

Космодром
Восточный.
Старт в будущее

Новости

Технологии
информационных
войн. Вызов пост-
индустриальной
эпохи

Антитеррор

«Союз-СТ» будет
стартовать из
Гвианы

Новости

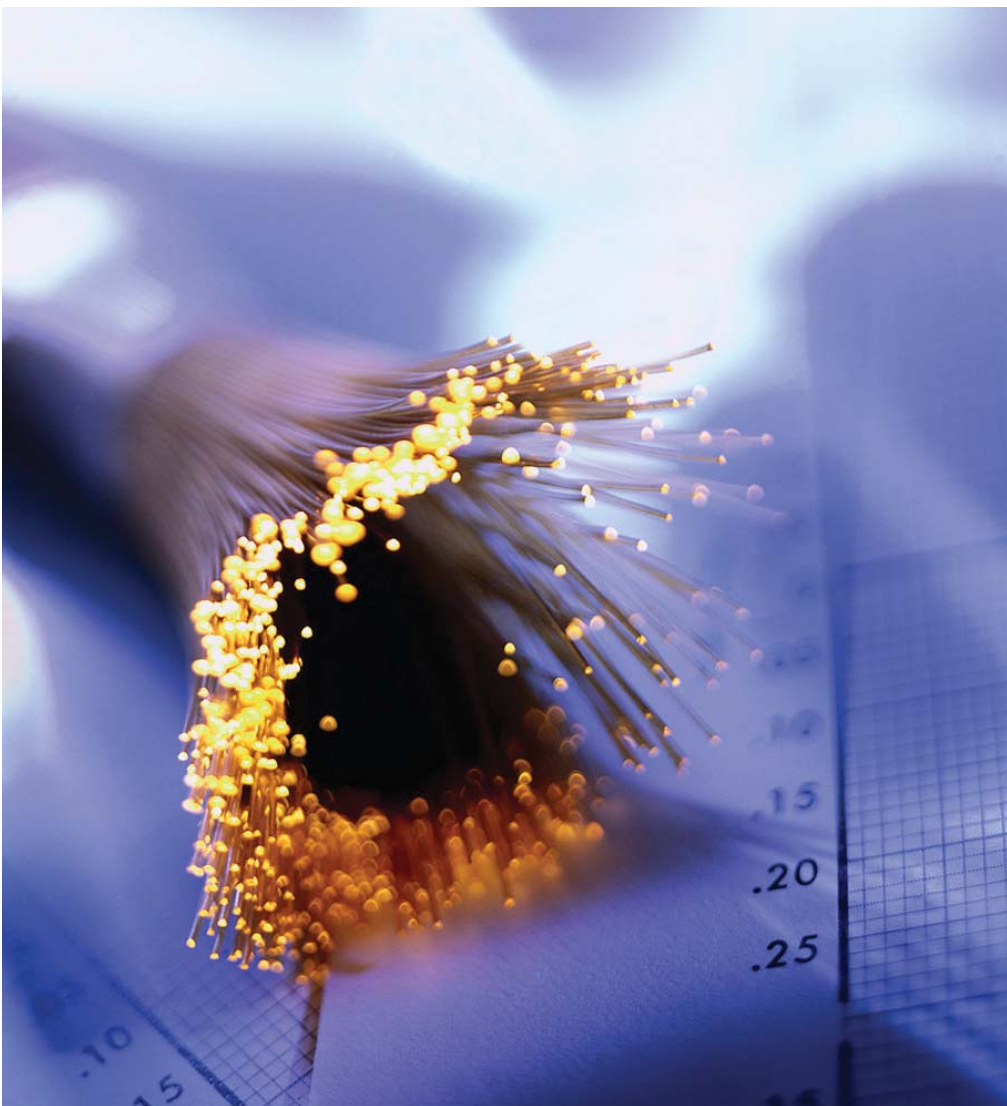
ВОЛС —
толщиной с волос

Технологии

ТЕХНОЛОГИИ

ВОЛС — толщиной с волос

История развития волоконно-оптических технологий началась в конце 60-х годов прошлого века, когда появились опытные волноводные линии для передачи широкополосной информации. К началу 80-х годов были разработаны и испытаны волоконно-оптические системы связи. Основные сферы применения таких систем — телефонная сеть, кабельное телевидение, вычислительная техника, системы контроля и управления технологическими процессами



В основу построения волоконно-оптических линий связи (ВОЛС) положен принцип передачи по волокну световых волн на большие расстояния. При этом электрические сигналы (видеосигналы от видеокамер, сигналы управления видеокамерами и данные) поступают на вход оптического передатчика и далее преобразуются в световые импульсы, которые с минимальными искажениями передаются по оптоволокну.

Большое распространение волоконно-оптические системы получили благодаря целому ряду достоинств, которые отсутствуют при передаче сигналов по медным кабелям (коаксиальным и витой паре) или по радио:

- широкой полосе пропускания,
- малому затуханию сигналов,
- отсутствию электромагнитных помех,
- дальности передачи на десятки километров,
- длительному сроку службы (более 25 лет).

