Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 621.383.92

КОСАРИ
Араш Голамреза

ОБНАРУЖЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В ОПТОВОЛОКОННЫХ ЛИНИЯХ СВЯЗИ НА ОСНОВЕ МАЛОМОЩНЫХ ОПТИЧЕСКИХ ВОЗДЕЙСТВИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата
технических наук

по специальности 05.13.19 – Методы и системы защиты информации,
информационная безопасность

Минск 2016

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Научный руководитель	**Зеневич Андрей Олегович**, доктор технических наук, профессор, ректор учреждения образования «Белорусская государственная академия связи»
Официальные оппоненты	**Голиков Владимир Федорович**, доктор технических наук, профессор, заведующий кафедрой «Информационные технологии в управлении» Белорусского национального технического университета
	Иванов Николай Николаевич, кандидат технических наук, доцент, доцент кафедры электронных вычислительных машин учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
Оппонирующая организация	Государственное научно-производственное объединение «Оптика, оптоэлектроника и лазерная техника» Национальной академии наук Беларуси

Защита состоится «15» декабря 2016 г. в 14.00 на заседании совета по защите диссертаций Д 02.15.06 при Белорусском государственном университете информатики и радиоэлектроники по адресу: 220013, г. Минск, Ул. П. Бровки, 6, корп. 1, ауд. 232, e-mail: dissovet@bsuir.by, тел. 293-89-89.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Автореферат разослан «11 » ноября 2016 г.

Ученый секретарь совета
по защите диссертаций,
кандидат технических наук,
доцент Н.В. Насонова

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время для передачи данных широкое применение находят оптические волокна. Это связано с тем, что они позволяют обеспечить высокую скорость передачи данных, более 10 Тбит/с. Несмотря на то, что оптическое излучение, используемое для передачи данных, распространяется внутри оптического волокна, существуют способы несанкционированного доступа к эти данным [1–3]. Для защиты передаваемых данных в настоящее время применяются различные устройства. Работа эти устройств базируется на следующих принципах: обнаружение канала утечки информации и прекращение передачи данных; зашумление канала; передача зашифрованной информации.

Обнаружение канала утечки информации и прекращение передачи данных основывается на определении потери мощности оптического излучения, вызванной подключением несанкционированного пользователя. Этот способ становится неэффективным при использовании несанкционированного метода компенсации мощности оптического излучения, забранной им из волокна, для доступа к передаваемым данным.

Оборудование, необходимое для создания зашумления канала, сложно в реализации и является достаточно дорогостоящим.

Шифрование передаваемой информации при помощи ключа также не всегда является эффективным способом защиты информации. При шифровании симметричным ключом, для того чтобы несанкционированный пользователь не смог расшифровать передаваемую информацию, необходимо, чтобы длина ключа соответствовала длине передаваемых данных. В этом случае потребуется создания большой базы секретных ключей, которая должна быть доступна только санкционированным пользователям. Создание такой базы потребует большого хранилища информации, а также процедуры постоянной замены этих ключей. Все это усложняет процесс передачи данных. Во всех других случаях расшифровка информации зависит от вычислительных мощностей несанкционированного пользователя.

Поэтому необходимо отметить, что создание простых в реализации и эффективных устройств защиты информации, передаваемой по оптическому волокну, является важной и актуальной задачей.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Тема диссертации соответствует утвержденному научному плану работ учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» и следующим приоритетным направлениям фундаментальных и прикладных научных исследований Республики Беларусь:

1. Информационно-коммуникационные, авиационные и космические технологии и аппаратура.

2. Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы.

3. Средства контроля параметров систем и средств связи и телекоммуникаций.

Результаты, полученные в диссертационной работе, связаны с выполнением научно-исследовательских работ, договор № Т14М-130 от 23 мая 2014 г. «Квантовые системы безопасной связи на основе одноквантовых фотоприемников», срок выполнения 23.05.2014–31.03.2016, № ГР 20141955 от 27.08.2014 г.

Цель и задачи исследования

Цель работы состоит в разработке способов и устройства для обнаружения каналов утечки информации из оптического волокна, основанного на взаимодействии маломощных оптических сигналов с неоднородностями оптического волокна.

Для достижения поставленной цели в работе решаются следующие взаимосвязанные задачи:

1) установить физические принципы формирования каналов утечки информации из оптического волокна;

2) предложить методы обнаружения каналов утечки информации из оптического волокна независимо от способа съема информации и мощности передаваемого оптического сигнала;

3) разработать на основе предложенных методов устройства по обнаружению каналов утечки информации из оптического волокна;

4) определить влияние на время обнаружения канала утечки информации параметров оптического волокна, характеристик источников и приемников оптического излучения;

5) предложить метод защиты информации, перехваченной несанкционированным пользователем, в течение времени его обнаружения.

Исследуемыми объектом являются оптическое волокно, источники оптического излучения, лавинные фотоприемники (ЛФП), работающие в режиме одноквантовой регистрации. Предметом исследования являются принципы формирования каналов утечки информации из оптического волокна и способы обнаружения этих каналов.

Научная новизна

В основу разработанного метода защиты передаваемых данных по оптическому волокну от несанкционированных пользователей и обнаружения канала утечки информации положены установленные зависимости между вероятностью потери оптического сигнала и диаметром макроизгиба оптического волокна для различных длин волн оптического излучения, передаваемого по волокну. Доказано, что оптическое излучение с длиной волны 850 нм необходимо использовать для защиты предаваемых данных маломощными оптическими импульсами, а мощные оптические импульсы с длиной волны 1630 нм для обнаружения каналов утечки информации.

Предложено выражение для оценки пропускной способности квантового канала связи на участке между санкционированными пользователями, учитывающее вероятность несанкционированного вывода мощности излучения из оптического волокна, и параметры счетчика фотонов.

Установлена нелинейная зависимость обнаружительной способности устройства от напряжения питания фотоприемника, позволяющая определять напряжение питания, соответствующее минимальному времени обнаружения.

