

App Store



Google play



<http://www.lanmag.ru> СЕНТЯБРЬ 2017

# ЖУРНАЛ СЕТЕВЫХ РЕШЕНИЙ

# LAN



## Как выбрать КЦОД?

ISSN 1027086-8

17 009



771027 086001

Инженерная инфраструктура от одного поставщика  
Плюсы и минусы автоматизированной защиты  
Что должен включать план защиты периметра

<http://www.lanmag.ru>

ЖУРНАЛ  
СЕТЕВЫХ  
РЕШЕНИЙ

# LAN

СЕНТЯБРЬ 2017



Читайте нас на Facebook



Читайте нас в Twitter



## 1 КОЛОНКА РЕДАКТОРА

Да будет свет! И связь  
Дмитрий Ганьжа

## 2 КАНАЛ НОВОСТЕЙ

Горячая десятка технологий  
Ciena — за автономность (сетей)  
Yealink расширяет линейку продуктов для ВКС

## 10 ИНТЕРВЬЮ

Павел Колмычек: российские заказчики  
используют потенциал облаков только на 10%  
Александр Барсков

## 13 МНЕНИЕ ЭКСПЕРТА

Автоматизированные системы защиты:  
плюсы и минусы  
Рустэм Хайретдинов

## 16 ТЕМА НОМЕРА

Как выбрать КЦОД  
Александр Барсков

## 20

Инженерная инфраструктура в комплексе.  
Часть I  
Александр Барсков

## 27 КАБЕЛЬНЫЕ СИСТЕМЫ

Транковые кабели для систем параллельной  
оптической передачи  
Андрей Семенов

## 32 БИЗНЕС-ВИДЕО

Шесть вопросов, которые вы,  
возможно, забыли задать,  
разрабатывая план защиты периметра  
Кванг Трин

## 36 ЗАЩИТА ИНФОРМАЦИИ

Летняя коррекция прогнозов  
Дерек Мэнки

## 40 НОВШЕСТВА

JC-WebClient v. 4 реализует  
единую технологию работы с токенами  
Неуправляемые коммутаторы  
CentreCOM GS920  
Коммутаторы Aruba серии 8400  
с новой ОС OS-CX

ЦИФРОВАЯ ЭКОНОМИКА – наше будущее ЦИФРОВАЯ ТРАНСФОРМАЦИЯ – наше настоящее

SMART  
INDUSTRY&CITY  
2017



25 ОКТЯБРЯ



### ОСНОВНЫЕ ТЕМЫ:

- Индустрия 4.0: процессы, технологии, решения
- Промышленный интернет для производства и ТЭК
- Драйверы инноваций в промышленности и ЖКХ: smart&big data, Интернет вещей, искусственный интеллект, робототехника
- Полная цифровизация жизненного цикла продукции – возможности и риски
- Виртуальная и дополненная реальность для производственных задач
- Перспективы аддитивных технологий
- Безопасность на цифровом производстве



[kon@osp.ru](mailto:kon@osp.ru)



[www.osp.ru](http://www.osp.ru)



+ 7 495 725 47 80

Реклама 12+

# Да будет свет! И связь

С распространением энергосберегающих светодиодных ламп появилась возможность обеспечить их питание по традиционной проводке Ethernet посредством PoE. Соответствующие решения, предлагаемые Cisco, Philips и другими вендорами, позволяют реализовать умное и экономичное освещение помещений на базе слаботочной проводки. Распространение LED-ламп прокладывает путь для использования еще одной перспективной технологии, которая в последнее время привлекает все больше внимания — Light Fidelity (Li-Fi), названной по аналогии с Wireless Fidelity (Wi-Fi), то есть достоверная передача информации с помощью света.

Традиционно «отцом Li-Fi» считается профессор Эдинбургского университета Харальд Хаас, который и дал технологии имя. Однако разработки в этой области начались гораздо раньше 2011 года, когда профессор Хаас впервые представил ее широкой публике. Значительное количество патентов (более полусотни) на Li-Fi (конечно, тогда такого названия не существовало) было выдано до 2011 года.

По данным Южно-Корейского бюро интеллектуальной собственности, первые два патента были получены авторами соответствующих изобретений по теме Li-Fi еще в 2004 году. С тех пор разработка значительно ускорилась, и в настоящее время ежегодно выдается примерно 30 патентов. Наибольшую активность в этой области проявляют корейские компании и университеты, прежде всего Samsung, которая зарегистрировала уже больше сотни.

Кроме того, разработки этой технологии ведут компании Qualcomm, Panasonic, Philips, GE, не говоря уже о множестве стартапов. Много шума наделала в прошлом году информация о предполагаемом тестировании Li-Fi компанией Apple. Однако, несмотря на столь высокую активность и продолжительную историю разработок, гото-

вых продуктов на рынке раз-два и обчелся. Даже PureLiFi, основанная Харальдом Хаасом и считающаяся лидером этого направления, предлагает всего два продукта: точку доступа LiFi-X Access Point и USB-модем LiFi-X Station.

С чем же связано такое внимание к Li-Fi?

Естественным ограничением для беспроводных технологий является нехватка доступных радиочастот. В наибольшей степени эта проблема касается Wi-Fi, где применяется нелицензируемый диапазон. Li-Fi использует излучение в видимой части спектра: здесь доступный диапазон в 10 000 раз шире, чем весь радиочастотный спектр Wi-Fi. Соответственно, гораздо выше и потенциально достижимые скорости. Так, в лабораторных тестах удалось продемонстрировать возможность передачи со скоростью 224 Гбит/с.

Серьезным ограничением для обеспечения связи с помощью Li-Fi является тот факт, что приемник и передатчик должны находиться в пределах прямой видимости (в принципе возможен и прием отраженного света, но скорость будет заметно ниже). Впрочем, этот недостаток становится преимуществом, если оценивать его с точки зрения безопасности: чтобы исключить перехват сигнала, достаточно плотно задернуть шторы.

Однако на практике скорости Li-Fi намного ниже расчетных: так, USB-модем PureLiFi обеспечивает передачу и прием со скоростью 43 Мбит/с. Так что сторонникам Li-Fi стоит поторопиться с представлением продуктов, оснащенных поддержкой гигабитных скоростей. Но даже если им это удастся, Li-Fi в лучшем случае сможет претендовать на место технологии, применяемой в качестве замены Wi-Fi, если, например, использование последней невозможно из-за создания помех для чувствительного оборудования. **LAN**



Дмитрий Ганьжа

<http://www.lanmag.ru>

ЖУРНАЛ  
СЕТЕВЫХ  
РЕШЕНИЙ

**LAN**

12+

№ 9, сентябрь 2017

## РУКОВОДИТЕЛЬ ПРОЕКТА

Чекалина Е. В. [lena@osp.ru](mailto:lena@osp.ru)

## ГЛАВНЫЙ РЕДАКТОР

Ганьжа Д. Х. [diga@lanmag.ru](mailto:diga@lanmag.ru)

## ВЕДУЩИЙ РЕДАКТОР

Барсков А.

## ЛИТЕРАТУРНЫЙ РЕДАКТОР

Качинская Т.

## КОМПЬЮТЕРНАЯ ВЕРСТКА

Рыжкова М.

## МАРКЕТИНГ И КОММУНИКАЦИИ

Данильченко Е.

## ПРОИЗВОДСТВЕННЫЙ ОТДЕЛ

Блохина Г.

## УЧРЕДИТЕЛЬ И ИЗДАТЕЛЬ

ООО «Издательство «Открытые системы»

Адрес издателя и редакции:

Россия, 127254, г. Москва,

проезд Добролюбова, дом 3, строение 3, каб. 13

Адрес для корреспонденции:

123056, г. Москва, а/я 82, [lan@lanmag.ru](mailto:lan@lanmag.ru),

Тел.: +7 495 725-4780/83, +7 499 703-1854

Факс: +7 495 725-4783

© 2017 ООО «Издательство «Открытые системы»

Все права защищены.

Запрещается полное или частичное воспроизведение статей и фотоматериалов без письменного разрешения редакции.

В номере использованы иллюстрации и фотографии издательства «Открытые системы», [123rf.com](http://123rf.com).

Журнал зарегистрирован в Роскомнадзоре.

Свидетельство о регистрации СМИ

ПИ №ФС77-63550 от 30 октября 2015 г.

Отпечатано в ООО

«Богородский полиграфический комбинат», 142400, Московская обл., г. Ногинск, ул. Индустриальная, д. 406

Журнал выходит 10 раз в год.

Общий тираж 13000 экз.

(включая 3000 экз. PDF-версии)

Цена свободная.

Редакция не несет ответственности за содержание рекламных материалов.

Дата выхода в свет:

19.09.2017 г.



**ОТКРЫТЫЕ  
СИСТЕМЫ**  
Open Systems Publications

## ПРЕЗИДЕНТ

Михаил Борисов

## ГЕНЕРАЛЬНЫЙ ДИРЕКТОР

Галина Герасина

## ДИРЕКТОР ИТ-НАПРАВЛЕНИЯ

Павел Христов

## КОММЕРЧЕСКИЙ ДИРЕКТОР

Татьяна Филина

## Горячая десятка технологий

30 августа под вывеской Vendor's Day компания «Крок» провела день открытых дверей, в рамках которого был организован бизнес-диалог об инновационных технологиях.

Свои инновационные решения на мероприятии представили более 30 вендоров. В их числе как давно зарекомендовавшие себя на рынке бренды, так и новые перспективные нишевые производители. На круглом столе для представителей СМИ эксперты «Крок» рассказали о тех инновациях, которые они держат в фокусе своего внимания.

В области сетевой инфраструктуры одна из наиболее горячих тем — программно определяемые сети (SDN), в том числе территориально распределенные (SD-WAN). Основные практические преимущества таких решений для заказчиков — повышение автоматизации развертывания и эксплуатации сетей, ускорение внедрения новых сетевых сервисов, а также существенное снижение расходов на их обслуживание. По словам Наталии Дьяконовой, директора департамента телекоммуникаций «Крок», объем средств, выделяемых заказчиками на решения SDN, в следующем году вырастет многократно.

позволяет выстроить доверенную экосистему для всех участников и автоматизировать запуск смарт-контрактов на реализацию определенных действий в рамках бизнес-процесса. Одним из крупных проектов может стать внедрение платформы блокчейна Национальной ассоциацией негосударственных пенсионных фондов, в рамках которой сейчас активно обсуждается целесообразность развертывания такой платформы.

Валентин Губарев, директор департамента вычислительных систем, особое внимание уделил развитию технологий виртуальной и дополненной реальности. В «Крок» уже пять лет существует центр VR, и в прошлом году был отмечен бурный рост интереса к таким проектам. В этом году компания планирует реализовать уже несколько десятков проектов с использованием систем виртуальной и дополненной реальности. По словам эксперта, эти технологии позволяют увеличить продажи элитной недвижимости, упрощают и ускоряют работу архитекторов над проектами, повышают качество обучения персонала промышленных предприятий. И это лишь несколько примеров их использования.

Представитель департамента интеллектуальных зданий, главный инженер компании «Крок» Петр Вашкевич выделил самую горячую технологию в этом сегменте: информационное моделирование зданий и объектов (Building Information Modeling, BIM). По его словам, сейчас в России совместно с экспертами Британского института стандартов (British Standards Institution, BSI) ведутся работы над созданием отечественных стандартов по BIM. Минстроем подписана дорожная карта по внедрению BIM на всех этапах жизненного цикла объекта, а через год-два использование BIM станет обязательным при госзаказе. «Крок» уже несколько лет активно применяет системы BIM в проектах. В частности, они были использованы для проектирования административного здания в одной из особых экономических зон России, а также одного из зарубежных ЦОДов. Как утверждает Петр Вашкевич, в случае с ЦОДом применение BIM позволило на 30% сократить расходы на его строительство.

Сама компания «Крок» активно использует названные технологии для собственных нужд. Так, на основании двумерных чертежей, выполненных пять лет назад, специалисты компании реализовали BIM-модель офисного здания «Крок». После чего эта модель была дополнена средствами виртуальной реальности и сейчас используется инженерными службами для обслуживания объекта и внедрения новых сервисов.

### 10 наиболее перспективных технологий. Версия «Крок»

- Программно-определяемые сети (SDN)
- Wi-Fi-аналитика поведения клиентов в многолюдных местах
- Омниканальная платформа для обслуживания клиентов контакт-центров
- Big Data и BI — технологии работы с Большими Данными и их анализа
- Чат-боты для бизнеса
- Блокчейн как распределенная база данных, гарантирующая прозрачность всех процессов
- Публичные облака и управляемые сервисы — доступ к инфраструктуре здесь и сейчас
- Миграция на открытые платформы и на стандартные архитектуры (x86)
- VR-технологии
- BIM — информационное моделирование зданий и объектов

Основным драйвером развития беспроводных сетей Wi-Fi, по мнению этого эксперта, станут средства анализа поведения клиентов в многолюдных местах. На основе данных использования Wi-Fi создаются тепловые карты, которые в онлайн-режиме отражают потоки движения посетителей. Современные решения позволяют выявить перспективные и неперспективные торговые зоны или магазины, установить лояльных посетителей, управлять эффективностью рекламных кампаний, отправлять на устройства пользователей актуальный контент.

В тройку технологических направлений, которые выделил Игорь Малышев, директор по системным решениям «Крок», вошли технологии работы с Большими Данными, чат-боты для бизнеса и блокчейн. По его словам, блокчейн как распределенная база данных, гарантирующая прозрачность всех процессов,



# Аудиотракт под ключ с Converge Pro 2

Сегодня мы покажем, как шаг за шагом создать полностью масштабируемую систему для маршрутизации и настройки аудиотракта. Премиальная линейка ClearOne Converge Pro 2 (CP2) предоставляет для этого максимум инструментов: мощные цифровые аудио-платформы, многоканальные усилители класса D, модули расширения с поддержкой сервисов унифицированных коммуникаций и тач-панели управления. Мы бы даже сказали, что она избыточна, если бы не количество предлагаемых вариантов — от небольших переговорных с парой аудиоканалов до платформ 96×96 с возможностью дальнейшего расширения. Но обо всем по порядку.

В основе качественной передачи речи систем Converge Pro лежит запатентованная технология распределенного эхоподавления DEC (Distributed Echo Cancellation). Широкополосная эмуляция ClearEffect, в свою очередь, обеспечивает кристально чистый звук — во время обсуждения создается впечатление, что все участники конференции находятся в одной комнате. При подключении к конференции коллег из другого города активируется функция TEC (подавление телефонного эха). Каждая аудио-платформа имеет несколько уровней mic/line с поддержкой протокола Dante, встроенные модули VoIP и Telco. Это позволяет с легкостью адаптироваться к различным акустическим условиям: в переговорных, конференц-залах и залах судебных заседаний, лекториях и системах телемедицины (закон об использовании которых уже подписан и вступит в силу с 1 января 2018 года).

DSP-процессор помогает осуществлять обработку сигналов, фильтрацию, задержки, Mute, регулировку уровней на входе и выходе, компрессию, микширование каналов и многое другое. За счет этого аудио-платформа незаменима в коммерческих инсталляциях — от бутиков до ТРЦ. Благодаря открытой архитектуре, каждый выход можно легко настроить под разные задачи обработки и маршрутизации на базе ПО Converge Console. Также управление возможно через Ethernet при помощи оборудования Crestron, AMX и др. В зависимости от числа микрофонов и иных источников предпочтительней будет одна из конфигураций: от Converge Pro 2 48V размерностью 6×12 с AEC, VoIP до Converge Pro 2 128V размерностью 14×10 с AEC, VoIP и возможностью расширения.

Следующим шагом будет подбор усилителя. Предлагаются две 4-канальные модели — мощностью 60 Вт (PA 460) или 120 Вт (PA 4120), работающие как в режиме 8 Ом, так и в режиме 70/100 В. Это компактные



усилители класса D форм-фактора 1U с защитой от короткого замыкания, перегрузки и нагревания, а также со сбалансированной нагрузкой на каждый канал. Для точечной подстройки уровня усиления, ВЧ-фильтра и активации режима ожидания предусмотрено ручное переключение. Для экономии электроэнергии — автоматический переход в режим ожидания (отдельно для каждого канала).

Далее идут модули расширения Converge Pro 2 USB и Converge Pro 2 GPIO. При помощи первого вы сможете проводить полноценные переговоры без затрат на покупку дорогостоящих кодеков. К одной аудио-платформе теперь можно подключить до трех дополнительных ноутбуков или ПК на базе Windows либо Mac с установленным ПО унифицированных коммуникаций: Skype, Hangouts, Spontania, Webex, GoToMeeting. Поддержка USB 3.0 и 2.0, частота дискретизации 48 кГц. Модуль GPIO выполняет чисто утилитарную функцию управления через сухие контакты и триггеры. 12 клеммных входов и 12 выходов, помимо звука, позволяют удаленно менять настройки PTZ-камер, микрофонов, даже системы регулировки жалюзи в офисе.

Подключение модулей осуществляется по витой паре CAT5 и выше с PoE.

При последовательном соединении между устройствами должно быть не более 61 м (ограничение шины P-Link), увеличение расстояния возможно через ретрансляторы. Добавьте к этому совместную работу с микрофонными массивами Beamforming Mic Array 2 и 2-канальными беспроводными приемниками Dialog 20, заложенную в базовый функционал аудио-платформы, и вы получите по-настоящему эффективный бизнес-инструмент.

Финальный штрих — контроллер Touch Panel Controller, устанавливаемый на стол/стену или с любым сторонним VESA-креплением. Большой сенсорный экран 10,1" позволяет управлять контактами, принимать, удерживать и завершать VoIP-вызовы и систематизировать телефонную книгу. Для удобства работы в корпоративном и госсекторе можно использовать общую базу контактов, хранящихся в MS Outlook, к которой Converge сможет обращаться по протоколу LDAP. Помимо этого, при помощи Touch Panel можно удаленно изменять настройки конференц-системы: активировать Mute микрофона, регулировать громкость динамика, программировать предустановки и др. Управление: RS-232, Ethernet, Wi-Fi.

**[www.clearone.pro](http://www.clearone.pro)**  
**[marketing@clearone.pro](mailto:marketing@clearone.pro)**

## Ciena — за автономность (сетей)

Новые решения Ciena нацелены на повышение уровня автоматизации, гибкости и открытости.

На пресс-конференции в Москве компания Ciena представила свои подходы и решения для построения сетей нового поколения. Выступивший на ней вице-президент Ciena Джо Марселла напомнил, что пару лет назад зародилась третья «волна цифрового прогресса». Первая волна (1990–2015 годы) была связана с активным развитием проводного Интернета, а ключевым приложением была электронная почта. Вторая волна (2010–2025 годы) принесла с собой развитие мобильного Интернета и широкое распространение смартфонов и других мобильных устройств, а также вызвала перенос приложений в облака, при этом существенно выросло значение видеоприложений. Третья волна (2015–2030 годы), которая долгое время будет распространяться вместе со второй, характеризуется активным внедрением Интернета вещей, технологий Больших Данных, искусственного интеллекта и виртуальной реальности.

Волны цифрового прогресса несут с собой стремительное увеличение числа подключенных устройств, работающих в сети приложений и, как следствие, объемов трафика. Все это ужесточает требования к сетевым инфраструктурам. И дело не только в необходимости повышения скорости передачи данных. Как полагает Джо Марселла, сети должны стать более открытыми, масштабируемыми и гибкими, кроме того, уровень автоматизации предоставления и изменения сетевых сервисов следует существенно повысить. Заказчики больше не готовы ждать дни и недели, когда будут вручную выполнены все необходимые настройки, они хотят получать нужные им сетевые ресурсы мгновенно, в режиме «по требованию».

Адаптивность и автоматизация невозможны без широкого внедрения программируемых систем, которые применяются в том числе и на уровне оптического транспорта. Предлагаемый Ciena набор технологий и приложений для построения программно определяемой оптической сети

в компании называют Liquid Spectrum. Они, в частности, позволяют оптимизировать производительность работы сети, используя получаемые в реальном времени данные. Еще одна важная функция Liquid Spectrum — повышение уровня доступности сетевых сервисов с возможностью гибкой настройки пропускной способности

для восстановления передачи трафика в случае аварии или возникновения иных проблем на отдельных участках сети.

Реализация подобных функций невозможна без интеллектуальной элементной базы сетевых узлов. Одним из ключевых элементов технических решений Ciena является новый процессор WaveLogic Ai. Он повышает емкость одного канала до 400G, при этом пропускная способность канала может настраиваться с шагом 50G (начиная с уровня 100G). Кроме того, в WaveLogic Ai встроены функции мониторинга каналов в реальном времени, что как раз и дает возможность повысить надежность связи и максимально эффективно использовать имеющиеся ресурсы.

Данный процессор уже используется в ряде продуктов Ciena, в частности в оборудовании Waveserver Ai. Эти устройства обеспечивают передачу 400G на одной несущей на расстояние до 300 км. При снижении скорости до 300G дальность увеличивается до 1000 км, что позволяет связать объекты, расположенные, например, в Москве и Санкт-Петербурге. К слову, предыдущее поколение этих устройств, Waveserver, активно применяется в России, в первую очередь для соединения крупных ЦОДов.

Ciena предлагает и программируемые решения для пакетных сетей с централизованным управлением сетевыми устройствами с помощью SDN-контроллера. Это, в частности, решения по распределенной виртуализации сетевых функций — D-NFV. В качестве оконечных устройств доступа в них могут использоваться обычные серверы на базе процессоров x86, а интеллект реализуется централизованно с применением ПО D-NFVI и операционной системы SAOS (Service-Aware Operating System).

