УДК 621.383.92

О.К. БАРАНОВСКИЙ, А.О. ЗЕНЕВИЧ, А.Г. КОСАРИ
Учреждение образование «Высший государственный колледж связи», Республика Беларусь
Е.В. ВАСИЛИУ
Одесская национальная академия связи им. А.С. Попова, Украина

ОБНАРУЖЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ПО ОПТИЧЕСКОМУ ВОЛОКНУ

Разработано устройство для обнаружения несанкционированного доступа к оптическому волокну путем использования компенсационного способа съема информации. Определены характеристики этого устройства. Предложен метод дополнительной защиты информации, которую может перехватить несанкционированный пользователь за время его обнаружения.

Ключевые слова: оптическое волокно, обнаружение несанкционированного доступа, фотодиод, режим счета фотонов, метод защиты информации.

A.K. BARANOUSKI, A.O. ZENEVICH, A.G. KOSARI
Education establishment «The Higher State College of Communications», The Republic of Belarus
E.V. VASILIU
Odessa National Academy of Telecommunications named after O.S. Popov, Ukraine

DETECTION OF UNAUTHORIZED ACCESS DURING INFORMATION TRANSMISSION THROUGH AN OPTICAL FIBER

The device is developed for detection of unauthorized access to optical fiber by using compensation method of eavesdropping. The characteristics of this device are found. The method for additional information security until unauthorized user will be detected is suggested.

Keywords: optical fiber, unauthorized access detection, photodiode, photon-counting mode, methods of information security.

Введение. В последние годы для передачи информации используются оптические волокна. Они дают возможность получить скорость передачи информации до 10 Тбит/с. В определенных случаях необходимо обеспечить конфиденциальность информации, передаваемой по оптическому волокну. Одним из таких способов является обнаружение несанкционированных пользователей, подключенных к оптическому волокну [1-2]. Устройства, реализующие этот способ, зачастую основаны на измерении потери мощности оптического излучения при съеме информации несанкционированным пользователем [1-2]. Однако такие устройства малоэффективны при использовании компенсационного способа съема информации. Этот способ основывается на регистрации части излучения несанкционированным пользователем, а затем компенсации этой части излучения путем ввода его в оптическое волокно. В устройствах [1-2] для обнаружения потери мощности, вызванных несанкционированных подключением, применяются фотоприемники, работающие в токовом режиме. Согласно работе [3] токовый режим имеет большую величину пороговой чувствительности по абсолютному значению по сравнению с режимом счета фотонов. При заборе несанкционированным пользователем достаточно малой мощности оптического излучения из волокна, он может быть не обнаружен.

Для обнаружения несанкционированного пользователя требуется некоторый интервал времени. За этот интервал времени некоторая часть данных, передаваемых по оптическому волокну, станет известна несанкционированному пользователю. Поэтому **целью** данной работы является создание устройства для повышения эффективности обнаружения несанкционированного доступа при передаче информации по оптическому волокну, а также разработка метода дополнительной защиты передаваемой информации.

Описание устройства. Для обнаружения несанкционированного пользователя при передаче информации по оптическому волокну было разработано устройство, структурная схема которого представлена на рис.1.

Принцип работы устройства заключается в том, что на блок управления УУ подается входная последовательность данных. Первый выход УУ соединен с входом источника информационного сигнала И1 (см. рис. 1). Блок УУ управляет работой источника И1 таким образом, что при появлении на входе УУ символа «1» на его первом выходе, устанавливается уровень напряжения, соответствующий логической единице. Тогда на выходе источника И1 появляется оптическое излучение. Источник И1 излучает до тех пор, пока на его входе присутствует напряжение, соответствующее логической единице. При появлении на входе УУ символа «0» на его выходе устанавливается уровень напряжения, соответствующий логическому нулю. При этом оптическое излучение на выходе источника И1 отсутствует.

Второй выход УУ соединен с источником контрольного сигнала И2 (см. рис. 1). После момента времени появления на первом выходе УУ логической единицы на втором выходе УУ с некоторой временной задержкой τ формируется управляющий электрический импульс. При появлении на входе источника И2 электрического импульса на его выходе формируется однофотонный импульс (контрольный сигнал).