Современное оптоволокну представляет собой прозрачные стеклянные волокна, которые проводят свет от одного конца до другого с минимальными потерями, благодаря эффекту полного внутреннего отражения. Конструктивно такое оптоволокну состоит из ядра, оптической оболочки и защитной пленки. Ядро и оптическая оболочка обычно выполнены из стекла, реже из пластика, защита, как

правило, из пластика. Ядро оптоволокну пропускает световой сигнал, а оптическая оболочка обеспечивает полное внутреннее отражение света в ядре и его прохождение по всей длине. Толщина оптоволокну сопоставима с толщиной человеческого волоса (125 мкм — толщина оптоволокну, 85 мкм — волоса). Обладая низкими потерями, оптоволоконная линия связи способна транслировать видеосигналы на расстояния до десятков километров без использования промежуточных усилителей. Как правило, частота передачи видеосигнала через оптоволоконные системы составляет более 10 млрд бит/с. В ряде случаев это может значительно превышать потребности в

скорости и объеме передаваемой информации, необходимой для решения конкретных задач, например для видеонаблюдения. Поэтому оптоволоконные системы чаще всего используются на особо ответственных объектах либо для передачи больших объемов информации, в том числе и видеосигналов (телевидение, телефония и пр.). В настоящее время промышленность выпускает два типа оптоволокну: одномодовое (от англ. mode — здесь «режим») оптоволокну 9/125 нм с одной траекторией распространения видеосигнала по ядру оптоволокну и многомодовое оптоволокну 50/125 нм и 62,5/125 нм с несколькими траекториями распространения световых волн. При этом многомодовое оптоволокну обеспечивает передачу сигналов на расстояние 1–5 км, а одномодовое — на десятки километров. Это объясняется меньшими потерями при прохождении сигнала. Одномодовое волокно имеет очень тонкую сердцевину (диаметром 10 мк или менее). Из-за малого диаметра световой пучок отражается от поверхности сердцевины реже, а это ведет к меньшей дисперсии. Именно поэтому такие оптические волокна имеют наилучшие характеристики и наиболее активно используются при строительстве ВОЛС. В то же время одномодовое волокно стоит намного дороже. Системы видеонаблюдения используют чаще всего многомодовое оптоволокну, поскольку в них необходимо осуществлять не только передачу видеосигнала, но и аудиосигнала, и сигналов управления.

Состав оборудования оптоволоконной системы

Как правило, оптоволоконная система включает: передатчик видеосигнала, преобразующий электрические видеосигналы в оптическое излучение, приемник видеосигнала, преобразующий оптическое излучение обратно, и собственно оптическое волокно, соединяющее передатчик и приемник. Основной особенностью оптоволоконных систем является их высокая

продолжение на стр. 4

ПОЗДРАВЛЯЕМ!

**День
защитника
Отечества!**

День защитника Отечества — праздник, олицетворяющий силу и воинскую славу российских Вооруженных Сил. Это поистине всенародный праздник, над которым не властно время, который останется с нами навсегда. В этот день мы поздравляем всех, кто верой и правдой служил и продолжает служить на благо Родины, для кого сохранение мира и благополучия наших сограждан стало судьбой.

Для Объединения на протяжении многих десятилетий работа плечом к плечу с Вооруженными Силами нашей Родины также стала судьбой, неотделимой от судьбы страны. Сердечно поздравляем всех военнослужащих, ветеранов, гражданский персонал армии и флота с Днем защитника Отечества! Пусть наша армия всегда будет великой и могучей, пользуется всеобщим уважением и доверием народа, высоким авторитетом в мире!

НОВОСТИ

Космодром
Восточный.
Старт в
будущее

Состоялось расширенное заседание коллегии Федерального космического агентства, на котором обсуждался вопрос «О порядке развертывания и проведения работ на космодроме Восточный»



Определяющим в системе намеченных действий является создание нового космодрома научного и социально-экономического назначения. К настоящему времени осуществлены следующие мероприятия.

Совместная рабочая группа представителей Роскосмоса, организаций ракетно-космической промышленности и Амурской области 11–14 февраля 2008 год провела рекогносцировку возможного района расположения космодрома с уточнением перечня объектов, которые целесообразно использовать из состава расформированного космодрома Свободный для создания и функционирования космодрома научного и социально-экономического назначения Восточный; Роскосмосом с привлечением ряда организаций подготовлен план первоочередных мероприятий по космодрому Восточный, учитывающий сроки создания космодрома и осуществления первых пусков с него. Разработано техническое задание на системный проект, который будет подготовлен ФГУП «ЦНИИмаш» с привлечением ведущих коллективов ракетно-космической промышленности и рассмотрен в июне-июле с. г. на заседании научно-технического совета Роскосмоса.

В обеспечение скоординированной работы структур Роскосмоса и организаций ракетно-космической промышленности сформированы рабочие группы, задачи которых определены соответствующими приказами.

Роскосмос, понимая сложность и масштабность предстоящих задач, стремится к максимальной открытости и рассчитывает на консолидированные действия министерств и ведомств, а также, и в первую очередь, на тесное сотрудничество с Амурской областью.

