

УДК 621.383

UDC 621.383

05.00.00 Технические науки

Technical sciences

**МОДЕЛИРОВАНИЕ ОПТИЧЕСКИХ  
ИМПУЛЬСНЫХ СИГНАЛОВ В КВАНТОВО-  
КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ  
СВЯЗИ**

**MODELLING OF OPTICAL PULSE SIGNALS  
IN QUANTUM CRYPTOGRAPHY  
COMMUNICATION SYSTEMS**

Лойко Валерий Иванович  
Заслуженный деятель науки РФ, доктор  
технических наук, профессор  
*Кубанский государственный аграрный  
университет, Краснодар, Россия*

Loyko Valeriy Ivanovich  
Honoured science worker of the Russian Federation,  
Dr.Sci.Tech., professor  
*Kuban state agrarian university, Krasnodar, Russia*

Кулиш Ольга Александровна  
Кандидат физико-математических наук, доцент  
*Кубанский институт информационной защиты,  
Краснодар, Россия*

Kulish Olga Aleksandrovna  
Candidate of physical and mathematical sciences,  
associate professor  
*Kuban institute of information protection, Krasnodar,  
Russia*

Шарифуллин Сергей Равильевич  
кандидат технических наук, доцент

Sharifullin Sergey Ravilievich  
Candidate of technical sciences, associate professor

Хисамов Франгиз Гильфанетдинович  
Доктор технических наук, профессор

Khisamov Frangiz Gilfanetdinovich  
Dr.Sci.Tech., professor

Чернуха Юрий Владимирович  
Кандидат технических наук, доцент

Chernukha Yuriy Vladimirovich  
Candidate of technical sciences, associate professor

Пшеничный Игорь Сергеевич  
Адъюнкт  
*Краснодарское высшее военное училище,  
Краснодар, Россия*

Pshenichniy Igor Sergeevich  
Postgraduate student  
*Krasnodar high military academy, Krasnodar, Russia*

Для моделирования прохождения лазерного излучения в системах квантовой криптографии необходимо знать точное значение полной дисперсии волноводов, которая приводит к уширению и уменьшению амплитуды импульса. Целью работы являлось получение зависимостей различных видов дисперсии волоконных линий в квантовых системах связи от длины волны с учетом уравнения Селмейера и моделирование оптического импульсного излучения в квантово-криптографических системах. Получены зависимости материальной, волноводной и хроматической дисперсий от длины волны с учетом формулы Селмейера, которая позволяет учесть материал оптического волокна. Смоделировано распространение криптографического импульса через волоконно-оптические линии связи различной протяженности

It is necessary to know exact value of the full dispersion of waveguides, which leads to broadening and reduction of pulse amplitude for modeling laser radiation passage in quantum cryptography systems. The operation purpose was obtaining of dependences on a wavelength of various dispersion types according to the Sellmeier' sequeationand optical pulse radiation modelling in quantum communication systems. Dependences of the material, waveguide and chromatic dispersions on length of a wave according to the Sellmeier's equation which allows to consider an optical fiber's material are received. Distribution of a cryptographic impulse through fiber-optical communication lines of various extent is simulated

Ключевые слова: ОПТИЧЕСКОЕ ВОЛОКНО,  
ОДНОФОТОННЫЙ ИМПУЛЬС, ДИСПЕРСИЯ,  
ДЛИНА ВОЛНЫ, ПОКАЗАТЕЛЬ  
ПРЕЛОМЛЕНИЯ

Keywords: OPTICAL FIBER, SINGLE-PHOTON  
PULSE, DISPERSION, LENGTH OF WAVE,  
REFRACTION INDEX

**Doi: 10.21515/1990-4665-123-098**

В квантовых системах связи для передачи криптографического ключа применяют сверхслабые лазерные импульсы. С точки зрения квантовой оптики, при распространении однофотонного импульса в волоконно-оптической линии связи он рассматривается как электромагнитная волна. Влияние дисперсии на оптический импульс приводит к его уширению и уменьшению амплитуды. Поэтому крайне важно, чтобы в квантовых системах связи под воздействием дисперсии сверхслабый импульс не исчез на выходе системы и был зафиксирован фотодиодом. Для моделирования прохождения лазерного импульса по оптическим линиям связи необходимо знать точное значение полной дисперсии волноводов, изготовленных из различных материалов.