Джо Марселла также выделил такую важную тенденцию, как развитие пограничных вычислений (edge computing), что требует создания сети распределенных мини-ЦОДов, максимально приближенных к оконечным устройствам. Для поставщиков сетевых решений это означает, что наряду с организацией межсоединений крупных ЦОДов появляется новая задача: подключение множества разбросанных по большой территории малых центров обработки данных. При ее решении, считает эксперт Ciena, ключевое значение будут играть стоимость и масштабируемость технических решений, а также предложение эффективных гибридных устройств, сочетающих функции узлов пакетной связи и оптического транспорта.

В Ciena рассчитывают открыть двери к автономным сетям благодаря своим новым разработкам



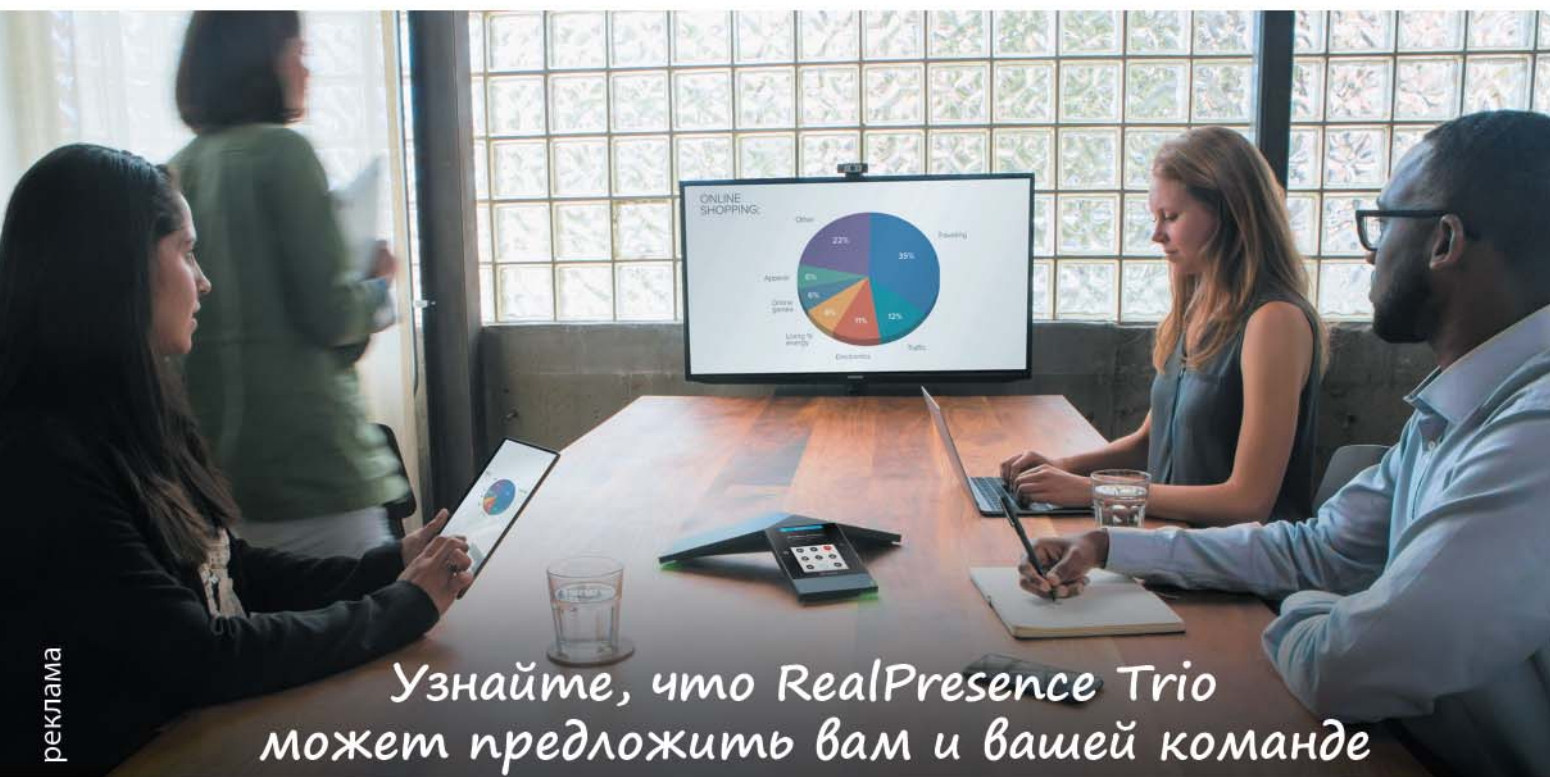
Фото: Ciena

Александр Барсков





Polycom® RealPresence Trio™ -  
первый интеллектуальный центр для групповой работы,  
превращающий легендарный конференц-телефон Polycom  
в целую систему для голосовой и видеосвязи  
с возможностью обмена контентом,  
которую можно разместить в комнатах любого размера

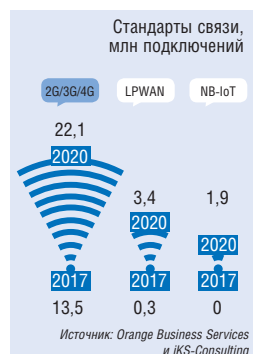


*Узнайте, что RealPresence Trio  
может предложить вам и вашей команде*

ЗАО «Авикон Текнолоджис»  
Тел.: +7 (495) 788-31-84  
E-mail: [info@avicon.ru](mailto:info@avicon.ru)

## IoT: рост неизбежен

Orange Business Services и iKS-Consulting представили результаты исследования текущего состояния и прогнозы развития корпоративного сегмента российского рынка Интернета вещей на период до 2020 года.



Согласно данным исследования, объем анализируемого рынка в России в 2017 году составит 20,8 млрд рублей, а к 2020 году ожидается его увеличение до 30 млрд при среднегодовых темпах роста около 12%. Следует сразу заметить, что исследование охватывало только шесть отраслей: транспорт, финансы, сельское хозяйство, розничную торговлю, строительство («умные» здания) и промышленность. По мнению экспертов, именно эти отрасли наиболее готовы технологически к внедрению решений IoT. Исследование не затрагивало направления и проекты, финансируемые государством, такие как «Безопасный город», «Платон», «ЭРА-ГЛОНАСС» и пр. Поэтому общий объем российского рынка IoT, по-видимому, существенно больше.

Эксперты констатируют заметное увеличение интереса заказчиков и числа проектов, в которых используются технологии IoT. Одним из свидетельств этого, по словам Владимира Ласовского, менеджера по развитию бизнеса в области Интернета вещей Orange Business Services, является существенный рост продаж ИТ-услуг. Так, за первую половину текущего года у этого провайдера он составил 117% (по сравнению с первой половиной 2016 года), тогда как продажи традиционных телекоммуникационных услуг выросли всего лишь на 15%. Orange Business Services делает большую ставку на IoT-проекты: по всему миру компания управляет уже 14 млн подключенных устройств, предоставляя комплексные (end-to-end) решения для крупных организаций из разных отраслей.

Согласно данным исследования, по объему рынка IoT на данный момент в России лидирует транспортная отрасль: 13,1 млрд рублей (2,3 млн подключений) в 2017 году с прогнозируемым увеличением к 2020 году до 19,8 млрд (3,2 млн подключений) — без учета государственных проектов «Платон» и «ЭРА-ГЛОНАСС». Основным драйвером развития здесь — активное внедрение M2M-систем и набирающих популярность систем мониторинга контейнерного транспорта с помощью геолокации и радиочастотных

меток RFID. Как заметил Сергей Езык, генеральный директор компании «Центр 2М», если раньше информация с подключенного автомобиля предоставлялась только одной стороне, то сейчас число сторон, осуществляющих мониторинг подключенных объектов, постоянно растет: лизингодатели, муниципалитеты, страховщики, автопроизводители, автосервисы и пр. Увеличение числа участников рынка, очевидно, способствует его развитию.

Наибольшего роста числа внедрений IoT-решений в период до 2020 года аналитики ожидают в ретейле. Сегодня в этой отрасли насчитывается 1,4 млн подключенных IoT-устройств, к 2020 году их количество должно вырасти до 4 млн единиц. Среди драйверов внедрения IoT-решений в этой отрасли — высокая конкуренция, стимулирующая внедрение таких технологий, как отслеживание товара с помощью радиочастотных меток RFID, мониторинг движения покупателей с мобильными устройствами, распознавание лиц и пр.

Как отмечается в исследовании, основными игроками рынка Интернета вещей в России являются производители платформ и ПО, а также системные интеграторы; эксперты оценивают их суммарную долю почти в 80% рынка. Оставшуюся часть рынка делят между собой операторы связи и производители датчиков и устройств.

Среди стандартов связи, используемых на рынке Интернета вещей, лидируют традиционные технологии сотовой связи (2G/3G/4G): на конец 2017 года ожидается около 13,8 млн IoT-подключений на базе этих технологий, к 2020 году их количество вырастет на 63%. На технологию LPWAN на конец текущего года будет приходиться лишь 300 тыс. подключений. Такой сравнительно небольшой объем эксперты связывают с необходимостью развертывания специализированной инфраструктуры. К 2020 году число подключений по стандарту LPWAN, по прогнозу, вырастет более чем в 10 раз.

Новейший стандарт связи на рынке Интернета вещей — NB-IoT — может быть развернут на базе существующей инфраструктуры мобильных сетей при ее незначительной модернизации. Эксперты предсказывают высокий интерес к этому стандарту со стороны сотовых операторов — 1,9 млн подключений в 2020 году. Но основной рост прогнозируется на период после 2020 года, что связано с необходимостью реализации программы инвестиций в развитие сетей.





# Yealink расширяет линейку продуктов для ВКС

2017 год стал для компании богатым на новинки.

Летом текущего года компания «АйПиМатика», стратегический партнер Yealink Network Technology в России, объявила о выводе на рынок новых продуктов для видео-конференц-связи. Предварительная информация о них была представлена еще в марте, на форуме «Бизнес-Видео», однако официальные данные и полные характеристики опубликованы только сейчас.

Одна из новинок, терминал Yealink VC500, предназначена для такого быстрорастущего сегмента, как оборудование средних и малых конференц-комнат. Этот продукт, пришедший на смену терминалу VC110, оснащен PTZ-камерой с 5-кратным оптическим зумом и разрешением 1080p. Широкий (83°) угол обзора камеры гарантирует, что все присутствующие будут видны во время встречи, даже если они сидят близко к камере.

Устройство VC500 предлагается в двух вариантах. Комплектация VC500-CP960 включает конференц-телефон нового поколения с сенсорной 5-дюймовой панелью управления, оснащенный акустикой Harman Kardon и технологией защиты от фонового шума. Это решение обеспечивает точность воспроизведения и качественный захват звука в радиусе до 6 м. Второй вариант — VC500-CPW90 — позволяет обходиться без лишних проводов на конференц-столе благодаря двум беспроводным микрофонам, каждый из которых способен улавливать звук в радиусе до 3 м.

Другая новинка — ВКС-терминал для больших и средних переговорных VC800 со встроенным MCU. Кодек этого терминала выполнен в виде подставки для PTZ-камеры, а сама камера обеспечивает 12-кратный оптический зум и разрешение 1080p. Встроенный MCU позволяет подключить к видеоконференции с высокой четкостью изображения (до 1080p) до 24 участников. Его можно разделить на два виртуальных сервера многоточечной ВКС. Учитывая, что 24 порта могут оказаться невостребованными в небольших организациях, Yealink предлагает варианты поставки усеченной емкости — на 8 и 16 портов.

А если требуется поддержка большей емкости и числа одновременных конференций, то поможет глубокая интеграция VC800 с программным сервером ВКС Yealink Meeting Server (YMS). Это еще одна новинка, которая объединяет все основные инфраструктурные компоненты ВКС: программный MCU, серверы регистрации, прохождения NAT и хранения контактов. На сервере YMS можно создать несколько виртуальных конференц-комнат и параллельно проводить несколько сеансов ВКС. YMS, поддерживающий среды виртуализации VMware и Microsoft Hyper-V, можно развернуть в корпоративном ЦОДе или использовать из публичного облака.

Как и VC500, VC800 оснащается конференц-телефоном с сенсорным экраном 5". Этот конференц-телефон — вполне самостоятельное изделие, поэтому пользователь, если его бюджет ограничен, может на первом этапе приобрести только его и начать с голосовых конференций, а более дорогую часть, видеокамеру с кодеком, докупить позднее, нарастив таким образом систему до полноценного видеотерминала. Это значительно снижает начальную ценовую планку для потенциальных пользователей, что всегда считалось одним из главных препятствий для приобретения качественных терминалов ВКС.

Интересным компонентом решения VC800 является концентратор проводов. Инженеры Yealink решили вынести коммутационный узел из кодека и приблизить его к пользователю в зону «вытянутой руки», чтобы дать ему возможность осуществлять необходимые во время конференции подключения (например, компьютера для показа контента или USB-накопителя для записи видеоконференции), не вставая из-за стола. Соединение с кодеком при этом осуществляется всего одним кабелем, спрятать который значительно проще, чем пучок проводов. По нему кодек и встроенная видеокамера получают электропитание, все необходимые сигналы и данные.

Специалисты «АйПиМатики» отмечают высокую производительность специализированных процессоров видеообработки, используемых в новых терминалах. Они позволяют реализовать компрессию видео 1080p/30 для передачи в канале 512 Кбит/с (используется новый протокол H.265/HEVC) и обеспечить защиту сеанса ВКС от потерь до 30% видеопакетов. Последнее особенно важно, когда сеанс видеосвязи организуется по плохим каналам через Интернет.



**Терминал VC500 с конференц-телефоном нового поколения, оснащенный сенсорной панелью управления**

**Встроенный в терминал VC800 сервер MCU позволяет подключить к видеоконференции до 24 участников**



Александр Барсков

## Dahua открывает представительство

Dahua Technologies Rus будет отвечать за продажи, маркетинг и сервис в России и СНГ.

Китайская компания Hejiang Dahua Technology открыла полнофункциональное представительство в Москве: за деятельность в России будет отвечать дочерняя компания Dahua Technologies Rus. Как заявил на церемонии открытия представительства Майкл Чен, генеральный директор предприятий по зарубежным рынкам, главными целями являются повышение осведомленности заказчиков и пользователей о технических решениях компании и повышение качества коммерческой и технической поддержки партнеров и клиентов. В новом офисе планируется открыть демонстрационный центр и сервисный пункт.

Dahua присутствует в России с 2008 года, однако до этого интересы компании представляли многочисленные партнеры, число которых постоянно увеличивается. Так, нынешним летом к пяти имеющимся дистрибьюторам, в число которых входят OCS и «Софт-Троник», присоединился Merlion. Российский офис будет отвечать также за бизнес в странах СНГ и Монголии. В 2015 году Dahua изменила свою стратегию, сделав акцент на решениях для вертикальных рынков. По словам Майкла Чена, до 80% продаваемого оборудования поставляется для конкретных проектов.

Компания известна прежде всего своими решениями для видеонаблюдения. По данным IHS, на этом рынке Dahua занимает второе место в мире на протяжении последних трех лет (2014–2016 годы). Однако наряду с видеокameraми и видеорегистраторами она предлагает решения для контроля доступа, аварийной сигнализации, умной блокировки и т. д. A&S International отвела ей четвертое место на мировом рынке средств (физической) безопасности — после Hikvision, Honeywell и Bosch. Поставляемые в другие страны решения для организации видео-конференц-связи, в том числе системы телеприсутствия, на российском рынке пока не представлены.

Бизнес Dahua Technologies растет как на дрожжах: среднегодовой рост оборота составляет 46,67%. Согласно опубликованному отчету, за первое полугодие 2017 года валовой доход компании увеличился в полтора раза (на 50,81%) и достиг 1,1 млрд долларов, при этом операционная выручка выросла почти в два раза (на 94,36%) и превысила 165 млн долларов. До 10% дохода инвестируется в НИОКР: свыше половины из 11 тыс. сотрудников компании осуществляют исследования и разработки в таких областях, как искусственный интеллект, IoT, облачные сервисы, кибербезопасность и др. Компания вывела на рынок ряд оригинальных разработок, в частности 8-канальный видеорегистратор.

Среди наиболее интересных технических решений Dahua Сергей Бутузов, директор по развитию бизнеса «Софт-Троник», выделил технологию аналогового видео высокой четкости. Качество обычного аналогового видео не идет ни в какое сравнение с разрешением цифровой картинки. Переход же на цифру с уже развернутых систем затруднен тем, что IP-камеры не рассчитаны на работу по коаксиальной кабельной инфраструктуре. Dahua первой предложила подобное решение еще в 2012 году, соответствующий стандарт получил название High Definition Coaxial Video Interface (HDCVI).

В начале года Dahua Technologies представила камеру третьего поколения с разрешением 4K. Новые 8-мегапиксельные камеры 4K стандарта HDCVI 3.0 имеют различное исполнение: корпусное, купольное, цилиндрическое. Камеры поддерживают широкий динамический диапазон (Wide Dynamic Range, WDR): 120 дБ для купольных и цилиндрических камер и 140 дБ для корпусных. Благодаря эффективной схеме модуляции сигнала и технологии подавления шума, дальность передачи потока видео с разрешением Ultra HD 4K по коаксиальному кабелю составляет до 700 м.

Как отметил Виталий Манкевич, председатель Русско-Азиатского союза промышленников, открытие представительства стало частью «нового цикла выхода китайских производителей на российский рынок» в рамках расширения российско-китайского сотрудничества. А полномочный министр посольства КНР в России Чжан Сяо выразил надежду, что Dahua внесет свой скромный вклад в увеличение товарооборота между двумя странами, который, по предварительным оценкам, в 2017 году превысит 100 млрд долларов. По мнению Чжао Ченбо, директора компании Dahua по развитию рынка России и СНГ, уже достигнуты отличные результаты и в этом году ожидается высокий рост оборота на рынке РФ, однако никаких конкретных цифр названо не было.

Открыв представительство в Москве, Dahua Technologies надеется еще больше увеличить продажи на российском рынке



Фото: Дмитрий Ганьжа

Дмитрий Ганьжа

# Aruba завоевывает российский рынок: обзор основных решений

**A**ruba, a Hewlett Packard Enterprise company — производитель проводного и беспроводного оборудования и программных решений для сетей передачи данных корпоративного уровня. Приставка HPE появилась в названии в 2015 году, когда компанию Aruba Networks, известную до того 13 лет, купил гигант Hewlett Packard Enterprise.

Aruba — относительно молодой игрок в области корпоративного сетевого оборудования на российском рынке, хотя имеет прочные позиции за рубежом. В число лидеров компания вошла благодаря простоте внедрения решений, дальнейшего обслуживания и управления всем функционалом. Сети на базе Aruba уже оценили UNESCO, DreamWorks Animation, Microsoft, KFC, крупнейшие аэропорты и гостиницы.

По отношению к другим производителям аналогичного оборудования на российском рынке линейку Aruba выделяют:



Пожизненная гарантия на большинство коммутаторов



Сети Wi-Fi без выделенного контроллера



Доступность всего функционала маршрутизаторов и коммутаторов без приобретения лицензии

Особенности основных программных и аппаратных решений Aruba комментирует системный интегратор КОМПЛИТ, одним из первых начавший работать с новым оборудованием. Специалисты КОМПЛИТ по сетевым решениям прошли обучение и успешно сдали экзамены по беспроводным технологиям Aruba, включая настройку сети, различные схемы аутентификации, контроль доступа, ARM, Mesh, архитектуру Master-Local и защиту Control Plane.

## Точки доступа без выделенного контроллера

В линейку точек доступа Aruba входят устройства с базовым функционалом Wi-Fi и точки доступа для сетей с высокой плотностью абонентов и скоростями до 1,73 Гбит/с в диапазоне 5 ГГц и до 600 Мбит/с в диапазоне 2,4 ГГц.

Для малого и среднего бизнеса с высокими требованиями к сети Wi-Fi созданы точки доступа Aruba Instant, которые не требуют выделенного контроллера. В кластер объединяются до 128 IAP (Instant Access Point), где первая из развернутых точек доступа выполняет функции контроллера, продолжая параллельно обеспечивать



беспроводной доступ. В том случае, если точка-контроллер выйдет из строя, другая точка доступа автоматически берет эту роль на себя.

«В линейке Aruba также представлены точки, самостоятельно устанавливающие защищенное соединение с центральным офисом, что удобно для связи с удаленными филиалами», — комментирует начальник отдела сетевых решений КОМПЛИТ Андрей Ковязин.

Точки доступа Aruba соответствуют стандарту 802.11ac Wave2, работают одновременно в диапазонах 2,4 и 5 ГГц и поддерживают технологию MIMO (Multiple Input Multiple Output), увеличивающую скорость передачи данных.

## Контроллеры для сети любого масштаба

В линейке контроллеров есть решения как для небольших офисов с поддержкой до 16 точек доступа, так и для крупных объектов с поддержкой до 2 тыс. точек и 32 тыс. клиентов.

---

*Dreamworks Animation увеличил покрытие сети с 60 до 100% на территории площадью более 16 тыс. кв. м. Беспроводная сеть с поддержкой личных устройств сотрудников в мультипликационной студии построена на базе контроллеров серии 7200 и точек доступа серии 320 внутри помещений, серии 270 снаружи и серии 205 для удаленных офисов.*

---

Контроллеры управляют аутентификацией, шифрованием, выступают в роли VPN-концентраторов, межсетевых экранов, используют технологию адаптивного управления радиочастотами ARM (Adaptive Radio Management), спектральный анализ RFPect и средства защиты от беспроводных атак.

## Коммутаторы с гарантией на всю жизнь

Коммутаторы Aruba имеют две важные особенности: они не требуют приобретения лицензий для расширения их функционала, и практически все модели обладают пожизненной гарантией, которая действует в России.

Линейка включает коммутаторы доступа с поддержкой 1-, 10- и 40-гигабитных портов Ethernet и коммутаторы ядра с поддержкой



широкого набора сетевых протоколов. На роль последних отлично подходят серии 5400R/8400 с поддержкой функционала Layer 3 и портами 10/40/100 Гбит/с.

