ФОТОНИКА В СИСТЕМАХ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

В.Гришачев, к.ф.-м.н.,
Академия АйТи, Российский Государственный Геологоразведочный Университет
grishachev@mail.ru,

В работе кратко представлены основные вопросы защиты от утечки информации объектов информатизации, использующих волоконно-оптические технологии. Дано описание возможных каналов утечки информации через волоконно-оптические коммуникации, технических средств разведки и способов защиты информации. Статья будет интересна широкому кругу разработчиков и пользователей технических средств защиты информации.

Роль информации в современном обществе повышается. Пришло время обратить особое внимание на защиту информации от угроз различного вида. Ведь развитие информационной техники создает все новые и неизвестные каналы утечки информации. Особую опасность несут технологии, которые используют ранее не известные физические принципы реализации процессов. В последних технологиях и технике проявляется некоторое внутреннее противоречие, связанное с неизученностью всех особенностей функционирования. С одной стороны, внедрение современных технологий создает иллюзию большей защищенности информации, что объясняется новизной используемых принципов, для которых еще не разработаны каналы утечки. С другой стороны, существует опасность появления каналов утечки еще не выявленных, функционирующих на физических принципах, не рассматриваемых ранее.

Подобная проблема возникает с применением фотонных технологий в обработке, передаче и хранении информации. Ведь они позволяют достичь значительных преимуществ по сравнению с другими технологиями. Решение проблемы возможно после проведения физико-технического анализа существующих каналов утечки информации в новых технологиях, разработке современных технических средств и систем защиты информации. Необходимо довести это знание до широкого круга специалистов в области обеспечения безопасности: руководителей служб безопасности, сотрудников технических отделов по защите информации, разработчиков технических средств защиты информации.

Поэтому в Академии АйТи [1] на кафедре информационной безопасности разработан публичный учебный курс под названием *"Обеспечение безопасности при использовании волоконно-оптических технологий связи"*. В первую очередь, создание курса продиктовано необходимостью решения задач, поставленных перед российскими предприятиями и организациями в связи с принятием Федерального закона №152 – ФЗ "О персональных данных". Материал строится на открытых источниках и нормативно-методических документах регулирующих органов. Он является отражением современного состояния проблемы. В курсе обсуждается широкое распространение волоконно-оптических технологий в системах передачи информации, измерения и обеспечения безопасности в различных областях деятельности и связанные с ними вопросы сохранения безопасности информации. Основное внимание уделено физико-техническим принципам реализации утечки информации на основе оптических кабельных коммуникаций; техническим каналам утечки информации через оптические структурированные кабельные системы, развернутые в пределах контролируемой зоны объекта информатизации, путем измерения параметров физических полей. Особое внимание уделяется анализу существующих предложений по применению организационных мер и технических средств защиты информации для обеспечения безопасности объектов информатизации.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ [2–6]

Фотоника – одно из основных направлений развития не только в информационной, но и в общей технике. В ней условно можно выделить лазерные,

оптоэлектронные, волоконно-оптические и интегрально-оптические технологии. В информатике находят широкое применение волоконно-оптические технологии связи. В настоящее время кабельные инфраструктуры в основном строятся на волоконно-оптических технологиях. Все новые телекоммуникации проектируются и реализуются на оптическом кабеле. Наиболее перспективным абонентским доступом (первая/последняя миля) является оптический доступ в виде пассивных оптических сетей (*Passive Optical Network, PON*), который позволяет связать оптоволокном без промежуточного активного оборудования центральный сетевой терминал с абонентом. Предполагается, что в будущем вся система связи, как локальная, так и дальняя, должна быть полностью оптической (*All-Optical Network, AON*). Доля оптической составляющей в современной связи определяется уровнем развития информационной составляющей на данной территории и непрерывно растет.

Подобная перспектива связана в первую очередь с преимуществами фотонного транспорта над электронным в кабельных сетях. Это меньшие энергетические потери, большая информационная емкость канала связи, долговечность, надежность, инертность к внешним полям и агрессивным средами. Немаловажным преимуществом является отлаженность технологий монтажа и эксплуатации оптических кабельных сетей. Технологичность строительства оптических сетей разного уровня связывается с широким ассортиментом монтажного, испытательного и эксплуатационного оборудования, которое позволяет проводить строительство подводных, подземных и воздушных телекоммуникаций. Общая протяженность оптических кабельных сетей превышает миллиард километров, пересекая континенты и океаны.