Целью данной работы является получение зависимостей различных видов дисперсии волоконных линий в квантовых системах связи от длины волны с учетом уравнения Селмейера и моделирование оптического импульсного излучения в квантово криптографических системах.

Хроматическая дисперсия волокна состоит из материальной и волноводной составляющих и имеет место при распространении света как в одномодовом, так и в многомодовом волноводе [1]. Материальная дисперсия обусловлена зависимостью показателя преломления волокна от длины волны и определяется электромагнитным взаимодействием волны со связанными электронами материала среды, которое носит, как правило, нелинейный (резонансный) характер и вдали от резонансов может быть описано с приемлемой точностью уравнением Селмейера. Волноводная дисперсия обусловлена процессами внутри моды. Она характеризуется зависимостью групповой скорости моды от длины волны оптического излучения, что приводит к различию скоростей распространения частотных составляющих излучаемого спектра.

Материальную дисперсию рассчитывали по формулам [2]:

$$M = \frac{\lambda \partial^2 n}{c \partial \lambda^2} = \frac{\lambda \sum_{i=1}^3 A_i l_i^2 \frac{(3\lambda^2 + l_i^2)}{(\lambda^2 - l_i^2)^3} - \left(\frac{\partial n}{\partial \lambda}\right)}{n}, \quad (1)$$

$$\frac{\partial n}{\partial \lambda} = -\frac{\lambda}{n_1} \sum_{i=1}^3 \frac{A_i l_i^2}{(\lambda^2 - l_i^2)^2}, \quad (2)$$

где  $A_i$  и  $l_i$  – коэффициенты, значения которых находятся экспериментально,  $n_1$  – показателя преломления сердцевины волокна ( $n_1 = 1,468$ ),  $n$  – относительная разность показателей преломления,  $\lambda$  – длина волны ( $\lambda = 1550$  нм),  $c$  – скорость света.

Расчёты проводились для силикатного стекла ( $SiO_2$ ). Зависимость материальной дисперсии волокна от длины волны приведена на рисунке 1.

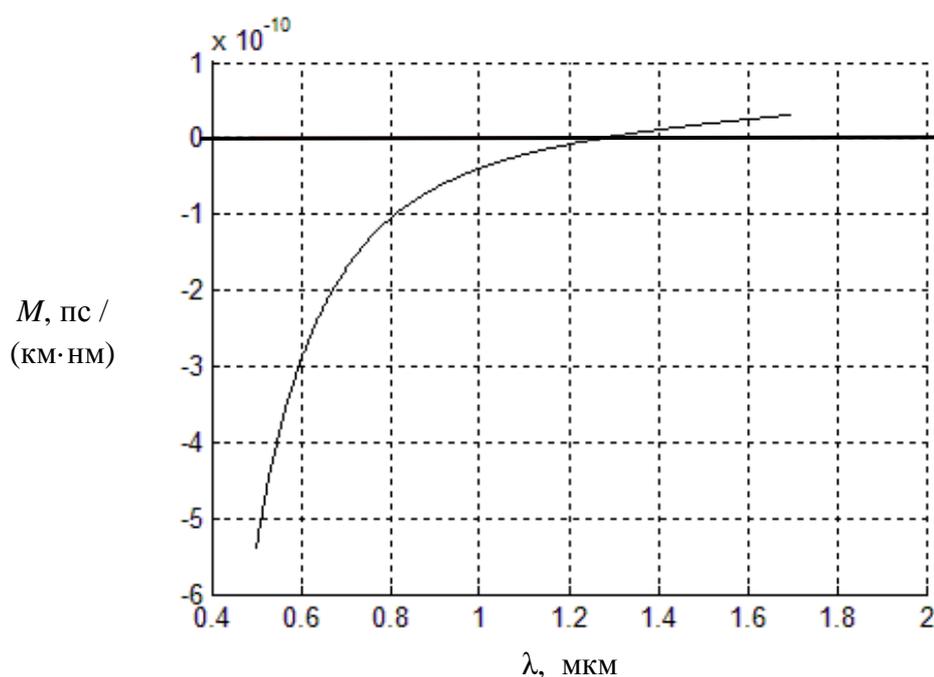


Рис. 1. Зависимость материальной дисперсии от длины волны

Расчёт волноводной дисперсии производили по формуле:

$$M_B = \frac{2n_1^2 n}{\lambda c} 10^9. \quad (3)$$

Зависимость волноводной дисперсии волокна от длины волны приведена на рисунке 2.

