УДК 621.383.92

ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ КВАНТОВОГО КАНАЛА СВЯЗИ

И.Р. ГУЛАКОВ, А.О. ЗЕНЕВИЧ, А.М. ТИМОФЕЕВ, А.Г. КОСАРИ

Высший государственный колледж связи
Ф. Скорины, 8/2, Минск, 220114, Республика Беларусь

Поступила в редакцию 26 ноября 2014

Построена математическая модель квантового канала связи, содержащего в качестве приемного модуля счетчик фотонов, позволяющая учесть влияние квантовой эффективности регистрации, вероятности образования темновых импульсов приемного модуля легитимного пользователя, вероятности потери оптического излучения из-за его несанкционированного вывода из оптического волокна на пропускную способность квантового канала связи.

Ключевые слова: макроизгиб оптического волокна, канал утечки информации, счетчик фотонов, лавинный фотоприемник, пропускная способность.

Введение

В настоящее время для передачи данных широкое применение находят оптические волокна [1]. В некоторых случаях при трансляции данных по таким каналам связи особенно важно обеспечивать конфиденциальность передаваемой информации. Канал утечки информации, передаваемой по волоконно-оптическим линиям связи, может быть создан путем формирования макроизгиба оптического волокна [2]. При этом несанкционированный доступ к передаваемой информации становится возможным за счет того, что при определенной величине макроизгиба волокна угол падения электромагнитной волны на границе раздела сердцевина-оболочка становится меньше угла полного внутреннего отражения, в результате чего оптическое излучение проходит сквозь обе границы раздела, и часть оптического излучения в месте изгиба оптического волокна выводится во внешнее пространство и регистрируется несанкционированным пользователем. Существуют устройства [3, 4], которые позволяют обнаруживать каналы утечки информации, созданные путем формирования макроизгиба волокна, однако они не позволяют выявлять несанкционированный доступ при выводе из оптического волокна небольшой части излучения, соответствующей не более десяти фотонам излучения за время передачи одного бита. В этих случаях для передачи конфиденциальной информации целесообразно создавать квантовый канал связи [5], в котором применяются оптические импульсы малой мощности, содержащие не более десяти фотонов для передачи одного бита информации. Наличие в квантовом канале утечки информации, реализуемой посредством макроизгиба оптического волокна, приведет к росту количества ошибок при передаче данных и уменьшит пропускную способность этого канала. Одной из основных характеристик счетчика фотонов является квантовая эффективность регистрации, однако до настоящего времени оценка влияния квантовой эффективности регистрации счетчика фотонов на обнаружение несанкционированного пользователя квантового канала связи отсутствует. В связи с этим целью данной работы являлось установить влияние квантовой эффективности регистрации счетчика фотонов на возможность обнаружить несанкционированное пользование квантовым каналом связи, осуществляемое посредством макроизгиба оптического волокна.

Математическая модель одноквантовой системы передачи и приема данных

При построении математической модели квантового канала связи будем называть легитимных пользователей на передающей и приемной сторонах соответственно Алисой и Бобом, а Евой – нелегитимного пользователя.

Дальнейшие рассуждения будут основаны на том, что передача информации осуществляется двоичными символами («0» и «1»). Причем при передаче символа «1» одноквантовый оптический импульс передается в волокно, а при передаче символа «0» – излучение отсутствует. Приемный модуль Боба выполнен в виде счетчика фотонов, который регистрирует фотоны оптического излучения только в течение времени передачи синхроимпульса, генерируемого на передающей стороне только на время передачи каждого символа, аналогично, как в работе [6]. Синхроимпульсы используются для обеспечения согласованной работы передающей и приемной сторон.

Существует вероятность приема символа «0» при передаче символа «1» $P(0/1)$ и вероятность приема символа «1» при передаче символа «0» $P(1/0)$, которые определяют вероятность ошибки передачи данных. Согласно [6], такие ошибки обусловлены несовершенством приемной аппаратуры и связаны с квантовой эффективностью регистрации счетчика фотонов η_p, меньшей единицы, и вероятностью появления темновых импульсов P_t, большей нуля. Другими ошибками передачи данных можно пренебречь.