Коммутаторы представлены в модульной и фиксированной конфигурации.

«Из коммутаторов фиксированной конфигурации можно отметить коммутатор Layer 3 серии 3810. В корпусе 1RU есть версии с 24 и 48 портами, поддерживающие Smart Rate Multi-gigabit Ethernet, с PoE и без, слотом для аплинк-модуля с интерфейсами SFP+ и QSFP+, а также коммутатор полностью SFP+. А расширенной поддержкой протоколов динамической маршрутизации IPv6 и MPLS отличается линейка FlexNetwork. Такие коммутаторы, например, мы использовали при построении сетевой инфраструктуры крупного склада в Московской области», — комментирует Андрей Ковязин.

### **AirWave: отслеживайте состояние сети**

AirWave — удобная в работе система для мониторинга сети, которая управляет проводной и беспроводной инфраструктурой, построенной как на оборудовании Aruba, так и на оборудовании других вендоров.

Благодаря централизованному и интуитивно понятному пользовательскому интерфейсу, AirWave дает возможность мониторить состояние сети в реальном времени, создавать отчеты и быстро устранять неполадки. Программа отслеживает охват сети с привязкой к карте местности, действия и трафик подключенных пользователей, позволяет выбирать конфигурацию существующих устройств и добавлять новые.

«Еще одна полезная функция — планировщик зоны покрытия сети Wi-Fi, — отмечает ведущий инженер отдела сетевых решений КОМПЛИТ Юрий Бельченко. — Имея планы помещения с информацией о размерах и применяемых материалах, с его помощью можно выбрать оптимальные места установки точек доступа и рассчитать зоны покрытия. Такое планирование обязательно проводится на начальном этапе любого проекта по внедрению Wi-Fi».

### **ClearPass: задавайте политики доступа**

ClearPass — программа для управления политиками доступа, в которой задаются параметры подключения и аутентификации пользователей в сети.

*Имея ограниченные ИТ-ресурсы, музей науки и искусства в Денвере построил легкоуправляемую сеть с высокими требованиями к безопасности, объединив имеющиеся мультивендорные ИТ-решения на базе платформы ClearPass.*

Возможности программы позволяют задать гибкие и максимально индивидуальные условия. Новый пользователь, например, может авторизоваться в сети, используя постоянный или разовый пароль, полученный у администратора или по SMS, пройти аутентификацию по сертификату или другим способом, удобным для владельца сети.

После авторизации для каждого пользователя настраиваются специальные условия доступа, учитывающие тип и состояние устройства, используемые протоколы, состояние устройства, принадлежность к определенной группе и т. д.

По словам Юрия Бельченко, способность определять тип и производителя устройства позволяет программе также работать со многими моделями принтеров и другими устройствами, не имеющими никаких средств аутентификации.

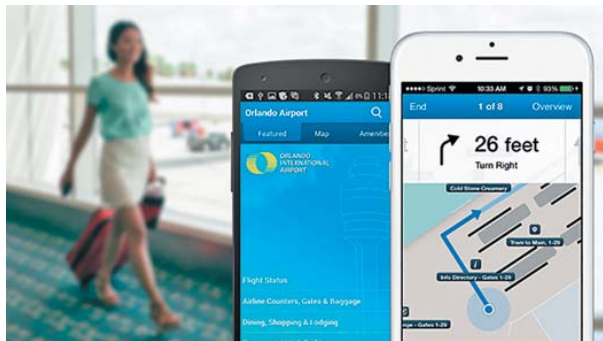
Кроме того, программа делает возможным использование личных устройств сотрудников для доступа к корпоративным ресурсам — реализует концепцию Bring Your Own Device (BYOD). Чтобы безопасность сети не нарушалась, новые аппаратные средства проходят тщательную проверку на наличие антивирусов и свежих обновлений.

### **Meridian: взаимодействуйте с аудиторией**

Программа Meridian создана для определения местоположения пользователей по данным из сети Wi-Fi, дополненной маячками Bluetooth Low Energy (BLE). Маячки позволяют устройству получить информацию о нахождении и через приложение запустить нужное действие. Например, предлагают получить скидочный купон в магазин неподалеку или воспользоваться аудиогидом в музее, где вы находитесь в данный момент.

*Крупнейшая библиотека университета Оклахомы в США площадью более 40 тыс. кв. м создала собственное приложение, с помощью которого пользователи легко могут найти нужные им материалы, план здания и путь до нужной точки. Приложение использует данные BLE-маячков и платформы Aruba Meridian.*

Само приложение создается компанией и публикуется в App Store либо Play Market.



Эти и другие решения Aruba вы всегда можете протестировать в демонстрационном центре КОМПЛИТ в Санкт-Петербурге, чтобы на практике убедиться, отвечает ли выбранный вариант задачам вашей организации.

Информация предоставлена платиновым партнером Hewlett Packard Enterprise — системным интегратором КОМПЛИТ.

[www.aruba.complete.ru](http://www.aruba.complete.ru)

Павел Колмычек,  
руководитель сети  
дата-центров компании  
«КРОК»



Даже в сложные для экономики страны годы рынок коммерческих ЦОДов устойчиво растет, при этом особенно впечатляют двухзначные цифры роста облачных сервисов. Как дальше будет развиваться этот рынок, какое влияние окажет на него внедрение элементов цифровой экономики, каковы перспективы строительства новых ЦОДов — эти и другие вопросы мы обсудили с Павлом Колмычком, руководителем сети дата-центров компании «КРОК».

Александр Барсков

# Павел Колмычек: российские заказчики используют потенциал облаков только на 10%

**Журнал сетевых решений/LAN:** Как бы вы оценили общую ситуацию в российской отрасли коммерческих ЦОДов? Какие факторы роста и факторы риска вы видите?

**Павел Колмычек:** Рынок коммерческих ЦОДов находится в достаточно зрелой фазе развития. Услуги уже сформированы, а стоимость сервисов достаточно стабильна; многие заказчики четко знают свои потребности и приходят к провайдерам с конкретными запросами. На мой взгляд, основной прирост в среднесрочной перспективе будет обеспечен главным образом за счет переноса серверов на коммерческие площадки в результате старения локальной инфраструктуры ЦОДов заказчиков. Кроме того, стоит отметить, что рынок продолжает консолидироваться и небольшие игроки в силу устаревания инфраструктуры ЦОДов будут вынуждены либо уходить с рынка, либо становиться реселлерами услуг более крупных и современных провайдеров. В ближайшие три-пять лет рост рынка колокейшн сохранится в пределах 10–15% в год.

**LAN:** Российский рынок услуг коммерческих ЦОДов составляет 1% от глобального, тогда как доля России в мировом ВВП (рассчитанная по паритету покупательной способности) — 3,17%. Как можно объяснить такую диспропорцию?

**Колмычек:** Во многом это связано с тем, что в России очень высока доля компаний с государственным участием: на них приходится примерно две трети экономики. Но они практически не пользуются услугами коммерческих ЦОДов. По моим оценкам, в структуре доходов коммерческих центров обработки данных на государственных заказчиков приходится не более 5%. На Западе ситуация иная: доля госпредприятий в экономике существенно ниже, при этом они гораздо шире пользуются ресурсами коммерческих ЦОДов.

Доля рынка услуг коммерческих ЦОДов может приблизиться к доле ВВП, когда завершатся работы по формированию законодательных актов, касающихся использования государственными организациями аутсорсинговых услуг, и они начнут активно сотрудничать с ЦОдами. Но на существующих игроках рынка коммерческих ЦОДов это может отразиться не сильно, так как госкомпании с высокой вероятностью будут задействовать ресурсы «Ростелекома», расширяющего свои площадки. Речь идет об инициативе по созданию гособлака и системы федеральных ЦОДов, которая сейчас находится на рассмотрении в правительстве.

Впрочем, определенные шансы получить проекты с госзаказчиками у существующих игроков, конечно, есть, с учетом их опыта, накопленной экспертизы, быстрого реагирования на запросы рынка, гибкости в плане внедрения инноваций. Эти факторы позволяют нам уверенно чувствовать себя на поле конкуренции с развивающимися государственными провайдерами услуг ЦОДов.

**LAN:** Как меняется или будет меняться спрос на услуги коммерческих ЦОДов в условиях цифровизации бизнеса все большего числа компаний и постепенного внедрения элементов цифровой экономики?

**Колмычек:** Цифровизация экономики, с одной стороны, открывает новые возможности для развития пула услуг ЦОДов, но с другой — соответствующие проекты заказчики предпочитают реализовывать своими силами. Взяв, например, блокчейн. Да, у нас уже есть проекты с конкретными банками по внедрению таких решений. Но пока большинство банков, причем даже не из первой десятки, предпочитают реализовывать такие проекты самостоятельно. На мой взгляд, это объясняется незрелостью самой технологии и отсутствием ее массового

проникновения на рынок. В то же время предприятия стали легче переносить в облако и в аутсорсинговые ЦОДы критическую инфраструктуру, чтобы снизить затраты и переложить риски на провайдеров услуг.

Полагаю, что цифровизация экономики сама по себе на отрасль коммерческих ЦОДов напрямую не повлияет. Скорее, влияние будет косвенным, его сейчас трудно оценить. Если цифровизация пойдет «рука об руку» с облачными вычислениями, то это позитивно скажется на рынке в целом и такие проекты будут стимулировать его рост. Но возможен и другой сценарий: цифровизация приведет к возвращению части сервисов из коммерческих ЦОДов в серверные комнаты самих заказчиков. По какому пути пойдет ИТ-отрасль, сказать пока сложно.

**LAN:** Ощущается ли дефицит площадей коммерческих ЦОДов в России и насколько активно будет происходить процесс строительства новых площадок?

**Колмычек:** Многие значительные проекты, которые воспринимаются сегодня как новые, на самом деле стартовали в 2012–2013 годы. О крупных проектах, которые начались после 2014 года, мне не известно. Причем какой-то нехватки стоек не ощущается. По ряду оценок, российские КЦОДы загружены не более чем на 70%. В любом заметном конкурсе всегда есть конкуренция, всегда есть три-пять игроков, которые готовы предоставить свои площади. С учетом предполагаемого роста экономики на 1–2% в год, имеющих площадей коммерческих ЦОДов будет достаточно еще на несколько лет.

Во многом благодаря крупным проектам, заложенным в 2012–2013 годы, на рынке практически сохранились рублевые цены, несмотря на существенное падение курса национальной валюты. Сейчас ситуация такова, что любому новому игроку выйти на рынок с предложением, в первую очередь по аренде площадей (колокейшн), затруднительно. Существующие цены не оправдают инвестиции в строительство нового коммерческого ЦОДа, поэтому мы практически и не видим новых проектов. Построить новый центр обработки данных и заполнить его за два-три года, конечно, можно, но вернуть инвестиции — маловероятно.

**LAN:** Но площади ЦОДов «КРОК» уже загружены более чем на 90%. Как вы

видите дальнейшее развитие бизнеса без строительства новых площадок?

**Колмычек:** На данный момент мы, как и отрасль коммерческих ЦОДов в целом, движемся в сторону облачных вычислений, услуг IaaS (Infrastructure as a Service), управляемых сервисов (Managed Services), сложных комплексных услуг «поверх» выделенных инфраструктур и облаков. И этот бизнес успешно растет.

**LAN:** Каковы доля отдельных сервисов в общем доходе и темп прироста по каждому сервису?

**Колмычек:** Услуги коммерческих ЦОДов занимают стабильную долю в общей выручке «КРОК», несмотря на замедление темпов роста российского рынка и снижение спроса на колокейшн. По итогам 2016 года рост по данной услуге сохранился на уровне 1% в годовом выражении. Выручка от облачных сервисов по результатам 2016 года увеличилась на 43%. Основным драйвером здесь остается аренда инфраструктуры (IaaS) с двойным SLA, гарантирующим доступность серверов и производительность дисков на уровне 99,9%. Суммарный рост выручки по услугам ЦОДов составил 14,4%. На сегодняшний день в сети аутсорсинговых центров обработки данных «КРОК» резервируют инфраструктуру свыше 150 крупных российских и международных компаний, в числе которых крупнейшие банки, розничные сети, операторы связи.

Как я уже сказал, акцент смещается в сторону управляемых сервисов. Ввиду увеличения спроса на управляемые услуги мы предоставляем нашим заказчикам комплексный мониторинг инфраструктуры, администрирование аппаратного обеспечения ЦОДа, поддержку резервных площадок заказчиков или комплексное обслуживание оборудования командой инженеров коммерческого ЦОДа в рамках услуги по эффективному управлению ИТ-инфраструктурой (Managed Infrastructure). Это характерно как для существующих долгосрочных проектов, так и для проектов с новыми заказчиками.

**LAN:** Можете привести примеры сложных комплексных услуг, предлагаемых на базе вашей сети ЦОДов?

**Колмычек:** Показателен пример интернет-магазинов. Некоторые из них покупают у нас «простой» IaaS и используют собственную команду системных администраторов. Но все больше заказчиков в данном сегменте предпочитают передать ИТ-инфраструктуру на аутсорсинг более профессиональной команде специалистов «КРОК». Мы занимаемся всем, включая администрирование сети,

Если цифровизация пойдет «рука об руку» с облачными вычислениями, то это позитивно скажется на рынке в целом и такие проекты будут стимулировать его рост.

сервисов безопасности и обновлений, обслуживание всей инфраструктуры и баз данных, отслеживание загрузки дисков и пр. Для развития управляемых услуг мы ведем собственные разработки: например, у нас есть услуга «Мониторинг аппаратных компонентов ЦОДа на базе открытого ПО Zabbix», которая успешно заменяет дорогостоящие вендорские инструменты. Уже есть несколько заказчиков как раз из сферы торговли, активно пользующихся нашим сервисом.

Другой пример — миграция прикладных систем из зарубежных ЦОДов, например, для соблюдения законодательства о персональных данных. Был показательный случай, когда заказчик 31 сентября 2015 года в шесть вечера «погасил» свои сервисы за рубежом, а через сутки «поднял» их в ЦОДе «КРОК» (ситуация позволяла безболезненно отключить сервисы на сутки). Заказчик выбирал площадку с возможностью обеспечить вычислительными ресурсами весь проект в комплексе, причем он хотел получить не только ИТ-инфраструктуру (серверы, сеть, СХД), но и резервирование, сервисы безопасности, администрирование баз данных и т. д. На тот момент (начало 2015 года) это было вызовом для рынка коммерческих ЦОДов, поскольку мало кто мог выполнить все эти условия на высоком уровне. Нам, с учетом большого интеграторского опыта и широкой экспертизы в бесшовной миграции ИТ-систем, удалось решить все задачи заказчика в короткий срок.

**LAN:** В чем, на ваш взгляд, причина роста интереса к услугам аренды оборудования — HaaS?



**Колмычек:** Основная причина — это, конечно, экономия средств. Если сравнивать общую стоимость владения (ТСО) за длительный период, то стоимость облачных ресурсов может оказаться дороже затрат на покупку и обслуживание оборудования. Это обусловлено значительным объемом ПО и трудозатрат, необходимых для превращения «железа» в управляемый сервис. Поэтому облако лучше подходит для задач, ограниченных во времени или предполагающих четкие пики нагрузок. Например, в онлайн-ритейле это дни распродаж и акций, а в банковском секторе — праздничные дни, во время которых в несколько раз возрастает количество транзакций. В такие моменты облако придает инфраструктуре дополнительную эластичность, расширяя ее возможности без капитальных затрат.

**Проблема в том, что в России очень немного специалистов, которые умеют делать такие системы. Немного даже тех, кто знает, что так можно делать.**

Помимо этого, вариант с арендой по модели *НaaS* нередко оказывается выгоднее, чем покупка собственного оборудования, — экономия может составить от 5% на коротких до 15–20% на длинных сроках расчета ТСО за период три-пять лет.

**LAN:** Я правильно понял, что *НaaS* по деньгам выгоднее виртуальной инфраструктуры?

**Колмычек:** *НaaS* окажется выгоднее, если заказчик готов взять вычислительное оборудование в аренду на три-пять лет, например, под сервер для электронной почты — сервис, потребность в котором практически не будет меняться. Тогда он действительно может получить цены в два раза ниже, чем при покупке соответствующих ресурсов в облаке. Но если ему нужна инфраструктура, скажем, под интернет-магазин, нагрузка на который в преддверии 23 февраля и 8 марта вырастает в три раза, то выделенное оборудование окажется существенно дороже, чем облако.

*НaaS* прекрасно вписывается в модель финансирования вендоров, и мы сотрудничаем со многими из них в этом направлении, например с Dell EMC. Эта компания предлагает гибкую систему финансирования комплексных решений

в одном пакете: оборудование, программное обеспечение и услуги. Это позволяет не только экономить, но и эффективно управлять ресурсами и развертывать готовые инфраструктуры без проводов, например, на базе производительных вычислительных комплексов из семейства гиперконвергентных решений Dell EMC VxRail.

К сожалению, российские заказчики задействуют только 10% потенциала облаков. Большинство внедрений — это стандартные инфраструктуры на базе ПО VMware. И заказчики часто используют такие облака так же, как они использо-

вали бы кластер VMware, установленный в своей серверной комнате. А ведь облако — это не просто вычислительные мощности, вынесенные в ЦОД, это не просто «VMware поверх серверов». Облако — это удобная консоль управления, высокий уровень автоматизации, выгодный бил-

линг, интерфейсы API для интеграции с другими системами и много чего еще. Например, публичное облако «КРОК» имеет свой API, максимально приближенный к Amazon Web Services. Это позволяет использовать широкий перечень ПО автоматизации и управления облачными инфраструктурами, доступный в отрасли. Благодаря этому международные заказчики могут легко переносить в наше облако компоненты инфраструктуры и данные, используя привычные инструменты, а российские — получать дополнительную экономию от миграции в облако.

Вместе с тем радует, что появляются заказчики, которые переходят к модели использования облака, максимально задействующей его возможности. Пример — система одного из наших заказчиков, торговой сети Castorama, реализованная с высокой долей автоматизации. Чтобы запустить дополнительный сервер, им не нужен администратор, все создается автоматически в облаке: поднимается виртуальная машина, синхронизируется с базой данных, включается в кластер, подключается к балансировщику нагрузки и т. д. Кроме того, в системе реализован мониторинг нагрузки: при ее снижении часть серверов автоматически отключается, а при

увеличении — подключаются дополнительные. Очевидно, что такая облачная система существенно выгоднее содержания собственного «железа».

Проблема в том, что в России очень немного специалистов, которые умеют делать такие системы. Немного даже тех, кто знает, что так можно делать. У «КРОК» накоплена большая экспертиза по реализации подобных проектов, и это одно из наших конкурентных преимуществ. В целом облачный рынок может вырасти на порядок, когда начнут массово реализовываться проекты, подобные описанному выше.

**LAN:** Какие вы видите основные драйверы развития российской отрасли коммерческих ЦОДов?

**Колмычек:** Как я уже говорил, рынок находится в зрелой фазе, когда уже решены основные проблемы и вряд ли появятся факторы, ведущие к бурному росту. Структура портфеля услуг, предоставляемых на базе коммерческих ЦОДов, будет меняться в сторону увеличения доли облачных управляемых сервисов, что позволит заказчикам расширить возможности собственной ИТ-инфраструктуры за счет более гибкой арендной модели. Наряду с этим спрос на аутсорсинг ЦОДа и облака стимулируется законодательными требованиями в области регулирования персональных данных и импортозамещения. В этом случае переезд на аутсорсинговую площадку или миграция инфраструктуры в облако становятся в глазах заказчиков не только привлекательными сценариями снижения издержек, но и способом более взвешенного управления рисками в области обеспечения непрерывности бизнеса.

Основной драйвер — это, конечно, развитие дополнительных сервисов, таких как облачные вычисления и управляемые услуги. С точки зрения бизнеса использование коммерческих ЦОДов позволяет наращивать оборот быстрее, чем обращение к услуге колокейшн, но требует наличия серьезной экспертизы. Существующие на рынке кризисные явления не мешают, а иногда даже помогают развитию этой тенденции, которая на ближайшие два-три года станет доминирующей. Что касается существенного роста продаж стойко-мест, то он возможен только при увеличении темпов развития экономики страны в целом. **LAN**

Рустэм Хайретдинов,  
генеральный директор  
компании «Атак Киллер»



## Автоматизированные системы защиты: плюсы и минусы

Для некоторых процессов удалось радикально повысить точность определения атак, причем настолько, что достигнутая точность превысила показатели человека.

Процессы легко автоматизируются, когда они однозначны и повторяемы. Вспомните благословенные антивирусы — их надо было только установить, остальное они делали сами: скачивали обновления баз данных, определяли и блокировали вирусы, иногда запрашивая подтверждение (скажем честно, не из-за того, что сомневались, удалять вирус или нет, а чтобы напомнить: мы есть, мы бдим, не забудь вовремя заплатить за продление подписки).

Определения вирусов, сигнатуры атак и другие простые методы защиты работали безотказно до тех пор, пока атаки не стали персонифицированными. Иначе говоря, злоумышленники стали учитывать особенности конкретного объекта защиты и саму систему защиты. Выявлять вирусы и атаки с помощью уже известных образцов теперь удавалось не всегда, что вынудило прибегнуть к гораздо менее точному способу — поведенческому анализу: ни на один известный вирус это не похоже, но ведет оно себя как вирус. Первые системы такого рода вызвали протесты пользователей: количество ложных срабатываний по сравнению со старыми технологиями было неприемлемым, пользователю приходилось постоянно отвлекаться от работы, чтобы разбираться с сообщениями антивируса.