Оптическое излучение от источника И1 поступает на поляризатор П1, а от И2 − на поляризатор П2. Оптические излучения от источников И1 и И2 имеют одинаковую длину волны λ_1. Поляризаторы линейно поляризуют оптическое излучение источников И1 и И2 во взаимно перпендикулярных направлениях. После

поляризаторов излучения подаются на оптический смеситель СМ. Также оптическое излучение от рефлектометра Р с длиной волны λ_2 поступает на оптический смеситель СМ.

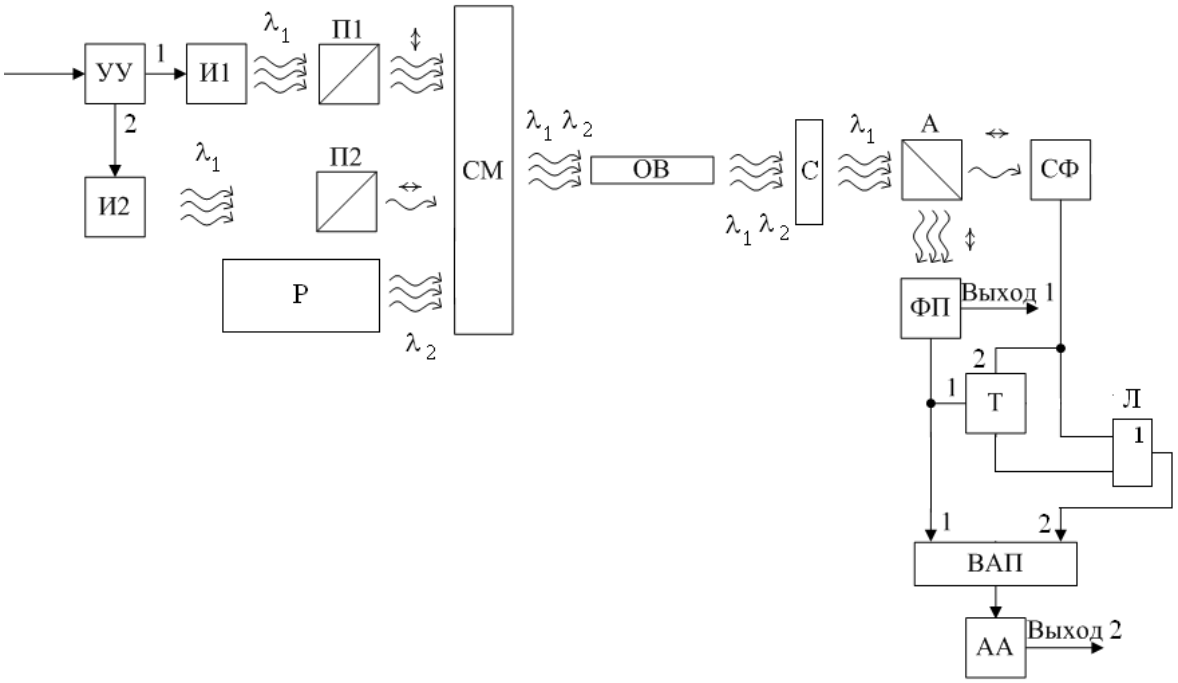

Рис. 1. Структурная схема устройства
УУ – блок управления, И1 – источник информационного сигнала, И2 – источник контрольного сигнала, П1 и П2 – поляризаторы, СМ – оптический смеситель, ОВ – оптическое волокно, А – анализатор, ФП – фотоприемное устройство, СЧ – счетчик фотонов, Т – таймер, Л – логический элемент «или», ВАП – время – амплитудный преобразователь, АА – амплитудный анализатор, С – светофильтр, Р - рефлектометр.

Смеситель СМ смешивает оптические излучения от источников И1, И2 и рефлектометра Р направляет эти излучения в оптическое волокно ОВ. С выхода волокна ОВ оптические излучения через светофильтр С подаются на анализатор А. Светофильтр С не позволяет излучению с длиной волны λ_2 поступать на анализатор А. Анализатор разделяет оптические излучения с длиной волны λ_1 в зависимости от их поляризации (см. рис. 1). Оптическое излучение от источника И1 подается на фотоприемное устройство ФП, а от источника И2 – на счетчик фотонов СФ.