(По данным пресс-службы Роскосмоса)

АНТИТЕРРОР

Технологии информационных войн.
Вызов постиндустриальной эпохи

Технологическая революция привела к появлению термина «информационная эра» из-за того, что информационные системы стали частью нашей жизни и изменили ее коренным образом. Современное общество перенасыщено информацией различного рода. Новая эра также изменила способ ведения боевых действий, обеспечив командиров беспрецедентным количеством и качеством информации



Войны новой эры

Информация играет в любой войне важнейшую роль. Это разведка, коммуникация, контрразведка, пропаганда — все то, без чего невозможны эффективные действия. Предположим, что стоит задача ограничить стратегические возможности врага путем уменьшения запасов топлива. Сначала необходимо выявить нефтеперегонные заводы, которые будут наиболее подходящими целями. Потом нужно установить, какие заводы производят больше всего топлива. Для каждого завода надо выявить местоположение перегонных емкостей. Организующая в последствии атака, при значительной экономии сил, выводит заводы из строя, уничтожая только их перегонные емкости и оставляя все остальное оборудование нетронутым. Это классический пример стратегической атаки. Теперь посмотрим, как добиться той же цели в информационной войне. Все современные нефтеперегонные заводы имеют большие автоматизированные системы управления. Эти информационные функции и являются потенциальной целью. На ранней стадии конфликта проходит разведывательная информационная операция по анализу системы управления нефтеперегонным заводом и проникновению в нее. В ходе анализа устанавливается ряд уязвимых информационных зависимостей, дающих средства воздействия на работу нефтеперегонного завода в нужное время. Позднее, в ходе конфликта, используются именно эти уязвимые места. Заводы просто останавливаются. Это тоже классический пример стратегической атаки.

Следует, однако, разделить понятия «война информационной эры» и собственно «информационная война». Первая использует информационные технологии как средство для успешного проведения боевых операций. Вторая рассматривает информацию как отдельный объект или потенциальное оружие и как выгодоносную цель. Что же такое информация? Как известно, ин-

формация появляется на основе отражения событий окружающего мира. События эти должны быть не просто восприняты как-то образом, но и правильно интерпретированы, чтобы стать информацией. Таким образом, информация — результат двух вещей: воспринятых событий (данных) и команд, требуемых для интерпретации данных и связывания с ними значений. Чем быстрее происходит отражение и интерпретация, тем большее преимущество имеет та или иная сторона. А скорость обработки информации — это уже технологии. И побеждает в этой войне тот, чьи технологии, связанные с получением, передачей, хранением и трансформацией информации, более успешны и более совершенны. Совокупность всех этих действий носит название «информационная функция». Таким образом, для того чтобы парализовать деятельность противника, достаточно поразить его информационные функции, то есть заставить либо видеть (слышать) не то, что есть на самом деле, либо неправильно интерпретировать увиденное (услышанное). Все это справедливо как для «войны информационной эры», так и для «информационной войны». В последней сама информация стала оружием. Не менее мощным и смертоносным, чем любое оружие массового поражения, потому что объектом воздействия в этой войне становится мозг человека, его интеллект. И несколько затертая от частого повторения формула «кто владеет информацией — владеет миром» в последнее время приобрела новый смысл.

Искусственно вызванный дефицит информации открывает неограниченные возможности для манипуляций как индивидуальным, так и коллективным сознанием, что, в свою очередь, открывает путь к капиталу и власти. Полковник ВВС США Р. Шафрански в статье «Теория информационного оружия» (перевод опубликован в российском Интернете) приводит следующее мнение: «Целью войны стало не уничтожение, а управление...

<...> Информационная технология в наше время делает возможным «управление» при минимальном насилии и кровопролитии.

Семь правил управления

Информационные войны ведутся постоянно. Их элементы более или менее осознанно используются практически в любом бизнесе, в общественной деятельности, даже частная жизнь от них не

застрахована. Информационные войны ведут государства, политики, корпорации. Интерес к информационному противоборству породил немало публикаций на эту тему, однако все они, за редким исключением, не касаются механизмов и систем управления информационным противоборством, методов и технологий его ведения.

С.Н. Бухарин и В.В. Цыганов в книге «Методы и технологии ин-

формационных войн» выделяют семь основных правил, которыми руководствуются стороны при управлении факторами разной природы в ходе информационных войн.

1. Нарращивание контролируемых факторов, контроль над ресурсами соперника, ослабление и ограничение контролируемых им факторов. Пополнение собственных интеллектуальных ресурсов и нанесение ущерба

Скрытые угрозы и атаки

Угрозы	Атаки
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование защищаемой информации на отчуждаемый носитель (например, на флеш-карту) и его вынос за пределы контролируемой зоны
Хищение и/или подлог информации на жестких дисках АРМ без изменения эталонного состояния аппаратной среды	Несанкционированная загрузка операционной системы со съемного носителя, логическое монтирование жестких дисков с защищаемой информацией, копированием ее на несанкционированный носитель. Подлог информации
Хищение и/или подлог информации на жестких дисках АРМ с нарушением эталонного состояния аппаратной среды	Физическое извлечение жесткого диска с атакуемого компьютера, физическое и логическое монтирование этого диска на другом компьютере. Съем и/или подлог защищаемой информации
Маскировка под зарегистрированного пользователя	Добытие пароля зарегистрированного пользователя (подбором, перебором, перехватом или наблюдением), вход в систему под его именем и выполнение любых несанкционированных действий, включая хищение информации
Хищение и/или подлог информации в процессе передачи	При передаче по каналу связи: несанкционированное подключение к каналобразующей аппаратуре, перехват и/или подлог передаваемых данных. При передаче на съемном носителе: несанкционированное копирование защищаемой информации со съемного носителя, подлог информации на съемном носителе

АНТИТЕРРОР

Начало на стр. 2

интеллектуальным ресурсам соперника.