Вначале рассмотрим случай, когда Ева в канале связи отсутствует. При этом численные значения вероятностей $P(0/1)$ и $P(1/0)$ будут равны соответственно

$$P(0/1)=1-\eta_p,\ P(1/0)=P_t. \tag{1}$$

Тогда вероятность приема символа «0» при передаче символа «0» $P(0/0)$ и вероятность приема символа «1» при передаче символа «1» $P(1/1)$ равны:

$$P(0/0)=1-P_t,\ P(1/1)=\eta_p. \tag{2}$$

Пропускная способность рассматриваемого квантового канала связи определяется по формуле [6]:

$$\begin{aligned} C_{\max}\big|_{\text{А–Б}} = \Big\{ &-\left(1-P_t/2-\eta_p/2\right)\log_2\left(1-P_t/2-\eta_p/2\right)-\left(P_t/2+\eta_p/2\right)\log_2\left(P_t/2+\eta_p/2\right)+ \\ &+0{,}5\left[\left(1-P_t\right)\log_2\left(1-P_t\right)+P_t\log_2 P_t\right]+0{,}5\left[\left(1-\eta_p\right)\log_2\left(1-\eta_p\right)+\eta_p\log_2\eta_p\right]\Big\}/\tau_b, \end{aligned} \tag{3}$$

где τ_b – среднее время передачи одного бита.

Рассмотрим случай, когда в канале связи присутствует Ева, осуществляя несанкционированный съем данных путем формирования канала утечки информации при помощи макроизгиба оптического волокна. Обозначим вероятность выхода фотона излучения из оптического волокна в результате такого съема данных как $P_{\text{пот}}$. Будем считать, что используемое Евой оборудование для регистрации фотонов является идеальным. Получить выражение для расчета пропускной способности между легитимными пользователями в этом случае можно по методике, описанной в [6] с учетом того, что вероятности $P(0/0)$, $P(1/0)$, $P(1/1)$ и $P(0/1)$ запишутся в следующем виде:

$$P(0/0)=1-P_t,\ P(1/0)=P_t,\ P(1/1)=\eta_p\left(1-P_{\text{пот}}\right),\ P(0/1)=1-\eta_p\left(1-P_{\text{пот}}\right). \tag{4}$$

Таким образом, пропускная способность квантового канала связи на участке «Алиса-Боб» равна:

$$\begin{aligned} C_{\max}\big|_{\text{А–Е–Б}} = \Big\{ &-\left(1-P_t/2-\eta_p/2+\eta_p P_{\text{пот}}/2\right)\log_2\left(1-P_t/2-\eta_p/2+\eta_p P_{\text{пот}}/2\right)- \\ &-\left(P_t/2+\eta_p/2-\eta_p P_{\text{пот}}/2\right)\log_2\left(P_t/2+\eta_p/2-\eta_p P_{\text{пот}}/2\right)+ \\ &+0{,}5\left[\left(1-P_t\right)\log_2\left(1-P_t\right)+P_t\log_2 P_t\right]+ \\ &+0{,}5\left[\left(1-\eta_p+\eta_p P_{\text{пот}}\right)\log_2\left(1-\eta_p+\eta_p P_{\text{пот}}\right)+\left(\eta_p-\eta_p P_{\text{пот}}\right)\log_2\left(\eta_p-\eta_p P_{\text{пот}}\right)\right]\Big\}/\tau_b. \end{aligned} \tag{5}$$

Следует отметить, что выражение (3) также можно получить на основании формулы (5), подставив в (5) $P_{\text{пот}} = 0$.

Несмотря на то, что используемое Евой оборудование для регистрации фотонов является идеальным, вероятность ошибки при приеме данных Евой не равна нулю. Это объясняется тем, что вероятность выхода фотона излучения из оптического волокна в результате съема данных при помощи макроизгиба волокна зависит от его диаметра [5]. Из этого следует, что на участке «Алиса-Ева» при регистрации данных Евой вероятности ошибки при передаче символа «0» и символа «1» равны соответственно нулю и $1 - P_{\text{пот}}$, а вероятности правильного приема символа «0» и символа «1» – единице и $P_{\text{пот}}$. Пропускную способность квантового канала связи на участке «Алиса-Ева» будем называть пропускной способностью канала утечки информации, для расчета которой можно использовать методику [6], с учетом приведенных выше рассуждений.