Положения, выносимые на защиту

1. Способ обнаружения каналов утечки информации через макроизгибы оптического волокна, заключающийся в передаче данных оптическими импульсами с длиной волны 850 нм и мощностью, меньшей 10^{-12} Вт, синхронизации работы источника и приемника данных оптическими импульсами мощностью, большей 10^{-11} Вт, имеющими длину волны 1630 нм, регистрации данных лавинными фотоприемниками, работающими в режиме счета фотонов, позволяющий выявлять канал утечки информации с диаметром макроизгиба менее 60 мм.

2. Модель канала утечки информации при подключении несанкционированного пользователя к оптическому волокну при помощи пассивного и активного метода съема данных, основанная на том, что передача данных осуществляется маломощными оптическими импульсами,

содержащими в среднем от одного до десятка фотонов, и регистрация этих импульсов выполняется счетчиком фотонов, позволяющая оценить уменьшение скорости передачи данных между легитимными пользователями при подключении несанкционированного пользователя к оптическому волокну, и обнаружить канал утечки информации при квантовой эффективности регистрации фотоприемника более 15 % .

3. Способ защиты передаваемой по оптическому волокну информации, основанный на разбиении данных на блоки, генерации ключа в виде случайной обратной матрицы, шифровании блоков ключом, формировании временной задержки между информационным и маломощным контрольным оптическими сигналами, линейной поляризации этих сигналов во взаимно партикулярных направлениях и их передаче по оптическому волокну с последующей регистрацией временной задержки между ними, позволяющий обнаружить несанкционированного пользователя, подключенного к оптическому волокну, для скоростей передачи данных не более 10 Мбит/с, при этом время обнаружения не превышает 20 мкс.

Личный вклад соискателя ученой степени

Изложенные в диссертации результаты отражают личный вклад автора. В работах, выполненных в соавторстве, автор принимал участие в выборе направлений исследований, обосновании и постановке конкретных научных задач, выработке методических путей их решения, выборе объектов исследования, разработке теоретических принципов, создании экспериментальных установок и проведении измерений, получении и интерпретации основных результатов, а также в создании новых способов и устройств. Все описанные эксперименты проводились автором лично или с его непосредственным участием.

С соавторами работ: А.О. Зеневичем (научный руководитель), И.Р. Гулаковым, О.К. Барановским и А.М. Тимофеевым был поставлен ряд научных задач.

Соавтором А.М. Тимофеевым была оказана помощь в проведении экспериментальных измерений и проведении обработки полученных результатов. И.Р. Гулаковым и А.М. Тимофеевым оказана помощь при построении математических моделей каналов утечки информации из оптического волокна. С соавтором Е.В. Василиу совместно разработан способ защиты данных, полученных несанкционированным пользователем за время его обнаружения. Со всеми соавторами совместно проводился анализ и обсуждение полученных результатов.

Апробация диссертации и информация об использовании ее результатов.

Основные результаты диссертации докладывались на следующих научно-технических конференциях: Международная Белорусско-российская научно-техническая конференция «Технические средства защиты информации», Минск, БГУИР (28–29 мая, 2014 г.), Международная научная техническая конференция приуроченная, к 50-летию МРТИ–БГУИР, Минск, БГУИР (18–19 марта, 2014 г.), Международная научная техническая конференция «Современные средства связи», Минск, Высший государственный колледж связи (15–16 октября, 2013 г.), Международная научная техническая конференция «Современные средства связи», Высший государственный колледж связи, Минск (14–15 октября 2014 г.), Международная конференция «Современные средства связи», Белорусская государственная академия связи, Минск (14–15 октября 2015 г.).

Опубликование результатов диссертации

По материалам диссертационной работы опубликовано 10 работ, в том числе 5 статей в научных реферируемых журналах и 5 тезисов докладов. Общий объем публикаций по теме диссертации, соответствующих пункту 18 Положения о присуждении ученых степеней и присвоения ученых званий Республики Беларусь, составляет 5,25 авторского листа.

Структура и объем диссертации

Работа состоит из перечня условных обозначений и сокращений, введения, общей характеристики работы, четырех глав, заключения и библиографического списка. Общий объем диссертации составляет 107 страниц, из них 96 страниц основного текста, 15 рисунков на 15 страницах, 4 таблицы на 4 страницах, библиографический список из 106 наименований на 8 страницах и список собственных публикаций соискателя из 10 наименований на 2 страницах.

ОСНОВНАЯ ЧАСТЬ

Во **введении** обоснована актуальность диссертационной работы.

В **первой главе** выполнен анализ методов формирования каналов утечки информации из оптического волокна, который показал, что подключение несанкционированного пользователя с использованием разрывного способа подключения к оптическому волокну хорошо обнаруживается при помощи методов рефлектометрии или организационных мероприятий. Из неразрывных способов подключения наиболее незаметным является туннелирование оптического излучения. Однако он требует специальной подготовки оптического волокна (шлифовки оболочки волокна), что является трудоемким и сложным процессом. Наиболее простым в реализации способом съема информации является создание макроизгиба волокна. Используя небольшие радиусы изгиба и чувствительную аппаратуру для регистрации оптического излучения, можно добиться незаметного съема данных с боковой поверхности оптического волокна.

Из рассмотренных способов регистрации оптического излучения с боковой поверхности оптического волокна следует, что наилучшую скрытность позволяют обеспечить пассивный и компенсационный способы. Для реализации пассивного способа необходимо знать местоположение неоднородностей оптического волокна. Определение таких мест для несанкционированного пользователя порой невозможно. В некоторых случаях при прокладке волокна удается избежать наличия таких мест. Поэтому лучше использовать компенсационный метод. В случае использования активного способа необходимо формировать макроизгибы оптического волокна с таким диаметром, чтобы его нельзя было обнаружить методами диагностики оптических волокон на наличие дефектов. Для регистрации выводимого оптического излучения необходимо использовать сверхчувствительные фотоприемники. В связи с этим рассматривается только два способа съема информации – активный и компенсационный.

Анализ способов защиты информации, передаваемой по волоконно-оптическим линиям связи, показывает, что использование способов квантовой криптографии позволяет обеспечить абсолютную защищенность передаваемой информации по оптическому волокну. Однако из-за сложной процедуры обмена данными между санкционированными пользователями для формирования секретного ключа не удается получить высокую скорость передачи информации. С увеличением длины оптического волокна скорость передачи информации уменьшается из-за эффектов, связанных с поглощением фотонов и отражением на оптических неоднородностях в волокне.