2. Превращение детерминированных факторов для соперника в случайные и неопределенные.

3. Обеспечение доступа к информации о случайных факторах, исключив доступ к ней соперника. Дезинформирование соперника относительно законов и параметров их распределения.

4. Ориентирование разработчиков стратегии соперника на значения природных факторов, наносящие ему максимальный ущерб.

5. Не жалеть ни сил, ни средств для того, чтобы соперник не понимал своих целей. Пользуясь непониманием соперника своих целей, направлять его в нужном направлении.

6. Агрессор начинает конфликт с низкой степени эскалации. В случае оказания соперником сопротивления, надо дойти до высокой степени эскалации, при которой соперник быстро израсходует свои ресурсы. При такой стратегии агрессор должен иметь превосходство в ресурсах, а соперник — не иметь источников их пополнения.

7. Потенциальная жертва агрессии должна делать все, чтобы

повысить неопределенность при принятии решения инициатором конфликта, скрывать информацию, необходимую агрессору для оценки его ущерба. Она демонстрирует решимость немедленно перейти на высокие стадии конфликта, что приведет агрессора к неприемлемым потерям. Она должна вводить агрессора в заблуждение относительно своих ресурсов, средств отражения и источников их пополнения.

Отметим, что большинство из этих правил с успехом применялись и применяются пропагандой в войнах «традиционных» — сокрытие собственных потерь, преувеличение потерь противника, приписывание случайному успеху свойств закономерности и т. д.

Информационный щит

Оборонительной стороной информационной войны являются меры безопасности, имеющие своей целью защитить информацию — не позволить противнику провести успешную информационную атаку на наши информационные функции. Современные меры защиты, такие как компьютерная безопасность, включают в себя дей-

ствия по предотвращению, обнаружению прямых информационных действий противника и организации контрдействий. Сегодня защита информации в автоматизированных системах (АС) конфиденциального производства на базе ПЭВМ, как правило, основана на шифровании и применении электронных идентификаторов. Основным направлением нейтрализации указанных в таблице скрытых угроз является разработка и внедрение программно-аппаратных средств защиты информации.

Однако основной причиной утечек конфиденциальной информации является человеческий фактор. Причин у этого множество. И лежат они в сфере, скорее, этико-философской, чем чисто технологической. Это может быть недостаточное внимание, уделяемое исследованию мотивов, толкающих сотрудников на нарушение корпоративных соглашений и правонарушений. Это могут быть не должным образом разрабатываемые и осуществляемые программы управления секретносителями. Практически не исследована проблема воздействия охраняемой информации на санкционированных пользователей автоматизированных систем и др. Так что вполне разумно может считаться постановка вопроса: «При каких условиях программно-аппаратные комплексы защиты конфиденциальной информации оправдывают средства на их закупку и/или разработку, а при каких, соответственно, — нет?» Действительно, бессмысленно навешивать хитроумные замки, устанавливать коды и ловушки, когда у потенциального предателя на совершенно законных основаниях имеется ключ и коды. В современном мире информацию охранять чрезвычайно трудно, если иметь в виду под понятием «охраны» исключительно лишь обеспечение ограниченного доступа. Технологии копирования, звукозаписи, фотографирования, передачи информации настолько совершенны, по сравнению даже с серединой прошлого века, что восприятие охранной системы как большого крепкого сейфа с электронным замком несколько устарело. Безусловно, обеспечение сохранности информации не может обойтись без ограничения доступа, систем контроля и т. д. Но сегодня все чаще можно увидеть в действии

методы не столько собственно охраны, сколько маскировки информации. Как выдать значимое за незначительное? Как скрыть существенное за миллионом ненужных деталей? Пока противник будет вести анализ этой ненужной, мусорной информации, которая ничего не даст для него, пока он будет отвлекать на это ценный интеллектуальный ресурс, другая сторона уже совершит прорыв, который лишит ценности даже расшифрованные, вытасканные из-под груды информационного мусора сведения. Современные войны делятся уже не годы, а порой минуты. Получается, что, с одной стороны, окружающий мир буквально трещит от распирающей его информации, а с другой — ощущается ее острейший дефицит. При внимательном рассмотрении проблемы она не кажется парадоксом. В огромном информационном потоке чрезвычайно трудно выловить действительно ценную, значимую информацию.

Линия обороны

Немаловажным является вопрос «Какую именно информацию следует охранять?» Максималистский ответ «Всю!», во-первых, ставит перед исполнителем заведомо невыполнимую задачу, а во-вторых — ставит невыполнимую задачу, отвлекающую большое количество ресурсов, которые всегда ограничены и, возможно, требуются в другом месте. То есть такой ответ уже сам по себе является средством управления в пользу противника, а значит — средством ведения информационной войны. На рис. 1 показана зависимость объема информации L от ее ценности Q для противника (конкурента). Прирост коэффициента полезности информации для конкурента на участке от 0 до q_1 незначителен, поскольку по ней практически невозможно восстановить необходимые сведения в полном объеме. На участке от q_2 до Q рост полезности информации также невелик, поскольку резко возрастает вероятность восстановления нужных сведений по уже приобретенной информации. Система доступа к конфиденциальной информации имеет иерархическую структуру. Оператор, стоящий на нижнем уровне иерархии доступа к конфиденциальной информации, контролирует определенный ее фрагмент. Руководители подразделений контролируют информацию своих подчиненных и т. д. Наконец