Таким образом, пропускная способность канала утечки информации равна:

$$C_{\max}\big|_{\text{A–E}} = \left\{-\left(1-P_{\text{пот}}/2\right)\log_2\left(1-P_{\text{пот}}/2\right)-\left(P_{\text{пот}}/2\right)\log_2\left(P_{\text{пот}}/2\right)+ \right.$$
$$\left. +0{,}5\left[\left(1-P_{\text{пот}}\right)\log_2\left(1-P_{\text{пот}}\right)+P_{\text{пот}}\log_2 P_{\text{пот}}\right]\right\}/\tau_b. \quad (6)$$

Экспериментальные результаты и их обсуждение

В качестве объектов исследования использовались счетчики фотонов на лавинных фотодиодах ФД-115Л, лавинных фотоприемниках со структурой металл – резистивный слой – полупроводник, серийно выпускаемое одномодовое оптическое волокно G.652.

Общая длина оптического волокна составляла 398 м. Макроизгиб формировался на расстоянии 198 м от источника оптического излучения; в процессе проведения эксперимента это расстояние не изменялось. Для создания макроизгибов использовались цилиндры различных диаметров D, на которых формировался один виток оптического волокна.

Диапазон изменения температуры фотоприемника счетчика фотонов составлял 150 ÷300 К.

На рис. 1 приведены зависимости пропускной способности канала утечки информации от диаметра макроизгиба для длин волн оптического излучения, наиболее часто используемых при передаче данных по оптическому волокну. Все графики нормированы на величину $1/\tau_b$.

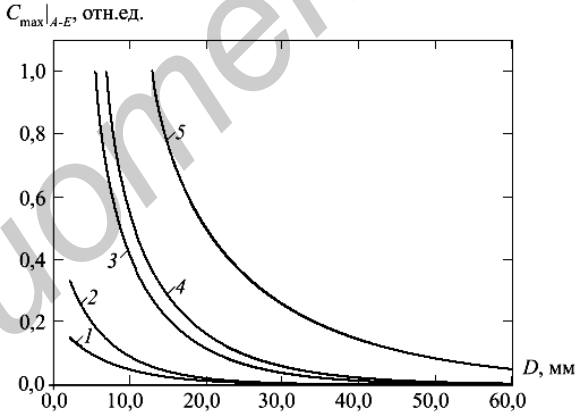

Рис. 1. Зависимость пропускной способности канала утечки информации от диаметра макроизгиба оптического волокна при длинах волн оптического излучения: 1 – 850 нм; 2 – 1310 нм; 3 – 1490 нм; 4 – 1550 нм; 5 – 1625 нм

Получено, что с уменьшением диаметра макроизгиба волокна увеличивается пропускная способность канала утечки информации. Наиболее сильно эта зависимость проявляется для длины волны 1625 нм и в меньшей мере – для длины волны 850 нм. С ростом длины волны оптического излучения увеличивается значение пропускной способности канала утечки информации. Таким образом, для обеспечения защиты информации от несанкционированного доступа, реализуемого посредством макроизгиба оптического волокна, для передачи данных целесообразно выбирать длину волны 850 нм, поскольку, в сравнении с другими исследуемыми длинами волн оптического излучения, для одного и того же диаметра макроизгиба количество информации, получаемой несанкционированным пользователем, будет наименьшим. В связи с этим далее все исследования проведены с использованием длины волны оптического излучения 850 нм.

Из формулы (5) видно, что пропускная способность канала связи на участке «Алиса-Боб» зависит от квантовой эффективности регистрации η_p и вероятности образования темновых

импульсов P_t счетчика фотонов. Согласно [6], уменьшение вероятностей ошибок в квантовом канале связи приводит к увеличению его пропускной способности. Таковыми вероятностями в рассматриваемом канале связи являются $P(0/1)$ и $P(1/0)$, которые зависят соответственно от η_p и P_t. Из выражения (4) следует, что при постоянной величине $P_{пот}$ с ростом η_p и с уменьшением P_t вероятности $P(0/1)$ и $P(1/0)$ уменьшаются, что приведет к росту $C|_{А\text{-}Е\text{-}Б}$. Повысить η_p и уменьшить P_t можно за счет снижения рабочей температуры фотоприемника, используемого в счетчике фотонов [7].