Постепенно все сошлись на том, что ради защиты придется смириться с ложными срабатываниями, но отличить ложную тревогу от реальной атаки может не каждый. Так появились профессиональные операторы систем защиты, которые анализировали сообщения систем безопасности и разрешали коллизии. «Системы защиты» — устоявшийся, но неправильный термин, ведь по сути речь идет о системах мониторинга, поскольку такая система лишь сообщает оператору о подозрительной активности, а те или иные меры принимает человек,

от квалификации которого во многом зависят их эффективность.

Защита еще более осложнилась с повсеместным внедрением методологий гибкой (agile) разработки, для которой характерны частые, многочисленные и небольшие изменения защищаемой системы, а также замена подробной документации на приложение с использованием поверхностных «userstories». Каждое изменение порождает поведенческие аномалии, о которых система защиты сообщает как о подозрительной активности. Их очень много, без знания особенностей (документации) защищаемой системы справиться с ними невозможно и остается только наращивать штат операторов. Дефицит таких специалистов привел к процветанию аутсорсинга по обработке подозрительных аномалий (это называется «обработка инцидентов», однако реальными инцидентами оказываются менее 5% из них, все остальное — ложные срабатывания).

Автоматизация бизнес-процессов — отличный способ сэкономить, поэтому банки, розничные торговцы, телеком-операторы и даже государственные органы стараются как можно быстрее внедрить такие решения. Очевидно, что при росте количества и сложности автоматизированных бизнес-систем потребность в операторах с опытом использования средств мониторинга активности растет даже быстрее, чем потребность в собственно «автоматизаторах». Поэтому идея автоматизировать труд операторов систем мониторинга не могла не найти отклика в душе тех, кто оплачивает все это, с болью наблюдая, как растет сложность защиты.

Попытки заменить человека в непростой роли оператора, где приходится не просто реагировать на аномальную активность, а разбираться в запутанных процессах

бизнес-приложений и инфраструктуры, на которой они развернуты, предпринимались постоянно, но в большинстве случаев удавалось лишь сделать более удобным для оператора процесс анализа аномалий. Поручить машине принимать окончательное решение, как было с антивирусами в старые добрые времена, никто не решался.

В последние годы произошло сразу два прорыва: выросла вычислительная мощность и появились алгоритмы машинного обучения, — благодаря чему для некоторых процессов удалось радикально повысить точность определения атак, причем настолько, что достигнутая точность превысила показатели человека. Снова стало возможно делегировать принятие решений машине. Уже появились автоматизированные системы, способные работать в режиме не мониторинга, а именно блокирования атак, что позволяет сократить нагрузку на людей, для чего изначально и создавались вычислительные системы.

Не стоит сегодня преувеличивать возможности искусственного интеллекта, особенно в области систем защиты. Точность его выводов пока недостаточна для большинства процессов защиты, однако, например, защиту Web-приложения уже можно смело доверять машине, справляющейся с работой лучше, чем средней руки специалист, и, уж конечно, более выносливой и неутомимой. По мере накопления данных об атаках, совершенствования алгоритмов обучения и роста вычислительной мощности будут автоматизироваться и другие системы защиты. Человек станет заниматься творческой деятельностью: обучать искусственный интеллект, изучать новые алгоритмы атак, вести расследования и выполнять другие интересные задачи, где интеллект важнее скорости, производительности и безошибочности. **LAN**

# КОМПЛЕКСНЫЕ РЕШЕНИЯ ДЛЯ ЦОД НА БАЗЕ ПРОДУКЦИИ «ИМПУЛЬС»

*Быстрое развитие облачных вычислений и мобильных интернет-бизнесов, рост требуемых вычислительных мощностей, повышение плотности ИТ-оборудования и рост энергопотребления вызывают множество проблем для традиционных центров обработки данных (ЦОД). Чтобы соответствовать будущим требованиям облачных вычислений и виртуализации, повысить эффективность ЦОД и контролировать стоимость инвестиций, ЦРИ «ИМПУЛЬС» представляет решения «всё в одном». Они основаны на универсальной, энергоэффективной, модульной архитектуре, которая позволяет заказчикам осуществлять быстрое развертывание, гибкое расширение и простую эксплуатацию ЦОД, а также удобное управление этими объектами.*

Ключевые характеристики решений:

- **Быстрое развертывание.** Модульная структура, стандартизация интерфейсов, заводская предустановка, быстрая установка на месте будущей эксплуатации.
- **Энергоэффективность.** Модульный ИБП с высоким КПД, прецизионная система охлаждения, термоизоляция от окружающего пространства (единая гермозона для установки ИТ-оборудования и ИБП).
- **Экономическая эффективность.** Низкие затраты на построение, содержание и обслуживание, низкие проектные затраты.
- **Комплексное обслуживание.** Единое решение, которое включает ключевое оборудование для построения основных подсистем, услуги по установке и послепродажное обслуживание.

ЦРИ «ИМПУЛЬС» предлагает два вида интегрированных решений для ЦОД разных размеров.

## РЕШЕНИЕ ПО ОРГАНИЗАЦИИ ИНТЕГРИРОВАННОГО БЛОКА ДЛЯ МИКРОЦОД (ИБЦОД)

ИБЦОД содержит стойки для размещения ИТ-оборудования, системы мониторинга и электропитания, аккумуляторные батареи, рядную систему распределения воздушных потоков и другие инфраструктурные подсистемы.



Модульные компоненты системы ИБЦОД, соответствующие всем международным стандартам, могут быть полностью развернуты и настроены в течение одного дня, что значительно сократит расходы бизнеса на этапе установки. Размещение системы кондиционирования в одном ряду с источниками тепла обеспечивает эффективное распределение воздушных потоков, а полностью закрытая конструкция и разделение горячих и холодных воздушных потоков значительно снижают потребление электроэнергии. Этому же способствует использование модульного ИБП с высоким КПД.

Система централизованного мониторинга с локальным дисплеем позволяет отслеживать температуру и уровень влажности, состояние средств электроснабжения, а также других подсистем. Возможность круглосуточного удаленного мониторинга состояния систем и загрузки оборудования минимизирует затраты на обслуживание, ремонт оборудования и потери от внеплановых простоев.

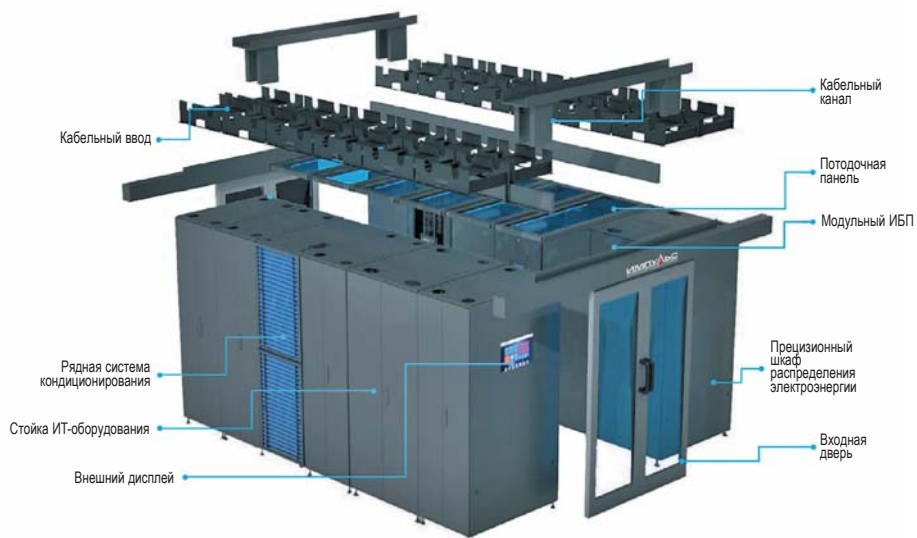
Закрытая микросреда обеспечивает эффективную шумоизоляцию, полную защиту от попадания пыли и грязи, что значительно снижает частоту отказов ИТ-оборудования и продлевает жизненный цикл ИТ-системы в целом. Решение оснащено многоступенчатыми средствами автоматической сигнализации, а также автоматического запуска системы пожаротушения. Мониторинг состояния всех компонентов системы осуществляется в режиме реального времени.

## РЕШЕНИЕ ПО ОРГАНИЗАЦИИ ИНТЕГРИРОВАННОГО МОДУЛЯ ДЛЯ МАЛЫХ И СРЕДНИХ ЦОДОВ (ИМЦОД)

Решение ИМЦОД включает в себя стойки для установки ИТ-оборудования, системы бесперебойного электропитания, распределения электроэнергии, охлаждения, мониторинга и структурированную кабельную систему (СКС). Благодаря подходу «всё в одном», ИМЦОД обеспечивает быстрое развертывание, высокую энергоэффективность, интеллектуальное управление, безопасность и надежность.

Система ИБП размещена в шкафу 19", который идентичен шкафам с ИТ-оборудованием, и оснащена независимой системой контроля, благодаря которой неисправный модуль может быть отключен автоматически. Мощность ИБП масштабируется от 20 до 520 кВА, его КПД составляет 95%, в экорезиме — 98%. Модуль прецизионной системы распределения мощности установлен в таком же шкафу. Он обеспечивает мониторинг напряжения, обеспечивает звуковое и световое оповещение при пропадании питания. Среди опций: функция ЕРО (отключение





электропитания в аварийной ситуации) и выходной автоматический выключатель с горячей заменой. По протоколу связи Modbus можно легко подключить ИБП к внешней системе мониторинга и анализа энергопотребления.

В ИМЦОД используются шкафы, передняя и задняя двери которых имеют сотовую шестиугольную перфорацию, площадь воздухопотока составляет 75% от площади дверей. Благодаря использованию качественной холоднокатаной стали и крепкой

рамы, статическая несущая нагрузка шкафа составляет 1300 кг. Шкафы разных размеров прекрасно совместимы с системой разделения воздушных потоков.

В решении применяется рядная система кондиционирования с разделением горячего и холодного воздушных потоков, что значительно повышает эффективность системы в целом. Может применяться как воздушное, так и водяное охлаждение с применением чиллера, холодопроизводительность системы от 20 до 60 кВт. Плотность мощности ИТ-оборудования может достигать 15 кВт на стойку.

Для повышения энергоэффективности используется сочетание технологий и решений: частотно-регулируемый компрессор, ЕС-вентилятор, электронный расширительный клапан, наружный блок с бесступенчатым регулированием скорости вращения и т. д. Когда температура внешней окружающей среды становится ниже температуры в помещениях, компрессор может быть выключен и хладагент будет охлаждаться за счет циркуляции через внешний блок. При этом применяется энергосберегающая технология адиабатического охлаждения: на теплообменник наружного блока распыляется вода, разделенная на маленькие капли до состояния водяного облака; при испарении вода поглощает большое количество тепла.

Система мониторинга обеспечивает контроль за всеми системами, входящими в состав ИМЦОД, включая систему распределения электропитания, ИБП, кондиционирования, отслеживания протечек, контроля доступа, видеонаблюдения и пр. Она также собирает данные с различных датчиков, включая датчики дыма и температуры.

Использование ПО моделирования воздушных потоков в ЦОДе помогает прогнозировать температуру в помещении, траекторию воздушных потоков и охлаждающий эффект, позволяет избежать потерь холодопроизводительности и появления точек перегрева, а также обеспечить наилучшую схему размещения оборудования в ЦОДе.

Инжиниринговая компания «ЦРИ «ИМПУЛЬС»» — российский разработчик и поставщик комплексных решений по защите электропитания ответственных потребителей. Компания имеет техническую поддержку и экспертизу для подбора оборудования с возможностью выезда к заказчику. Располагает производственными площадками в России, Китае и Турции, а также собственным центром разработок, в котором трудятся выпускники ведущих российских и иностранных технических вузов.

### НОВИНКА! РОССИЙСКИЙ ИБП «ИМПУЛЬС» СЕРИИ ФРИСТАЙЛ 11

Инжиниринговая компания ЦРИ «ИМПУЛЬС» завершила разработку универсального источника бесперебойного питания для стоечного и напольного размещения серии ФРИСТАЙЛ 11. Этот ИБП предназначен для бесперебойного электропитания ответственной нагрузки с высокой плотностью мощности: серверного и сетевого оборудования, концентраторов телекоммуникационных сетей, сетей голосовой связи и передачи данных, систем пожарной сигнализации и видеонаблюдения, промышленного оборудования, организации дежурного освещения и пр.

Источник защиты электропитания ФРИСТАЙЛ 11 будет доступен в нескольких исполнениях. Модель ФРИСТАЙЛ 11-1 рассчитана на мощность 1 кВА, ФРИСТАЙЛ 11-2 — 2 кВА, ФРИСТАЙЛ 11-3 — 3кВА.

Среди преимуществ ИБП ФРИСТАЙЛ 11:

- универсальный корпус,
- удаленное администрирование,
- возможность замены встроенных АКБ в «горячем» режиме,
- масштабируемое время автономной работы,
- двойное преобразование (топология онлайн),
- функция сегментирования нагрузки.



# Как выбрать КЦОД

Исследование, проведенное аналитической группой OSP Data, позволило выявить основные критерии выбора коммерческого ЦОДа для аренды площадей под ИТ-оборудование, покупки виртуальной ИТ-инфраструктуры или получения других сервисов.

**Александр Барсков,**  
ведущий редактор «Журнала сетевых решений/LAN»



Прежде чем говорить о выборе коммерческого ЦОДа, остановимся на извечном вопросе: строить или арендовать? Столкнувшись с этой дилеммой, все больше компаний предпочитают второй вариант. Так, если в 2010 году, согласно исследованию, проведенному Headwork Analytics совместно с «Журналом сетевых решений/LAN», лишь 18% компаний в России прибегали к услугам КЦОДов, то в 2017 году, по данным OSP Data, их стало уже 50% (см. рис. 1).

Соответственно, сокращается доля компаний, которые предпочитают обеспечивать все свои ИТ-потребности на базе собственных площадок. Если в 2013 году половина компаний ориентировалась исключительно на собственные ЦОДы, то в текущем году таковых осталось всего 19% (см. рис. 2).

Рост числа заказчиков услуг КЦОДов объясняется многими причинами. В первую очередь это связано с тем, что компании осознали экономические преимущества модели аутсорсинга, позволяющей оперативно и эффективно решать ИТ-задачи без существенных капитальных затрат (CAPEX). В то же время российский рынок КЦОДов, по крайней мере в Москве и Санкт-Петербурге, можно характеризовать как хорошо развитый. В двух столицах находится немало современных площадок, отвечающих требованиям к отказоустойчивости Tier III.

Если говорить о тройке отраслей, наиболее активно пользующихся услугами КЦОДов, то это финансовые организации (63% используют услуги КЦОДов), промышленность (56%) и ретейл (50%). Среди других отраслей отметим высокий уровень потребления услуг КЦОДов компаниями ТЭК, транспортными и логистическими, а также занятыми в индустрии развлечений, туризма и спорта. На другом полюсе (мало используют КЦОДы) — государственные организации, образовательные и научные учреждения.

Собственные ЦОДы прежде всего строят крупные предприятия и организации, такие, например, как Сбербанк, «Росатом», ВТБ и пр. Приоритет созданию таких площадок для своих нужд отдают государственные структуры, а также организации, имеющие дело с государственной тайной. Кроме того, тяготение к своему ЦОДУ испытывают

компании с большим числом ИТ-стоек. Если число стоек превышает сотню, то всегда имеет смысл изучить вопрос организации собственной площадки.

Правда, надо ясно понимать, что даже при использовании предварительно собранных и протестированных на заводах комплексов (так называемых префабов — от prefabricated) понадобится немало времени для построения своего ЦОДа — полгода и более. Такой проект потребует серьезных капитальных вложений (CAPEX). Наконец, необходимо иметь в наличии (или быть готовым создать) квалифицированную команду для поддержки ЦОДа. И если ИТ-специалисты есть практически в любой серьезной организации, то команду профессионалов по обслуживанию инженерной инфраструктуры (энергетика, кондиционирование и т. д.), возможно, придется собирать с нуля.

К категории предприятий, которые, как правило, обращаются к услугам коммерческих ЦОДов, относятся компании, у которых просто нет времени и средств (CAPEX) на создание своего ИТ-объекта, например различные стартапы. Еще одна очевидная категория клиентов КЦОДов — компании с временными проектами, которым требуются значительные ИТ-мощности. Такие проекты могут быть связаны, например, с обслуживанием больших спортивных мероприятий (Олимпиада, чемпионат мира по футболу). Создавать свою ИТ-инфраструктуру для таких проектов нецелесообразно. Если компании сложно прогнозировать развитие своих ИТ-потребностей, то ей тоже прямая дорога в КЦОД, где можно добавлять ресурсы по мере необходимости. На рынке есть примеры, когда крупные предприятия строят свои ЦОДы с запасом ресурсов на 20 лет, изначально заполняя их лишь на 20–30%, но это сложно назвать экономически оправданным решением.

Вывод ИТ в коммерческие ЦОДы и в облака — это в первую очередь более выгодная экономическая модель получения необходимых сервисов. Поэтому вопрос стоимости всегда был, есть и будет в числе ключевых для заказчиков. Согласно данным исследования, проведенного OSP Data в 2014 году, примерно каждая пятая компания не обращалась к услугам КЦОДов именно по причине их высокой стоимости. А среди

пользователей таких услуг каждый третий жаловался на их дороговизну.

В рейтинге 2017 года стоимость сервиса — в тройке ключевых критериев при выборе площадки, однако не на первом месте. Более важными для заказчиков оказались оперативность получения сервисов и эффективность системы безопасности (см. рис. 3). Собственно, эластичность и оперативность получения сервисов — это ключевые преимущества ИТ-аутсорсинга. По мере того как бизнес становится все более динамичным, а рыночные условия все более изменчивыми, значимость данного критерия только растет.

Очевидно, что оперативность получения сервисов во многом определяется возможностью практически в онлайн-режиме подключать или отключать нужные ресурсы в виртуализированной ИТ-инфраструктуре. Но в этом контексте не следует забывать и о физических процессах, если заказчик размещает в ЦОДе свое оборудование или обслуживает арендованные системы своими силами. Так, при выборе ЦОДа нелишне выяснить возможность круглосуточного доступа к своему оборудованию, а также разгрузки и установки новых устройств. Это обеспечивают далеко не все коммерческие ЦОДы, на ряде объектов операции погрузки/разгрузки могут проводиться только в будние дни и в рабочие часы.

На оперативность добавления дополнительных физических серверов и выполнения других операций, требующих присутствия в ЦОДе, существенно влияет место расположения площадки. У многих заказчиков существует убеждение, что коммерческий ЦОД должен находиться в пределах МКАД и в шаговой доступности от метро, чтобы персонал мог в любое время и без проблем до него добраться. Неудивительно, что большинство российских центров обработки данных сконцентрировано в двух столицах. Однако высокая стоимость аренды земли и дороговизна электричества негативно влияют на стоимость услуг КЦОДов. Кроме того, концентрация КЦОДов в двух городах препятствует тому, чтобы их услугами пользовались компании с головными офисами в регионах. Их отталкивает необходимость дорогостоящей и технически сложной миграции ИТ-ресурсов в одну из столиц, а также их



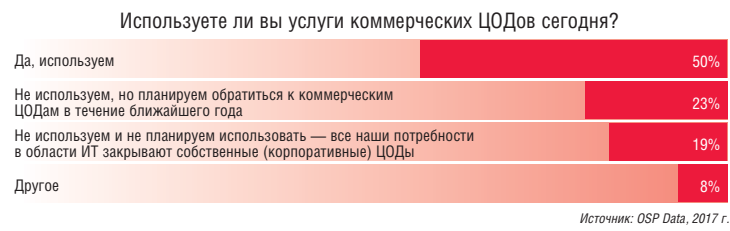


Рис. 1. Спрос на услуги КЦОДов по данным на начало 2017 года

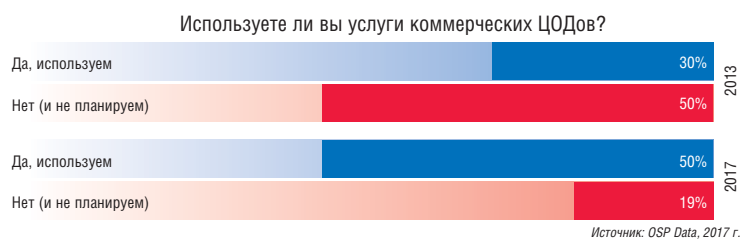


Рис. 2. Доли компаний, использующих услуги КЦОДов, и тех, кто решает все свои ИТ-задачи на собственных площадках

удаленность от основных производственных мощностей.

При анализе стоимости, помимо сравнения прайс-листов, необходимо учитывать массу факторов. Например, возможна ли постоплата (и на каких условиях) или обязательна предоплата? Какой уровень доступности ресурсов гарантируется в SLA, какие там указаны метрики качества сервиса и какова финансовая ответственность провайдера в случае нарушений? Каков временной «квант» оплаты используемых ресурсов: поминутный, почасовой, посуточный — либо провайдер практикует месячную оплату? Отдельный важный момент — необходимость и размеры одноразовых (инсталляционных) платежей и оплата дополнительных сервисов. Неприятным сюрпризом может оказаться для заказчика то, например, что плата за кроссировку от его стойки до шкафа оператора связи

окажется сопоставимой со стоимостью ее месячной аренды.

Сегодня практически все основные КЦОДы позиционируют себя как carrier neutral, то есть как не привязанные к конкретным операторам связи. В своих рекламных материалах они любят хвалиться числом операторов, присутствующих на их площадке, — 20, 30, 40... Однако заказчика чаще всего интересует не общее число операторов на площадке, а наличие возможности подключения к нужному ему. И если его не окажется в списке, а по другим критериям КЦОД вам подходит, то важно убедиться в возможности быстро и с минимальными затратами организовать нужное подключение.