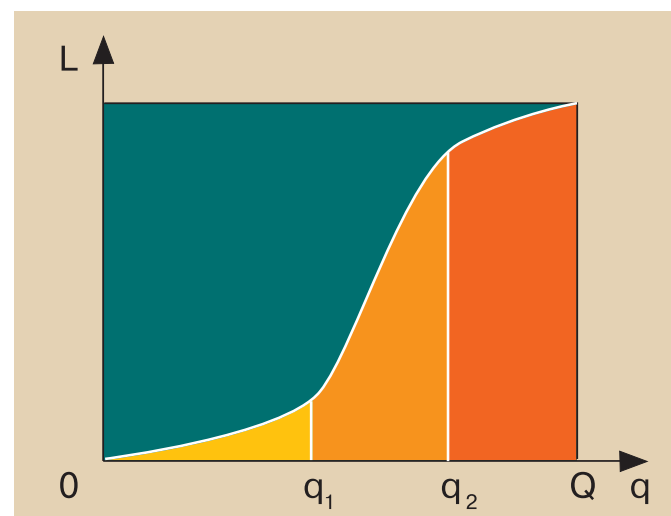
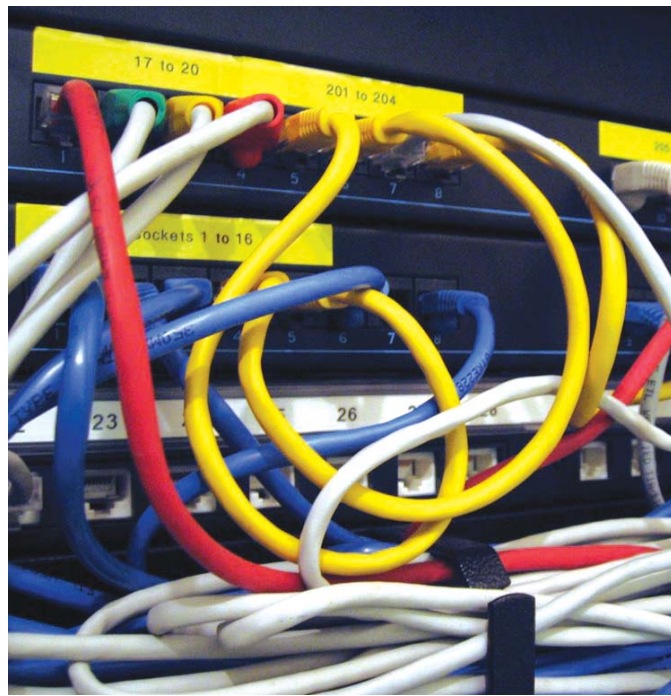


Рис. 1. Типовая зависимость коэффициента полезности информации $k(q_i)$ от ее объема q_i

находится то «слабое звено», на которое и производится атака. Для того чтобы это звено установить, необходимо соотнести уровень ценности для конкурента информации, которой владеет оператор с его возможностями эту информацию продать и его мотивировками. Образуется стойкая «очаговая» оборона именно тех ключевых информационных точек, которые нуждаются в этом. Ясно, что эффективно контролировать 5 человек реальнее, чем 100. Эффект при этом если и не одинаков, то возможные потери при реализации данного сценария существенно меньше потерь, связанных с отвлечением ресурсов при организации «сплошной» линии обороны.

Вопросы информационной безопасности корпорации всегда были в центре внимания «Вестника ОАО ЦНПО «Каскад». Сегодня актуальным становится уже не просто вопрос корпоративной безопасности, но речь идет об информационной безопасности государства. И.Н. Панарин, политолог, профессор Дипломатической академии МИД РФ, кандидат психологических наук, доктор политических наук, академик Академии военных наук, в книге «Технология информационной войны» так определил важность этого вопроса: «У России, как самой образованной страны в мире, есть шанс для процветания. Необходимо только серьезно подойти к проблеме информационной безопасности».



НОВОСТИ

«Союз-СТ» будет стартовать из Гвианы



«В настоящий момент во Французской Гвиане нет более масштабных строек, чем создание российского стартового комплекса на космодроме Куру. О размахе строительства говорит хотя бы такой факт, что два карьера, в которых добывается песок, получили русские женские имена «Ольга» и «Натasha» — об этом сообщил руководитель проекта запусков российских «Союзов-СТ» со стороны французского космического агентства КНЕС Жан-Марк Асторг. По его словам, российская часть территории в Гвианском космическом центре занимает площадь 120 гектаров. В настоящее время на месте будущей стартовой площадки вырыт огромный котлован глубиной около 30 метров и площадью 150 на 150 метров. Строительство идет пол-

ным ходом. Установлено два высотных крана. Из 320 человек, работающих на площадке, 280 занято на бетонных работах. Космодром Куру, или Гвианский космический центр (Centre Spatial Guyanais), расположен во Французской Гвиане (Южная Америка) в 50 километрах от города Кайенна, между городками Куру и Саннмари, на побережье Атлантического океана, на полосу длиной 60 и шириной 20 километров. Гвианский космический центр предназначен в основном для вывода на орбиты геостационарных спутников. Строительство своего экваториального космодрома Франция начала в 1965 году по инициативе Национального центра космических исследований (КНЕС). В настоящее время основные пусковые площадки космодрома