Кроме информационных коммуникаций волоконно-оптические технологии применяются в системах измерений. На оптоволокне можно построить широкий набор датчиков практически всех физических величин для механических воздействий, акустических, тепловых, радиационных, электромагнитных полей и т.д. Преимуществом оптоволокна как датчика является высокая чувствительность к внешним полям и воздействиям, распределенность измерений, возможность создания датчика нескольких величин на одном оптоволокне. На основе оптоволокна можно построить распределенные измерительные сети для контроля экологического состояния территорий и технологического состояния промышленных объектов. Например, оптоволокно, проложенное внутри дорожного покрытия автострад, способно контролировать состояние покрытия. Аналогичные задачи могут решаться в железнодорожном и трубопроводном транспорте. Одно из важных применений оптоволокна – использование его для решения задач безопасности. Преимущества оптического кабеля позволяют использовать его в системах видеонаблюдения, контроля доступа, охраны периметра, в системах пожарной сигнализации и других областях.

Переход от электронных технологий к фотонным, перевод значительной доли информационного транспорта на оптический кабель несет не только существенные преимущества, но и новые проблемы для информационной безопасности человека, общества и государства. Здесь необходимо оценить возможные угрозы. Современное правовое, нормативное и методическое обеспечение безопасности информации в волоконно-оптических коммуникациях явно недостаточно, оно охватывает только государственные и военные объекты, оставляя личность и предпринимательство без должного внимания.

Основные документы регулирующих органов в области защиты информации, к которым имеется открытый доступ, главным образом относятся к компьютерной безопасности, поэтому некоторые термины используются с расширенным толкованием. Хотя большая часть терминов, естественно, соответствует нормативным документам. К подобным понятиям относятся определения объекта информатизации, объекта защиты информации, выделенного помещения, контролируемой зоны, несанкционированного доступа (НСД) к информации, несанкционированного съема информации (НСИ), перехвата информации, технического канала утечки информации (ТКУИ), технических средств разведки (ТСР) и др.

В курсе вводится понятие перехвата трафика, к которому относится НСД к информации, передаваемой по оптическим сетям внутри контролируемой зоны с помощью штатных технических средств, и НСИ, передаваемой по оптическим сетям с помощью ТСР вне контролируемой зоны. Понятие ТКУИ относится только к информации, циркулирующей на объекте информатизации внутри контролируемой зоны, не являющейся трафиком сети. Вопросы НСД и НСИ (перехват трафика) относятся ко второму разделу, проблемы ТКУИ рассматриваются в третьем разделе курса. Надо отметить, что за рамками курса остаются вопросы, связанные с волоконно-оптическими ТСР, хотя проблема сбора специальной информации с помощью волоконно-оптических преобразователей остается в поле зрения автора курса.

Модели угрозы и нарушителя являются базовыми применительно к пониманию того, как осуществляется НСД к информации и как её защищать. В нормативных документах регулирующих органов это понятие чаще всего относится к компьютерной безопасности. Поэтому для понимания содержания угрозы информации используется понятие сценария угрозы. Сценарий угрозы – это последовательность

действий нарушителя (злоумышленника), направленных на получение доступа к конфиденциальной информации и их техническое обеспечение. Встают вопросы. Какого вида информация подвергается угрозе? Каким образом нарушитель получает доступ к конфиденциальной информации? Какие специальные технические средства могут использоваться? Определение сценария угрозы близко к понятию компьютерной атаки, переносить которое на наш случай автор считает не совсем корректно.

В нормативных документах используется понятие информативного сигнала. Это – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, передаваемая, хранимая или обрабатываемая в основных технических средствах и системах и обсуждаемая в защищаемом помещении.

Под объектом информатизации понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также помещения, предназначенные для ведения конфиденциальных переговоров. Следовательно, защищаемой информацией на объекте информатизации может выступать внутренний и внешний трафик. Другой защищаемой информацией является информация, циркулирующая на объекте. В соответствии с представленным делением в курсе выделены две главные темы по защите трафика и конфиденциальной информации объекта.