Рассмотрение способов обнаружения наличия подключения несанкционированного пользователя к оптическому волокну показало, что они не позволяют определить наличие такого подключения в случае забора этим

пользователем из информационного сигнала достаточно малой энергии оптического излучения, равной одному фотону. В этом случае изменение информационного сигнала будет незначительным и его обнаружить на фоне шумов регистрирующей аппаратуры будет практически невозможно. Для повышения обнаружительной способности необходимо повышать чувствительность фотоприемников, применяемых для детектирования излучения, и снижать уровень их шумов и регистрирующей аппаратуры. Также для лучшего выявления забора энергии информационного сигнала, соответствующей одному фотону, необходимо понизить энергию этого сигнала до десятка фотонов. При регистрации такого информационного сигнала необходимо использовать высокочувствительные фотоприемные устройства.

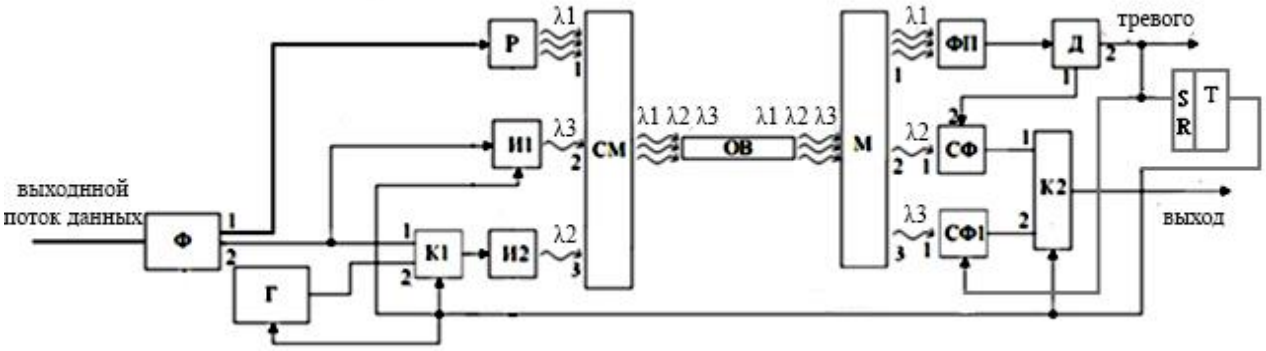
Во **второй главе** проведен анализ способов регистрации оптического излучения: регистрация фототока; измерения полного шума; счета фотонов. Выполнено сравнение этих способов регистрации. Показало, что при прочих равных условиях счет фотонов обеспечивает выигрыш по сравнению с другими способами регистрации по отношению к сигналу/шум не менее чем 10–15 %.

Определено, что для обнаружения несанкционированных пользователей, подключенных к оптическому волокну, необходимо использовать следующие фотоприемники: фотоэлектронные умножители, сверхпроводниковые фотоприемники, лавинные фотоприемники. Установлено что, для построения устройств обнаружения несанкционированных пользователей лучше всего использовать лавинные фотоприемники, поскольку эти фотоприемники имеют большую чувствительность в ближнем инфракрасном диапазоне, малые габариты, более высокую механическую прочность по сравнению с фотоэлектронными умножителями. Они не требуют такого глубокого охлаждения, как это необходимо для сверхпроводниковых фотоприемников.

Выявлено, что при использовании лавинных фотоприемников, работающих в режиме счета фотонов, для систем конфиденциальной передачи информации целесообразно применять две длины волны оптического излучения, передаваемой по одному оптическому волокну: λ_1 = 1630 нм для передачи мощных синхросигналов и контроля наличия несанкционированного доступа как наиболее чувствительную к макроизгибам оптического волокна и λ_2 = 850 нм для передачи данных слабыми оптическими сигналами как наименее чувствительную к макроизгибам волокна, а также наиболее близкую к максимальной спектральной чувствительности кремниевых ЛФП. Для регистрации синхроимпульсов необходимо использовать гермниевые лавинные фотоприемники и на основе соединений $A^{III}B^{V}$.

Разработана установка для передачи конфиденциальной информации с дезинформирующим каналом связи, позволяющая обеспечивать защиту передаваемой информации от несанкционированного пользователя с одновременным определением местоположения несанкционированного

пользователя (рисунок 1). При обнаружении несанкционированного пользователя передача данных не прекращается, а изменяется длина волны оптического излучения λ_2, на которой производится передача данных на другую длину волны λ_3 = 900 нм. На длине волны λ_2 осуществляется передача дезинформирующих несанкционированного пользователя данных. Это позволяет ввести в заблуждение несанкционированного пользователя и не дать возможности ему понять, обнаружен он или нет.



Р – рефлектометр; Ф – формирователь данных; Г – генератор дезинформирующих данных; К1 и К2 – коммутаторы; И1 и И2 – источники оптического излучения; СМ – смеситель; ОВ – оптическое волокно; М – мультиплексор; ФП – фотоприемник; Д – дискриминатор; СФ и СФ1 – счетчики фотонов; Т – триггер

Рисунок 1. – Структурная схема установки для передачи конфиденциальной информации с дезинформирующим каналом

В **третьей главе** построена математическая модель квантового канала связи, содержащего в качестве приемного модуля счетчик фотонов. Получены выражения, с помощью которых можно определять пропускную способность квантового канала связи на участках между санкционированными пользователями $C_{\max}$, и санкционированной передающей стороной и несанкционированным пользователем $C1_{\max}$:

$$C_{\max} = \left\{ -\left(1 - P_t/2 - \eta_p/2 + \eta_p P_{\text{пот}}/2\right)\log_2\left(1 - P_t/2 - \eta_p/2 + \eta_p P_{\text{пот}}/2\right) - \right.$$
$$-\left(P_t/2 + \eta_p/2 - \eta_p P_{\text{пот}}/2\right)\log_2\left(P_t/2 + \eta_p/2 - \eta_p P_{\text{пот}}/2\right) +$$
$$+0{,}5\left[\left(1 - P_t\right)\log_2\left(1 - P_t\right) + P_t \log_2 P_t\right] +$$
$$\left. +0{,}5\left[\left(1 - \eta_p + \eta_p P_{\text{пот}}\right)\log_2\left(1 - \eta_p + \eta_p P_{\text{пот}}\right) + \left(\eta_p - \eta_p P_{\text{пот}}\right)\log_2\left(\eta_p - \eta_p P_{\text{пот}}\right)\right]\right\} / \tau_b.$$

