоприёмного модуля на эффективность квантового распределения ключа. На эффективность квантового распределения ключа значительное влияние оказывают следующие параметры однофотонного приёмного модуля: частота поступления шумовых импульсов ОЛФД, время для восстановления работоспособности ОЛФД после регистрации фотона.

Для сравнительного анализа влияния параметров фотоприёмного модуля на вероятностные, временные и энергетические характеристики системы проведён вычислительный эксперимент. В качестве источника излучения выбран DFB-лазер с шириной спектра FWHM в 500 пм (наихудший случай с позиций FWHM) и длительностью импульса 300 пс. Нестабильность генерации импульсов стробирования исключена. В ВОЛС использовано одномодовое оптическое волокно SMF-28 ULL, а внутри передающей и приёмной станций – одномодовое оптическое волокно Panda. Центральная длина волны излучения равна 1550 нм, а среднее число фотонов за длительность квантового импульса на выходе однофотонного источника 0,2.

Проведённый ранее анализ показывает, что влияние частоты поступления шумовых импульсов ОЛФД f_b сказывается лишь на вероятность записи ошибочного бита в ключевую последовательность. Причём в силу того, что за длительность строб-импульса среднее число ИТТ значительно уступает среднему числу принимаемых фотонов влиянием на вероятность записи правильного бита можно пренебречь. Действительно, как следует из табл. 2, изменение частоты генерации шумовых импульсов ОЛФД с 1 до 100 Гц приводит к изменению вероятности записи правильного бита всего на 0,002 % при протяжённости ВОЛС 10 км, на 0,03 % при 50 км и на 0,67 % при 100 км.

Таблица 2

Умноженная на 100 000 вероятность записи правильного бита в сырую ключевую последовательность

Длина ВОЛС, км	Частота генерации шумовых импульсов ОЛФД, Гц						
	1	2	5	10	20	50	100
10	534,09	534,09	534,09	534,09	534,09	534,10	534,10
20	345,17	345,17	345,17	345,17	345,17	345,17	345,18
50	93,02	93,02	93,02	93,02	93,03	93,04	93,05
100	10,44	10,44	10,44	10,45	10,45	10,47	10,57

Это указывает на возможность при проектировании систем КРК на малошумящих ОЛФД не учитывать вклад шумовых импульсов ОЛФД и рассчитывать вероятность записи правильного бита по приближённой формуле

$$P_{bit} = \frac{(P_{bit}\{0|0\} + P_{bit}\{1|1\})}{2} \approx [1 - exp(-\overline{n_0})] \cdot [1 - exp(-\overline{n_1})] \approx \overline{n_0} \cdot \overline{n_1}.$$

Здесь $\overline{n_0}$ и $\overline{n_1}$ представляют средние числа регистрируемых событий за длительность строб-импульса в приёмной станции при условии передачи соответственно логического нуля «0» и логической единицы «1».

На рис. 8 представлены графики зависимостей вероятности записи ошибочного бита в сырую квантовую ключевую последовательность от длины ВОЛС при семи различных частотах генерации шумовых импульсов ОЛФД. По оси OY использован логарифмический масштаб.

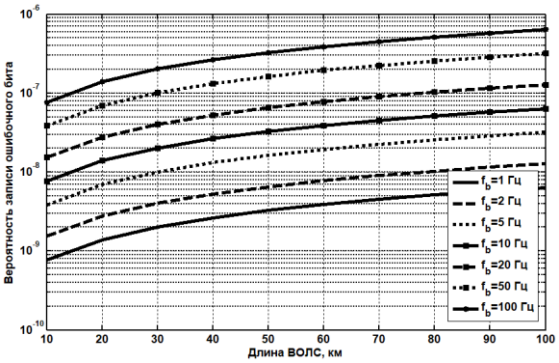

Рис. 8. Вероятность записи ошибочного бита в сырую квантовую ключевую последовательность

Числовой материал указывает на прямую пропорциональную зависимость вероятности записи ошибочного бита от частоты генерации шумовых импульсов ОЛФД.

