

App Store



Google play



<http://www.lanmag.ru> МАЙ 2017

ЖУРНАЛ  
СЕТЕВЫХ  
РЕШЕНИЙ

LAN



# Мониторинг ИТ-инфраструктуры

Проблемы мониторинга ИТ-инфраструктуры

Новинки ИБП и тенденции рынка

Как правильно организовать видеонаблюдение

ISSN 1027086-8

17005



771027 086001

<http://www.lanmag.ru>

ЖУРНАЛ  
СЕТЕВЫХ  
РЕШЕНИЙ

# LAN

МАЙ 2017  
ТОМ 23  
НОМЕР 5 (239)



Читайте нас на Facebook



Читайте нас в Twitter



## 1 КОЛОНКА РЕДАКТОРА

Всё под контролем?

Дмитрий Ганьжа

## 2 НОВОСТИ

Imperva открыла центр очистки трафика

ZyXEL меняет бизнес-модель

Allied Telesis: 30 лет на сетевом рынке

## 9 ИНТЕРВЬЮ

Интервью с Алексеем Севастьяновым,  
первым заместителем генерального  
директора, DataLine

Александр Барсков

## 10

Интервью с Владимиром Рубановым,  
управляющим директором, «Росплатформа»

Дмитрий Ганьжа

## 13 СОБЫТИЯ

Cisco Connect 2017: навстречу цифровой  
трансформации

Дмитрий Ганьжа

## 16

AIM — теперь в стандарте

Александр Барсков

## 20

IoT как инструмент цифровой экономики

Александр Барсков

## 22

«Абитех» подписала соглашение с GE  
о выпуске ИБП под маркой «А-ИСТ»

Дмитрий Ганьжа

## 24

Schneider Electric Innovation Summit 2017:  
акцент на EcoStruxure и IIoT

Александр Барсков, Дмитрий Ганьжа

## 28

### ТЕМА НОМЕРА

Системный мониторинг:  
сопровожаем СЭД проактивно

Алексей Корепанов

## 31

Проблемы стандартного и выгоды  
нестандартного мониторинга здоровья  
ИТ-инфраструктуры

Павел Рыцев

## 34

### НОВЫЕ ТЕХНОЛОГИИ И ПРОДУКТЫ

ИБП: тенденции и новинки

Александр Барсков

## 42

### БИЗНЕС-ВИДЕО

Как организовать видеонаблюдение «по уму»

Дмитрий Ганьжа

## 48

### НОВШЕСТВА

Бюджетное пополнение линейки ИБП

Smart-UPS On-Line

Многофункциональное устройство iBoot-PoE  
для управления питанием

Взрывозащищенные

тепловизионные камеры Axis

## Всё под контролем?

Мониторинг современной ИТ-инфраструктуры настолько усложнился, что многие компании только констатируют снижение производительности приложений, будучи не в состоянии выявить его причины. Истоки такой ситуации очевидны: чрезвычайная сложность сетей и приложений. Тем более что в результате органического роста инфраструктуры нередко образуется гремячая смесь из современных и унаследованных технологий и инструментов для их использования. Инфраструктура состоит из множества физических и виртуальных компонентов, приобретенных у разных вендоров, и зачастую распределена между несколькими площадками. А с переносом некоторых систем во внешнее облако задача контроля в такой гибридной среде еще более усложняется.

Пять? Десять? Пятьдесят? Число используемых для ИТ-инфраструктуры инструментов мониторинга, управления и планирования варьируется от нескольких единиц до нескольких десятков (когда для каждой платформы и системы предусмотрен отдельный инструментарий). При этом нередко та или иная часть инфраструктуры остается вообще без присмотра. По данным исследования SevOne, одного из ведущих поставщиков решений для мониторинга производительности приложений, мониторинг сетевого оборудования осуществляют 85% опрошенных компаний, но лишь 63% анализируют трафик. Мониторинг ЦОДов и серверов есть у 81% организаций, а отслеживают производительность приложений только 66% участников опроса.

Только 11% компаний полностью довольны возможностями используемых ими средств для управления и мониторинга и получаемой от них отдачей. Как отмечается в отчете, унаследованные инструменты не всегда масштабируются, несовместимы между собой, не предоставляют целостной картины общего состояния инфраструктуры и в конечном итоге оказываются не в состоянии поддерживать растущие требования бизнеса.

Согласно приводимой оценке, при использовании разрозненных средств мониторинга лишь от 20 до 40% всей инфраструктуры находится под контролем, хотя при такой неполноте получаемой картины о реальном контроле говорить вряд ли возможно.

Каков же выход? Использование централизованной масштабируемой платформы — зонтичного продукта, который консолидировал бы данные от различных средств мониторинга. Однако многим продуктам на базе открытого исходного кода не хватает необходимой функциональности, а платформы управления и мониторинга корпоративного класса чрезмерно дороги. И без того сложное положение дел усугубляется тем, что, как отмечается в статье Павла Рыцева, «Проблемы стандартного и выгоды нестандартного мониторинга здоровья ИТ-инфраструктуры», «даже внедрив довольно развитую и недорогую систему мониторинга, можно не получить желаемого результата из-за недостатка квалификации персонала».