С выхода 1 фотоприемного устройства снимается передаваемый информационный сигнал. Второй выход ФП соединен с первым входом время – амплитудного преобразователя ВАП и первым управляющим входом таймера Т. При приеме символа «1» на втором выходе ФП формируется электрический импульс, который является «стартовым» для ВАП. Передний фронт этого импульса запускает работу ВАП и таймера Т.

Выход счетчика фотонов СФ соединен с вторым управляющим входом таймера Т и через логический элемент «или» Л со вторым входом ВАП. При поступлении на вход СФ контрольного сигнала, на его выходе формируется электрический импульс, который является «стоповым» для ВАП. Передний фронт этого импульса останавливает работу ВАП и таймера Т. На выходе ВАП формируется электрический импульс, амплитуда которого прямо пропорционально времени задержки между появлением импульсов на его первом и втором входах.

Выход ВАП соединен с входом амплитудного анализатора АА. Анализатор выполняет сравнение амплитуды электрического импульса *U,* поступившего на его вход с ВАП, с некоторым заданным значением амплитуды $U_з$. Если выполняется соотношение $U > U_з$, то на выходе анализатора появляется уровень напряжения, соответствующий логической единице, и это свидетельствует о наличии несанкционированного пользователя в линии связи ОВ. В противном случае на выходе АА присутствует уровень напряжения, соответствующий логическому нулю.

Измерив задержку между символом «1» и контрольным сигналом τ и сравнив её с заданным значением $\tau_з$, делается вывод о наличии несанкционированного доступа к оптическому волокну, обеспечивающего вывод через ее боковую поверхность части оптического излучения с помощью специальных средств с компенсацией потерь мощности этого излучения.

Появления в линии связи такого пользователя будет приводить к увеличению времени задержки $\tau > \tau_з$.

Если счетчик фотонов СФ не зарегистрирует контрольный сигал, то таймер Т через некоторый интервал времени $t >> \tau$ сформирует «стоповый» импульс, который через логический элемент Л, поступит на второй вход ВАП.

При приеме данных подсчитывают число N_1 переданных символов «1» и количество N зарегистрированных контрольных сигналов за некоторый временной интервал. Если $N < N_1$, то принимается решение о наличии несанкционированного доступа к линии связи.

Отметим, что уменьшение N по сравнению с N_1 возможно при выводе через боковую поверхность волокна оптического излучения с помощью специальных средств без компенсации потерь мощности этого излучения.

Экспериментальные результаты и их обсуждение. Передачи информации по оптическому волокну осуществлялась на длине волны оптического излучения λ_1 = 850 нм. При регистрации однофотонных импульсов с этой длиной волны не требуется охлаждения фотоприемника счетчика фотонов.

Для регистрации излучения с λ_1 = 850 нм использовались кремниевые лавинные фотодиоды (ЛФД) ФД-115Л и ЛФД со структурой n^+p-π-p^+. Фотоприемное устройство ФП (см. рис.1) построено на основе ЛФД, работающем в токовом режиме, а счетчик фотонов СФ – на основе лавинных фотодиодов, работающим в режиме счета фотонов.

Оценка времени обнаружения несанкционированного пользователя $t_{об}$ проводилась для случая, когда вероятности передачи символов «1» и «0» равны между собой. Длительность передачи одного бита информации была равна 110 нс. Мощность оптического импульса для передачи символа «1» выбиралось такой, чтобы вероятность его не зарегистрировать была равной 10^{-12}. Величина $t_{об}$ определялась по формуле:

$$t_{\text{об}} = \frac{\eta n_{ф} + n_m}{\left(\eta n_{ф}\right)^2},$$

где η – квантовая эффективность регистрации счетчика фотонов, $n_{ф}$ – количество однофотонных импульсов, сгенерированных за одну секунду, n_m – количество ложных срабатываний счетчика фотонов за одну секунду. При проведении измерений $n_{ф} = 10^6$ с$^{-1}$, а для оценки $t_{об}$ использовалась скорость счета сигнальных импульсов $n_c = \eta\, n_{ф}$.