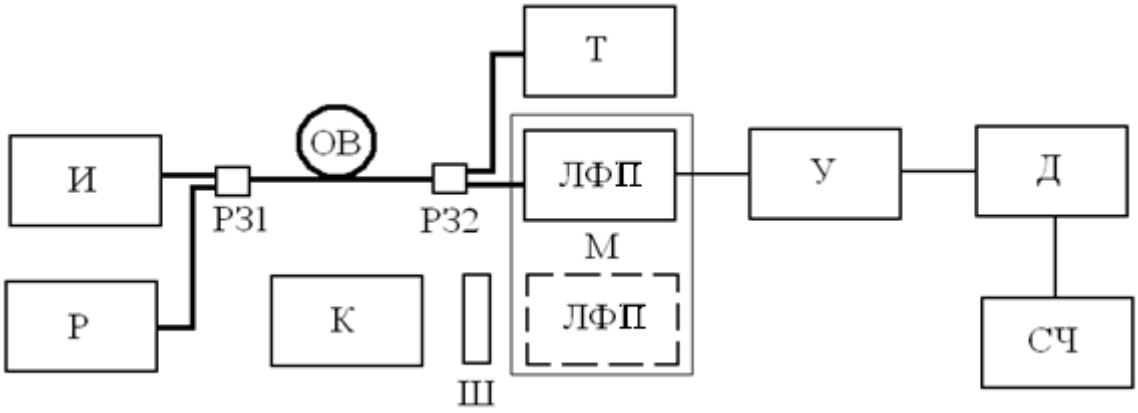
$$C1_{\max} = \left\{ -\left(1 - P_{\text{пот}}/2\right)\log_2\left(1 - P_{\text{пот}}/2\right) - \left(P_{\text{пот}}/2\right)\log_2\left(P_{\text{пот}}/2\right) + \right.$$
$$\left. +0{,}5\left[\left(1 - P_{\text{пот}}\right)\log_2\left(1 - P_{\text{пот}}\right) + P_{\text{пот}} \log_2 P_{\text{пот}}\right]\right\} / \tau_b.$$

где τ_b – среднее время передачи одного бита (символа). η_p – квантовая эффективность регистрации счетчика фотонов, P_t – вероятность появления темновых импульсов, $P_{\text{пот}}$ – вероятность выхода фотона излучения из оптического волокна.

Выражения для оценки пропускной способности $C_{\max}$ на участке между санкционированными пользователями учитывают вероятность несанкционированного вывода мощности излучения из оптического волокна, а также такие параметры счетчика фотонов, как вероятность P_t появления темновых импульсов и квантовую эффективность регистрации η_p.

Создана установка для определения наличие каналов утечки информации в оптическом волокне (рисунок 2). Сущность работы этой установки заключается в том, что она подразделяется на два цикла. Один из которых является калибровочным циклом, а другой – измерительным циклом. Во время калибровочного цикла выполняется измерение двух параметров: квантовой эффективности регистрации η_p и вероятности образования темновых импульсов в фотоприемнике P_t. При выполнении измерительного цикла определяется среднее число импульсов за время передачи одного символа «1», на основании чего делается заключение о наличии несанкционированного пользователя, подключенного к оптическому волокну. После чего выполняется оценка доступности информации, передаваемой между санкционированными пользователя, несанкционированному пользователю. Эта оценка производится на основании вычислений пропускной способности между санкционированными пользователями $C_{\max}$ и между санкционированным пользователем и несанкционированным $C1_{\max}$ по параметрам η_p и P_t, определенным во время калибровочного цикла.

При помощи этой установки оценивается влияние затухания оптического излучения в оптическом волокне, квантовой эффективности регистрации фотоприемника η_p, работающего в режиме счета фотонов, и вероятности P_t образования в нем темновых импульсов на эффективность обнаружения каналов утечки информации.



И – источник оптического излучения; Р – рефлектометр; РЗ1 и РЗ2 – оптические разветвители; ОВ – оптическое волокно; Т – оптический тестер; ЛФП – лавинный фотопремник; У – усилитель; Д – дискриминатор; СЧ – счетчик импульсов; Ш – светонепроницаемая шторка; М – механическая платформа; К – контрольный источник оптического излучения

Рисунок 2. – Структурная схема экспериментальной установки для исследования влияния параметров оптического волокна и характеристик фотоприемника на эффективность обнаружения каналов утечки информации

Получено условие утечки информации по каналу связи между санкционированной и несанкционированным пользователями, при котором несанкционированному пользователю будет доступна вся передаваемая информация между санкционированными пользователями. Таким условием является равенство пропускных способностей каналов связи между санкционированными пользователями и между санкционированной передающей стороной и несанкционированным пользователем. Установлено, что определить наличие такого несанкционированного пользователя в квантовом канале можно при значении $\eta_p > 0{,}15$ с относительной погрешностью, меньшей 13 %, и при вероятности образования темновых импульсов $P_t \leq 10^{-6}$.