Возможные проблемы, связанные с безопасностью, всегда были главным препятствием на пути прихода заказчиков

в КЦОДы. По данным 2014 года, примерно треть компаний отказались от использования услуг КЦОДов именно из-за опасений, связанных с безопасностью. При этом среди компаний, воспользовавшихся услугами КЦОДов, только 15% пожаловались на отсутствие должных средств информационной и/или физической безопасности.

При оценке эффективности физической безопасности необходимо учитывать массу вещей: надежный периметр безопасности, наличие видеонаблюдения, глубину хранения информации, как организована пропускная система и т. д. и т. п. Автор посетил около двух десятков различных ЦОДов в России и за рубежом. В некоторые было невозможно попасть даже при малейшем расхождении в написании имени на английском языке в паспорте и списке, имеющемся в службе охраны. При этом даже при-

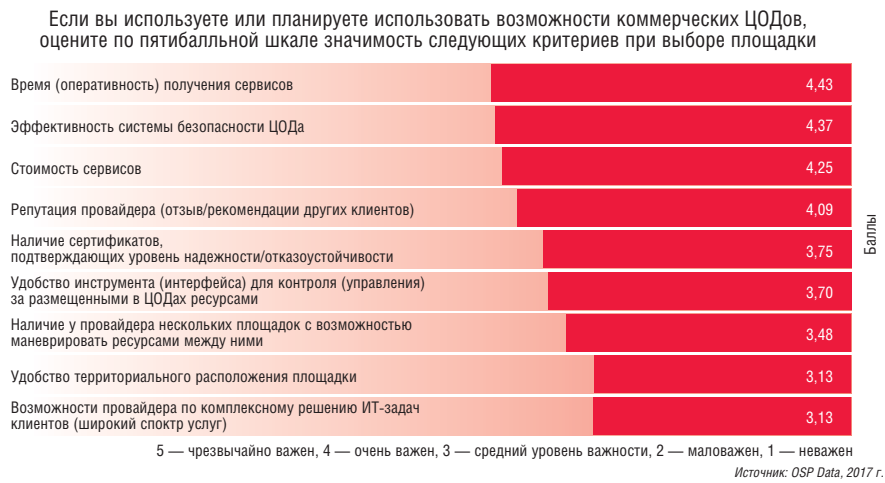


Рис. 3. Значимость различных критериев выбора КЦОДа

существование топ-менеджера ЦОДа, подтверждавшего личность посетителя, не помогало. В других же, особенно в российских, группы журналистов проходят на экскурсии в работающие залы даже без проверки документов. Чем чреват неосторожный разворот с рюкзаком за плечами вблизи важной стойки... ну вы понимаете.

Для многих заказчиков традиционно важно наличие у КЦОДа сертификата, подтверждающего уровень его надежности и отказоустойчивости. В первую очередь речь идет о сертификате Tier III организации Uptime Institute. На данный момент сертификаты Tier III на уже построенный объект в России имеют пять КЦОДов. Однако для многих заказчиков репутация провайдера, подтвержденная отзывами и рекомендациями других клиентов, важнее наличия сертификата. Как долго компания на рынке, кто ее основатели и владельцы, кто ее клиенты? Всегда имеет смысл побеседовать с теми, кто уже пользуется услугами данного ЦОДа. Их мнение может оказаться чрезвычайно важным.

Уровень Tier во многом определяет отказоустойчивость конкретного объекта. Но не будет лишним, конечно, напроситься на экскурсию по местам размещения основных элементов инженерной инфраструктуры. ИБП, аккумуляторы, дизель-генераторы, кондиционеры, чиллеры, система пожаротушения... Хороший специалист может на месте оценить состояние оборудования, качество его установки, профессионализм обслуживания. Существенно повысить отказоустойчивость предлагаемых сервисов и обеспечить их катастрофоустойчивость позволяет наличие у провайдера нескольких территориально разнесенных площадок с возможностью маневрировать ресурсами между ними. Этот критерий также чрезвычайно важен при выборе поставщика услуг.

Если ваша компания намерена активно развивать свой бизнес и планирует существенно расширять ИТ-инфраструктуру, то важно убедиться в наличии у выбранного провайдера свободных стойко-мест. По оценкам OSP Data, средняя загрузка российских КЦОДов составляет около 70%. Это немного по сравнению, скажем, с США, где этот показатель превышает 95%. Однако целый ряд ведущих российских КЦОДов загружены более чем на 90%. И если вы собираетесь прибавлять по 5–10 стоек каждые полгода, то эти варианты лучше отклонить — рост вашего бизнеса не должен сдерживаться ограничениями выбранного КЦОДа.

На последнем месте в списке критериев, предложенных экспертами OSP Data, оказались возможности провайдера по комплексному решению задачи клиента. Скорее всего, это связано с тем, что российские заказчики традиционно предпочитают потреблять услуги колокейшн, то есть арендовать площади или стойки для установки своего ИТ-оборудования. Однако рыночные тенденции таковы, что расширение экспертизы провайдера и предложение им комплексных услуг неизбежно будут пользоваться все большим спросом. Такие провайдеры способны предложить услугу «одного окна», полностью отвечая за переезд, размещение, интеграцию и обслуживание ИТ-систем заказчика. Наличие широкой экспертизы дает очевидные преимущества при реализации сложных проектов и организации гибридных схем, когда используются собственная площадка заказчика, КЦОД, а также публичные облака. **LAN**

**itk**

## РОССИЙСКИЙ ПРОИЗВОДИТЕЛЬ ТЕЛЕКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ



- Стабильно высокое качество
- Точное соответствие российским и мировым стандартам
- Доступное ценовое предложение

ГРУППА КОМПАНИЙ ИЕК  
Тел.: (495) 542-22-24  
e-mail: [info@itk-group.ru](mailto:info@itk-group.ru)

[www.itk-group.ru](http://www.itk-group.ru)

# Инженерная инфраструктура в комплексе. Часть I

В последнее время все чаще приходится слышать термин «моновендорный ЦОД». Речь идет об объекте, инженерная инфраструктура которого построена на базе продуктов одного производителя. Преимущества такого подхода: отличная согласованность различных компонентов, единый сервисный контракт, отсутствие спорных ситуаций, когда один вендор обвиняет в возникших проблемах другого, и т. д. При этом существует мнение, что на рынке всего два-три вендора способны предложить сразу все основные системы инженерной инфраструктуры. Так ли это на самом деле?

**Александр Барсков,**  
ведущий редактор «Журнала сетевых решений/LAN»



Фото: Александр Барсков



Фото: Александр Барсков



Фото: Александр Барсков



Фото: Александр Барсков



Фото: Александр Барсков



«Журнал сетевых решений/LAN» проанализировал портфель продуктов основных игроков с точки зрения их способности предложить целостное решение для построения инженерной инфраструктуры. В этом материале мы представляем обзор предложений компаний Conteg, Delta Electronics, Eaton и Schneider Electric. О решениях других производителей — в одном из ближайших номеров журнала.

## МОНО ИЛИ МУЛЬТИ

Большинство экспертов из компаний-производителей однозначно выступают в пользу моновендорного подхода, что, в общем, неудивительно.

К многочисленным преимуществам такого подхода Алексей Бурочкин, директор по маркетингу Eaton, в первую очередь относит крайне низкий риск несовместимости используемых компонентов. Это заметно упрощает и ускоряет процесс установки оборудования и ввода ЦОДа в эксплуатацию. Он также говорит о гибкости решений, параметры, состав и компоненты которых могут быть изменены производителем с учетом требований и задач конкретного заказчика.

При использовании единого комплексного решения показатели надежности, эффективности и другие качественные параметры оцениваются для всего ЦОДа, а не для отдельных подсистем или компонентов. «Надежность отдельного ИБП сегодня меньше интересует заказчика, чем надежность всего центра обработки данных», — подчеркивает Алексей Соловьев, системный архитектор подразделения IT Division компании Schneider Electric. Кроме того, он указывает на то, что при комплексном подходе вопросы взаимной интеграции подсистем прорабатываются на этапе создания продукта, а не в ходе проектирования, поэтому сокращаются сроки этого процесса, как и процедуры внедрения, а также снижается вероятность ошибок при проектировании.

Очевидно, что, когда все решение предоставляет один производитель, зоны ответственности не размываются, а сервисное обслуживание осуществляется в рамках единого сервисного контракта. Кроме того, на комплексное решение вендор часто предоставляет существенную скидку.

По мнению Анатолия Бутенко, регионального менеджера Conteg в России, преимуще-

ства моновендорного подхода заключаются не только в технической, но и в эстетической целостности решения. Такое решение состоит из компонентов, которые полностью совместимы друг с другом с конструктивной и функциональной точек зрения, а также разработаны в рамках целостной дизайнерской концепции.

Как указывает Дмитрий Гуляев, руководитель направления инфраструктуры ЦОДов Delta Electronics, одним из технологических преимуществ внедрения решений от одной компании является повышение эффективности использования системы мониторинга и управления ЦОДом (DCIM), которая наилучшим образом совместима со всем оборудованием.

Конечно, при выборе решения от одного производителя может оказаться, что какие-то компоненты инфраструктуры противоречат внутренним стандартам заказчика и необходимо как минимум переучивать службу эксплуатации. Кроме того, возможны дополнительные затраты, если часть инженерной инфраструктуры уже имеется в наличии и заказчик захочет интегрировать ее в новое решение. Однако преимущества моновендорного подхода, опять-таки с точки зрения производителей, перевешивают недостатки. Посмотрим, насколько полны их портфели продуктов.

## CONTEG: ОТ ШКАФОВ ДО КОМПЛЕКСНЫХ РЕШЕНИЙ

Небольшая чешская компания Conteg за короткое время прошла путь от производителя шкафов до поставщика комплексных решений для инженерной инфраструктуры ЦОДов. Сегодня она предлагает шкафы и аксессуары, решения по управлению воздушными потоками, системы кондиционирования, ИБП, блоки распределения электропитания, системы мониторинга и контроля доступа, DCIM и другие продукты.

Поскольку Conteg начинала с производства шкафов, у нее исторически сформировался очень широкий ассортимент конструктивов, включая серверные и кроссовые шкафы, открытые стойки и шкафы для магистральных коммутаторов. К конкурентным преимуществам своих шкафов представители Conteg относят наивысший в своем классе процент перфорации дверей (86%), высокую номинальную грузоподъ-

емность (1500 кг), широкий ассортимент типоразмеров и аксессуаров.

В дополнение к шкафам предлагается система управления воздушными потоками, которая позволяет эффективно разделять потоки холодного и горячего воздуха внутри шкафа (всевозможные заглушки, разделительные рамы, уплотненные кабельные вводы и т. п.) и на уровне помещения (системы изоляции холодных/горячих коридоров, вытяжные трубы). Решения по изоляции делятся на два класса: предназначенные для монтажа на шкафы Conteg и универсальные, для монтажа на любые шкафы (они применимы, даже если ряды неравномерны по длине и высоте). Для обеспечения эффективного взаимодействия с системой пожаротушения помещения, в изолируемом коридоре могут быть установлены специальные крышные секции, которые открываются по сигналу системы пожаротушения. В результате отпадает необходимость во введении форсунок системы пожаротушения через крышные панели системы изоляции.

Системы кондиционирования Conteg представлены различными вариантами внутрирядных кондиционеров, а также инновационными устройствами CoolTop, которые устанавливаются на ряд шкафов сверху. Эти кондиционеры интегрируются в систему изоляции коридоров и не занимают полезную площадь ЦОДа, что позволяет установить дополнительные шкафы для размещения ИТ-оборудования.

Для мониторинга, контроля доступа и управления инженерной инфраструктурой ЦОДов Conteg предлагает масштабируемую программно-аппаратную систему для площадок любого размера — от небольших серверных комнат до крупных ЦОДов. Предлагается три уровня программного обеспечения: базовое (бесплатное), встроенное в контроллер, обеспечивает мониторинг до 500 датчиков и 80 параметров; ПО следующего уровня — Conteg Pro Server — подойдет для мониторинга площадок любого размера и реализации контроля доступа; система AEGIS класса DCIM предназначена для управления инфраструктурой ЦОДа любого масштаба.

В конце прошлого года Conteg обновила поколение интеллектуальных блоков распределения электропитания в шкафах (PDU). А этой осенью стартуют продажи



Источник: Conteg

Выпустив модульные ИБП, компания Conteg завершила формирование полного комплексного решения для построения инженерной инфраструктуры ЦОДов

модульных ИБП, что позволит говорить о наличии полного комплексного решения для ЦОДа. Готовится к запуску онлайн-вый 3D-конфигуратор ЦОДа, который, как утверждают специалисты Conteg, позволит техническому персоналу за считанные минуты разработать предварительную концепцию ЦОДа и комплекс технической документации, а менеджерам коммерческого отдела — получить оценку бюджета и необходимые презентационные материалы для представления концепции заказчику.

## DELTA ELECTRONICS: ВСЕ СВОЕ

Компания Delta Electronics — относительно новый игрок на рынке инженер-

ной инфраструктуры — существенно расширила свой портфель продуктов и предлагает все основные системы. Как подчеркивает Дмитрий Гуляев, руководитель направления инфраструктуры ЦОДов Delta Electronics, предлагая полный спектр решений для ЦОДов, компания все оборудование разрабатывает и производит сама. Ее система Delta InfraSuite включает в себя модульные ИБП, кабинеты/блоки распределения питания, оборудование прецизионного охлаждения, стойки, а также систему мониторинга и управления ЦОДом (DCIM) InfraSuiteManager.

В других странах Delta Electronics предлагает заказчикам предсобранные решения, в частности, в области энергетики —

префаб-модули систем бесперебойного энергоснабжения. Однако в России это направление только начинает развиваться. Такие системы предлагаются в основном лишь крупным клиентам. «Спрос на них, безусловно, растет, однако сам рынок весьма ограниченный и узкоспециализированный. Кроме того, стоят предсобранные решения дорого», — указывает Дмитрий Гуляев.

Ключевым преимуществом решений Delta Electronics ее представитель называет высокое качество при оптимальной цене. Как и другие ведущие игроки рынка инженерной инфраструктуры, компания предлагает клиентам обслуживание на всех этапах реализации и ведения про-



Источник: Delta Electronics

В состав системы Delta InfraSuite входят модульные ИБП, кабинеты/блоки распределения питания, оборудование прецизионного охлаждения, телекоммуникационные стойки, а также система мониторинга и управления InfraSuiteManager



Источник: Eaton

Основные решения, поставляемые Eaton для ЦОДов, — это представленные в широком ассортименте ИБП

екта. При этом Дмитрий Гуляев отмечает, что двухлетний срок гарантийного обслуживания для трехфазных ИБП отсчитывается со дня ввода оборудования в эксплуатацию, тогда как многие другие вендоры считают срок гарантии с даты производства. «В рамках постобслуживания мы осуществляем полный комплекс услуг: пусконаладочные работы, сервисное и превентивное обслуживание, ремонтно-восстановительные работы, замену аккумуляторных батарей, продажу запасных частей, обследование электросети заказчика. Все это крайне важно в условиях, когда заказчики стремятся просчитать заранее все затраты по проекту», — добавляет он.

В числе новинок Delta Electronics — представленные на выставке CeBIT 2017 модульный ИБП серии DPS 600 кВА, который обладает одним из наиболее высоких показателей плотности мощности в своем классе, а также модульные ИБП серии DPH 500 кВА, показатели плотности мощности которых достигают 55 кВА на один модуль 3U. Такие устройства позволяют решить актуальную задачу экономии пространства внутри серверной.

### ЕАТОН: С АКЦЕНТОМ НА ИБП

Основные решения, поставляемые Eaton для ЦОДов, — это представленные в широком ассортименте ИБП и модули для экономичного распределения питания (ePDU). Одна из изюминок систем ИБП Eaton — запатентованная технология Hot Sync, обеспечивающая равномерное распределение нагрузки. «Она избавляет систему от потенциально опасной единой точки отказа, сводя вероятность сбоев в ее работе практически к нулю, — говорит Алексей Бурочкин. — Кроме того,

ИБП Eaton обладают чрезвычайно высоким КПД, достигающим в режиме экономии энергии до 99%, и пониженным выделением тепла».

Среди новинок Eaton — устройства PDU третьего поколения (ePDU G3), которые, в частности, обеспечивают высокоточный контроль инженерных показателей ИТ-оборудования в ЦОДе. Стоит также отметить, что недавно Eaton первой среди производителей ИБП разработала систему резервного энергоснабжения, в которой вместо аккумуляторов используются суперконденсаторы собственного производства. Рассчитанные на 20 лет службы и обладающие низкой совокупной стоимостью владения, суперконденсаторы в сочетании с ИБП Eaton крайне полезны в случаях, когда требуется только кратковременная защита от отказов питания или невозможно использование аварийного питания от аккумуляторных батарей.

Для охлаждения установленного в ЦОДе оборудования компания предлагает набор решений по управлению воздушными потоками, которые оптимизируют отвод тепла. Для организации горячих и холодных коридоров выпускаются специальные коридорные решения с плоскими, направленными и вертикальными потолочными каналами, обеспечивающими высокую скорость воздушного потока при минимальном падении давления.

Система изоляции коридоров может устанавливаться в стойки, на пол и даже подвешиваться к потолку, что предоставляет клиенту большую свободу действий при размещении оборудования. Данное решение Eaton также является полностью модульным и позволяет устанавливать расширения или изменять конфигурацию

в зависимости от вносимых в ЦОД изменений.

ИТ-стойки компании сконструированы таким образом, чтобы утечка воздуха в них не превышала 3%. Стоечные решения для теплоотвода могут прикрепляться отдельно к каждой стойке и направлять тепло от ИТ-оборудования через верхний отвод и далее в потолочный канал.

Система Intelligent Power Manager (IPM) относится к числу программных инструментов управления ЦОДами. Как отмечают в компании, IPM способна автоматически интегрироваться с ведущими инструментами управления виртуализацией, гарантируя целостность данных и нулевое время простоя виртуальных машин.

Eaton не поставляет предсобранные ЦОДы в Россию, однако продуктовая линейка компании содержит другие компоненты высокой эксплуатационной готовности, включающие в себя компоненты заводской сборки. По мнению Алексея Бурочкина, в настоящее время префабы для российского рынка остаются достаточно новым направлением, а предложения не оптимальны по цене. «В сегменте коммерческих ЦОДов данные решения пока мало распространены, а существующие модели префабов реализованы в большинстве своем в рамках тестовых испытаний и экспериментальных проектов», — добавляет он.

Сегмент ЦОДов является для Eaton одним из наиболее приоритетных. Компания обладает одним из лучших решений в части бесперебойного электропитания, но ей недостает систем кондиционирования. Как отмечают в компании, в тех случаях, когда проект не может быть



реализован полностью на основе систем Eaton, привлекаются глобальные партнеры для создания совместного комплексного решения.

### SCHNEIDER ELECTRIC: ЧЕГО ЗАКАЗЧИК ИЗВОЛИТ

Компания Schneider Electric — безусловный лидер на рынке инженерной инфраструктуры ЦОДов в России. Для каждой из основных систем она предлагает заказчикам различные варианты реализации. Например, для организации бесперебойного электропитания в ее портфеле имеются решения на базе классических моноблочных ИБП, модульных ИБП с внутренним резервированием и горячей заменой модулей, а также блочные ИБП с внешним резервированием и компактными литий-ионными аккумуляторами.

В зависимости от плотности мощности, архитектурных особенностей объекта или требований по энергоэффективности компания предлагает различные системы охлаждения: внутрирядные или периметральные кондиционеры, чиллерные системы, DX-устройства или же экономайзеры. Изоляция воздушных потоков может быть выполнена как на уровне шкафа, так и для одного или нескольких рядов шкафов. Для изоляции горячих/холодных коридоров используются два конструктивных решения: система EcoAisle, в которой изоляция осуществляется непосредственно по установленным шкафам, и HyperPod — самонесущий каркас, который монтируется независимо.

В 2003 году Schneider Electric первой вышла на рынок инженерных систем ЦОДов с комплексным предложением InfraStruXure от одного производителя. С тех пор эта концепция бурно развивалась и превратилась в отдельное направление рынка. Если в первых комплексных решениях интегрировались только основные подсистемы (электропитание, охлаждение, средства размещения оборудования и мониторинга), то сейчас Schneider Electric предлагает порядка 80% всех инженерных систем ЦОДа, включая системы распределения электропитания от ввода на объект до розетки конечных потребителей, щитовое оборудование, СКС, средства автоматизации и управления, безопасности и др. Компанией накоплен большой опыт интеграции подсистем, не входящих в портфель предложения Schneider Electric, например дизель-генераторных установок, что позволяет предложить заказчикам полностью готовый ЦОД от одного поставщика.

Префабы — одно из перспективных и наиболее динамично развивающихся направлений в компании Schneider Electric. Она предлагает широкий ассортимент решений и систем высокой заводской готовности, позволяющих существенно сократить сроки реализации проекта и оптимизировать бюджет. По мнению Алексея Соловьева, префабы могут составить конкуренцию классическим комплексным решениям в отдельных случаях, в других же эффективно дополняют их, а целесообразность применения того или

инного подхода сугубо индивидуальна для каждого проекта.

Специалист Schneider Electric указывает на то, что в каждой из предлагаемых систем есть ряд отличительных особенностей, которые наряду с технологичностью оборудования позволяют заказчику получить дополнительную экономическую выгоду. Например, для трехфазных ИБП Galaxy VM и VX разработан режим работы EConversion, в котором КПД достигает 99% вместо классических 93–96%, характерных для ИБП двойного преобразования. Режим EConversion устраняет большинство недостатков, присущих традиционному ECO-режиму, обеспечивая мгновенное (то есть без пропадания выходного напряжения) переключение на работу от батарей при пропадании сетевого напряжения.