Напряжение пробоя $U_{пр}$ для исследуемых типов ЛФД были различны, для лавинного фотодиода ФД -115Л $U_{пр}$ = 51.01 В, а для ЛФД со структурой n^+p-π-p^+ $U_{пр}$ = 190,70 В. Режим счета фотонов на ЛФД реализуется при напряжениях питания U_n, близких или превышающих их напряжения пробоя [3]. Для сравнения характеристик исследуемых типов ЛФД, работающих в режиме счета фотонов, при различных напряжениях питания использовалось перенапряжение $\Delta U = U_n - U_{пр}$.

На рис. 2 представлены зависимости времени обнаружения несанкционированного пользователя от перенапряжения. Эти зависимости как для лавинного фотодиода ФД-115Л, так и для ЛФД со структурой n^+p-π-p^+ имели минимум. Минимальное время $t_{об}$ для лавинных фотодиодов ФД-115Л и со структурой n^+p-π-p^+ соответствовало ΔU= 0,6 В и составляло $t_{об}$ = 20 мкс. Минимум зависимости $t_{об}(\Delta U)$ наблюдается для перенапряжения, при котором $n_c > n_m$ и разность между этими величинами максимальна (см. рис. 2).

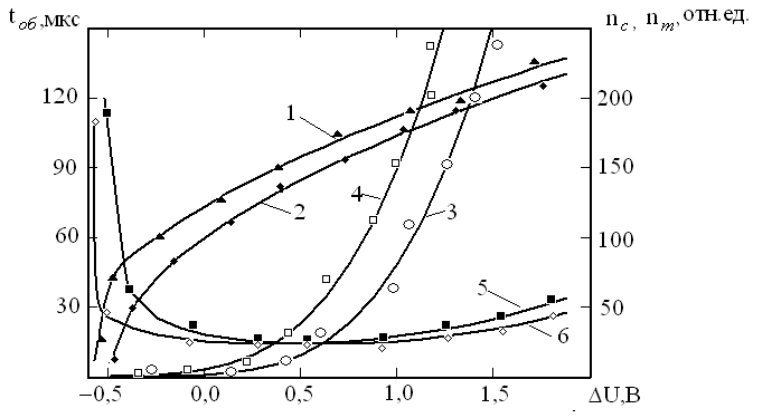

Рис. 2. Зависимость времени обнаружения несанкционированного пользователя от перенапряжения:
1 – n_c для ФД-115Л; 2 – n_c для n^+p-π-p^+;3 – n_m для ФД-115Л; 4 – n_m для n^+p-π-p^+; 5 – $t_{об}$ для ФД-115Л; 6 – $t_{об}$ для n^+p-π-p^+.

Выполнено измерение времени задержки между символом «1» и контрольным сигналом τ и определено, что его наименьшее значение составляло 8,0 нс и 8,1 нс для лавинных фотодиодов ФД-115Л и ЛФД со структурой n^+p-π-p^+ соответственно.

На рис. 3 представлены статистические распределения времени задержки τ для лавинных фотодиодов ФД-115Л и со структурой n^+p-π-p^+. Из статистических распределений получено, что погрешность измерения времени задержки между символом «1» и контрольным сигналом $\Delta\tau$ имело значение для лавинных фотодиодов ФД-115Л – 0,1 нс, а для n^+p-π-p^+ – 0,2 нс.

Быстродействие лавинных фотоприемников в режиме счета фотонов определяется также мертвым временем $\tau_м$ [4]. Под мертвым временем понимается промежуток времени после регистрации однофотонного импульса, в течение