Характеристики применяемых ОЛФД отличны от характеристик идеального однофотонного фотодетектора. Во-первых, ОЛФД регистрирует только первый фотон за время анализа. Во-вторых, в случае приёма фотона ОЛФД потребует время для восстановления рабочего состояния. Основные параметры ОЛФД, применяемых в системах КРК с рабочей длиной волны оптического излучения в диапазоне 900…1700 нм, сведены в табл. 3 [15].

Таблица 3

Параметры фотоприёмных модулей на основе ОЛФД

Наименование изделия	Частота появления ИТТ, не более, Гц	Типовое (максимальное) время восстановления рабочего состояния, нс
id201	100	0,1
id210	40	100 000
id220	6 000	25 000
id230	50	100 000

На рис. 9 представлены графики зависимостей вероятности записи ошибочного бита в сырую квантовую ключевую последовательность от длины ВОЛС при использовании конкретных фотоприёмных модулей.

Необходимо отметить, при увеличении частоты появления ИТТ в 60 раз (с 100 до 6000 Гц) вероятность записи ошибочного бита также увеличивается в 60 раз (например, при длине ВОЛС 100 км – 6,39 против 383,3), что указывает на прямую пропорциональную зависимость вероятности записи ошибочного бита от частоты появления ИТТ. Оптимальным выбором с точки зрения соотношения частоты появления ИТТ и типового времени восстановления рабочего состояния фотоприёмного

модуля является модуль id201. Вероятность записи ошибочного бита при использовании модуля id201 в 2…2,5 раза больше при длине ВОЛС 100 км ($3{,}20 \cdot 10^{-7}$ и $2{,}56 \cdot 10^{-7}$ против $6{,}40 \cdot 10^{-7}$), по сравнению с модулями id230 и id210 соответственно.

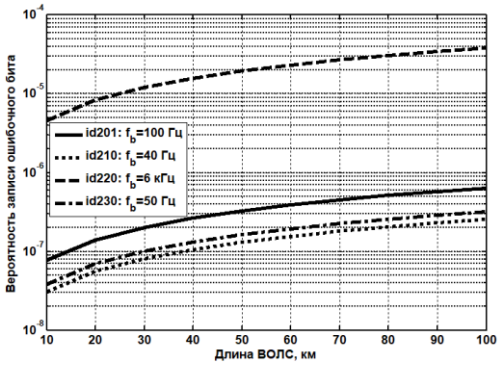

Рис. 9. Вероятность записи ошибочного бита в сырую квантовую ключевую последовательность

Отметим, что время восстановления рабочего состояния фотоприёмного модуля не сказывается на вероятностных характеристиках системы. С другой стороны, время восстановления работоспособности ОЛФД ограничивает максимально-допустимое значение частоты следования оптических импульсов, а следовательно, и предельную скорость формирования ключа. Это подтверждают графики на рис. 10, где представлены зависимости максимальной требуемой частоты следования оптических импульсов от длины ВОЛС при использовании 4-х модулей на основе ОЛФД, в которых время восстановления рабочего состояния различается в 1 000 000 раз (от 0,1 нс до 100 мкс). На рис. 10 графики для модулей id210 и id230 совпадают, что является следствием равенства τ_{SAPD}=100 мкс.