Необходимо отметить высокую защищенность волоконно-оптических коммуникаций от утечек. Это связано с практическим отсутствием значительных побочных электромагнитных излучений и наводок (ПЭМИН) в оптическом кабеле, который может быть полностью диэлектрическим. Еще одно преимущество состоит в малом поперечном сечении канала связи, благодаря чему практически вся световая энергия информационного сигнала сосредоточена внутри оптоволокна и выходит в виде света за его пределы только при внешнем воздействии. Есть и другие преимущества, изначально повышающие защищенность оптического кабеля от утечек информации по сравнению с проводным (медным) кабелем.

УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ [7–20]

Оптическая кабельная инфраструктура объекта информатизации может включать не только локальную сеть, но и сети телефонной связи, кабельного телевидения, систем видеонаблюдения, различных измерительных систем и другие кабельные системы. Передаваемый по оптическим кабелям трафик носит конфиденциальный характер и имеет важное значение для функционирования объекта независимо от вида сети. Трафик может подвергаться различным опасностям, таким как нарушение конфиденциальности, целостности и доступности. Угрозы реализуются различными способами, но одним из основных способов является перехват посредством НСД или НСИ. В схеме перехвата нарушитель обладает техническими возможностями на уровне современной техники и способен реализовать любой сценарий по получению доступа к конфиденциальной информации, не противоречащий законам физики.

Обобщенный сценарий утечки информации путем перехвата трафика можно рассмотреть на основе локальной сети, созданной по технологии PON. Первое действие, предпринимаемое нарушителем, состоит в определении топологии сети и ее типа. Следующий шаг – получение физического доступа к оптическому кабелю и подключение к каналу связи. В НСД для этого используются штатные возможности PON по разъемному соединению оптического кабеля, присоединения к активному оборудованию. При реализации НСИ нарушитель предпринимает попытку присоединиться с помощью разрыва оптоволокна или без разрыва канала связи путем отвода части светового информационного потока с помощью специальных технических средств. В схеме НСИ возможен дистанционный перехват информации. Последний этап перехвата – регистрация сигнала утечки.

Представленный общий сценарий угрозы снятия информации в каждом конкретном случае имеет свою реализацию на основе применяемых технических средств разведки. Как видно из сценария, при этом основными техническими элементами являются приспособления отвода светового потока и регистрации его параметров. Физические принципы осуществления перехвата могут строиться на нарушении полного внутреннего отражения при внешнем воздействии, например на макроизгибе оптического кабеля или волокна. Дистанционный способ перехвата связан с регистрацией индуцированных изменений параметров оптического волокна или возможных побочных неоптических излучений, вызванных штатными оптическими излучениями. Оборудование для перехвата трафика не является строго регламентируемым для продажи и применения. Нарушитель может использовать общедоступное стандартное оборудование, не выявленные или не декларированные возможности которого позволяют использовать его как техническое средство разведки. Если учесть, что многие возможности современного оборудования определяются программным обеспечением, то нелегитимное изменение драйвера отдельного блока позволит превратить обычное устройство в специальное.

Технические средства защиты информации (трафика) могут строиться на особенностях оптического канала связи – его малом поперечном сечении, в котором заключен световой поток. Первый эшелон защиты связан с техническими средствами контроля доступа к кабелю, к волокну, а также состоянием оптического канала связи. Другой способ защиты трафика – зашумление или искажение сигнала при его передаче в канале связи и очистка от шума или его восстановление при приеме из канала связи.

В волоконно-оптической линии связи для защиты трафика могут быть применены стандартные методы шифрования, которые применяются для любых других систем связи. В последнее время разрабатываются и предлагаются на рынок системы защиты передаваемой информации от перехвата на основе квантовой криптографии. Есть основания считать такие системы защиты абсолютными по самой природе реализации.

В инженерно-технической защите информации предлагается рассмотреть существующие системы защиты, предлагаемые на рынке. Основу большинства систем защиты составляют методы оптической рефлектометрии, например программно-аппаратный комплекс "Сапфир" (НЕЛК, Москва). Защита трафика является функцией более общих эксплуатационных систем контроля состояния оптических кабельных коммуникаций, таких как системы удаленного контроля оптоволокна (Remote Fiber Test System, RFTS) или системы управления оптическими сетями (Optical Network Management System, ONMS), предлагаемые различными фирмами. Существуют системы мониторинга волоконно-оптических линий связи (КБПМ, Москва), применяемые в российских государственных структурах, суть которого сводится к контролю прохождения тестовых сигналов.