Надлежащий мониторинг позволяет не только предупредить и разрешить проблемы в функционировании ИТ-систем, но и повысить эффективность внутренних бизнес-процессов (см. например, статью Алексея Корепанова «Системный мониторинг: сопровождаем СЭД проактивно») и, как следствие, успешность бизнеса. Помимо решения текущих задач, мониторинг позволяет спланировать потребность в ресурсах и оборудовании при росте бизнеса, то есть, как и ИТ, является интегральной частью бизнеса. Однако до сих пор он нередко рассматривается в качестве побочного процесса. Если в компании все же осознают важность ИТ-мониторинга, но не обладают собственными ресурсами и кадрами для его внедрения, можно воспользоваться услугами соответствующих провайдеров. **LAN**



Дмитрий Ганьжа

<http://www.lanmag.ru>

ЖУРНАЛ  
СЕТЕВЫХ  
РЕШЕНИЙ

**LAN**

12+

№ 5, май 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.

### КОРРЕКТОР

Карпушина И.

### 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:  
26.05.17 г.



**ОТКРЫТЫЕ  
СИСТЕМЫ**  
Open Systems Publications

### ПРЕЗИДЕНТ

Михаил Борисов

### ГЕНЕРАЛЬНЫЙ ДИРЕКТОР

Галина Герасина

### ДИРЕКТОР ИТ-НАПРАВЛЕНИЯ

Павел Христов

### КОММЕРЧЕСКИЙ ДИРЕКТОР

Татьяна Филина

- 3 Imperva открыла центр очистки трафика
- 5 ZyXEL меняет бизнес-модель
- 8 Allied Telesis: 30 лет на сетевом рынке

## 3data строит моновендорный ЦОД на основе оборудования Legrand

Уже в сентябре новый ЦОД будет готов принять первых клиентов.



Фото: Александр Барсков

**Илья Хала:**  
«Мы понимаем все минусы моновендорного подхода, но в данном случае плюсы перевешивают»

**Алексис Конан:**  
«Стратегия Группы Legrand — предлагать законченные решения для ЦОДов»



Фото: Александр Барсков

В середине апреля компания 3data и Группа Legrand объявили о строительстве в Москве первого в России ЦОДа, который будет полностью базироваться на технических решениях Legrand. Согласно объявленному плану, ЦОД примет первых клиентов уже 1 сентября текущего года. За обеспечение телеком-решений отвечает оператор связи «Мастертел».

Компания 3data уже построила в Москве сеть из 10 небольших коммерческих ЦОДов (до 100 стоек) недалеко от мест концентрации бизнес-центров. В течение ближайших 10 лет их число планируется увеличить до 50. Вместо организации крупных (мега-) ЦОДов в промышленных зонах компания делает ставку на реализацию принципа «шаговой доступности» и предоставление сервиса с «премиальным качеством».

По словам генерального директора 3data Ильи Халы, в своих ЦОДах компания эксплуатирует оборудование практически всех основных производителей. В какой-то момент появилась идея реализовать ЦОД полностью на базе оборудования одного поставщика. В 3data хорошо понимают потенциальные минусы такого варианта (зависимость от поставщика, ограниченный выбор продуктов), но все же плюсов, по мнению Ильи Халы, значительно больше. В первую очередь это экономия средств, сокращение сроков поставки и реализации, а также высокая степень интеграции. Сегодня, уверен Илья Хала, только три компании способны предложить полное решение. Хотя он и не назвал их, помимо Legrand, видимо, имелись в виду Schneider Electric и Huawei. При реализации обсуждаемого проекта выбор был сделан в пользу Legrand, чему в немалой степени способствовали серьезные инвестиции со стороны этого производителя.

Новый центр обработки данных сооружается на первом этаже технологического центра Legrand на Садовом кольце. На втором этаже будут находиться офисные помещения для обслуживания заказчиков, на третьем — учебный комплекс. Уникальность создаваемого учебного центра заключается в том, что его посетителям можно будет продемонстрировать

решения компании непосредственно на примере действующего ЦОДа — естественно, с соблюдением строгого регламента доступа.

Как отметил Алексис Конан, генеральный директор представительства Группы Legrand в России и СНГ, компания уже более 20 лет работает в России и ее продукция пользуется устойчивым спросом во многих отраслях экономики. Однако решение об активизации деятельности на рынке решений для ЦОДов было принято относительно недавно. С этой целью компания пополнила свой портфель новыми предложениями, в том числе путем покупки таких производителей, как Minkels и Raritan. Первая известна прежде всего своими системами изоляции коридоров и оптимизации воздушных потоков, что позволяет существенно повысить эффективность охлаждения ЦОДов. Вторая — один из ведущих разработчиков переключателей KVM и блоков распределения электропитания.