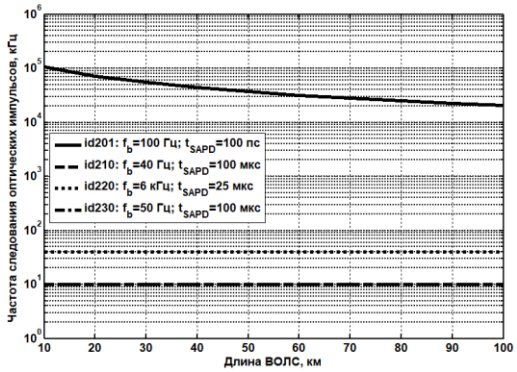

Рис. 10. Максимальная частота следования оптических импульсов

Следствием разного времени рабочего состояния ОЛФД является различие на 3…4 порядка частот следования оптических импульсов (предельных скоростей формирования ключа). При переходе с модуля id201 с τ_{SAPD}=100 пс на модуль id210 с τ_{SAPD}=100 мкс максимально-допустимая частота следования оптических импульсов уменьшается в 10 452 раз при протяжённости ВОЛС 10 км, в 7 176 раз – при протяжённости ВОЛС 20 км, и в 2 046 раз – при протяжённости ВОЛС 100 км.

В связи со значительным временем восстановления рабочего состояния модулей id210, id220 и id230, максимальная частота следования оптических импульсов постоянна при изменении протяжённости ВОЛС. Лишь для модуля id201, где время восстановления рабочего состояния 100 пс меньше исходных длительностей оптических импульсов (а тем более длительностей импульсов стробирования), при увеличении длины ВОЛС в 10 раз (с 10 до 100 км) максимальная частота следования оптических импульсов уменьшается в 5,1 раза.

Исследования показывают, что большое время восстановления рабочего состояния ОЛФД может значительно снизить скорость и увеличить время формирования ключа. За счёт этого злоумышленник получает большее время для атак на систему КРК. Следовательно, при выборе фотоприёмного модуля необходимо учитывать как частоту генерации ИТТ, так и время восстановления его рабочего состояния.

Выводы. Проанализировано влияние параметров функциональных элементов на энергетические, временные и вероятностные характеристики системы КРК на основе протокола B92.

Установлено, при увеличении длины ВОЛС значительно снижается вероятность записи правильного бита. Так, при увеличении длины ВОЛС в 10 раз (с 10 до 100 км) вероятность записи правильного бита снижается в 50,9 раза (при ширине спектра FWHM=80 пм). С другой стороны, изменение вероятности записи ошибочного бита менее значительно и составляет 3,3 раза при увеличении длины ВОЛС с 10 до 100 км. Это обусловлено резким ростом вероятности отсутствия регистрации на приёмной станции фотонов и/или ИТТ при увеличении протяжённости ВОЛС.

Отметим, среднеквадратичное отклонение времени задержки фотона прямо пропорционально длине ВОЛС и ширине спектра, причём при увеличении длины ВОЛС в 10 раз среднеквадратичное отклонение времени задержки фотона также увеличивается в 10 раз.

Анализируя рассмотренные зависимости, отметим целесообразность использования лазера с минимальной шириной спектра излучения, например, EML-лазера, для достижения наилучших характеристик системы КРК в целом. Однако EML-лазеры считаются самыми сложными и дорогостоящими из всех рассмотренных типов лазеров, поэтому использование EML-лазеров значительно повышает стоимость всей системы КРК.

Полученный числовой материал указывает, что оптимальным выбором с точки зрения соотношения частоты появления ИТТ и типового времени восстановления рабочего состояния фотоприёмного модуля является модуль id201.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Scarani V.* Quantum Physics: A First Encounter: Interference, Entanglement, and Reality. Translated by Rachael Thew. – Oxford: University Press, Mar 2006. – 125 p.
2. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / под ред. Д. Боумейстера, А. Экерта, А. Цайлингера: пер. с англ. С.П. Кулика, Е.А. Шапиро. – М.: Постмаркет, 2002. – 376 с.
3. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
4. Ростелеком объявил о внедрении квантовой криптографии на своих сетях. – URL: https://tass.ru/ekonomika/5685597 (дата обращения 17.10.2018).
5. *Румянцев К.Е.* Системы квантового распределения ключа: монография. – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 264 с.
6. *Bennett C., Brassard G.* Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE international conference on computers, systems and signal processing. Bangalore. India. – New York: Institute of Electrical and Electronics Engineers. – 1984. – P. 175-179.