Системы охлаждения Schneider Electric эффективно работают на чиллерной воде с температурой 20°C, что дает возможность использовать фрикулинг большую часть года и экономить на электропитании. Глубокая аналитика DCIM-системы StruxureWare позволяет выявлять тенденции и прогнозировать динамику потребления ресурсов ЦОДа, проводить моделирование воздушных потоков, рассчитывать сценарии с добавлением или отключением отдельных устройств в ЦОДе. По мнению специалиста Schneider Electric, это значительно упрощает обслуживание и развитие ЦОДа на всех уровнях — от службы эксплуатации до инвесторов — и снижает риски человеческих ошибок и принятия



Фото: Александр Барсков

В портфеле решений Schneider Electric представлен практически весь набор решений для инженерной инфраструктуры ЦОДа, включая чиллеры

# Мы предлагаем комплексное решение для центров обработки данных

Решение для ЦОД Delta Infrasuite



Микро  
ЦОД



Модульный  
ЦОД



Контейнерный  
ЦОД



Периферийный  
ЦОД



DCIM



Охлаждение



ИБП



Гибридные  
системы



## ПРОЕКТЫ

Чтобы получить более полное представление о распространности предсобранных решений, мы попросили компании привести примеры проектов ЦОДов, в которых инженерные системы реализованы преимущественно на базе продуктов одной компании.

Conteg завершает в этом году реализацию ЦОДа ВТБ «Невская Ратуша» в Санкт-Петербурге. В рамках данного проекта была установлена комплексная инженерная инфраструктура Conteg на базе 64 внутрирядных кондиционеров на охлажденной воде. Решение также включает в себя шкафы для закрытой архитектуры охлаждения и соответствующие аксессуары, системы изоляции холодных коридоров, мониторинга, пожаротушения, блоки распределения электропитания, а также наружные шкафы и различные аксессуары.

Delta Electronics предоставила комплексное решение для ЦОДа «Миран». В спектр услуг этого провайдера входит размещение оборудования в собственных центрах обработки данных, предоставление виртуальных и выделенных серверов, услуги телефонной связи, доступа в Интернет и другие сервисы. В числе его клиентов не только малый и средний бизнес, но и крупные российские и зарубежные компании, поэтому «Миран» уделяет особое внимание решениям, которые способны обеспечить непрерывную работу оборудования, размещенного в его ЦОДах. Предложение Delta Electronics включало в себя промышленные ИБП НРН 120 кВА, системы кондиционирования воздуха и распределения питания, средства мониторинга и стойки.

Специалисты Eaton выделили ЦОД «Курчатовского института», одного из ведущих мировых научных центров. На этом объекте компанией создана система распределения электропитания. Выделенное помещение было ограничено по размерам, в связи с чем остро встал вопрос теплоотвода, который невозможно было решить стандартными средствами. В проекте использованы устройства серии Moeller (от вводных автоматических выключателей до систем питания конечных серверов) и около 230 распределительных щитов xEnergy,

которые на 20% компактнее стандартных решений. Как подчеркивают представители производителя, высокая отказоустойчивость оборудования Eaton позволила организовать надежную систему распределения питания.

Среди большого числа реализованных проектов специалисты Schneider Electric выделили два. Первый — это построение инженерной инфраструктуры одного из ведущих операторов коммерческих ЦОДов Европы — компании Interxion, которая владеет более чем 40 центрами обработки данных. Для объектов в Амстердаме, Париже, Марселе и в других городах Schneider Electric не только поставила оборудование инженерной инфраструктуры ЦОДа, но и осуществила проектирование и внедрение, а после ввода в эксплуатацию обеспечивает комплексное сервисное обслуживание инфраструктуры. Для коммерческих площадок особенно актуален быстрый выход на рынок, и решения Schneider Electric позволяют осуществить оперативное внедрение. Строительство ЦОДа в Марселе в этом году было завершено за два месяца, при этом надежность ЦОДа соответствует высоким стандартам заказчика.

Второй пример — введенный недавно в эксплуатацию центр обработки данных, объединивший ИТ-ресурсы группы «ФосАгро». Инфраструктура ЦОДа полностью базируется на оборудовании Schneider Electric. В ЦОДе установлены модульные ИБП Symmetra PX мощностью до 500 кВт, система охлаждения выполнена на базе чиллерных установок Uniflair, а кондиционирование воздуха в машинном зале осуществляется с помощью внутрирядных кондиционеров APC InRow. ИТ-системы размещены в шкафах NetShelter с изолированным горячим коридором. Система распределения электроэнергии, щитовое оборудование, DCIM-система, а также сервисная поддержка — все от одного вендора. Решение заказчика об использовании оборудования одного производителя позволило значительно сократить сроки внедрения проекта: ЦОД был спроектирован, построен и введен в эксплуатацию менее чем за полгода.

неверных решений, что в конечном итоге повышает экономическую эффективность ЦОДа.

Одна из новинок Schneider Electric — платформа EcoStruxure, — как считают в компании, станет технологическим фундаментом ее будущих решений. «EcoStruxure совмещает в себе последние наработки в сфере промышленных и информационных технологий и позволяет максимально повысить энергетическую эффективность и стабильность, оптимизировать доступность и производительность ресурсов, получить доступ к информации через мобильные устройства и тем самым пре-

вентивно снизить риски», — отмечает Алексей Соловьев. В рамках единой платформы все компоненты инженерной инфраструктуры обмениваются данными друг с другом, данные от одного или нескольких ЦОДов обрабатываются с применением облачных технологий и технологий Больших Данных, и в результате заказчик получает более широкие возможности для надежной и эффективной эксплуатации и развития своего объекта.

## ЗАКЛЮЧЕНИЕ

Необходимо отметить, что продуктовые портфели у всех производителей отлича-

ются и степень моновендорности предложения можно оценивать по-разному. Заметим, что даже очевидный лидер, Schneider Electric, как уже говорилось, сам производит только 80% инженерных систем для ЦОДов. Да, наверное, и невозможно требовать, чтобы какая-то одна компания выпускала абсолютно все для таких сложных комплексов. Важны технические особенности и наработки в части интеграции сторонних продуктов, чтобы заказчик мог получить ЦОД «как законченный продукт» и имел возможность за его надежность и другие показатели спрашивать с одной компании. Это главное для заказчика. **LAN**



# Транковые кабели для систем параллельной оптической передачи

При формировании каналов связи, обеспечивающих скорость передачи 40 Гбит/с и выше, сегодня используется преимущественно схема параллельной передачи. Из-за малого энергетического потенциала волоконно-оптических сетевых интерфейсов и большого количества линий применяются кабельные изделия заводского изготовления, поскольку они обладают более высокими техническими характеристиками. Ключевым компонентом соответствующего решения являются транковые кабели.

Андрей Семенов,  
директор по развитию СУПР, профессор МТУСИ

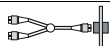


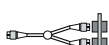

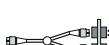
	Наименование	40 Гбит/с	100 Гбит/с
a)	Однокабельная	 24F	 24F
b)	Двухкабельная	 2 x 12F	 2 x 12F
в)	На X-образном кабеле	 24F	 24F

Рис. 1. Варианты формирования трактов параллельной передачи при различном исполнении линейной части стационарных линий (на примере 12- и 24-волоконных транковых кабелей)



Рис. 2. Разновидности вилок транковых кабелей для параллельной передачи

Транковый кабель представляет собой предоконцованное изделие. Используемая для его изготовления технология по своим функциональным параметрам обычно заметно превосходит мобильные полевые варианты. Это позволяет внедрить в конструкцию выпускаемых компонентов ряд новшеств, что, в свою очередь, дает возможность максимально учесть особенности применения и заметно повысить ценность продукта для его пользователей. Некоторые из таких особенностей рассматриваются далее.

### СХЕМЫ ОРГАНИЗАЦИИ ЛИНЕЙНОЙ ЧАСТИ СТАЦИОНАРНЫХ ЛИНИЙ

В многомодовых сетевых интерфейсах 100 и 400 Gigabit Ethernet могут использоваться различные схемы уплотнения кабельного тракта, среди которых в большинстве случаев присутствует «чистое» пространственное мультиплексирование. Обращение к такому приему вызвано тем, что при передаче десятков и сотен гигабит в секунду ограничения в быстродействии современной электроники позволяют обеспечить скорость для отдельного субканала не более 10 или 25 Гбит/с. Это вынуждает задействовать одновременно большое количество световодов: до 20 при 100 Гбит/с и до 32 для 400-гигабитной техники. Указанное количество световодов может быть выделено в линейной части тракта различными способами.

При формировании линейного тракта параллельной передачи необходимо обеспечить соблюдение норм по оптическому рассогласованию (параметру skew). Для этого все световоды одного направления выбираются в пределах одной ленты, что минимизирует влияние на skew разброса физических длин. Данное правило применимо при всех вариантах реализации сердечника транкового кабеля, например с использованием квазимодульных элементов или лент SWR.

Групповые оптические соединители MPO/MTP и их функциональные аналоги, изготовленные на основе наконечника MT, реализуют как однорядную, так и двухрядную схему расположения волокон в армирующем наконечнике. В первом случае соединяются 12 или 16 волокон, во втором — 24 или 32 (в зависимости от типа наконечника). Преимуществом однорядной схемы можно считать несколько меньшие вносимые потери и лучшие характеристики по обратным отражениям.

Кроме того, разъемы на основе однорядного наконечника оказываются не столь капризными в текущей эксплуатации. Наиболее сильной стороной двухрядной схемы, которая проявляется при большом количестве организуемых линий, можно считать двукратное увеличение плотности конструкции кабельных изделий.

Отсутствие решающего преимущества по ключевым параметрам одного вида разъема над другим приводит к тому, что 12(16)- и 24(32)-волоконные варианты соединителей имеют сопоставимую популярность. Схемы соединения розеток, образующих аппаратный (пользовательский) интерфейс и находящихся на разных концах стационарной линии, изображены на рис. 1, а и 1, б. По аналогии с сетями связи общего пользования стационарные линии, сформированные таким образом, условно называются однокабельными и двухкабельными. Для поддержания единообразной терминологии данные обозначения распространяются и на тракты.

Схема на основе кабеля X-типа (рис. 1, в) представляет собой промежуточное решение, в котором объединены основные характерные черты и преимущества однокабельного и двухкабельного вариантов. Единственным серьезным недостатком является необходимость применения кабеля со специальной структурой сердечника, чтобы отдельные световоды ленты можно было распределить по разным вилкам с помощью простых средств.

### РАЗНОВИДНОСТИ ПРЕТЕРМИНИРОВАННЫХ КАБЕЛЬНЫХ ИЗДЕЛИЙ ПО ГЕНДЕРНОСТИ И ПОЛЯРНОСТИ, ОБЛАСТИ ИХ ПРИМЕНЕНИЯ

Механизм взаимного выравнивания армирующих наконечников стандартного для параллельной передачи разъема MPO/MTP построен по схеме «штырь — отверстие», причем штырьки и отверстия разнесены на разные вилки. Соответственно, эти компоненты имеют различную гендерность. Вилка со штырьками обозначается как male (m), тогда как с отверстием — female (f). С учетом претерминированного характера кабельных изделий для параллельной передачи, данная особенность должна указываться в их индексе.

Для транковых кабелей могут применяться вилки четырех различных конфигураций (см. рис. 2).

С учетом гендерности вилок кабельные изделия разделены на несколько типов: m-m, f-f и m-f, где буквой m (от англ. male) обозначены вилки со штырьками, а буквой f (от англ. female) — вилки без штырьков. Основная масса кабельных компонентов относится к симметричному типу m-m и f-f, причем первые из них представлены преимущественно линейными кабелями, тогда как вторые — шнуровыми изделиями.

В стандартах, начиная с ANSI/TIA-568B, указывается, что коммутируемое часто изделие не должно иметь центрирующих штырьков. Это объясняется высокой опасностью их загрязнения и сложностью очистки торцевой поверхности вилок стандартных разъемов MPO/MTP. Кроме того, поскольку диаметр центрирующих штырьков невелик, они не отличаются высокой механической прочностью и в процессе эксплуатации должны находиться в защищенном месте. Таковым считается гнездо розетки.

Необходимость использования несимметричных шнуров отображения m-f возникает крайне редко. Относительно большое распространение они получили только в одномодовой технике и трактах Base8, что в первом случае объясняется широким применением транковых кабелей с гендерностью типа female как способа блокировки неправильного подключения к ним многомодовых шнуров и кассет, а во втором — 12-волоконных шнуров.

Кроме того, в полном индексе транкового кабеля указывается взаимная ориентация ключевых элементов вилок противоположных концов, необходимая для правильного построения тракта с точки зрения его полярности. Существуют два варианта такой ориентации (совпадающая и несовпадающая), соответствующие им разновидности обозначаются как A и B.

В изделиях типа A номер посадочного места для световода в разных вилках всегда один и тот же, то есть 1 соединяется с 1, 2 с 2 и т. д. Поэтому такие вилки развернуты ключами в разные стороны.

Изделия типа B характеризуются тем, что вилки имеют «естественную» однотипную ориентацию: ключевые элементы развернуты в одну сторону. При такой структуре происходит скрещивание световодов и тем самым облегчается достижение правильной полярности.

Из соображений единообразия данная классификация распространяется и на коммутационные шнуры.

Еще одна разновидность транкового кабеля (обозначается как тип С) рассчитана на передачу сигналов исключительно дуплексных интерфейсов и имеет специальную раскладку волокон. Изделия типа С отличаются тем, что в них выполнено скрещивание волокон в пределах одной пары, которое требуется при дуплексной передаче. Кроме того, при такой схеме нет смысла изготавливать шнуры I-типа и такая структура применима только для транковых кабелей.

Сводка стандартных разновидностей кабельных изделий для параллельной передачи по полярности и областям применения представлена на рис. 3.

### ОБОСНОВАНИЕ СТРУКТУРЫ ТРАНКОВЫХ КАБЕЛЕЙ

Большое количество вариантов исполнения вилок и линейных кабелей существенно усложняет как проектирование информационной проводки, так и ее последующую эксплуатацию.

Ситуация заметно, хотя и не радикально, облегчается тем, что количество минимально необходимых для решения важных задач разновидностей конфигураций сокращается при использовании следующих приемов:

- соблюдение положений стандартов в отношении структур трактов, имеющих разновидности А и В (вариант С из-за его ограниченных функциональных возможностей не рассматривается);
- использование для оконцевания кабельных изделий универсальных вилок, в которых предусмотрена возможность изменения гендерности и полярности в зависимости от конкретной производственной ситуации;
- подбор структуры кабеля таким образом, чтобы она в максимально полной

степени соответствовала потребностям построения и эксплуатации проводки.

На физическом уровне систем параллельной передачи, в отличие от прочих разновидностей СКС, во время текущей эксплуатации может осуществляться плановое изменение структуры стационарных линий. Потребность в этом возникает в процессе решения следующих задач:

- переход от дуплексной схемы передачи к параллельной;
- увеличение степени уплотнения кабелей в случае построения проводки по схемам Base12 и Base24.

Обычно переход выполняется от дуплексной передачи к параллельной. По мере внедрения техники SWDM не исключен возврат к двухволоконной схеме организации связи при условии внедрения соответствующей аппаратуры следующего поколения.

С учетом перечисленных обстоятельств, при выборе структуры транкового кабеля за основу целесообразно взять следующие положения:

- переход к иной конфигурации стационарной линии осуществляется с помощью адаптера;
- вилки транкового кабеля могут формировать пользовательский интерфейс информационной проводки.

При параллельной передаче часто используются адаптеры, интерфейс которых может быть пользовательским (традиционным) и скрытым. Первый предполагает прямой доступ к отдельным волокнам транкового кабеля, а второй характерен для линейной стороны модульно-кассетного решения. В обоих случаях могут применяться разветвительные шнуры. Некоторые из возможных вариантов организации трактов представлены на рис. 4.

С учетом перечисленных особенностей оконцевание многоволоконного транкового кабеля наиболее целесообразно выпол-

нять с помощью вилки со штырьками (исполнение male). Это позволяет:

- подключать сетевые интерфейсы к кабельной системе симметричными по виду гендерности аппаратными шнурами с вилками типа female (интерфейс всегда выполняется по схеме male);
- улучшить эксплуатационные параметры кабельной системы за счет того, что штырьки всегда находятся в розетке и меньше подвергаются загрязнению;
- упростить переход от модульно-кассетного исполнения стационарной линии к традиционному;
- добиться однотипности исполнения аппаратных и коммутационных шнуров.

Исключения из указанного правила имеет смысл делать, только когда требуется обеспечить механическую блокировку ошибочного подключения и коммутации. Например, вилками с гендерностью female часто снабжаются одномодовые транковые кабели и транковые кабели системы Base8.

В первом случае проблема нетипового интерфейса решается установкой разветвительной кассеты (в подавляющем большинстве одномодовых сетевых интерфейсов используется дуплексная схема организации связи). Во втором случае в состав штатных компонентов кабельной системы вводятся переходные шнуры с вилками male и female на разных концах. Дополнительно применяются различные маркирующие компоненты. Стандартом де-факто в этой области является серый цвет различных накладок и декоративных элементов дизайна, а также нанесение цифры 8 на корпус вилок и кассет.

### СПОСОБЫ ДОСТИЖЕНИЯ КРУГЛОГО ПОПЕРЕЧНОГО СЕЧЕНИЯ

Исторически сложилось так, что в системах параллельной передачи применяются преимущественно ленточные кабели, а в силу особенностей структуры этих изделий сердечник оптического кабеля



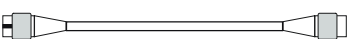
Тип изделия	Структура изделия	Тип устанавливаемых вилок	Область применения
A (straight trough)		Key-up – key-down	Транковые кабели и коммутационные шнуры
B (flipped)		Key-up – key-up	Транковые кабели и коммутационные шнуры
C (pairwise flipped)		Key-up – key-down	Транковые кабели

Рис. 3. Основные разновидности оконцеванных кабельных изделий I-типа (условно показаны с вилками типа female)



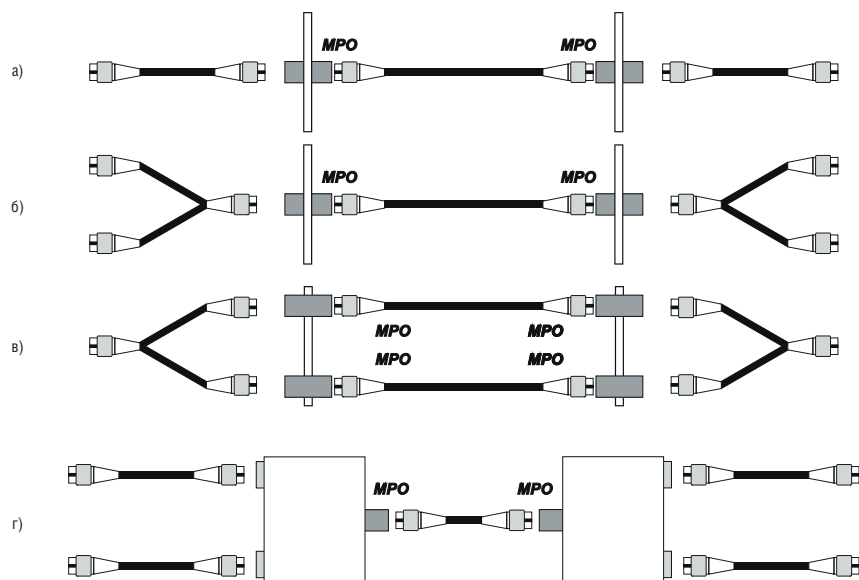


Рис. 4. Основные варианты реализации интерфейсов кабельной системы при параллельной передаче: а, б, в — традиционный интерфейс; г — скрытый интерфейс

имеет форму, которую никак нельзя назвать круглой. Нередкое использование в составе конструкции облегченных упрочняющих покрытий не помогает исправить ситуацию. В результате регулярную укладку кабеля трудно обеспечить, что ведет к неоптимальному использованию доступной емкости каналов, а нередко и к механическому повреждению отдельных волокон и даже самого кабеля (при нарушениях технологии прокладки и перекручивании изделия).

Для устранения этого недостатка предложен ряд решений. Большинство из них так и не были востребованы, но при современном уровне техники необходимые кабели легко могут быть запущены в серийное производство.

К традиционным средствам достижения поставленной цели отнесем конструкции, в которых используются отдельные ленты.

Первое из таких решений обеспечивает придание круглой формы поперечному сечению кабеля за счет размещения под оболочкой одного или нескольких заполняющих элементов. Каждый из них содержит в своей центральной части вырез для укладки в него ленты световодов. Очевидным недостатком является неизбежное увеличение жесткости всей конструкции, что, впрочем, компенсируется наличием разрезов в заполняющем элементе: четыре отдельные идентичные части могут перемещаться относительно друг друга при изгибах кабеля (рис. 5, а).

Поперечное сечение транкового кабеля становится более округлым в случае замены одной типовой, например 8-волоконной, ленты на две или три типовые 4-волоконные, которые укладываются в стопку. «Двухленточный» вариант такой структуры, который хорошо согласуется со схемой построения стационарной линии Base8, изображен на рис. 5, б.

Сечение имеет овальную форму, которая мало отличается от круглой.

Отдельно укажем на то, что, помимо центрального расположения подобной многоэлементной структуры, для многоволоконных конструкций характерна укладка стопок ленточных волокон в радиальные камеры фигурного сердечника (рис. 5, в).

Сердечник круглой формы вполне может формироваться из отдельных изделий (рис. 5, б) по известной схеме break-out кабеля внутренней прокладки. Структура, соответствующая такой схеме, показана на рис. 5, г.