В **четвертой главе** построена модель асинхронного, двоичного, дискретного, несимметричного, однородного без памяти и со стиранием оптического канала связи. В качестве приемника оптического излучения в таком канале использовался счетчик фотонов. Получено выражение, позволяющее определять пропускную способность C_{max} асинхронного канала, учитывать статистические распределения числа импульсов на выходе счетчика фотонов при передаче символа «0» и символа «1», и значениях пороговых уровней регистрации импульсов при передаче этих символов:

$$C_{\max} = \{-[0{,}5[P(0/0)+P(0/1)]]\log_2[0{,}5(P(0/0)+P(0/1))]-$$
$$-[0{,}5[P(1/0)+P(1/1)]]\log_2[0{,}5[P(1/0)+P(1/1)]]-$$
$$-[0{,}5[P(-/0)+P(-/1)]]\log_2[0{,}5[P(-/0)+P(-/1)]]+$$
$$+0{,}5[P(0/0)\log_2 P(0/0)+P(1/0)\log_2 P(1/0)+P(-/0)\log_2 P(-/0)]+$$
$$+0{,}5[P(0/1)\log_2 P(0/1)+P(1/1)\log_2 P(1/1)+P(-/1)\log_2 P(-/1)]\}/\tau_b.$$

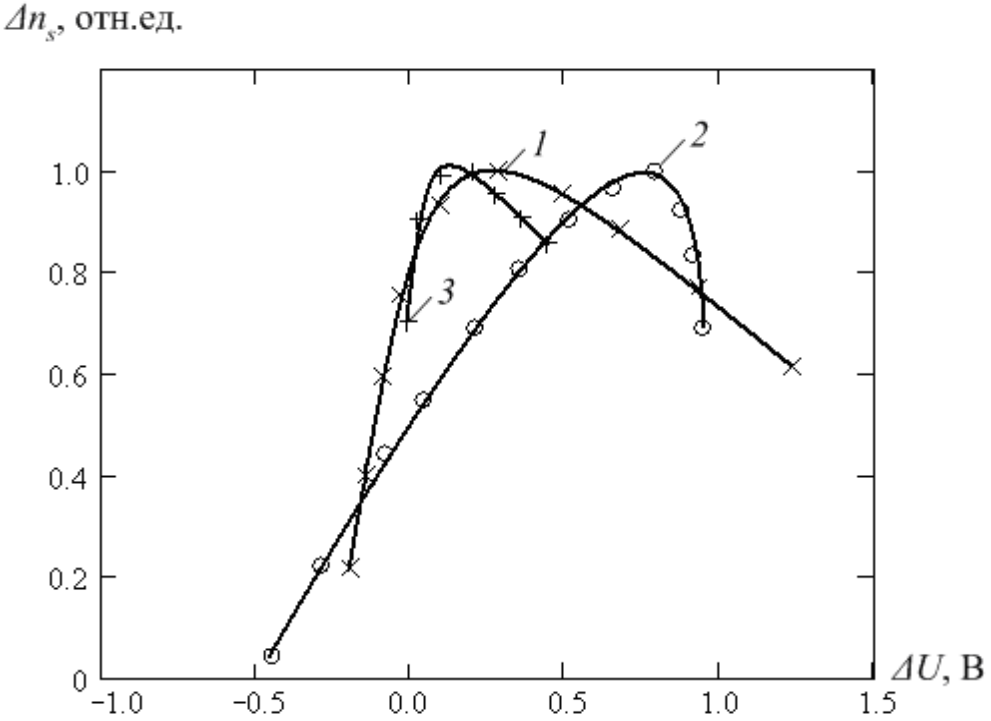
где *P(0/0)* и *P(0/1)* – вероятности регистрации счетчиком фотонов «0» при наличии на входе его символов «0» и «1» соответственно, *P(1/0)* и *P(1/1)* – вероятности регистрации счетчиком фотонов «1» при наличии на входе его символов «0» и «1» соответственно, *P(-/0)* и *P(-/1)* – вероятности того, что счетчик фотонов не зарегистрирует ни символа «0», ни символа «1», при наличии на его входе символа «0» или символа «1» соответственно.

Выполнены экспериментальные исследования, направленные на оптимизацию длительности двоичного символа τ_b с целью получения наибольшей пропускной способности асинхронного канала связи C_{max}. При этом оптимизация осуществлялась по зависимости пропускной способности канала C_{max} от длительности двоичного символа τ_b. Получено, что зависимость имеет максимум, который соответствовал длительности 20 мкс для всех исследуемых типов лавинных фотоприемников. Определено, что для обеспечения максимальной пропускной способности канала C_{max} длительность защитного интервала необходимо выбирать равной длительности двоичного символа τ_b.

Проведены исследования зависимости динамического диапазона Δn_s от величины перенапряжения лавинного фотоприемника ΔU (рисунок 3). Получено, что эти зависимости имеют одинаковый вид с ярко выраженным максимумом. Таким образом, для получения максимального значения динамического диапазона Δn_{smax} необходимо выбирать перенапряжение лавинного фотоприемника ΔU, соответствующее этому максимуму. Установлено, что данному значению перенапряжения соответствует наибольшая величина пропускной способности C_{max} асинхронного оптического канала связи для всех типов исследуемых фотоприемников. Получено, что среди исследуемых типов фотоприемников наибольшая величина пропускной способности достигается при использовании лавинных фотоприемников со структурой p^+n-ν-n^+.

Показано, что определяющее влияние на пропускную. способность $C_{\max}$ асинхронного оптического канала связи оказывает длительность мертвого времени счетчика фотонов. Уменьшение длительности мертвого времени приводит к увеличению пропускной способности. Добиться уменьшения мертвого времени счетчика фотонов на основе лавинного фотоприемника можно путем использования схемы активного гашения лавины. Получено, что в этом случае увеличить пропускную способность $C_{\max}$ канала можно в результате применения схемы активного гашения лавины ЛФП, что в сравнении со схемой

пассивного гашения повышает пропускную способность канала связи до 100 кбит/с за счет уменьшения мертвого времени счетчика фотонов.