являются собственностью Европейского космического агентства (ЕКА). Первый запуск с Куру был осуществлен 9 апреля 1968 года. Проект строительства стартовой площадки для запуска модернизированных ракет-носителей «Союз-СТ» во Французской Гвиане — одно из приоритетных направлений сотрудничества Роскосмоса и ЕКА. Приглашение об участии России в запусках «Союзов» с космодрома Куру было подписано 19 ноября 2002 года. В декабре 2002 года российские специалисты российской-французского совместного предприятия «Старсем» приступили к выбору места для сооружения стартовой позиции для запусков модернизированной российской ракеты-носителя «Союз-СТ».

Пусковая площадка для коммерческих запусков российских «Союзов» на французском космодроме обойдется в 344 миллиона евро, все средства на постройку стартового комплекса выделяются европейской стороной. Благодаря расположению Гвианского космического центра в экваториальной области Земли, модернизированная российская ракета «Союз-СТ» сможет выводить на орбиты более тяжелые спутники, чем при запусках с российских космодромов Байконур и Плесецк. Кроме того, реализация проекта позволит России существенно расширить область коммерческого использования семейства ракет-носителей «Союз» на мировом рынке пусковых услуг.

(По данным РИА «Новости»)

ТЕХНОЛОГИИ

ВОЛС — ТОЛЩИНОЙ С ВОЛОС

Начало на стр. 1

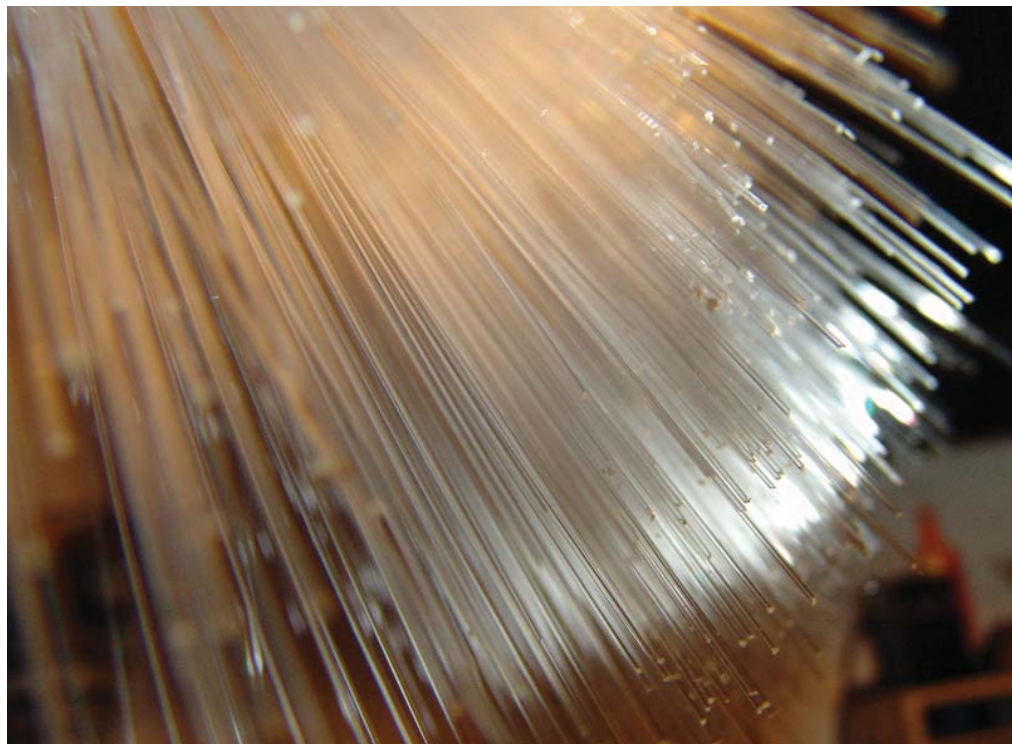
пропускная способность, которая обусловлена высокой частотой колебаний световых волн, распространяющихся по оптоволокну. Скорость передачи видеосигналов через оптоволоконные системы ограничивается только пропускной способностью передающего и приемного модуля системы.

Все оптоволоконные системы имеют примерно одинаковую структуру. На передающем конце оптоволоконной линии находится светодиод или лазерный диод, излучение которого модулируется по амплитуде передаваемым сигналом, поступающим от источника информации. В качестве передаваемого сигнала может выступать видеосигнал от телекамеры, сигнал управления поворотным устройством телекамеры, аудиосигнал и другие сигналы, подлежащие передаче. Прежде чем направить такой сигнал на излучающий светодиод, он предварительно модулируется в амплитудном, частотном или импульсном модуляторе. Использование в оптоволоконной системе такого модулятора в передатчике в паре с демодулятором приемника позволяет одновременно передавать по оптоволокну несколько сигналов различного типа.

При передаче световое излучение лазерного диода модулируется по яркости в такт с передаваемым сигналом модулятора. Оптическое излучение передается по оптоволоконной линии на приемный модуль, где установлен фотодиод, преобразующий модулированный по яркости свет в электрические колебания. После детектирования модулированного оптического видеосигнала он поступает на демодулятор, который разделяет принятый комбинированный сигнал на сигналы отдельных передаваемых каналов. Вид модуляции оптического сигнала и количество одновременно передаваемых по оптоволоконной линии сигналов выбирается исходя из решения конкретных технических задач.