7. *Shor P.W., Preskill J.* Simple proof of security of the BB84 quantum key distribution protocol // Physical Review Letters. – 2000. – Vol. 85. – P. 441-444.
8. *Mironov Y.K., Rumyantsev K.E.* Single-Photon Algorithm for Synchronizing the System of Quantum Key Distribution with Polling Sections of a Fiber-Optic Line // Futuristic Trends in Networks and Computing Technologies. – 2020. – P. 87-97. – DOI: https://doi.org/10.1007/978-981-15-4451-4_8.
9. *Румянцев К.Е.* Синхронизация в системе квантового распределения ключа с автоматической компенсацией поляризационных искажений // Телекоммуникации. – 2017. – № 2. – С. 32-40.
10. *Румянцев К.Е., Плёнкин А.П.* Безопасность режима синхронизации системы квантового распределения ключей // Известия ЮФУ. Технические науки. – 2015. – № 5 (166). – С. 135-153.
11. *Курочкин В.Л. и др.* Экспериментальные исследования в области квантовой криптографии // Фотоника. – 2012. – Т. 5. – С. 54-66.
12. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8. – С. 81-96.
13. *Rumyantsev K.E., Pljonkin A.P.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security // International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang. – P. 1-4. – DOI: 10.1109/ELINFOCOM.2016.7562955. WOS:000389518100035. IDS: BG5KP.
14. *Rumyansev K., Rudinsky E.* Parameters of the two-stage synchronization algorithm for the quantum key distribution system // Proceedings of the 10th International Conference on Security of Information and Networks (SIN'17). – 2017. – P. 140-147. – DOI: 10.1145/3136825.3136888.
15. *Румянцев К..Е., Shakir H.H.* Проектирование системы квантового распределения ключа с интерферометрами Маха-Цендера: учеб. пособие. – Ростов-на-Дону; Таганрог: Изд-во ЮФУ, 2020. – 108 с.
16. *Румянцев К.Е.* Квантовые технологии в телекоммуникационных системах: учебник. – Ростов-на-Дону; Таганрог: Изд-во ЮФУ, 2021. – 346 с.
17. Лазерные диоды Фабри-Перо. – URL: http://www.electroncom.ru/product/nanoplus/fp_diodes.php (дата обращения: 10.01.2022).
18. Поверхностно-излучающие лазеры с вертикальным резонатором. – URL: http://msd.com.ua/optoelektronika/poverxnostno-izluchayushhielazery-s-vertikalnym-rezonatorom-vcsel/ (дата обращения: 10.01.2022).
19. Лазеры с внешним резонатором. – URL: http://fmnauka.narod.ru/lazery_s_vneshnim_rezonatorom.pdf (дата обращения: 10.01.2022).
20. Основные параметры и сертификация оптических SFP модулей. – URL: https://deps.ua/knowegable-base-ru/articles/1961-osnovnye-parametry-i-sertifikatciia-opticheskikh-sfp-modulei.html (дата обращения: 10.01.2022).

REFERENCES

1. *Scarani V.* Quantum Physics: A First Encounter: Interference, Entanglement, and Reality. Translated by Rachael Thew. Oxford: University Press, Mar 2006, 125 p.
2. Fizika kvantovoy informatsii: Kvantovaya kriptografiya. Kvantovaya teleportatsiya. Kvantovye vychisleniya [Physics of Quantum Information: Quantum Cryptography. Quantum teleportation. Quantum computing], ed. by D. Boumeystera, A. Ekerta, A. TSaylingera, transl. from eng. by S.P. Kulik, E.A. Shapiro. Moscow: Postmarket, 2002, 376 p.
3. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics*, 2002, Vol. 74, No. 1, pp. 145-195.
4. Rostelekom ob"yavil o vnedrenii kvantovoy kriptografii na svoikh setyakh [Rostelecom announced the introduction of quantum cryptography on its networks]. Available at: https://tass.ru/ekonomika/5685597 (accessed 17 October 2018).
5. *Rumyantsev K.E.* Sistemy kvantovogo raspredeleniya klyucha [Systems of quantum key distribution: monograph]. Taganrog: Izd-voTTI YuFU, 2011, 264 p.
6. *Bennett C., Brassard G.* Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE international conference on computers, systems and signal processing. Bangalore. India.* New York: Institute of Electrical and Electronics Engineers, 1984, pp. 175-179.