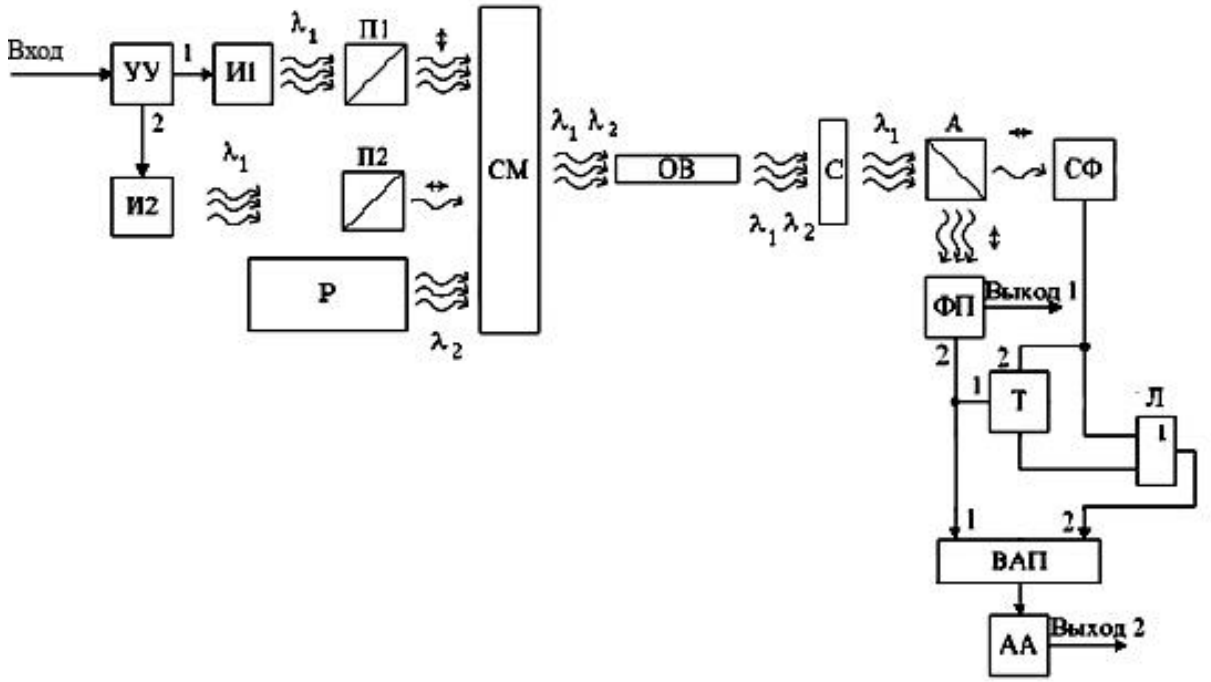


1 – ФД-115Л; 2 – ЛФП со структурой p^+n-ν-n^+;
3 – ЛФП со структурой n^+p-π-p^+
Рисунок 3. – Зависимость величины динамического диапазона Δn_s от перенапряжения лавинного фотоприемника ΔU.

Установлено, что для определения несанкционированного пользователя в асинхронном оптическом канале связи необходимо использовать лавинные фотоприемники с квантовой эффективностью регистрации не менее 30%, при этом погрешность определения значения коэффициента понижения пропускной способности должна не превышать ± 0,05. При таких значениях квантовой эффективности регистрации несанкционированному пользователю необходимо создать макроизгиб оптического волокна с диаметром, меньшим 10 мм, для того чтобы ему была доступна вся информация, передаваемая между санкционированными пользователями.

В **пятой главе** предложен метод обнаружения несанкционированного доступа при передаче данных по волоконно-оптической линии связи. Сущность этого метода заключается в том, что по одному оптическому волокну на одной длине волны передаются информационный сигнал, используемый для трансляции символа «1», и контрольный сигнал. Причем передачу контрольного сигнала задерживают на некоторый промежуток времени относительно передачи информационного сигнала. Кроме того, оптические излучения информационного и контрольного сигналов линейно поляризуют во взаимно

перпендикулярных направлениях. При регистрации этих сигналов измеряют задержку между ними, сравнив ее с некоторым заранее заданным значением. После чего делают заключение о наличии или отсутствии несанкционированного доступа к оптическому волокну. Это позволяет обнаружить несанкционированного пользователя, использующего компенсационный метод съема информации. Структурная схема устройства, реализующего этот метод, представлена на рисунке 4.



УУ – блок управления; И1 – источник информационного сигнала; И2 – источник контрольного сигнала; П1 и П2 – поляризаторы; СМ – оптический смеситель; ОВ – волоконно-оптическая линия связи; 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

Рисунок 4. – Структурная схема устройства для обнаружения несанкционированного пользователя при передаче информации по оптическому волокну

Для обнаружения несанкционированного пользователя, использующего для съема информации пассивный или активный способ, устройство подсчитывает число переданных символов «1» и количество зарегистрированных контрольных сигналов за некоторый временной интервал, а также выполняет сравнение их между собой. Если число переданных символов «1» меньше количества зарегистрированных контрольных сигналов, то на выходе 2 появляется сигнал (рисунок 4), что свидетельствует о наличии несанкционированного доступа к оптическому волокну.

Определено, что основными параметрами устройства, влияющими на его обнаружительную способность, являются: время задержки между передачей информационным сигналом, используемым для передачи символом «1», и контрольным сигналом; погрешность измерения времени этой задержки; время обнаружения несанкционированного доступа. Выполненные экспериментальные исследования показали, что погрешность измерения среднего значения времени задержки между передачей информационного сигнала, применяемого для передачи символом «1», и контрольного сигнала, зависит от типа лавинного фотоприемника, используемого в устройстве. Получено, что такое время задержки 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.

Установлено, что для числа сгенерированных за одну секунду однофотонных импульсов, равного 10^6, 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 $t_{об}(\Delta U)$. Определено, что несанкционированный доступ к оптическому волокну, обеспечивающий вывод 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 ЛФП со структурой n^+p-π-p^+.

Предложен способ дополнительной защиты данных, перехваченных несанкционированным пользователем, за время его обнаружения. Сущность этого метода заключается в том, что перед началом передачи данных санкционированный пользователь разбивает всю передаваемую информацию на блоки. Затем пользователь генерирует ключ в вид случайной обратимой двоичной матрицы. Далее выполняется умножение первого блока информации на эту матрицу и передача результата умножения по оптическому волокну другому санкционированному пользователю. Если во время такой передачи несанкционированный пользователь не обнаружен, то передается ключ. С помощью этого ключа санкционированный пользователь расшифровывает полученный им блок информации. В случае обнаружения несанкционированного пользователя ключ не передается. Таким образом, последовательно передаются все блоки информации. Этот метод позволяет сделать перехваченную несанкционированным пользователем информацию бесполезной для него.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Доказана возможность использования длины волны 850 нм для защиты передаваемых данных по оптическому волокну при помощи маломощных оптических импульсов, а для обнаружения канала утечки информации применяются мощные оптические импульсы с длиной волны 1630 нм [2, 3].