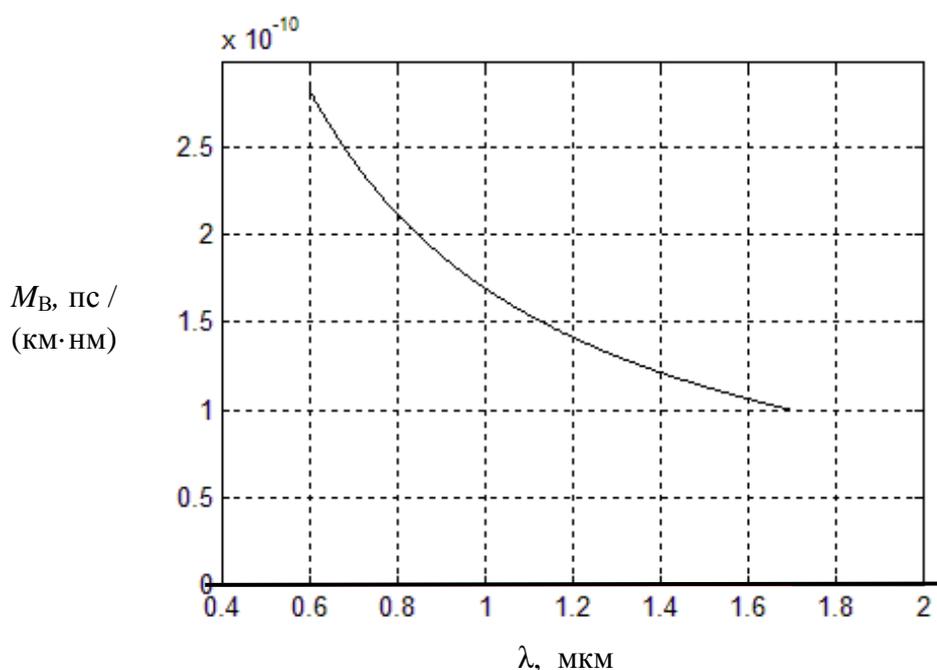


Рис. 2. Зависимость волноводной дисперсии от длины волны

Хроматическую дисперсию находили по формуле:

$$M_{xp} = M + M_B. \quad (4)$$

Зависимость хроматической дисперсии волокна от длины волны приведена на рисунке 3.

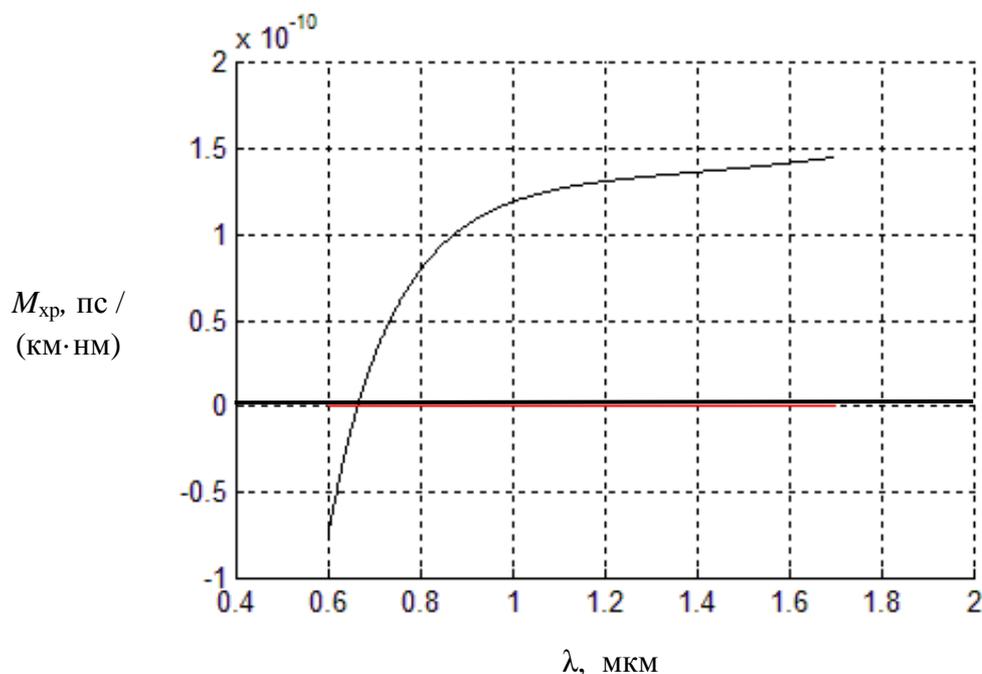


Рис. 3. Зависимость хроматической дисперсии от длины волны

В квантовой криптографии оптический импульс должен быть как можно слабее и короче, вплоть до однофотонного импульса, поэтому длительность импульса принимали  $t_{\text{вх}}=0,3$  пс.