Защищенность от помех и несанкционированного доступа

Одним из преимуществ, отличающих оптоволоконные системы, является абсолютная защищенность оптоволоконной линии от электрических помех, наводок и полное отсутствие излучения во вне. Это объясняется тем, что в оптическом канале связи для передачи информации используется световой сигнал, никак не взаимодействующий с электромагнитными полями, а само оптоволоконно является диэлектриком и по своей природе не может никак с ними взаимодействовать. Несмотря на чрезвычайно малый диаметр, оптическое волокно может выпускаться в прочной внешней оболочке, выдерживающей большие механические нагрузки, а также гарантирующей длительную работу в сырых помещениях и агрессивных средах. Некоторые типы оптических кабелей допускают их прокладку непосредственно в земле, что резко удешевляет и ускоряет монтажные работы. Все оптоволоконные системы отлича-



ются повышенным уровнем безопасности, так как передаваемый сигнал не излучается за пределы оптического волокна и к нему невозможно подключиться для несанкционированного перехвата. Однако разговор об оптоволокну был бы не полным, если ограничиваться только лишь сферой передачи информации.

Как приручить свет

Уже несколько десятилетий назад в повседневной жизни стали активно применяться оптоволоконные системы освещения. Однако, несмотря на этот опыт, волоконно-оптические технологии для многих все-таки остаются экзотикой. Между тем применение оптоволоконка позволяет легко и эффективно решать сотни технических проблем, возникающих при разработке световых проектов: провести свет сквозь стены, землю, воду, огнибывающую и обходя препятствия, и извлечь его именно там, где это нужно. Основной компонент системы — это оптоволоконный проектор. Существует множество моделей таких проекторов мощностью от 35 Вт с различной степенью защиты от воздействия окружающей среды. Благодаря фильтру, установленному в проекторе, свет выходящий из кабеля не имеет ни УФ-, ни ИК-излучения, что в ряде случаев немаловажно. Оптоволоконные кабели не проводят ни электричества, ни тепла. Диапазон рабочих температур пластикового оптоволоконка от -40 до +80 °С. Пластиковое волокно не боится воды, гибкое, легко устанавливается на любую поверхность. Стекланные оптоволоконные кабели выдерживают температуру до +130 °С, они идеально подходят для безопасного освещения бань и саун. Пожаробезопасность, герметичность, отсутствие выделяемого тепла, низ-

кие эксплуатационные расходы, большая механическая прочность, удобство размещения в труднодоступных местах делает оптоволоконное освещение незаменимым, а порой единственно возможным решением. Система практически не нуждается в обслуживании и исправно служит в течение многих лет. Но, как правило, не экономическая целесообразность, а возможность создания безопасного освещения и уникальных декоративных эффектов играет решающую роль. Свет можно загнать внутрь гибкого световода, а когда необходимо — извлечь в нужном количестве и использовать по назначению. Проходя через границу раздела двух сред, свет преломляется. И здесь оптоволоконные технологии имеют ряд преимуществ:

- световолокно не проводит электричество;
- структура используемого материала не проводит ультрафиолетовые и инфракрасные лучи, т. е. независимо от яркости свечения свет остается холодным;
- световолокно обладает способностью проводить большие световые потоки при минимальном диаметре кабеля или нити, что позволяет подсвечивать места, которые до этого были труднодоступны, а их освещение — чрезмерно затратно;
- сам источник света находится на расстоянии от места свечения, и это дает возможность обслуживать и заменять лампы вне места свечения;
- система позволяет легко контролировать смену цвета или светового эффекта, в том числе механически с помощью светофильтров, что открывает огромные возможности для дизайна, рекламы и визуальной информации.

«Звездное небо»

Этот эффект является, пожалуй, самым популярным в фиброоптике. Световые моноволокна могут быть различного диаметра, в зависимости от того, какую яркость свечения «звезд» необходимо получить. Возможен также и комбинированный вариант:

световые моноволокна различного диаметра объединены и подключены к одному источнику. В этом случае «звезд на небе» будет различной яркости. «Стандартное» фиброоптическое «звездное небо» содержит в среднем 75 «звезд» на 1 кв. м площади, но, разумеется, это количество может быть любым, в зависимости от пожеланий и финансовых возможностей заказчика. Для установки моноволокна на потолок можно натянуть темную ткань, можно же провести волокна над подвесным потолком и вывести через плитку. Аналогично создается «звездная подсветка» на стенах. На полах также возможно создание «звездных ковров» или же протяжка волокон в других материалах. Светоизлучающий элемент (светодиод) имеет колоссальный ресурс работы (до 100 тыс. часов), и светоотдача отдельных волокон при небольшой длине (1–1,5 м) почти такая же, как и при мощных излучателях.