7. *Shor P.W., Preskill J.* Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 2000, Vol. 85, pp. 441-444.
8. *Mironov Y.K., Rumyantsev K.E.* Single-Photon Algorithm for Synchronizing the System of Quantum Key Distribution with Polling Sections of a Fiber-Optic Line. *Futuristic Trends in Networks and Computing Technologies*, 2020, pp. 87-97. DOI: https://doi.org/10.1007/978-981-15-4451-4_8.
9. *Rumyantsev K.E.* Sinhronizatsiya v sisteme kvantovogo raspredeleniya klyucha s avtomaticheskoy kompensatsiey polyarizatsionnykh iskazheniy [Synchronization in a quantum key distribution system with automatic compensation of polarization distortions]. *Telekommunikatsii* [Telecommunications], 2017, No. 2, pp. 32-40.
10. *Rumyantsev K.E., Plenkin A.P.* Bezopasnost' rezhima sinhronizatsii sistemy kvantovogo raspredeleniya klyuchey [Security of the synchronization mode of a system of quantum key distribution]. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (166), pp. 135-153.
11. *Kurochkin V.L. i dr.* Eksperimental'nye issledovaniya v oblasti kvantovoy kriptografii [Experimental research in the field of quantum cryptography], *Fotonika* [Photonics], 2012, Vol. 5, pp. 54-66.
12. *Rumyantsev K.E., Plenkin A.P.* Sinhronizatsiya sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchyonnosti [Synchronization of the system of quantum key distribution when using photon pulses to increase security]. *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8, pp. 81-96.
13. *Rumyansev K.E., Plenkin A.P.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security. *International Conference on Electronics, Information, and Communications (ICEIC)*, 2016. Vietnam, Danang. pp. 1-4. DOI: 10.1109/ELINFOCOM.2016.7562955. WOS:000389518100035. IDS: BG5KP.
14. *Rumyansev K., Rudinsky E.* Parameters of the two-stage synchronization algorithm for the quantum key distribution system. *Proceedings of the 10th International Conference on Security of Information and Networks (SIN'17)*, 2017, pp. 140-147. DOI: 10.1145/3136825.3136888.
15. *Rumyantsev K..E., Shakir H.H.* Proektirovanie sistemy kvantovogo raspredeleniya klyucha s interferometrami Makha-Tsendera: ucheb. posobie [Designing a quantum key distribution system with Mach-Zehnder interferometers: a tutorial]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2020, 108 p.
16. *Rumyantsev K.E.* Kvantovye tekhnologii v telekommunikatsionnyh sistemakh: uchebnik [Quantum technologies in telecommunication systems: textbook]. Rostov-on-Don; Taganrog: Izd-vo YuFU, 2021, 346 p.
17. Lazernye diody Fabri-Pero [Fabry-Perot laser diodes]. Available at: http://www.electroncom.ru/product/nanoplus/fp_diodes.php (accessed 10 January 2022).
18. Poverkhnostno-izluchayushchie lazery s vertikal'nym rezonatorom [Surface-emitting lasers with a vertical cavity]. Available at: http://msd.com.ua/optoelektronika/poverxnostno-izluchayushhielazery-s-vertikalnym-rezonatorom-vcsel/ (accessed 10 January 2022).
19. Lazery s vneshnim rezonatorom [External cavity lasers]. Available at: http://fmnauka.narod.ru/lazery_s_vneshnim_rezonatorom.pdf (accessed 10 January 2022).
20. Osnovnye parametry i sertifikatsiya opticheskikh SFP module [Main parameters and certification of optical SFP modules]. Available at: https://deps.ua/knowegable-base-ru/articles/1961-osnovnye-parametry-i-sertifikatciia-opticheskikh-sfp-modulei.html (accessed 10 January 2022).