2. Разработано устройство, позволяющее обнаруживать каналы утечки информации через макроизгибы. Для передачи данных в этом устройстве используются оптические импульсы мощностью, меньшей 10^{-12} Вт, и с длиной волны оптического излучения 850 нм, для синхронизации работы источника и приемника оптического излучения применяются оптические импульсы мощностью, большей 10^{-11} Вт, и с длиной волны 1630 нм, регистрация данных осуществляется лавинными фотоприемниками, работающими в режиме счета фотонов [2, 3] .

3. Получено выражение для оценки пропускной способности квантового канала связи при наличии несанкционированного пользователя. Определено условие, при котором несанкционированному пользователю будет доступна вся передаваемая информация между санкционированными пользователями: равенство пропускных способностей каналов связи между санкционированными пользователями и между санкционированной передающей стороной и несанкционированным пользователем [1, 4].

4. Предложена модель канала утечки информации при подключении несанкционированного пользователя к оптическому волокну при помощи пассивного и активного метода съема данных. Модель позволяет оценить снижение скорости передачи данных между легитимными пользователями при подключении несанкционированного пользователя к оптическому волокну. На основании этой модели получено, что при квантовой эффективности регистрации фотоприемника для приема данных легитимным пользователем более 15 % можно обнаружить канал утечки информации [4].

5. Установлена зависимость времени обнаружения несанкционированного пользователя устройством, содержащим счетчик фотонов, от напряжения питания фотоприемника счетчика фотонов для случая передачи данных по оптоволоконной линии связи. Она позволила определить

оптимальное напряжение питания фотоприемника, соответствующее минимальному времени обнаружения [5].

6. Разработан метод обнаружения несанкционированного пользователя, подключенного к оптическому волокну, и на его основе создано устройство, позволяющее определять наличие несанкционированного пользователя независимо от способа его подключения к оптическому волокну, при скорости передачи данных не более 10 Мбит/с, при этом время обнаружения не превышает 20 мкс, а также осуществляющее кодирование той части данных, которая стала доступной несанкционированному пользователю, при помощи обратной матрицы, что обеспечивает неуязвимость передаваемой информации [5].

Рекомендации по практическому использованию результатов

Применение разработанных моделей, методов и устройств позволит разработать и создать принципиально новое оборудование для передачи конфиденциальных данных по оптическому волокну с возможностью обнаружения каналов утечки информации из оптического волокна.

В частности:

- разработанное устройство для обнаружения каналов утечки информации через макроизгибы может быть использовано в банковских системах передачи данных, военном деле, правительственной связи [8,10].

- предложена модель канала утечки информации при подключении несанкционированного пользователя к оптическому волокну, которая может быть использована при проектировании волоконных оптических линий связи для передачи конфиденциальной информации [7,9].

- созданный метод защиты информации, передаваемой по оптическому волокну, может найти применение в современных оптических линиях связи, со скоростями передачи данных до 10 Мбит/с, для защиты передаваемой информации и обнаружения канала утечки информации [6].

Результаты диссертационной работы нашли практическое применение в настоящее время, что подтверждается следующими актами внедрения: в образовательный процесс УО «Белорусская государственная академия связи» при разработке топовой программы по дисциплине «Квантовые системы для обеспечения информационной безопасности»; в учебный процесс факультета новых знаний и технологи Тегеранского университета (Иран); в ООО "Белкабельоптик" для определения наличия макроизгибов в оптических волокнах.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ УЧЕНОЙ СТЕПЕНИ

Статьи в рецензируемых научных журналах

1. Исследование пропускной способности асинхронного оптического канала связи с приемником на основе счетчика фотонов / И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев, А.Г. Косари // Приборы и методы измерений. – 2013.– № 2 (7). – С. 80–87.
2. Лавинные фотоприемники в режиме счета фотонов для систем конфиденциальной передачи информации / И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев, А.Г. Косари // Вестник связи. – 2014. – № 3 (125). – С. 46–49.
3. Использование одноквантовой регистрации для систем передачи конфиденциальной информации по волоконно-оптическим линиям связи / И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев, А.Г. Косари // Доклады БГУИР. – 2014. – № 7(85). – С. 38–43.
4. Обнаружение несанкционированных пользователей квантового канала связи / И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев, А.Г. Косари // Доклады БГУИР. – 2015. – № 1(87). – С.41–46.
5. Обнаружение несанкционированного доступа при передаче информации по оптическому волокну / О.К. Барановский, А.О. Зеневич, А.Г. Косари, Е.В. Василиу // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2015. – № 2 (51). – С. 212–216.

Статьи в сборниках материалов научных конференций

6. Математическая модель канала однофотонной связи / Е.В. Василиу, И.Р. Гулаков, А.О. Зеневич, А.М. Тимофеев, А.Г. Косари // Современные средства связи: материалы XVIII Междунар. науч.-техн. конф., Минск, 15–16 октября 2013 г. / Высш. гос. колледж связи; редкол.: А.О. Зеневич [и др.]. – Минск, 2013. – С. 13.
7. Многоканальная квантовая система связи для передачи конфиденциальной информации / А.О. Зеневич, А.М. Тимофеев, А.Г. Косари, А.А. Липай, Е.В. Мороз, В.С. Толкачева // Междунар. науч.-техн. конф., приуроченная к 50-летию МРТИ-БГУИР: материалы конф.: в 2 ч., Минск, 18–19 марта 2014 г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: А.А. Кураев [и др.]. – Минск, 2014. – Ч.1. – С. 426–427.
8. Влияние квантовой эффективности регистрации на пропускную способность каналов связи при создании макроизгиба оптического волокна / А.О. Зеневич, А.М. Тимофеев, А.Г. Косари, Е.И. Шулежко // Современные средства связи: материалы XIX Междунар. науч.-техн. конф., Минск, 14–15

октября 2014 г. / Высш. гос. колледж связи; редкол.: А.О. Зеневич [и др.]. – Минск, 2014. – С. 205–206.

9. Одноквантовая система передачи конфиденциальной информации по волоконно-оптической линии связи / А.О. Зеневич, А.М. Тимофеев, А.Ю. Зябликов, А.Г. Косари, А.А. Липай, В.С. Толкачева // Технические средства защиты информации: материалы XII Белорусско-российской науч.-техн. конф., Минск, 28–29 мая 2014 г. / Белорус. гос. ун-т информатики и радиоэлектроники; редкол.: Л.М. Лыньков [и др.]. – Минск, 2014. – С. 26.