УГРОЗА РЕАЛИЗАЦИИ ТЕХНИЧЕСКИХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ [21–25]

В соответствии с определением объекта информатизации, конфиденциальностью обладает не только внутренний и внешний трафик, но также и информация, циркулирующая внутри объекта в виде речи сотрудников, различных звуков работающего оборудования, физических параметров окружающего пространства и т.д. Волоконно-оптические коммуникации являются распределенной волоконно-оптической измерительной сетью с нештатными измерительными возможностями. Волоконно-оптические коммуникации, располагаясь внутри объекта информатизации, проходят через помещения, в которых может свободно циркулировать конфиденциальная информация. Нарушитель, используя ТСР через штатные световые потоки сети или внешние зондирующие излучения, может получить доступ к ней. Так же, как в предыдущем разделе, технические возможности нарушителя ограничены только современным состоянием ТСР. В отличие от угрозы трафику, такой канал утечки информации можно считать техническим, использующим не декларируемые или не известные, не контролируемые возможности оптической кабельной инфраструктуры.

Обобщенная схема ТКУИ на основе волоконно-оптических коммуникаций объекта информатизации повторяет схему НСИ и НСД к трафику, только для формирования сигнала утечки требуется выявить и учесть воздействие на оптоволокно физического поля, связанного с конфиденциальной информацией. Воздействие вызывает модуляцию светового потока в оптоволокне, которое переносит информацию за пределы контролируемой зоны. Преобразующие возможности оптоволокна определяют уровень опасности технического канала утечки информации. В угрозе конфиденциальности информации играет большую роль и топология сети. Прокладка оптического кабеля вблизи или через охраняемые помещения существенным образом влияет на защищенность от утечек.

Другие особенности связаны с возможностью использования для формирования сигнала утечки в дополнение к штатным излучениям еще и внешних нештатных источников, создающих зондирующие излучения. При этом трудности подключения к оптоволокну сохраняются, оптическая схема может быть усложнена, но повышаются возможности нарушителя путем варьирования параметров источника излучения.

Сценарии по реализации ТКУИ через волоконно-оптические коммуникации могут быть различны в зависимости от возможности модуляции света в оптоволокне и целей преследуемых нарушителем. Здесь играют большую роль специальные сценарии доступа к информации, обсуждение которых наиболее интересно для служб безопасности.

Технические средства разведки, используемые нарушителем для формирования технического канала утечки информации через волоконно-оптические коммуникации, делятся на источники излучения, технические средства подключения к оптическому каналу и системы регистрации излучения. Дополнительно необходимо оценить модуляционные возможности оптоволокна для различных физических полей. Многие экспериментальные и теоретические исследования доступны по открытым литературным источникам, в которых приводятся результаты эксплуатации, контроля надежности оптических сетей. Эти источники могут быть использованы в нашем случае угрозы конфиденциальности информации.

Особое внимание необходимо уделить стандартному волоконно-оптическому оборудованию, используемому при монтаже, наладке и эксплуатации оптической кабельной системы. Это оборудование

общедоступно и не требует специальных разрешений для использования, но его не декларируемые возможности позволяют применить данное оборудование в качестве технических средств разведки. Оно не вызывает подозрений у служб безопасности и может быть использовано без каких-либо согласований. Спектр оборудования с двойным назначением достаточно широк и включает практически весь парк приборов эксплуатационников оптических сетей.

Отдельным направлением разведки являются технические каналы утечки акустической (речевой) информации. Предотвращение подслушивания разговоров специалистов или конфиденциальных переговоров играет большую роль в обеспечении безопасности объектов, а выявление новых каналов всегда является важной задачей. Акустооптический (волоконный) канал утечки речевой информации относится к таковым. Он связан с возможностью модуляции в оптоволокне светового потока по одному из его параметров – акустическому полю, создаваемому речью человека. В этом случае оптический кабель и его волокна являются нештатным распределенным волоконно-оптическим преобразователем (микрофоном) акустических колебаний воздуха или вибраций конструкций зданий с высокой чувствительностью. Выбор параметров зондирующего сигнала, повышение акустического или виброакустического контакта с оптоволокном, топология и другие обычно не учитываемые характеристики кабельной инфраструктуры позволяют создать высокую угрозу подслушивания, в том числе конфиденциальных переговоров. Как показывают экспериментальные исследования, наибольшую опасность несут модуляции света на неоднородных участках оптического кабеля, связанные с виброакустическим воздействием, а также возможность применения в качестве TCP стандартного волоконно-оптического оборудования, например волоконно-оптического тестера-телефона с амплитудной модуляцией.