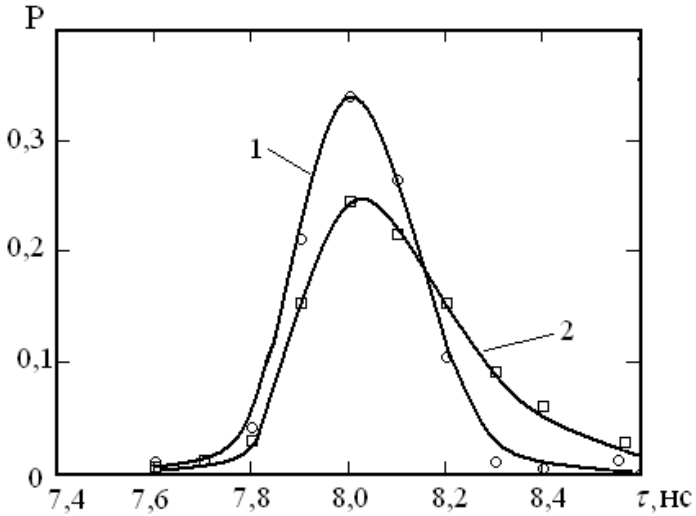

Рис. 3. Статистические распределения времени задержки:
1 – ФД-115Л; 2 – n^+p-π-p^+

которого фотоприемник не чувствителен к падающему на него оптическому излучению. Для исследуемых лавинных фотодиодов минимальное значение $\tau_м$ = 100 нс при включении их по схеме активного гашения лавины.

Так как в эксперименте время передачи одного бита информации составляло 110 нс, то за время обнаружения $t_{об}$ = 20 мкс несанкционированный пользователь может получить 181 бит информации, что для систем конфиденциальной связи может быть недопустимо. Поэтому необходима дополнительная защита. Метод такой защиты может быть разработан на основе известного метода усиления безопасности пинг-понг протоколов квантовой прямой безопасной связи [5], который позволяет сделать перехваченную несанкционированным пользователем информацию бесполезной для него.

Следует отметить, что несанкционированный пользователь имеет возможность снять передаваемую по оптическому волокну информацию более сложным способом, чем просто съем с боковой поверхности волокна. Для этого он должен сделать врезку в оптическое волокно и установить анализатор, разделяющий фотоны в зависимости от их поляризации, аналогичный анализатору, который находится на приемной стороне предлагаемого устройства (см. рис. 1). Анализатор несанкционированного пользователя будет отделять контрольные сигналы, имеющие горизонтальную поляризацию, от информационных, поляризованных вертикально. Далее несанкционированный пользователь будет сразу отправлять контрольные сигналы далее в волокно ОВ, практически не создавая задержки. Таким образом, он будет иметь возможность отводить часть информационного сигнала, не подвергаясь опасности быть обнаруженным предлагаемым устройством.

Однако, врезка несанкционированного пользователя может быть обнаружена с помощью рефлектометра. Рефлектометр периодически посылает оптические импульсы в оптическое волокно и анализирует их обратное рассеяние с целью обнаружения врезки.

Для тестирования оптического волокна при помощи рефлектометра использовались оптические импульсы с длиной волны λ_2 = 1625 нм. Согласно работе [6], использование этой длины волны позволяет наиболее эффективно обнаруживать наличие все возможных дефектов волокна, в том числе обусловленных врезками, по сравнению с другими длинами волн, применяемыми для передачи информации по оптическому волокну.

Метод дополнительной защиты информации, передаваемой по оптическому волокну. Передающая сторона (субъект *A*) перед передачей сообщения разбивает свою двоичную последовательность данных на *m* блоков некоторой фиксированной длины *r*, обозначим эти блоки через a_i ($i = 1,\ldots m$). Величина *r* должна выбираться таким образом, чтобы блок был передан за время $t_{пер}$, заведомо превышающее время обнаружения несанкционированного пользователя $t_{об}$. Согласно экспериментально полученных данных, за $t_{об}$ = 20 мкс несанкционированный пользователь может получить 181 бит, следовательно, длину блока можно выбрать *r* = 200 бит.

Затем субъект *A* генерирует для первого блока a_1 случайную обратимую двоичную матрицу L_1 размера $r \times r$ и умножает полученную матрицу на блок сообщения (умножение выполняется по модулю 2):

$$b_1 = L_1 \cdot a_1 .$$

После этого субъект *A* передает блок b_1 принимающей стороне (субъект *B*) согласно схеме (рис. 1). Если за время передачи блока несанкционированный пользователь не был обнаружен, то субъект *A* передает субъекту *B* матрицу L_1. Субъект *B* обращает матрицу и, умножив ее на принятый блок данных, восстанавливает исходный блок a_1:

$$a_1 = L_1^{-1} \cdot b_1 .$$

Если же во время передачи b_1 легитимные пользователи обнаруживают несанкционированное снятие информации в канале, то субъект *A* не передает матрицу L_1, и протокол связи прерывается. При этом несанкционированный пользователь, не зная матрицы, практически не имеет возможности восстановить исходный блок данных a_1. Так, известно, что для двоичных матриц размером 16×16 и более, вероятность того, что сгенерированная случайным образом матрица будет обратимой, является константой, равной 0,289 [7]. Таким образом, уже для матриц размером 16×16 количество случайных обратимых матриц равно $0{,}289\cdot 2^{256}$, что делает атаку прямого перебора матриц абсолютно не реализуемой (при текущем уровне быстродействия вычислительной техники). Для случая длины блока *r* = 200 количество обратимых матриц равно $0{,}289\cdot 2^{40000}$.

Описанная выше процедура затем повторяется для всех последующих блоков данных a_i. При этом важно для каждого блока a_i использовать свою матрицу L_i. При повторном использовании одной матрицы для многих блоков данных (не менее *r* блоков с одной матрицей) несанкционированный пользователь имеет возможность с использованием криптоаналитических методов получить некоторую информацию.

Следует подчеркнуть, что предложенный метод дополнительной защиты никак не связан с шифрованием и соответственно с распределением секретных ключей. Случайные двоичные матрицы не являются ключами и могут передаваться открыто, но только после того, как легитимные пользователи убедились в отсутствии несанкционированного съема информации в канале, что обеспечивается предложенным в статье устройством.

Выводы. Разработано устройство обнаружения несанкционированного доступа при передаче данных по волоконно-оптической линии связи, позволяющее обнаруживать несанкционированных

пользователей, использующих компенсационный метод съема данных.

Выполнены исследования таких характеристик устройства, как время задержки τ между символом «1» и контрольным сигналом, погрешность измерения времени задержки между символом «1» и контрольным сигналом, время обнаружения несанкционированного доступа.

Получено, что среднее значение времени задержки τ составляет 8,0 ± 0,1 нс и 8,1± 0,2 нс для лавинных фотодиодов ФД-115Л и со структурой n^+p-π-p^+ соответственно.

Определено, что для количества сгенерированных за одну секунду однофотонных импульсов, равного 10^6 c^{-1}, минимальное время обнаружения несанкционированного пользователя для лавинных фотодиодов ФД-115Л и со структурой n^+p-π-p^+ составляет $t_{об}$ = 20 мкс. Для получения минимального значения времени обнаружения несанкционированного пользователя необходимо выбирать напряжение питания фотоприемника, которое соответствует минимуму зависимости $t_{об}(\Delta U)$.

Таким образом, при использовании несанкционированным пользователем вывода оптического излучения через боковую поверхность волокна без компенсации потерь мощности этого излучения, он будет обнаружен за $t_{об}$ = 20 мкс. Несанкционированный доступ к оптическому волокну, обеспечивающий вывод через его боковую поверхность части оптического излучения с помощью специальных средств с компенсацией потерь мощности этого излучения, будет выявлен при создании им временной задержки, большей 0,1 нс для лавинных фотодиодов ФД-115Л и 0,2 нс для ЛФД со структурой n^+p-π-p^+.

Предложен метод дополнительной защиты, состоящий в умножении блоков данных на случайные обратимые двоичные матрицы. Этот метод позволяет сделать перехваченную несанкционированным пользователем информацию (до момента его обнаружения) бесполезной для него.

Работа выполнена при поддержке Белорусского республиканского фонда фундаментальных исследований (договор №Т14М-130).