На рис. 2 представлена зависимость $C|_{А\text{-}Е\text{-}Б}$ от вероятности $P_{пот}$ для счетчика фотонов, построенного на базе лавинного фотодиода ФД-115Л, поскольку $C|_{А\text{-}Е\text{-}Б}(P_{пот})$ для всех исследуемых фотоприемников имели схожий вид. Все графики нормированы на величину $1/\tau_b$.

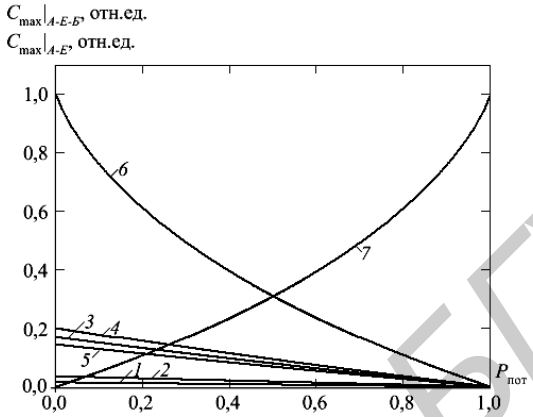

Рис. 2. Зависимость пропускной способности канала связи на участке «Алиса-Боб» (кривые 1–6) и канала утечки информации (кривая 7) от вероятности несанкционированного вывода оптического излучения из волокна: 1 – η_p = 0,03, T = 300 К; 2 – η_p = 0,07, T = 263 К; 3 – η_p = 0,30, T = 233 К; 4 – η_p = 0,35, T = 193 К; 5 – η_p = 0,26, T = 150 К; 6 – η_p = 1,00 (для идеального случая, рассчитанного теоретически)

При проведении исследований средняя длительность времени передачи одного бита τ_b оставалась неизменной и составляла 5 мкс. Это позволяло обеспечить вероятность появления темновых импульсов не более 10^{-6}, которой при расчетах можно было пренебречь. Зависимости 6 и 7 рассчитаны согласно выражениям (5) и (6).

Как видно из приведенных зависимостей, с увеличением $P_{пот}$ пропускная способность $C_{max}|_{А\text{-}Е\text{-}Б}$ уменьшается, а $C_{max}|_{А\text{-}Е}$ растет. Такой характер изменения $C_{max}|_{А\text{-}Е\text{-}Б}(P_{пот})$ обусловлен тем, что осуществляемый Евой вывод мощности оптического излучения из волокна приводит к увеличению количества ошибочных регистраций символов «1» Бобом, за счет чего увеличивается энтропия потерь, и пропускная способность квантового канала связи на участке «Алиса-Боб» уменьшается. Напротив, увеличение $P_{пот}$ уменьшает вероятность ошибки при приеме символов «1» и энтропию потерь канала связи «Алиса-Ева», поэтому $C_{max}|_{А\text{-}Е}$ растет.

Из рис. 2 видно, что чем большую квантовую эффективность регистрации имеет счетчик фотонов, тем большей пропускной способностью обладает канал связи на участке «Алиса-Боб» при неизменной величине $P_{пот}$. Это объясняется тем, что при прочих равных условиях увеличение η_p приводит к увеличению вероятности $P(1/1)$, за счет чего снижается количество ошибочных регистраций символов «1» Бобом, и, следовательно, уменьшается энтропия потерь, как видно из формул (4) и (5).

Для случая, когда $C_{max}|_{А\text{-}Е\text{-}Б} = C_{max}|_{А\text{-}Е}$, Еве будет известна вся информация, передаваемая от Алисы к Бобу. Из рис. 2 видно, что при $\eta_p = 1$ точка пересечения зависимостей $C_{max}|_{А\text{-}Б}(P_{пот})$ и $C_{max}|_{А\text{-}Е\text{-}Б}(P_{пот})$ соответствует значению вероятности $P_{пот} = 0{,}5$, однако с уменьшением квантовой эффективности счетчика фотонов эта точка сдвигается по оси $P_{пот}$ в сторону нуля. Потеря информации в квантовом канале связи обусловлена выводом оптического излучения Евой через канал утечки информации. Оценить эту потерю можно с помощью коэффициента K, равного отношению $C_{max}|_{А\text{-}Е\text{-}Б}$ к $C_{max}|_{А\text{-}Б}$. В случае появления несанкционированного пользователя (Евы) в квантовом канале связи величина K становится меньшей единицы.