Вполне возможен и отказ от ленточной конструкции. При выборе такого пути в первом случае речь идет о круглой квазимодульной структуре fiberUnit. Основным недостатком такого решения является сложность получения подобных компонентов с количеством волокон

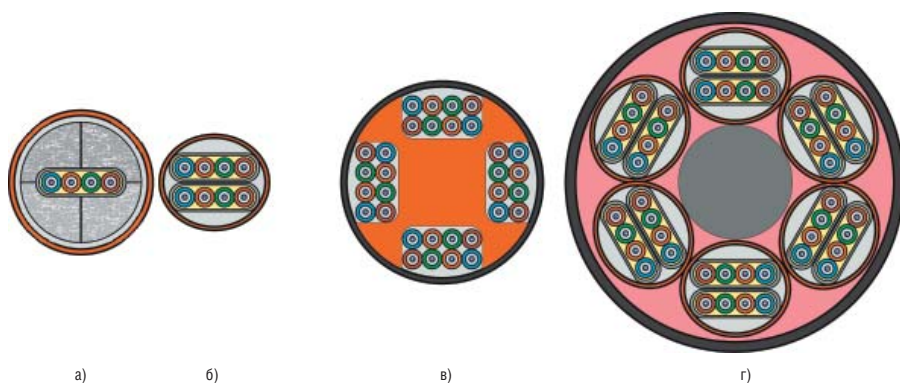


Рис. 5. Основные способы достижения круглой формы поперечного сечения транкового кабеля: а — применение внутренних профилированных элементов-заполнителей; б — замена одной ленты на несколько с сохранением общего количества волокон; в — применение профилированного сердечника; г — обращение к конструкции типа break-out

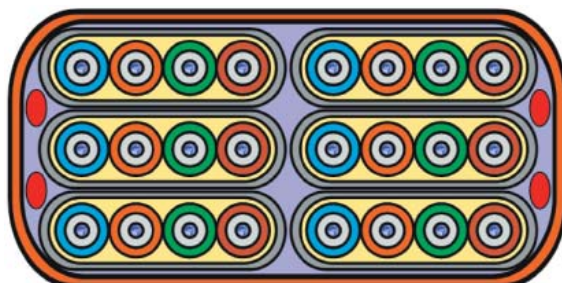


Рис. 6. Низкопрофильный ленточный кабель

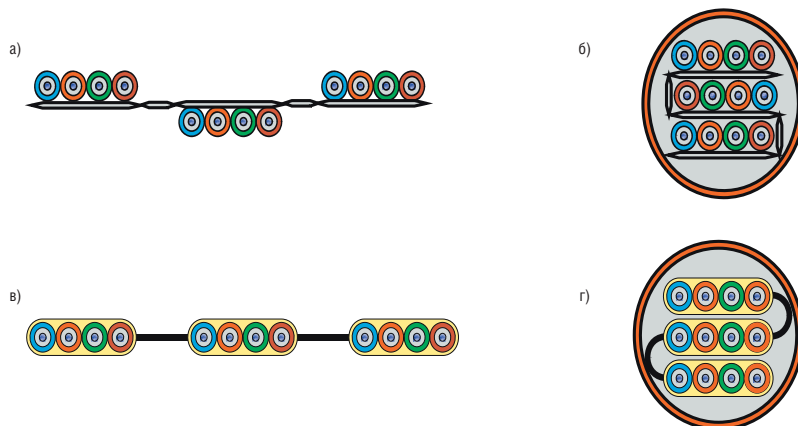


Рис. 7. 12-волоконные транковые кабели на основе групповых ленточных волокон: а, б — с двухсторонней наклейкой на ленту; в, г — с соединением отдельных 4-волоконных рядных сборок по схеме zip-cord

свыше 12. Второй случай относится к лентам SWR.

Еще один подход к обеспечению более полного использования доступной площади кабельного канала основан на применении так называемых низкопрофильных конструкций. Их суть состоит в укладке под оболочку нескольких стопок лент с относительно небольшим количеством волокон. Таким образом, кабель в поперечном сечении приобретает форму, близкую к квадратной со скругленными углами (рис. 6). Для обеспечения необходимой механической прочности изделия сердечник дополняется силовыми элементами, которые укладываются в периферийные пустоты между отдельными лентами.

## ОРИГИНАЛЬНЫЕ КРУГЛЫЕ КОНСТРУКЦИИ

Возможности обычного «стопочного» исполнения сердечника на ленточных волокнах (рис. 5, б) ограничены тем, что из-за неровности укладки отдельных лент при формировании кабельного сердечника нарастает оптическое рассогласование (skew). Этот недостаток устраняется главным образом путем применения так называемых групповых ленточных волокон. Ленточное исполнение световодов с их жестким механическим выравниванием

по длине сохраняется, но сама лента изготавливается с изломами — волокна разделяются на отдельные группы. Известны две разновидности «сэндвич»-структур из четырехволоконных групп световодов с их размещением на ленте.

Первая конструкция представляет собой изделие с двухсторонней наклейкой волокон на ленточное основание. Установка отдельных групп выполняется с разрывами, ширина которых несколько превышает диаметр оболочки световода, а сами разрывы отделяются от участков с волокнами перетяжками (рис. 7, а). Перед началом формирования сердечника такая лента сгибается и складывается в форме стопки (рис. 7, б).

В основу второй конструкции положено соединение отдельных четырехволоконных рядных сборок с помощью узких перемычек по образцу дуплексных кабелей со структурой zip-cord (рис. 7, в). Длина перемычки выбирается таким образом, чтобы сборки можно было уложить в стопку (рис. 7, г).

Отметим, что из-за выпуклой формы фиксирующих перемычек структуры zip-cord внешний диаметр кабеля оказывается несколько больше, чем в предыдущем случае.

## ЗАКЛЮЧЕНИЕ

Серийные транковые кабели имеют ряд разновидностей исполнения, что позволяет формировать все те варианты линий, которые предусмотрены стандартами и востребованы на практике.

При прочих равных условиях транковые кабели целесообразно армировать вилками МРО/МТР типа male (со штырьками). Это облегчает переход между различными схемами построения стационарных линий и наращивание скоростей передачи по мере возникновения такой необходимости.

Отказ от соблюдения предыдущего правила имеет смысл, только когда требуется обеспечить механическую блокировку некорректного подключения специальных разновидностей транковых кабелей к обычным. К специальным относятся одномодовые изделия и кабели системы Base8.

Технологические возможности производственных предприятий позволяют добиться круглой или близкой к ней формы поперечного сечения, что заметно ускоряет создание и упрощает последующую эксплуатацию информационной кабельной системы ЦОДа. **LAN**

# Шесть вопросов, которые вы, возможно, забыли задать, разрабатывая план защиты периметра

Для защиты периметра той или иной территории требуется нечто большее, чем высокий забор с колючей проволокой наверху. Успешно противостоять угрозам можно только в том случае, когда имеется множество уровней защиты, оснащенных надежными системами безопасности. Однако немало предприятий по-прежнему испытывают трудности с разработкой и внедрением такого комплексного решения.

Кванг Трин,  
системный архитектор в Axis Communications





Сегодня организации острее, чем когда-либо ранее, ощущают важность блокирования действий злоумышленников, прежде чем те успеют нанести ущерб имуществу и навредить клиентам или сотрудникам. Эксперты IFSEC Global, ссылаясь на данные ведущего центра исследования рынков Research and Markets, прогнозируют, что к 2020 году объем продаж на глобальном рынке средств безопасности для защиты периметра достигнет 21 млрд долларов.

Несмотря на это, существует одна фундаментальная проблема: многие по-прежнему испытывают трудности с разработкой и внедрением всеобъемлющего плана защиты периметра. Вот шесть вопросов, которые стоит задать себе при подготовке такого проекта.

## 1. Что понимается под периметром?

Периметр — это любая граница, которая отделяет одну область от другой. Цель защиты заключается в обеспечении безопасности находящихся внутри него уязвимых мест и структур.

При разработке плана защиты периметра в первую очередь надо оценить его протяженность. Как правило, для длинных периметров потребуется больше ограждений и средств безопасности.

Возьмем, к примеру, международный аэропорт Денвера. По сообщению Denver Post, только за последние десять лет на охраняемую территорию площадью 137 км², вокруг которой выстроен

забор протяженностью 48 км, проникли восемь человек. Другие крупные аэропорты имеют ограждения аналогичной или даже большей длины.

А теперь представьте, что вам нужно разработать и реализовать план, в котором равное внимание уделяется каждому квадратному метру внутри многокилометрового периметра. Добиться этого нелегко, но можно выполнить следующие действия:

**Определите все входы и выходы.** Как правило, злоумышленники проникают через указанные зоны, потому что сделать это легче всего.

**Изучите физический периметр:** он может состоять из стен, заборов, какой-то иной инфраструктуры и естественных преград, таких как живые изгороди из кустов и деревьев.

**Оцените последствия проникновения.** Нужно ли подавать сигнал тревоги, как только нарушитель начнет перелезать через забор, или важнее определить направление его движения и пройденное расстояние? Важность охраняемой собственности можно описать концентрическими кругами: в центре находится самая ценная его часть, а на границе — наименее значимая.

## 2. Насколько актуальна используемая технология?

Целесообразность применения самых современных решений безопасности обосновывается целым рядом причин.

**Соблюдение требований регуляторов.** Организации, работающие в сфере здравоохранения, а также предприятия, выполняющие заказы правительственных структур, вынуждены поддерживать свои решения в области безопасности в актуальном состоянии, для того чтобы избежать штрафов.

Например, в США медицинские организации должны соблюдать требования Закона об отчетности и безопасности медицинского страхования (HIPAA) и другие предписания штатов и федеральных структур. В числе прочего им необходимо регулярно обновлять свои решения безопасности, что позволяет гарантировать лучшую защиту физической инфраструктуры и данных.

**Повышение эффективности продуктов.** Технологии, позволяющие распознавать движение на видео, постоянно совершенствуются, и на смену анализа пикселей приходят интеллектуальное распознавание объектов и выдача предупреждений с учетом размеров нарушителя и скорости его движения. Вычислительная мощность IP-устройств на границах сети растет, и с их помощью можно выполнять более сложный анализ, позволяющий уменьшить число ложных срабатываний.

Это сулит сразу несколько преимуществ. Перемещение вычислений на границу сети означает, что освободившаяся вычислительная мощность центрального сервера может быть направлена на решение других задач. Зачастую это дает возможность снизить затраты на оборудование и сократить ресурсы, выделяемые на выполнение тех же самых операций.

Кроме того, использование распределенных конечных устройств для выполнения различных задач позволяет изолировать системные сбои. Представьте, что произойдет при отказе центрального сервера, выполняющего сложный анализ. Аналитика будет недоступна для всех подключенных устройств. Благодаря распределенной системе ее нельзя будет получить только от тех устройств, на которых непосредственно происходят сбои.

**Защита от кибератак.** Подключенные к сети устройства Интернета вещей (IP-камеры и другое оборудование) потенциально уязвимы. В новом отчете Deloitte говорится, что число и масштабы распределенных атак, нацеленных на отказ в обслуживании (DDoS-атаки), также растут. Это может привести к выводу из строя систем безопасности или как минимум к блокированию доступа к видеоматериалам. Установка

последних обновлений помогает лучше защитить компании от подобных угроз.

Прежде чем обновлять решение, уточните, как другие методы защиты и обна-

ружения (электрические ограждения и контуры заземления, пассивное инфракрасное оборудование, радары, двойные датчики, тепловизионные камеры, громкоговорители и освещение) вписыва-

ются в общий план защиты периметра. Выясните, открыта ли используемая технология для интеграции или же она доступна через общую платформу в виде отдельного блока.

### 3. Влияют ли на точность обнаружения климат и особенности окружающей среды?

Климат и особенности окружающей среды способны оказать серьезное воздействие на оборудование систем безопасности и качество распознавания угроз. Когда освещение слишком яркое, объектив захватывает лучи восходящего или закатного солнца либо съемка проводится ночью, аналоговые камеры вряд ли сумеют выдать четкое изображение. Для таких ситуаций лучше подходят IP-камеры с широким динамическим диапазоном или тепловизионные технологии.

Освещение — не единственная потенциальная проблема для специалистов по безопасности. При сильном ветре и разной степени вибрации возникает эффект дрожания, избавиться от которого помогут электронные стабилизаторы изображения.

В экстремальных условиях операторам нужно учитывать не только функциональные возможности решений безопасности. Необходимо принять во внимание

и другие факторы, влияющие на качество видео:

**Влажность.** Конденсат, образующийся внутри объектива, размывает изображение и разрушает электронные компоненты. У камер, подвергающихся переменному давлению воздуха и воздействию дождя, может нарушиться изоляция, и влага проникнет внутрь. Для предотвращения сбоев камеры оснащаются внутренними вентиляторами и системой быстрой сушки.

**Условия окружающей среды.** Из-за высокого содержания соли в воздухе оборудование, установленное на морском побережье, подвергается коррозии. То же самое происходит в цехах предприятий, где производятся пищевые продукты, медицинские компоненты, чистящие средства и применяются агрессивные химические соединения. В такой среде следует использовать камеры для наружного наблюдения, изготовленные из нержавеющей стали

и поликарбоната и обладающие устойчивостью к воздействию морской воды и чистящих реагентов.

**Температура.** Когда оборудование эксплуатируется при экстремально низких температурах, его нормальное функционирование нарушается. Если не поддерживаются технология быстрой сушки и температурный контроль, то объектив покрывается льдом, что приводит к размытию изображения. А при нарушениях в работе системы электропитания камера и вовсе перестает работать.

**Монтаж.** Не все поверхности одинаковы. Камеры, установленные на пористых или обладающих высокой теплопроводностью стенах, подвергаются дополнительному воздействию влаги. Заранее изучив все особенности размещения оборудования, вы сможете лучше защитить его от разрушительного воздействия окружающей среды и сильных перепадов температуры.

### 4. Кто и как принимает сигналы тревоги?

Для постоянного контроля за всем периметром часто используется технология удаленного IP-видеонаблюдения. Установленные в нескольких местах камеры позволяют сотрудникам службы безопасности постоянно быть в курсе событий, когда они следят за тем, что отображается на мониторах, совершают обход объекта и удаленно наблюдают за происходящим с помощью мобильных устройств.

Системы защиты периметра анализируют ситуации и уведомляют персонал только при возникновении реальной угрозы. Будучи избавлены от необходимости следить за субъектами и событиями, не представляющими какой-либо опасности, сотрудники способны лучше оценить природу риска и отреагировать соответствующим образом.

Такой уровень безопасности помогает предприятиям решить сразу три задачи:

**Уменьшение числа штрафов.** В 2014 году полиция и пожарные службы Канзаса зарегистрировали просто невероятное количество вызовов в городе Уичито. Всего поступило 18 461 сообщение, и только 659 из них информировали о реальной угрозе. При этом первое ложное сообщение не предусматривало никакого наказания, а вот последующие грозили штрафом в размере от 40 до 350 долларов. Сумма максимального штрафа составила 750 долларов, в общей сложности в городскую казну поступило 700 тыс. долларов.

Таким образом, ложные тревоги обходятся предприятиям в сотни, а то

и в тысячи долларов. Лучшие решения для мониторинга позволяют уменьшить число ложных срабатываний за счет идентификации только истинных угроз.

#### Минимизация ущерба и убытков.

Оперативная реакция на нарушения периметра помогает значительно сократить убытки, в том числе от ущерба, нанесенного имуществу. Но, как уже говорилось ранее, в масштабе страны количество ложных тревог превышает все разумные пределы. Возьмем, к примеру, Остин. В 2014 году городская полиция ежедневно выезжала на срочные вызовы в среднем 80 раз. При этом, по свидетельству myStatesman, девять сигналов из десяти оказались ложными.

В некоторых городах спецслужбы отказались выезжать по тревоге в те места, откуда поступало наибольшее количество ложных сигналов. Объекты, где отсутствуют надлежащие средства и протоколы защиты периметра, подвергаются повышенному риску несанкционированного проникновения и нанесения материального ущерба.

**Снижение числа сбоев в работе предприятий**, вызванных ложными сигналами тревоги. Особенно важное значение это имеет в аэропортах, где любое нарушение периметра может

привести к задержкам рейсов, что чревато многотысячными убытками от потерянных доходов и наложенных штрафов.

Вспомним случай, произошедший в международном аэропорту Филадельфии в марте 2012 года. По сообщению New York Daily News, мужчина, управлявший внедорожником, проследовал через ворота и выехал на взлетную полосу, куда как раз собирался приземлиться самолет, на борту которого находились 43 человека. В результате была задержана посадка не только этого

рейса, но и еще 75 самолетов, ушедших на дополнительный круг по требованию диспетчера. Кроме того, 80 самолетов, готовившихся к взлету, в течение полчаса оставались на своих местах.

Системы безопасности, оснащенные средствами дистанционного оповещения, помогают оперативно предупреждать персонал аэропорта, способствуя блокированию таких проникновений еще до несанкционированного пересечения границы периметра или, в крайнем случае, сразу после его обнаружения.

## 5. Как определить, что стало причиной тревоги?

Современные средства защиты периметра упрощают выявление причины тревоги.

Например, у тепловизионных камер, наделенных средствами интеллектуального видеоанализа, не только гораздо меньше, по сравнению с оптическими, ложных срабатываний, но они лучше подходят для работы в условиях дождя, снега и тумана. Некоторые такие устройства оснащаются электронными стабилизаторами изображений, которые делают их более устойчивыми при воздействии ветра.

Конечно, возможности тепловизионных камер ограничены. Но если они дополняются средствами удаленного мониторинга, сотрудники службы безопасности оперативно получат уведомления о потенциально опасной ситуации и смогут проверить наличие угрозы лично или при помощи визуальных камер.

В условиях слабой освещенности или при очень ярком свете идентификация нарушителей затруднена. В качестве примера можно привести ситуацию, когда камера направлена на автомобиль с мощными фарами. Решения с поддержкой широкого динамического диапазона позволяют менять структуру сцены таким образом, чтобы при больших перепадах освещения объекты были видны лучше.

Другая идея заключается в использовании камер, оснащенных инфракрасной подсветкой с длиной волны 950 нм и позволяющих рассмотреть затемненные места. Хотя инфракрасные приборы не отображают естественные цвета, они отлично подходят для скрытого наблюдения, поскольку инфракрасное излучение невидимо для человеческого глаза.

Однако, как и у любого другого решения, у инфракрасных камер имеются слабые места:

1. Они менее эффективны в сырую погоду, потому что капли воды отражают и преломляют свет, ухудшая качество изображения.
2. Как правило, инфракрасные камеры эффективно регистрируют отражение излучения от множества объектов, но, если какие-то объекты слишком темные или, наоборот, яркие, есть вероятность того, что инфракрасные лучи не будут отражаться должным образом.
3. Преступники могут увидеть тусклое красное свечение камер с малой длиной волны и попытаться сломать камеру или ее крепление.

Стоит отметить, что простое добавление источников освещения в темных зонах помогает лучше распознавать нарушителей, но в долгосрочной перспективе может привести к увеличению общих затрат на обеспечение безопасности периметра.

## 6. Какова дальность обнаружения?

Персонал службы безопасности должен прежде всего устранить так называемые слепые зоны по периметру. Если выявление угрозы на расстоянии 3 и 300 метров одинаково важно, то ознакомления лишь со спецификациями системы недостаточно — необходимо оценить ситуацию в целом.

Внедрение любого продукта может

завершиться неудачей, если его развертывание осуществляется ненадлежащим образом. Практические навыки использования технологий защиты периметра и знание ограничений на дальность распознавания помогут персоналу получить более высокую отдачу от внедрения решений безопасности.

К примеру, тепловизионная каме-

ра с дальностью действия 300 м отлично подходит для установки вдоль линии забора. Но что, если оператору нужно знать, кто нарушитель — человек или животное? Эти параметры накладывают дополнительные ограничения и сужают диапазон в зависимости от конкретных потребностей, условий окружающей среды и особенностей территории.



# Летняя коррекция прогнозов

Первая половина 2017 года показала, что поводов для беспокойства сегодня больше, чем когда-либо. Новые атаки, организуемые с опорой на технологическую базу и достижения последних двух лет, становятся все более искусными и изощренными.

**Дерек Мэнки,**  
директор по стратегии безопасности Fortinet

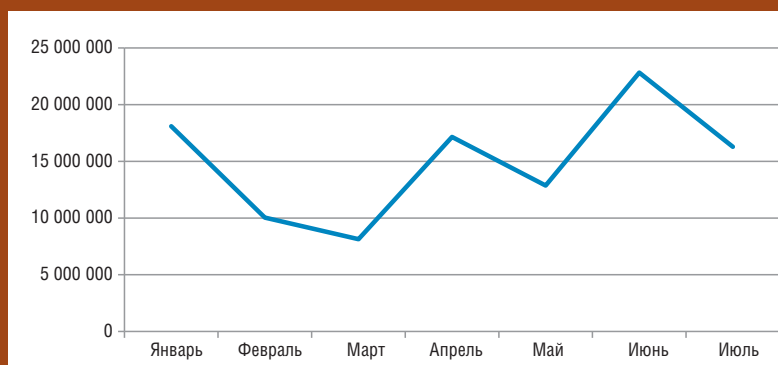


Рис. 1. Mirai 2017 — общее число атак за месяц



Рис. 2. Червь-вымогатель Najime нацелен прежде всего на Тайвань и США, где зарегистрированы уже миллионы скомпрометированных устройств

Наша статья, посвященная прогнозам в сфере безопасности на 2017 год, вышла под заголовком «The Year of Accountability» («Год ответственности»). В ней были перечислены все тенденции в области безопасности, сложившиеся в 2016 году, и подчеркивалось, что, если какие-либо из предлагаемых мер не будут приняты, возникнет реальный риск краха формирующейся цифровой экономики. Необходимость усиления ответственности на самых разных уровнях защиты данных является сегодня чрезвычайно актуальной.

А теперь давайте более подробно остановимся на некоторых моментах, которые ранее уже упоминалось в прогнозах на 2017 год.