Подсветка катков, фонтанов и бассейнов

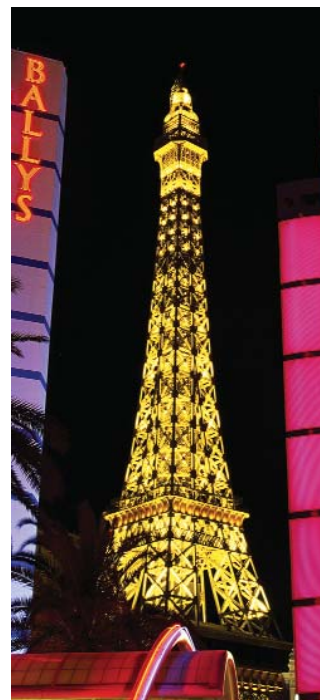
Абсолютная безопасность светопроводов создает большие возможности для подводной подсветки в бассейнах и освещения фонтанов. Необходимо только вынести сам источник света в объем без повышенной влажности. Этот объем может находиться на расстоянии от водного сооружения. При подводной подсветке катков кабеля бокового или торцевого свечения на специальных кронштейнах закрепляются несколько ниже предполагаемого уровня льда. С помощью устанавливаемого в источник света чейнджера цветов возможно мерцание «звезд» и смена цвета. Все фантазии дизайнеров при создании светящегося подводного царства, переливающейся подсветки струй воды и многое другое делается вполне доступным. Возможны также различные световые картины при подсветке: одно горит синим, другое — красным, третье — меняет цвет; затем меняет цвет, напри-

мер, первое и т. д. Смена картин происходит автоматически или управляемо, но для этого необходима другая, более сложная система управления чейнджерами.

Наружная реклама и ночная архитектура

Сегодняшние технологические требования производства рекламы приводят к неизбежной замене неоновых трубок более совершенными кабелями бокового свечения при дизайнерском оформлении ночных клубов, ресторанов и других мест развлечения. Фиброоптика — точечный яркий источник света, изящно вписывающийся в существующий дизайн. Свет на выходе не дает нагрева, т. к. тепловая часть излучения отсечена еще в светогенераторе. Размер светового пятна можно регулировать выходной насадкой с линзой. Пятно может быть контрастным, а может плавно сходиться на нет. Все это создает серьезные предпосылки для замены галогеновых ламп в витринах на оптоволоконно. Именно так и поступают в лучших ювелирных, антикварных, парфюмерных и других магазинах.

Фиброоптика решает многие проблемы освещения зданий и сооружений. Это особенно касается современной архитектуры, мостов, шпилей, радиотелевизионных башен. Первейшее применение фиброоптики в архитектуре — выделение контуров зданий и архитектурных форм по периметру. Для этого используются кабели бокового свечения. Но это еще не все. В архитектурно-художественном освещении возможно воплощение ряда совершенно уникальных решений. Например, высветить на высоте архитектурные элементы: барельефы, скульптуры, ниши, межоконные проемы и др. Использование любых, даже маленьких прожекторов создает ряд технических сложностей. Первая — портится вид здания в дневное время, вторая — лампы надо периодически менять, и не столько дорого стоят сами лампы, сколько их замена с подъемника. А ведь свет можно просто транс-



портировать наружу с тех самых близких мест за стеной, где нет никаких проблем ни с установкой, ни с обслуживанием. А зачастую даже и высотных работ по монтажу не требуется: просто сверлится отверстие в стене и через него выводится кабель торцевого свечения. Опять на помощь приходит «Светлячок»: ни шума в помещении, ни пространства не надо, не боится пыли, а для питания подойдет любая самая слабая розетка; энергопотребление — вообще символическое. Конечно, все здание одним выводом кабеля не осветить, но для точечной подсветки в ряде случаев оптоволоконно является незаменимым инструментом.

Специальные возможности

Световолокно успешно решает извечную проблему качественной подсветки экспонатов без разрушительного воздействия ультрафиолетовых лучей, используемых традиционными средствами освещения. Даже специальные лампы задерживают только 60–70 % ультрафиолетового излучения. Сотни музеев мира уже используют эту систему подсветки. Достаточно упомянуть Британский музей, Египетский музей, музей города Гента, а также подсветку всемирно известных экспонатов, сохранность которых обеспечена технологией, — Туринской плащаницы, Кодексов Леонардо да Винчи, статуи Нефертити и т. д. Отсутствие электричества позволяет использовать кабель в воде, пожаро- и взрывоопасных местах, бензохранилищах, на шахтах, мельничных комбинатах.

Оптическое волокно до сих пор не перестает удивлять. Ученые продолжают открывать новые и новые свойства этого материала. Известно, что оптоволоконно обладает незаурядной прочностью, что находит свое применение при армировании различных пластиковых конструкций, в частности в автомобилестроении. Недавно профессор Университета штата Огайо, индиец по происхождению, Прабхат Гупта со своими коллегами пришел к выводу, что оптоволоконно может быть значительно прочнее, чем представлялось ранее. Метод испытания на прочность основан на охлаждении и деформации стеклянных волокон. Для измерений использовались волокна толщиной в 100 мк, охлажденные до температуры –195 °С, затем образцы сгибались в U-образную форму и сдавливались между двумя металлическими пластинами. «Замороженные волокна» выдерживали давление до 1,5 млн фунтов на кв. см, что почти в 1,7 раза больше, чем показывали эксперименты ранее. По словам профессора, нет ничего удивительного в том, что ранее это свойство не было обнаружено. «Материалы совершенствуются для определенных задач», — говорит он. — Время для изучения побочных свойств приходит позже».

В статье использованы материалы web-ресурсов