В таблице приведены значения K для различных квантовых эффективностей регистрации исследуемых фотоприемников, рассчитанные для $P_{пот}$, при которой выполняется условие $C_{max}|_{А\text{-}Е\text{-}Б} = C_{max}|_{А\text{-}Е}$.

Сравниваемые параметры квантового канала конфиденциальной волоконно-оптической связи

Тип фотоприемника	Сравниваемые параметры	Рабочая температура, К				
		300	263	233	193	150
ФД-115Л	квантовая эффективность регистрации	0,03±0,01	0,07±0,01	0,30±0,03	0,35±0,04	0,26±0,03
	коэффициент K	1,0±0,3	0,9±0,1	0,8±0,1	0,7±0,1	0,8±0,1
	вероятность потерь $P_{пот}$	0,03	0,07	0,23	0,26	0,21
структура металл–резистивный слой–полупроводник	квантовая эффективность регистрации	0,04±0,01	0,06±0,01	0,30±0,03	0,27±0,03	0,15±0,02
	коэффициент K	1,0±0,2	0,9±0,2	0,8±0,1	0,8±0,1	0,9±0,1
	вероятность потерь $P_{пот}$	0,04	0,06	0,23	0,21	0,13

Примечание: данные приведены для длительности передачи одного бита τ_b = 5 мкс, длины волны оптического излучения λ = 850 нм и вероятности образования темновых импульсов $P_t \le 10^{-6}$.

Из представленных результатов видно, что с ростом квантовой эффективности регистрации уменьшается коэффициент K и увеличивается $P_{пот}$.

С учетом погрешности измерения квантовой эффективности регистрации и определения коэффициента K можно сделать вывод, что выявить наличие Евы в квантовом канале связи можно при значении $\eta_p > 0{,}15$ с относительной погрешностью меньшей 13 %.

Заключение

Построена математическая модель квантового канала связи, содержащего в качестве приемного модуля счетчик фотонов. Для этого канала связи получены выражения, с помощью которых можно определять его пропускную способность как на участке между легитимными пользователями, так и на участке между легитимной передающей стороной и нелегитимным пользователем. Выражения для оценки пропускной способности на участке между легитимными пользователями учитывают вероятность несанкционированного вывода мощности излучения из оптического волокна $P_{пот}$, а также такие параметры счетчика фотонов, как вероятность появления темновых импульсов P_t и квантовую эффективность регистрации η_p.

Установлено, что определить наличие Евы в квантовом канале можно при значении $\eta_p > 0{,}15$ с относительной погрешностью меньшей 13 % и при вероятности образования темновых импульсов $P_t \le 10^{-6}$.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договоры №Т13-018, Т14М-130).

DETECTION OF UNAUTHORIZED USERS OF QUANTUM COMMUNICATION CHANNEL

I.R. GULAKOV, A.O. ZENEVICH, A.M. TIMOFEEV, A.G. KOSARI

Abstract

A mathematical model of the quantum communication channel has been built. It contains a photon counter as a receiving unit and allows to take into account how the quantum efficiency of detection, probability of dark pulses formation of the legitimate user receiver module, probability of optical radiation loss due to its unauthorized output from the optical fiber affect the throughput of a quantum communication channel.

Список литературы

1. *Дмитриев С.А.* Волоконно-оптическая техника: современное состояние и новые перспективы. М., 2010.
2. *Шубин В.В.* Способ обнаружения участков волоконно-оптической линии передачи с повышенным боковым излучением / Патент РФ № 2252405.
3. *Шубин В.В., Овечкин С.И., Ивченко С.Н.* Способ обнаружения медленного вывода оптического излучения через боковую поверхность волоконно-оптической линии связи / Патент РФ № 2251810.
4. *Попов С.Н., Шубин В.В.* Способ защиты информации от несанкционированного доступа в волоконно-оптических линиях связи / Патент РФ № 2234194.
5. *Гулаков И.Р., Зеневич А.О., Тимофеев А.М. и др.* // Вестник связи. 2014. № 3(125). С. 46–49.
6. *Зеневич А.О., Комаров С.К., Тимофеев А.М.* // Электросвязь. 2010. № 10. С. 14–16.
7. *Гулаков И.Р., Зеневич А.О.* Фотоприемники квантовых систем: монография. Минск, 2012.