Литература

1. Способ защиты информации от несанкционированного доступа в волоконно-оптических линиях связи: пат. 2110894 Российской Федерации, МКП7 H 04B 10/00, С.Н. Ивченко, В.В. Шубин; заявитель Российский федеральный ядерный центр - Всероссийский научно - исследовательский институт экспериментальной физики; Министерство Российской Федерации по атомной энергии. - № а 95103579/09; заявл. 14.03.1995; опубл. 10.05.1998//Официальный бюл./Федеральная служба по интеллектуальной собственности. – 1998. - №13. – С.174

2. Способ обнаружения вывода излучения с боковой поверхности оптического волокна: пат. 2350018 Российской Федерации, МКП7 H 04B 10/08, В.В. Шубин; заявитель Российский федеральный ядерный центр - Всероссийский научно - исследовательский институт экспериментальной физики; Министерство Российской Федерации по атомной энергии. - № а 2006141906/09; заявл. 27.11.2006; опубл. 20.03.2009//Официальный бюл./Федеральная служба по интеллектуальной собственности. – 2009. - №8. – С.154

3. Гулаков, И.Р. Метод счета фотонов в оптико-физических измерениях / И.Р. Гулаков, С.В. Холондырев. – Мн.: Университетское, 1989. – 256 с.

4. Гулаков, И.Р. Фотоприемники квантовых систем: монография / И.Р. Гулаков, А.О. Зеневич. – Минск: УО ВГКС, 2012. – 276 с.

5. Василиу, Е.В. Синтез основанной на пинг – понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. – 2009, № 1. – С. 83–91.

6. Листвин А.В. Рефлектометрия оптических волокон // А.В.Листвин, В.Н. Листвин.- Москва: ЛЕСАРарт, 2005. – 208 с.

7. Overbey J. On the keyspace of the Hill cipher / J. Overbey, W. Traves, J. Wojdylo // Cryptologia. – 2005. – V. 29, issue 1. – P. 59– 72.

References

1. Sposob zaschityi informatsii ot nesanktsionirovannogo dostupa v volokonno-opticheskih liniyah svyazi: pat. 2110894 Rossiyskoy Federatsii, MKP7 H 04V 10/00, S.N. Ivchenko, V.V. Shubin; zayavitel Rossiyskiy federalnyiy yadernyiy tsentr - Vserossiyskiy nauchno - issledovatelskiy institut eksperimentalnoy fiziki; Ministerstvo Rossiyskoy Federatsii po atomnoy energii. - № a 95103579/09; zayavl. 14.03.1995; opubl. 10.05.1998//Ofitsialnyiy byul./Federalnaya sluzhba po intellektualnoy sobstvennosti. – 1998. - №13. – S.174

2. Sposob obnaruzheniya vyivoda izlucheniya s bokovoy poverhnosti opticheskogo volokna: pat. 2350018 Rossiyskoy Federatsii, MKP7 H 04V 10/08, V.V. Shubin; zayavitel Rossiyskiy federalnyiy yadernyiy tsentr - Vserossiyskiy nauchno - issledovatelskiy institut eksperimentalnoy fiziki; Ministerstvo Rossiyskoy Federatsii po atomnoy energii. - № a 2006141906/09; zayavl. 27.11.2006; opubl. 20.03.2009//Ofitsialnyiy byul./Federalnaya sluzhba po intellektualnoy sobstvennosti. – 2009. - №8. – S.154

3. Gulakov, I.R. Metod scheta fotonov v optiko-fizicheskih izmereniyah / I.R. Gulakov, S.V. Holondyirev. – Mn.: Universitetskoe, 1989. – 256 s

4. Gulakov, I.R. Fotopriemniki kvantovyih sistem: monografiya / I.R. Gulakov, A.O. Zenevich. – Minsk: UO VGKS, 2012. – 276 s.

5. Vasiliu, E.V. Sintez osnovannoy na ping – pong protokole kvantovoy svyazi bezopasnoy sistemyi pryamoy peredachi soobscheniy / E.V. Vasiliu, S.V. Nikolaenko // NaukovI pratsI ONAZ Im. O.S. Popova. – 2009, № 1. – S. 83–91.

6. Listvin A.V. Reflektometriya opticheskih volokon // A.V.Listvin, V.N. Listvin.- Moskva: LESARart, 2005. – 208 s.

7. Overbey J. On the keyspace of the Hill cipher / J. Overbey, W. Traves, J. Wojdylo // Cryptologia. – 2005. – V. 29, issue 1. – P. 59– 72.

Рецензія/Peer review : 27.5.2015 р. Надрукована/Printed :1.7.2015 р.
Стаття рецензована редакційною колегією