Для построения модели входного гауссова импульса использовали уравнение [3]:

$$A(t)_{\text{вх}} = \sqrt{P_0} \exp\left(-\frac{t^2}{2t_{\text{вх}}^2}\right), \tag{5}$$

где  $A_{\text{вх}}(t)$  – огибающая гауссового импульса на входе,  $P_0$  – мощность входного импульса ( $P_0 = 1$ ).

Огибающую импульса на выходе представили в виде:

$$A(t)_{\text{вых}} = \frac{\sqrt{P_0}}{\sqrt{4\left(1 + \frac{L\lambda^2 M_{\text{xp}}}{2\pi c t_{\text{вх}}^2}\right)}} \exp\left(-\frac{t^2}{2t_{\text{вых}}^2}\right) \tag{6}$$

$$t_{\text{ВЫХ}} = 1,1774 \sqrt{\left(\frac{t_{\text{ВХ}}}{1,1774}\right)^2 + \left(M_{\text{ХР}} \cdot \left|\frac{\lambda^2}{2\pi c} \cdot \frac{2 \cdot 1,1774}{t_{\text{ВХ}}}\right| \cdot L\right)^2}, \quad (7)$$

где  $L$  – длина волоконной линии связи.

Графики зависимости огибающей импульса от времени на входе и выходе волокна для различных длин линии связи приведены на рисунках 4-7.