10. Устройство обнаружения несанкционированного доступа при передаче информации по оптическому волокну / О.К. Барановский, А.О. Василиу, А.О. Зеневич, А.Г. Косари // Современные средства связи: материалы междунар. науч.-техн. конф., Минск, 2015 г. / Высш. гос. колледж связи; редкол.: А.О. Зеневич [и др.]. – Минск, 2015. – С. 138

РЭЗЮМЭ

Косары Араш Галамрэза

Вызначэнне каналаў уцечкі інфармацыі ў оптавалаконныя лініі сувязі на аснове маламагутных аптычных уздзеянняў

Ключавыя словы: аднаквантавая рэгістрацыя, лічыльнік фатонаў, лавінны фотапрыёмнік, макравыгін, хуткасць перадачы інфармацыі, мёртвы час, аптычнае валакно, уцечка інфармацыі.

Мэта работы: распрацаваць спосабаў і прылады для выяўлення каналаў уцечкі інфармацыі з аптычнага валакна, заснаванага на ўзаемадзеянні маламагутных аптычных сігналаў з неаднародным аптычнага валакна.

Метады даследавання: метады статыстычнага аналізу, метады хешыравання, метады рэалізацыі аднаквантавай рэгістрацыі на лавінных фотапрыёмніках, стартстопавы метад рэгістрацыі фатонаў.

Атрыманыя вынікі і іх навізна: прапанаваны метад вызначэння каналаў уцечкі інфармацыі з аптычнага валакна, сфарміраваных у ім па сродках мікравыгінаў, і абароны гэтай інфармацыі, заснаваны на выкарыстанні для перадачы даных маламагутных аптычных імпульсаў з даўжынёй хвалі 850 нм, а для трансляцыі сінхраімпульсаў і адначасовага выяўлення канала ўцечкі прымяняюцца магутныя аптычныя імпульсы з даўжынёй хвалі 1630 нм. Распрацавана ўстройства перадачы канфідэнцыяльнай інфармацыі па аптычным валакне з дапамогай маламагутных аптычных імпульсаў з магчымасцю выяўлення канала ўцечкі інфармацыі, месцазнаходжаннем падключэння несанкцыянаванага карыстальніка і фарміраваннем канала, які дэзынфармуе, што не дазваляе гэтаму карыстальніку ўстанавіць яго выяўленне.

Ступень выкарыстання: атрыманыя вынікі ўкаранёныя ў навучальны працэс, выкарыстоўваюцца ў навуковых і навукова-вытворчых арганізацыях Рэспублікі Беларусі.

Вобласць ужывання: оптыка, оптаэлектроніка, прыборабудаванне, сувязь, квантавая крыптаграфія.

РЕЗЮМЕ

Косари Араш Голамреза

Обнаружение каналов утечки информации в оптоволоконных линиях связи на основе маломощных оптических воздействий

Ключевые слова: одноквантовая регистрация, счетчик фотонов, лавинный фотоприемник, макроизгиб, скорость передачи информации, мертвое время, оптическое волокно, утечка информации.

Цель работы: разработать способы и устройство для обнаружения каналов утечки информации из оптического волокна, основанные на взаимодействии маломощных оптических сигналов с неоднородностями оптического волокна.

Методы исследования: методы статистического анализа, методы хеширования, методы реализации одноквантовой регистрации на лавинных фотоприемниках, стартстопный метод регистрации фотонов.

Полученные результаты и их новизна: предложен метод определения каналов утечки информации из оптического волокна, сформированных в нем посредством микроизгибов, и защиты этой информации, основанный на использовании для передачи данных маломощных оптических импульсов с длиной волны 850 нм, а для трансляции синхроимпульсов и одновременного обнаружения канала утечки применяются мощные оптические импульсы с длиной волны 1630 нм. Разработано устройство передачи конфиденциальной информации по оптическому волокну при помощи маломощных оптических импульсов с возможностью обнаружения канала утечки информации, местоположения подключения несанкционированного пользователя и формирования дезинформирующего канала, что не позволяет этому пользователю определить его обнаружение.

Степень использования: полученные результаты внедрены в учебный процесс, используются в научных и научно-производственных организациях Республики Беларусь.

Область применения: оптика, оптоэлектроника, приборостроение, связь, квантовая криптография.

SUMMARY

Kosari Arash Gholamreza

Detection of information leakage channels in optical fiber communication lines on the basis of low-power optical effects

Key words: one-quantum registration, quantum counter, avalanche photodetector, macro-bending, information transmission rate, dead time, optical fiber, data leakage.

Goal of research: to develop methods and devices for the detecting channels of data leakage from the optical fiber, based on the interaction of low-power optical signals with optical fiber inhomogeneities.

Methods of research: statistical methods, hashing methods, methods of one-quantum registration realization in avalanche photodetectors, start – stop method of photons registration.

Results obtained and their novelty: method of detecting channels of data leakage from optical fiber, shaped in it by means of microbends, and method of protection of this information based on usage of low-powered optical pulses with wave length 850 nm for data transmission, and for transmission of synchronization pulses and for simultaneous detection of data leakage channel powerful optical pulses with wave length 1630 nm are used. The device is developed for transmitting confidential information via optical fiber with the help of low-powered optical pulses with the possibility of detection of data leakage channels, location of unauthorized user connection and shaping misinformation channel, which does not allow this user to detect his discovery.

Extent of usage: the obtained results are included into teaching and learning process, are used in scientific and scientific and production organizations of the Republic of Belarus.

Field of application: optics, optoelectronics, tool engineering, communications, quantum theory-based cryptography.

Научное издание

КОСАРИ Араш Голамреза

ОБНАРУЖЕНИЕ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ В ОПТОВОЛОКОННЫХ ЛИНИЯХ СВЯЗИ НА ОСНОВЕ МАЛОМОЩНЫХ ОПТИЧЕСКИХ ВОЗДЕЙСТВИЙ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Подписано в печать . Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. . Уч.-изд. л. . Тираж экз. Заказ .

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя, распространителя печатных изданий №1/238 от 24.03.2014, №2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6