## ТЕНЕВАЯ СЕТЬ

Летом прошлого года мы наблюдали крупнейшую в истории атаку DDoS, в которой использовалась «теневая сеть на базе Интернета вещей». Под этим термином понимаются ботнеты Интернета вещей, которые невозможно выявить и классифицировать с помощью обычных инструментов. Теневая сеть Mirai была составлена из миллионов уязвимых устройств Интернета вещей и применялась для вывода из строя крупного сегмента Интернета. Интересно, что даже после мощного всплеска атак, произошедшего летом 2016 года, эксплойт Mirai продолжал успешно поражать уязвимые системы (см. рис. 1).

Хотя эффект был беспрецедентным, в своих прогнозах мы утверждали, что вирус Mirai не был самоцелью, а создавался прежде всего для тестирования возможностей подобных атак и в дальнейшем эта масса скомпрометированных устройств будет использоваться для проведения все более изощренных атак. Жизнь подтвердила нашу правоту. Наследником Mirai стал червь-вымогатель Hajime. Созданный на той же технической базе, он оказался намного сложнее.

В отличие от Mirai, который был достаточно тупым орудием, в Hajime был встроен целый ряд гораздо более изящных киберинструментов. Он точно так же был нацелен на устройства Интернета вещей, но при этом был уже кросс-платформенным. В настоящее время этот червь заражает пять различных

платформ, а в его составе имеются набор инструментов для автоматического выполнения различных задач и список динамических паролей, обновляемых дистанционно. Кроме того, он способен загружать и другой программный код, например BrickerBot.

Заветная цель разработок в области сетевых технологий — добиться автоматизации на уровне 99%. К сожалению, злоумышленники преследуют ту же цель. У Hajime есть несколько автоматических инструментов. Чтобы избежать обнаружения, червь старается проявлять минимальную активность, оставаясь невидимым на радарх средств безопасности за счет имитации поведения человека.

Одной из наиболее опасных его функций является встроенный инструмент для удаления правил. В частности, предпринимаются попытки удалить правила межсетевых экранов, используемые для обнаружения вредоносных программ такого рода. Hajime нацеливается также на интернет-провайдеров и поставщиков управляемых услуг защиты (см. рис. 2): он идентифицирует установленное у клиента телекоммуникационное оборудование и CPE LAN Management Protocol, а затем удаляет правила, которые позволяют этим устройствам взаимодействовать с поставщиком услуг.

Представьте себе провайдера, миллионы устройств которого внезапно исчезли из виду и не дают признаков жизни. Восстановить контроль над ними невозможно. Этот кошмарный сценарий не только блокирует предоставление услуг, но и порождает разрушительные побочные эффекты: служба поддержки перестает справляться со шквалом звонков раздосадованных клиентов.

В отличие от сети Mirai, управление которой осуществляется с одного командного сервера (и его относительно легко блокировать), Hajime имеет децентрализованную и очень устойчивую структуру управления. Естественно, чем больше поддерживается платформ, программных кодов и исполняемых модулей, тем сложнее управлять таким хозяйством. Но, решив эту задачу, злоумышленники

могут добиться многократного роста проникновения.

Появившийся не так давно ботнет Persirai нацелен на IP-камеры, подключенные к Интернету. Эта новейшая разработка уже наступает на пятки Mirai и Hajime. Persirai использует уязвимость, позволяющую похищать пароли, чтобы выполнять аутентифицированные команды. Вот вам еще один пример «горячего эксплойта», поскольку зараженная IP-камера тут же начинает атаковать другие камеры, используя уязвимость нулевого дня, ставшую известной всего несколько

**Автоматизация означает, что атакующие добиваются до цели быстрее, промежуток между обнаружением бреши и началом вредоносного воздействия сокращается, а тем временем эксплойты учатся избегать обнаружения.**

месяцев назад. И хотя число инцидентов пока невелико, процесс автоматического заражения позволяет использовать такой подход в самых разных отраслях (см. рис. 3).

В мире Интернета вещей мы наблюдаем эволюцию технологий эксплойтов (от уже наделенных интеллектуальными функциями к еще более совершенным). В их числе — кража паролей, которые потом используются для взлома других систем. Обычно такой подход применяется человеком, и вот теперь он автоматизирован.

Автоматизация означает, что атакующие добиваются до цели быстрее, промежуток между обнаружением бреши и началом вредоносного воздействия сокращается, а тем временем эксплойты учатся избегать обнаружения. Выявляя угрозы, мы больше не можем позволить себе вручную систематизировать связанные с ними данные — реагировать на происходящее нужно со скоростью машины.

В грядущей кибервойне предприятия должны применять против автоматизированных средств свои автоматизированные инструменты. Для этого нужно внедрять интегрированные экспертные системы безопасности, которые автоматически собирают данные, анализируют их взаимосвязь и передают полученные результаты другим устройствам, чтобы реагирование на угрозы было скоординированным во всей экосистеме распре-



Рис. 3. Число атак по отраслям

ленных сетей — от Интернета вещей до облака.

## ПРОГРАММЫ-ВЫМОГАТЕЛИ

Подобно теневым сетям на базе Интернета вещей, программы-вымогатели становятся все более изощренными. В недавнем отчете Fortinet говорится о росте числа атак на устройства цифровой видеозаписи. Целью злоумышленников является блокировка доступа к сервисам с последующим требованием выкупа. Ранее ограничивающим фактором здесь выступала масштабируемость атаки, но червь Najime автоматизирует процесс построения интеллектуальной инфраструктуры для реализации угрозы.

Особый интерес для вымогателей представляет сфера здравоохранения, и их активность непрерывно возрастает. Впрочем, медицинские учреждения — не единственная уязвимая мишень. Выкуп все чаще требуют за восстановление работоспособности ценных сервисов, причем речь идет не только о шифровании данных. Чтобы обезопасить себя, организациям необходимо идентифицировать и документировать все цифровые активы. Нужно заранее выяснить, чем обернется и к каким потерям приведет недоступность этих сервисов.

Раз уж процесс автоматизирован, злоумышленники не станут ограничиваться какими-то отдельными отраслями. Кто-то, возможно, считает, что распространение вируса WannaCry было целенаправленной атакой вымогателей, но на самом деле это напоминало лесной пожар, уничтожающий все на своем пути. Впрочем, как и Mirai, WannaCry представлял собой лишь бета-версию. Следующий за ним вирус Petya, может быть, и не

нанес такого ущерба, но оказался значительно сложнее.

Отказ в доступе к жизненно важным сервисам — ахиллесова пята не только отрасли здравоохранения. Промышленные системы (например, современные ветроэнергетические установки) тоже все чаще становятся объектом атак вымогателей. Потеря такой установки может стоить до 30 тыс. долларов в день. Если злоумышленнику удастся отключить сразу несколько, от поставщика электроэнергии, скорее всего, потребуют огромный выкуп за восстановление работоспособности всей системы.

Значительный доход приносят и атаки на оборудование, используемое в современном сельском хозяйстве. Уже зарегистрированы требования выкупа за восстановление функционирования сервисов (Интернета вещей и интегрированных систем связи), пострадавших от таких нападений и в этой отрасли. Очевидно, все чаще целью вымогателей будут критически важная инфраструктура и новые взаимосвязанные технологии.

Помимо усиления атак на предприятия, которые могут иметь огромные социальные последствия, наблюдается и рост числа микроатак, ставших возможными благодаря использованию интеллектуальных средств автоматизации. Сколько вы готовы заплатить за восстановление доступа к своему портативному компьютеру, умному телевизору и домашней системе безопасности? Или, скажем, за включение заблокированного холодильника?

Модель вымогательства весьма эффективна, а сами атаки и технологии обхода средств защиты непрерывно совершенствуются. Основным же выводом заклю-

чается в том, что после исправления хакерами всех ошибок и недочетов любая отрасль, которая подвергнется новым типам атак, рискует столкнуться с катастрофическими последствиями.

## СВЕЖИЕ ЭКСПЛОЙТЫ

Интересной общей чертой многих атак, выявленных за последние полгода, является то, что хакеры тратят меньше времени на разработку новых способов проникновения в систему и больше на технологии доставки вредоносного кода и сокрытия атак от средств защиты. Дело в том, что им удается с большим успехом использовать свежие эксплойты, нацеленные на недавно обнаруженные уязвимости, для которых еще не выпущены или не установлены обновления, закрывающие бреши. Червь-вымогатель WannaCry, к примеру, проникал через уязвимость, обновление для которой появилось всего за пару месяцев до этого.

Одна из основных причин успеха хакеров заключается в недостаточно ответственном отношении к принятию необходимых мер безопасности. Сети стремительно расширяются, пересекая границы и охватывая все новые области и среды. Скорость и эффективность имеют важнейшее значение для бизнеса, поэтому простой оборудования считаются недопустимыми. В результате уязвимые устройства не отслеживаются, не обновляются и не заменяются. А поскольку современные сети представляют собой ячеистую среду со связанными между собой элементами, потенциальный риск возрастает.

Возьмем, к примеру, появление «умных» городов. Небезопасный сервер с необновленной системой становится проводником атаки, которая отключает систе-



мы управления движением и аварийные службы. А по мере того, как в такие проекты включаются все новые важные инфраструктурные сети, число потенциальных рисков увеличивается в геометрической прогрессии.

## ОТВЕТСТВЕННОСТЬ ПРОИЗВОДИТЕЛЕЙ УСТРОЙСТВ ИНТЕРНЕТА ВЕЩЕЙ

Устройства и инфраструктура Интернета вещей лишь усложняют проблему. В уже переполненной сети появляется все больше платформ. А высокий уровень их мобильности превращает организацию их обновления в сущий кошмар. Многие устройства Интернета вещей используют жестко зашитые программное обеспечение и телекоммуникационные протоколы, поэтому обновить уязвимые системы не так-то просто, а многие и вовсе невозможны.

Миллионы устройств, подключаемых к Интернету, выпускаются с плохо написанным и уязвимым программным кодом. Более того, производители свободно обмениваются этим кодом друг с другом. В результате одна уязвимость может затронуть сотни различных устройств, предлагаемых десятками разных компаний.

Все это приводит к тому, что новые эксплойты оказываются более опасными, чем предыдущие. Например, эксплойт Devil's Ivy нацелен на уязвимость, которая присутствует в коде gSOAP, используемом в оборудовании физической безопасности — камерах и аппаратах для считывания карт. По меньшей мере 34 различные компании выпускают устройства Интернета вещей, в которых присутствует этот код. Уязвимыми оказываются тысячи разных моделей и миллионы уже установленных устройств.

К сожалению, в мире Интернета вещей наличие таких встроенных и широко распространенных уязвимостей далеко не редкость. А поскольку свежие эксплойты используются в совокупности с эффективными средствами их распространения, мы все чаще видим, как один глобальный киберпожар сменяется другим.

Конечно, эти вызовы не остались незамеченными. Пока производители еще только приступают к решению проблемы, наводняя рынок различными стандартами. Путаница и конкуренция затрудняют

даже правильную маркировку оборудования Интернета вещей, позволяющую понять, какому уровню безопасности оно соответствует, в результате потребителям оказывается сложно выбрать способ наилучшей защиты своих устройств и данных. Между тем время идет. Следующим шагом должно стать установление ответственности производителей за продажу легко взламываемых решений.

Недавно американские сенаторы Марк Уорнер и Кори Гарднер, возглавляющие комитет по кибербезопасности, представили новый проект «Закона об улучшении кибербезопасности Интернета вещей — 2017», выдвинутый сразу от двух партий. Он предусматривает соответствие устройств, приобретаемых правительством США, определенным нормам безопасности, а производители, поставляющие устройства Интернета вещей, должны гарантировать возможность их обновления, отсутствие жестко задокументированных неизменяемых паролей, устранение всех известных уязвимостей и выполнение других базовых требований к безопасности.

Билль № 327 Сената Калифорнии требует, чтобы все устройства Интернета вещей имели встроенные функции безопасности, соответствующие специфике устройства и собираемой им информации, а потребителям и агентствам предоставляется право подавать жалобы на те компании, которые не обеспечивают надлежащей защиты своего оборудования. В законе прописаны меры принуждения, а поскольку штат Калифорния обладает очень мощной экономикой, его принятие может оказать существенное влияние на всю отрасль Интернета вещей.

Таковы последние законодательные инициативы и меры регулирования штатов и федеральных властей США, направленные на то, чтобы побудить производителей устройств Интернета вещей более ответственно относиться к безопасности потребительских данных. Если этого не делать, нас ждет расцвет киберпреступности. Коль скоро у некоторых организаций нет достаточных стимулов к выпуску надежных и безопасных продуктов, сдер-

живающим фактором должна стать угроза штрафов и судебных разбирательств.

## ЗАКЛЮЧЕНИЕ

Технологии упрощают нашу жизнь. Мы получили доступ к беспрецедентному количеству информации, ресурсов, социальных медиа и развлечений — как говорится, только руку протяни. Однако

**Миллионы устройств, подключаемых к Интернету, выпускаются с плохо написанным и уязвимым программным кодом. Более того, производители свободно обмениваются этим кодом друг с другом. В результате одна уязвимость может затронуть сотни различных устройств, предлагаемых десятками разных компаний.**

наше доверие к этим технологиям в значительной мере поколеблено, начиная от систем управления движением и заканчивая медицинскими устройствами и приложениями, позволяющими выполнять и отслеживать финансовые транзакции. Новые типы подключаемых устройств, предоставляющих ценные сервисы, вплетены в сложную экосистему данных, устройств, приложений и сервисов, от которых мы с каждым днем зависим все сильнее.

В результате возрастают количество и сложность атак, использующих это явление. Регулярно появляются бета-версии все новых типов эксплойтов, а уже через несколько недель после выхода первоначальной бета-версии регистрируются атаки второго и третьего поколения, в которых задействованы значительно более сложные инструменты и автоматизированные эксплойты.

Борьбу с этими вызовами необходимо активизировать. Угрозы распространяются с цифровой скоростью, в то время как производители укрепляют безопасность своих продуктов черепашими темпами. Средства безопасности должны быть интегрированы в инструменты и системы еще до их выпуска на рынок. Необходимо искать способы эффективного обнаружения новых киберугроз и организации противодействия им. Нужен полный спектр интегрированных, автоматизированных и взаимодействующих между собой процедур и технологий, которые помогали бы контролировать и защищать ценные ресурсы в процессе их перемещения по расширяющейся цифровой сети. **IAN**

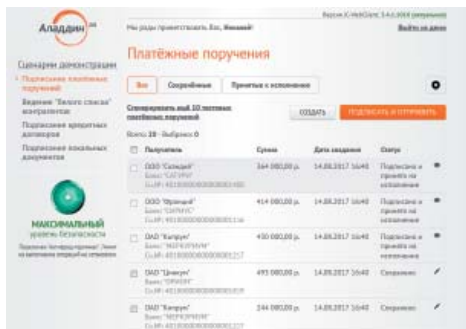
## JC-WebClient v. 4 реализует единую технологию работы с токенами

JC-WebClient компании «Аладдин Р.Д.» позволяет легко встроить в Web-приложения функции для работы с USB-токенами, смарт-картами и устройствами Trust Screen. Он обеспечивает строгую двухфакторную взаимную аутентификацию пользователя и Web-сервера, применение усиленной квалифицированной электронной подписи из Web-браузера, безопасное подтверждение транзакций/операций при работе в недоверенной среде.

Приложение JC-WebClient может легко установить даже неподготовленный пользователь. Оно работает на всех популярных платформах: Microsoft Windows, Apple macOS и Linux. В нем реализована единая технология для работы с браузерами. За счет этого JC-WebClient штатно поддерживает работу со всеми популярными браузерами, в том числе Google Chrome, Opera, Яндекс.Браузер, Mozilla Firefox, Apple Safari, Microsoft Internet Explorer, Microsoft Edge и др.

JC-WebClient легко встраивается в Web-приложение, так как предоставляет простой API и исчерпывающие примеры интеграции. Единая технология работы с токенами, лежащая в основе JC-WebClient, избавляет разработчиков от проблем с совместимостью при использовании различных браузеров. При этом JC-WebClient не накладывает ограничений на тип Web-сервера и язык разработки Web-приложений.

JC-WebClient предоставляет свободу выбора модели токена и вида применяемой ЭП как для разработчиков, так и для пользователей. Поддерживается работа с российскими криптографическими алгоритмами ГОСТ 28147-89, ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001, а также новыми алгоритмами ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012, переход на которые состоится в 2018 году, а кроме того, с алгоритмами 3DES, AES-128, SHA-1 и RSA-1024, которые могут использоваться для аутентификации, использования усиленной ЭП и шифрования данных.



## Неуправляемые коммутаторы CentreCOM GS920

Технические специалисты, обслуживающие небольшие сети, обычно осуществляют конфигурацию своих устройств посредством командной строки или графического интерфейса пользователя, однако многие предпочитают еще более простой способ настройки — как в коммутаторах серии CentreCOM GS920 компании Allied Telesis, где функции, используемые часто, настраиваются с помощью DIP-переключателя на передней панели.

Все модели CentreCOM GS920 поддерживают функцию Loop Guard, что помогает избежать образования петель на границе сети. Loop Guard позволяет обнаружить такие петли и блокирует попавшие в них порты, которые автоматически подключаются снова после устранения петли. Поддерживаются также необходимая скорость работы и дуплексная конфигу-



рация порта. Это помогает эффективно эксплуатировать более старые конечные устройства, где автоматическое согласование либо отсутствует, либо требует фиксированной скорости / дуплексного режима.

Коммутаторы CentreCOM GS920 доступны для заказа у официальных дистрибьюторов в России: Landata, Merlion, Soft-Tronik, Treolan. Для всех моделей возможно расширение гарантии с 2 до 5 лет при условии их регистрации на сайте вендора.

## Коммутаторы Aruba серии 8400 с новой ОС OS-CX

Компания Aruba, входящая в состав Hewlett Packard Enterprise, объявила о доступности новых коммутаторов уровня ядра и агрегации сети, а также продвинутой операционной системы ArubaOS-CX. Все эти продукты разработаны с учетом требований по обеспечению мобильности, поддержки облачных сред и Интернета вещей. Современная ОС ArubaOS-CX автоматизирует и упрощает многие критические и сложные сетевые задачи, обеспечивая автоматизированный мониторинг для раннего обнаружения проблем, ускоренное устранение неполадок благодаря наличию точных данных о состоянии сети и упрощенное программирование для масштабирования решения.

Решение Aruba Network Analytics Engine позволяет отслеживать сетевые, системные, прикладные и связанные с безопасностью события за счет мониторинга на основе правил и автоматической корреляции сетевых активностей. Благодаря встроенной базе данных для хранения временных рядов в сочетании с корреляцией событий, этот механизм позволяет анализировать тенден-

ции, чтобы на основании полученных результатов прогнозировать и предотвращать потенциальные проблемы, вызванные узкими местами производительности, безопасности и масштабируемости.

Коммутаторы Aruba серии 8400 оснащены полностью программируемой ОС и средствами интеллектуальной, реализуемой на основе политик, интеграции с инструментами мониторинга сети, производительности и безопасности, что позволяет оперативно выявлять неполадки в автоматическом режиме. Они являются полностью программируемыми, поскольку имеют встроенный интерпретатор Python и REST API.

Благодаря масштабируемому дизайну коммутационной фабрики Aruba 8400, можно осуществить бесшовную модернизацию, если потребуются увеличить пропускную способность сети. Технология организации стека Virtual Switching Framework (VSF), реализованная на двух шасси, обеспечивает поддержку до 512 портов 10GbE, 128 портов 40GbE или 96 портов 100 GbE

# ИНТЕРНЕТ

## ТЕЛЕФОНИЯ · ТЕЛЕВИДЕНИЕ

В ОФИСЕ, КВАРТИРЕ И КОТТЕДЖЕ



ЗОНА ПОКРЫТИЯ СЕТИ  
КРЕДО-ТЕЛЕКОМ



для физ. лиц

**до 100 Мбит/с**

для юр. лиц

**до 400 Мбит/с**

Срок подключения - от 3 до 7 дней.

Реклама



- широкополосный доступ в Интернет со скоростью до 400 Мбит/с;
- каналы связи VPN, L2 VPN, VPLS;
- подключение соединительных линий и телефонных номеров в кодах 495/496/498/499;
- виртуальная АТС;
- организация общественных хот-спот Wi-Fi и закрытых корпоративных Wi-Fi зон;
- виртуальный и физический хостинг;
- облачный сервер.

Оборудование предоставляется клиентам во временное пользование бесплатно.

**8-800-100-8281**

БЕСПЛАТНЫЙ КРУГЛОСУТОЧНЫЙ ТЕЛЕФОН

НАШ САЙТ: [WWW.RMT.RU](http://WWW.RMT.RU)



11 октября

мирцод

[2017]

[www.osp.ru/dcworld/](http://www.osp.ru/dcworld/)

# СЕРВИСЫ. ОБЛАКА

ЦОД для облака, облачные сервисы, услуги КЦОД.

В центре внимания – новые тенденции использования облачных сред с учетом перспектив перехода к цифровой экономике.

## Основные темы форума

- ◆ Развитие услуг и сервисов КЦОД
- ◆ Инфраструктура
- ◆ Территориально распределенные облака
- ◆ Безопасность
- ◆ Облака для разработчиков
- ◆ Децентрализация ЦОД

Золотые партнеры

ATLEX

ROS  
ПЛАТФОРМА

Партнеры

ИМПУЛЬС  
ИСТОЧНИКИ БЕСПЕРЕБОЙНОГО ПИТАНИЯ

Brain4Net

DATALINE  
Member of IMAC Technologies Group

Kingston  
TECHNOLOGY

laitecom

RIT



Реклама 12+

По вопросам участия: Ольга Пуркина



+7 (499) 703-1854, +7 (495) 725-4780



[kon@osp.ru](mailto:kon@osp.ru)