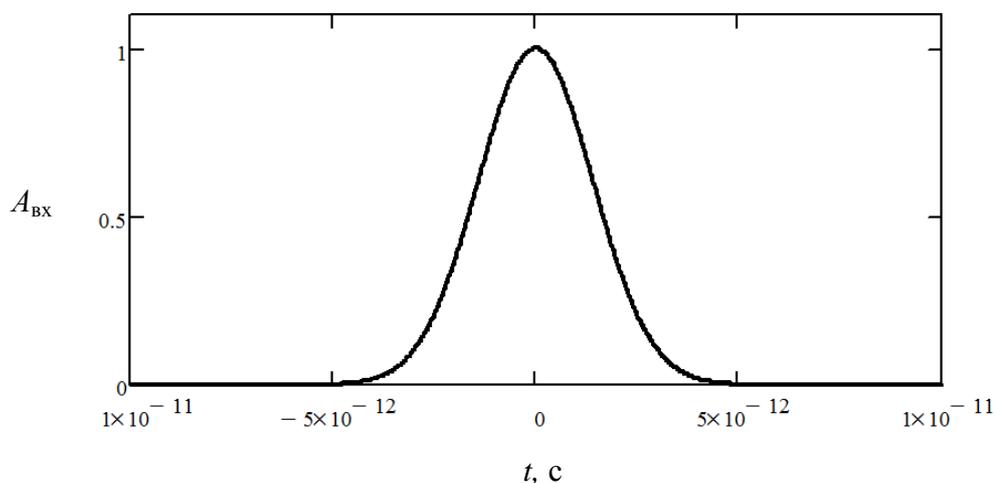


Рис. 4. Модель входного лазерного импульса

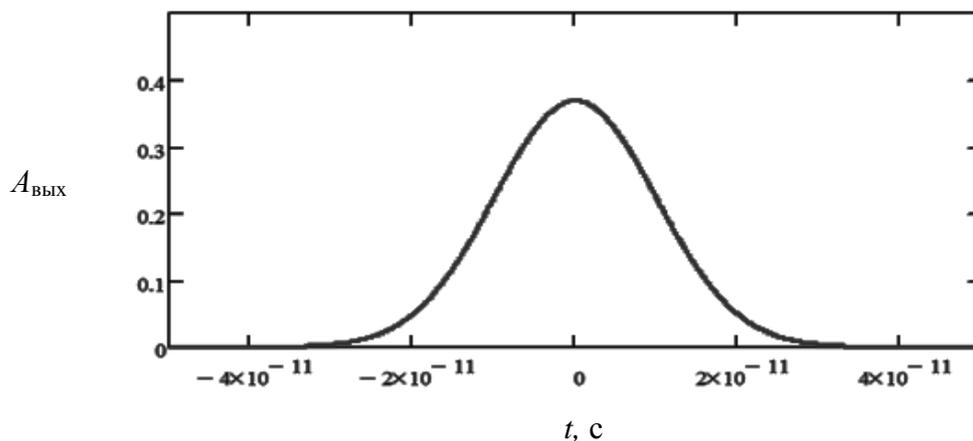


Рис. 5. Модель выходного импульса при прохождении волокна длиной  $L = 1$  км

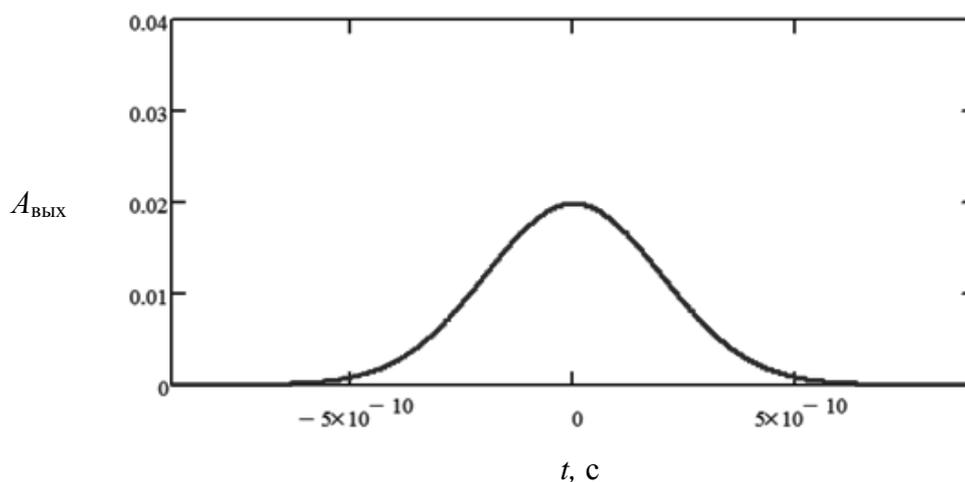


Рис. 6. Модель выходного импульса при прохождении волокна длиной  $L = 20$  км

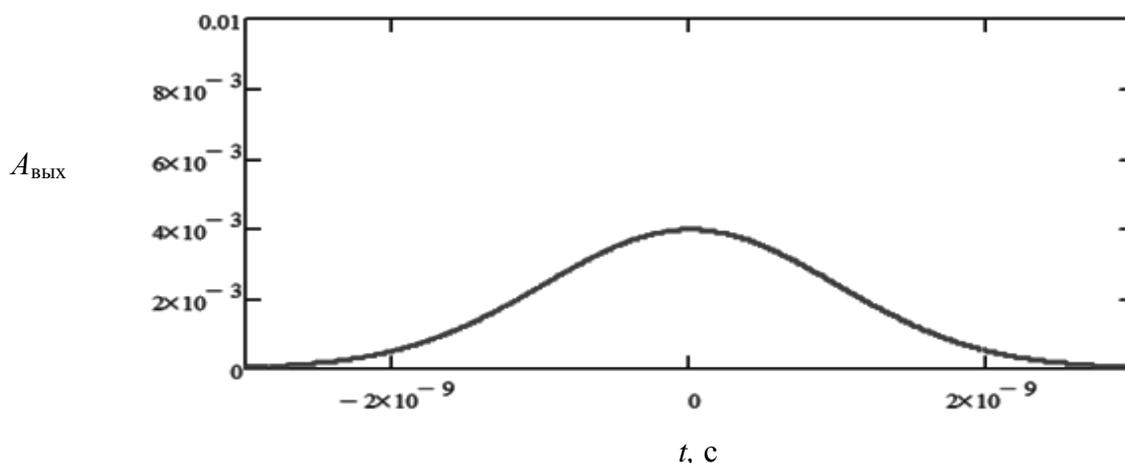


Рис. 7. Модель выходного импульса при прохождении волокна длиной  $L = 100$  км

Одним из важнейших элементов оптической квантово-криптографической системы, определяющим ее чувствительность и предельный энергетический потенциал, является приемная аппаратура. Для реализации предельных возможностей аппаратуры регистрации слабых световых сигналов и для обеспечения высокой точности измерения интенсивности импульсного излучения в системах оптической квантовой связи фотоприемный канал должен работать в однофотонном режиме.