Методы защиты акустической информации от утечки по акустооптическому (волоконному) каналу делятся на пассивные (звукоизоляция оптического кабеля, "правильный" монтаж сети и т.д.) и активные (фильтрация, маскировка, зашумление информационного сигнала и т.д.). Можно выделить еще один способ, заключающийся во включении в каждый оптический трансивер функции непрерывного мониторинга световых потоков на возможность применения технических средств акустической разведки. Снизить опасность подслушивания можно, разрабатывая новые рекомендации по монтажу и эксплуатации оптических кабельных систем.

* * *

Автор выражает благодарность заведующему кафедрой информационной безопасности Академии АйТи к.в.н И.В. Семенихину за обсуждение проекта. Предлагается развивать эту работу и рассмотреть вопросы оптической рефлектометрии, волоконно-оптического тестового оборудования в применении к задачам защиты информации, обсудить угрозы связанные с применением волоконно-оптической измерительной техники для задач разведки и возможности противодействия им.

ЛИТЕРАТУРА

1. Академия АйТи. http://www.academy.it.ru/
2. ФСТЭК России. Сведения по вопросам технической защиты информации. [http://www.fstec.ru/_razd/_workinfo.htm]
3. Волоконно-оптическая техника: современное состояние и новые перспективы: Сб. статей под ред. Дмитриева С.А. и Слепова Н.Н. 3-е изд., перераб. и доп. – М.: Техносфера, 2010.
4. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников /Под ред. Э. Удда. Пер. с англ. – М.: Техносфера, 2008.
5. **Гришачев В.В.** Проблемы безопасности информационных систем высокой доступности на основе фотонных технологий. – Системы высокой доступности, 2006, т. 2, №3–4, с. 80.
6. **Денисов В.И., Гришачев В.В., Косенко О.А.** Волоконно-оптические технологии в системах безопасности и защиты информации. – Специальная техника, 2010, №4, с.47 .
7. **Свинцов А.Г.** ВОСП и защита информации. – Фотон-Экспресс, 2000, №18, с. 16.
8. **Свинцов А.Г.** Оптимизация параметров оптического рефлектометра для обнаружения неоднородности при попытке несанкционированного доступа в ВОСП. – Фотон-Экспресс, 2006, №6(54), с.56.
9. **Боос А.В., Шухардин О.Н.** Анализ проблем обеспечения безопасности информации, передаваемой по оптическим каналам связи, и путей их решения. – Информационное противодействие угрозам терроризма, 2005, №5, с. 162.
10. **Рахманов В.Н.** Мониторинг несанкционированного доступа к оптическому кабелю ВОЛС. – Вестник СГК, июнь 2006, с.17 [http://www.sgk-urep.ru]
11. **Алексеев А.В.** Мероприятия по защите информации в волоконно-оптических линиях связи. – Энергетик, 2008, № 5, с. 34.
12. **Булавкин И.А.** Вопросы информационной безопасности сетей PON. – Технологии и средства связи, 2006, № 2, с.104.
13. **Булавкин И.А.** Обнаружение макроизгибов в сетях PON без использования рефлектометра. – Вестник связи, 2008, №3, с. 54.
14. **Карпуков Л.М., Щекотихин О.В., Сметанин И.Н.** Методы защиты информации в ВОЛС. – Фотон-экспресс, 2009, №4(76) с.34.
15. Похитители света. Методы несанкционированного съема информации с волоконно-оптических систем. – Информаци-