Статью рекомендовала к опубликованию к.т.н. К.Б. Дахкильгова.

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; г. Таганрог, Россия; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Миронова Полина Демьяновна – e-mail: linenkopdem@gmail.com; тел.: 89081924053; кафедра информационной безопасности телекоммуникационных систем; аспирант.

Шакир Хайдер Хуссейн – e-mail: hyder.almansoor@yahoo.com; кафедра информационной безопасности телекоммуникационных систем; аспирант.

Rumyantsev Konstantin Evgenievich – Southern Federal University; e-mail: rke2004@mail.ru; Taganrog, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr. of eng. sc.; professor.

Mironova Polina Demyanovna – e-mail: linenkopdem@gmail.com; phone: +79081924053; the department of information security of telecommunication systems; graduate student.

Shakir Hayder Hussein – e-mail: hyder.almansoor@yahoo.com; the department of information security of telecommunication systems; graduate student.

УДК 550.343.3+550.34.016 DOI 10.18522/2311-3103-2022-4-77-94

А.С. Черепанцев

ЗАКОНОМЕРНОСТИ ПЕРЕХОДНОГО РЕЖИМА В ДИССИПАТИВНОЙ КЛЕТОЧНОЙ МОДЕЛИ ЗЕМЛЕТРЯСЕНИЙ

Целью данной работы был анализ механизмов роста кластеров сбросов, приводящего на решетке конечных размеров к состоянию, близкому к критическому, со степенным распределением по размерам кластеров, подобных наблюдаемым в сейсмическом процессе. В то же время вопрос о применимости модели для описания процессов в реальной геофизической среде остается открытым. Анализ связи элементов в одномерной модели OFC с открытыми граничными условиями позволяет оценить изменчивость поступающей энергии к элементам решетки расположенными на разном расстоянии от границ. Построенная расчетная модель позволяет оценить размер граничных областей высокой изменчивости средней поступающей энергии при различных значениях параметра связи α. Показано, что с ростом α граница область неоднородности расширяется. Показано что существуют два различных режима синхронного образования системы сбросов, имитирующих землетрясение. Оба механизма определяются захватом соседнего элемента и последующей синхронизацией их сбросов. Этот процесс формирует устойчивый сброс большого размера. Наличие пограничных областей с высоким градиентом скорости вводимой энергии определяет основной механизм образования кластеров элементов решетки и демонстрирующий синхронный сброс накопленной энергии. Такая синхронизация достигается за счет высокой взаимной изменчивости энергии на каждом шаге итерации. Второй важный механизм роста кластеров характерен для формирующихся кластеров, размер которых превышает размер приграничной области высокой неоднородности притока энергии. По мере роста размера кластера область захвата соседних элементов, не входящих в кластер, расширяется. Соответственно вероятность того, что энергия соседнего элемента находится в зоне захвата, увеличивается. Расчеты показывают, что среднее время достижения заданного размера кластера на решетка при разных размерностях пространства d и при разных параметрах связи α подтверждает наличие двух временных интервалов с разным механизмом образования кластеров. В таком случае, рост больших кластеров носит степенной характер с показателем степени, определяемым размерностью пространства d.

Модель Олами–Федера–Кристенсена; самоорганизованная критичность; степенное распределение в критических системах.

A.S. Cherepantsev

THE TRANSIENT REGIME PATTERNS IN THE DISSIPATIVE CELL MODEL OF EARTHQUAKES

The purpose of this work was to analyze the mechanisms of the growth of drop clusters, leading on a finite-size lattice to a state close to a critical one with a power-law size distribution of clusters similar to that observed in a seismic process. At the same time, the question of applicability of this model to the description of processes in a real geophysical medium remains. Analysis of the elements coupling in the one-dimensional OFC model with open boundary conditions allows