Счет единичных фотонов может производиться лавинными фотодиодами на основе германия, охлаждаемыми жидким азотом и <http://ej.kubagro.ru/2016/09/pdf/98.pdf>

работающими в гейгеровском режиме. В этом режиме на фотодиоды подается высокое смещающее напряжение, такое, что одна электронно-дырочная пара, созданная поглощенным фотоном, должна быть способна произвести лавинное размножение тысяч носителей зарядов. Лавинные фотодиоды отличаются от обычных фотодиодов наличием процессов умножения. При достаточно большом обратном смещении напряженность электрического поля в р-п-переходе может достичь весьма больших значений – выше  $10^5 \text{ В}\cdot\text{см}^{-1}$ . Скорость носителей при такой напряженности насыщается, и их энергия становится достаточной для генерации новой пары электрон-дырка за счет ионизации. Генерированные носители могут, в свою очередь, ионизировать другие пары: таким образом, развивается процесс лавинного размножения.

На основе проведенных расчетов была проанализирована возможность регистрации импульса фотоприемными устройствами на выходе квантовой линии связи. Имея математическую модель влияния дисперсии на оптический импульс, можно оценить возможность лавинного фотодиода InGaAsIAG080X, использующегося для приёма криптографических импульсов [4], распознать оптический сигнал. Характеристики данного фотодиода: чувствительность (при  $\lambda = 1550 \text{ нм}$ ) равна 1,00 А/Вт, темновой ток при этом равен 15 нА. Следовательно, если максимальная мощность приходящего импульса будет менее 15 нВт, то фотоприёмник не сможет его распознать. Таким образом, изменение огибающей импульса может привести к невозможности его регистрации существующими фотоприемными устройствами и уменьшению длины квантовой линии связи. Учитывая влияние дисперсии на оптический сигнал и потери излучения на рассеивании, сварках, коннекторах, можно сделать вывод, что оптический импульс, отправленный на 100 км, ослабнет и отличить его от собственного шума фотодиод не сможет. Импульсы,

посланные на 20 км и 1 км, будут свободно распознаны и приняты фотодиодом. Поэтому при построении квантово-криптографических систем необходимо через каждые 100 км линии связи располагать станции, на которых информация будет расшифровываться и зашифровываться новым сгенерированным ключом.

В работе получены зависимости материальной, волноводной и хроматической дисперсий оптического волокна от длины волны с учетом формулы Селмейера. Смоделировано распространение криптографического импульса через волоконно-оптические линии связи различной протяженности. В результате анализа полученных графиков можно сделать вывод, что высокие значения дисперсии в стандартном волокне ограничивают эксплуатационные характеристики квантово-криптографических систем связи, работающих на длине волны 1550 нм. Данные, полученные в ходе работы, могут быть использованы в проектировании квантово-криптографических систем связи.

#### **Список литературы**

1. Фриман Р. Волоконно-оптические системы связи. –М.: Техносфера, 2004. – 496 с.
2. Розеншер Э. Оптоэлектроника.–М.: Техносфера, 2004. – 592 с.
3. Липинский А. Ю. Исследование дисперсионных характеристик интегрального оптического волновода. – Донецк: Донецкий национальный университет, кафедра радиофизики. 2005. – 39 с.
4. Гуртов В. А. Оптоэлектроника и волоконная оптика. – Петрозаводск: Издательство ПетрГУ. 2005. – 239 с.

#### **References**

1. Friman R. Fiber - optic communication systems, –М.: Tekhnosfera, 2004. – 496 s.
2. Rozensher E. Optoelectronics, –М.: Tekhnosfera, 2004. – 592 s.
3. Lipinskiy A.Y. Study of the dispersion characteristics of the integral optical waveguide. – Donetsk: Donetsk national university, radio physics department. 2005. – 39 s.
4. Gurtov V.A. Optoelectronics and fiber optics. – Petrozavodsk: Izdatel'stvo PetrGU. 2005. – 239 s.