онно-деловой ВЕСТНИК ОАО ЦНПО "КАСКАД", 2009, №7(54), №6(53). [http://www.kaskad.ru]
16. **Попова А.В., Тупота В.И.** Методика обоснования требований по защите информации, циркулирующей в волоконно-оптических системах передачи данных. – Телекоммуникации, 2009, №11, с.24.
17. **Глущенко А., Глущенко Л., Тупота В.** Оценка защищенности информации, циркулирующей в ВОЛП. – Фотоника, 2010, №4, с.36.
18. **Гришачев В.В., Кабашкин В.Н., Фролов А.Д.** Анализ каналов утечки информации в волоконно-оптических линиях связи: нарушение полного внутреннего отражения. – Информационное противодействие угрозам терроризма, 2005, №4, с. 194.
19. **Гришачев В.В., Кабашкин В.Н., Фролов А.Д.** Физические принципы формирования каналов утечки информации в волоконно-оптических линиях связи. – Информационное противодействие угрозам терроризма, 2004, №3, с. 74.
20. **Листвин А.В., Листвин В.Н.** Рефлектометрия оптических волокон. – М.: ЛЕСАРТарт, 2005.
21. **Гришачев В.В.** Выявление угроз утечки речевой информации через волоконно-оптические коммуникации. – Фотоника, 2011, №4, с.32.
22. **Гришачев В.В., Косенко О.А.** Практическая оценка эффективности канала утечки акустической (речевой) информации через волоконно-оптические коммуникации. – Вопросы защиты информации, 2010, №2, с.18.
23. **Гришачев В.В., Халяпин Д.Б., Шевченко Н.А.** Волоконно-оптический телефон в акусто-оптоволоконном канале утечки конфиденциальной речевой информации. – Вопросы защиты информации, 2009, №3, с. 22.
24. **Гришачев В.В., Халяпин Д.Б., Шевченко Н.А.** Внешнее оптическое зашумление волоконно-оптического канала СКС для предотвращения подслушивания по акусто-оптоволоконному каналу утечки речевой информации. – Специальная техника, 2009, №3, с. 2.
25. **Гришачев В.В., Халяпин Д.Б., Шевченко Н.А., Мерзликин В.Г.** Новые каналы утечки конфиденциальной речевой информации через волоконно-оптические подсистемы СКС. – Специальная техника, 2009, №2, с. 2.

Указатель статей, опубликованных в 2011 году в журнале "Фотоника"

№	Автор	Статья	Стр.
		Компетентное мнение	
2	С.М. Кобцев	Идеальная лазерная технология – есть ли она?	4
3	С.Тихонов	Изобретения в вакууме: гибкость и прозрачность	6
5	А.Рогачев	Фотоника – локомотив инноваций в современном мире	4
		Оптические устройства и системы	
1	В.Привалов, В.Шеманин	Зондирование молекул йода самолетным флуоресцентным лидаром	12
1	В.Комоцкий, В.Корольков, Ю.Соколов	Оптоэлектронные дифракционные датчики малых угловых перемещений	16
2	Е.Кудрявцев, И.Мацак, М.Макаренко	Оптический растровый датчик скорости	54
2	И.Болдов, А.Кучьянов, А.Плеханов, Н.Орлова, И.Каргаполова, В.Шелковников	Оптические химические сенсоры и датчик на бутиламин	56
3	В.Григорьев	Особенности применения оптических волокон в преобразователях давления	62
3	И.Байнева, В.Байнев	Оценка эффективности и надежности светодиодных источников света и приборов	66
		Лазеры и лазерные системы	
2	В.Кисель, А.Гулевич, Н.Кондратюк	Иттербиевые твердотельные лазерные системы	20
2	С.Мюллер	Лазеры с модуляцией добротности для обработки поверхностей	26
2	С.Шутов, Ю.Константинов	Сварочный лазер ЛИС-25	30
		Оптоэлектронные приборы	
1	Г.Лубегин, Д.Онищенко, В.Гуслянников	Инжекционные фотодиоды на основе монокристаллов $A^{II}B^{VI}$	34
2	А.Дирочка, А.Филачев	Международная конференция по фотоэлектронике и приборам ночного видения. Ч. 2	64
		Технологическое оборудование и технологии	
1	И.Савельев	Наноразмерная обработка	20
2	Л.Раткин	Полувековой юбилей лазерной техники: стратегия развития отрасли	12
2	Н.Истомина	Проекту "Выставка "Фотоника. Мир лазеров и оптики" шесть лет	18
3	М.Рютеринг	Сравнительный анализ лазерной техники	26
3	В.Бирюков	Лазерное упрочнение и легирование сталей	34
3	С.Полушкин	Эффективное управление комплексом лазерной гравировки	38
3	А.Керемжанов	Термосенсорика производства и ремонта металлических труб	44
3	Ю.Суздальцев	Лазерная и плазменная резка металлов	48
4	Р.Шаймарданов	Лазер CO_2: гибкое, надежное и испытанное средство	8