Помимо названных продуктов, Legrand предлагает источники бесперебойного питания, трансформаторы, структурированные кабельные системы, кабеленесущие системы для оптических трасс и т. д. Одна из немногих позиций, представленная пока продуктами сторонних производителей, — кондиционеры. В своих комплексных решениях Legrand применяет хорошо известные на рынке блоки охлаждения Stulz. Примечательно, что в других ЦОДах 3data использует оборудование Stulz, которое эксперты компании считают лучшим в своем классе.

Одним из важных положений деятельности Группы Legrand является локализация производства в России. В Ульяновской области уже работают два предприятия, где осуществляется сборка ИБП и конденсаторных установок, изготавливается защитно-коммутационное оборудование, кабеленесущие системы и прочее электрооборудование. В планах компании — открытие еще одной производственной площадки в Ульяновской области в 2018 году.

Александр Барсков



# Imperva открыла в России центр очистки трафика от DDoS-атак

Установленная в России система производительностью 100 Гбит/с стала частью распределенной сети узлов очистки с суммарной пропускной способностью более 3,5 Тбит/с.

Компания Imperva, один из ведущих мировых разработчиков продуктов для защиты Web-приложений и СУБД, сообщила об открытии первого в России центра очистки трафика от DDoS-атак — Incapsula. Соответствующий облачный сервис компания приобрела в 2014 году вместе с одноименным разработчиком (компания Incapsula). В России точка присутствия (PoP) Incapsula размещена в Москве на площадке коммерческого ЦОДа IXcellerate. Производительность этой точки PoP составляет 100 Гбит/с, при этом представители Imperva отмечают, что она может быть легко увеличена по мере необходимости.

Как поясняет Давид Шульман, руководитель направления Imperva Incapsula, ранее трафик российских клиентов приходилось направлять для очистки через Варшаву и Стокгольм, что негативно сказывалось на производительности и вело к задержке получения уже очищенного трафика. Кроме того, для многих крупных отечественных компаний критически важно, чтобы обрабатываемый трафик не выходил за пределы территории РФ.

До открытия PoP в России сервисом Incapsula пользовались около двух десятков частных компаний, для которых выход трафика за границы страны особого значения не имел. За первые три месяца после открытия узла к числу пользователей сервиса добавилось пять крупных заказчиков, среди которых — общенациональный платежный сервис и телеканал.

«Мы являемся единственным западным производителем (систем защиты от DDoS), который инвестировал средства в организацию собственного центра очистки в России, — подчеркивает Давид Шульман. — Это открывает нам двери к новым категориям заказчиков, включая государственный сектор, крупные банки, ведущие торговые сети и т. д.».

Помимо защиты от DDoS-атак, московский узел Incapsula поддерживает ряд других функций. Это интеллектуальное кеширование и оптимизация контента на основе технологий CDN, межсетевое экранирование Web-приложений (WAF), а также балансировка нагрузки для обеспечения высокого уровня доступности приложений.

По словам Александра Шахлевича, директора по продажам Imperva в России и СНГ, чтобы сегодня эффективно бороться с масштабными DDoS-атаками, нужна разветвленная сеть высокопроизводительных центров очистки. У Imperva таких центров уже 33, и число их будет постоянно увеличиваться. Суммарная производительность сети центров очист-

ки Incapsula составляет более 3,5 Тбит/с. Как рассказал представитель Imperva, буквально в декабре 2016 года система Incapsula заблокировала атаку общей мощностью 650 Гбит/с. Если бы эту атаку отразить не удалось, она могла бы «положить» сеть национального оператора связи крупной страны.

Защита от DDoS-атак крайне необходима организациям из различных отраслей экономики. Острота проблемы возрастает с развитием Интернета вещей (IoT). Подключаемые к Сети «вещи», как правило, не оснащаются средствами информационной защиты, при этом они постоянно находятся в режиме онлайн, чем активно пользуются злоумышленники. Как рассказал Александр Шахлевич, недавно в массовой атаке были задействованы около 100 тыс. подключенных устройств IoT.

Инвестиции в московский узел очистки трафика — лишь часть стратегического плана экспансии Imperva на российский рынок, в котором производитель видит огромный потенциал. Одна из важнейших задач компании — развитие канала продаж и дальнейшее увеличение числа пользователей продуктов и сервисов Imperva. Немаловажная роль в ее решении отводится взаимодействию Imperva с дистрибьютором — компанией RRC. По словам Юлии Грековой, менеджера по развитию бизнеса RRC Security, с открытием московского узла Incapsula существенно расширяется поле деятельности для партнеров, продающих решения SaaS. «Теперь в портфеле RRC Security есть полноценный пакет SaaS-продуктов: защита от DDoS-атак, балансировка нагрузки, WAF и прочее», — отметила Юлия Грекова.

Александр Барсков



**Давид Шульман:**  
«Мы являемся единственным западным производителем систем защиты от DDoS, который инвестировал средства в организацию собственного центра очистки в России»

## Злоумышленники копят силы

Согласно отчету «Лаборатории Касперского», в I квартале зафиксировано уменьшение числа DDoS-атак и снижение их продолжительности. Подобное начало года является достаточно традиционным — такая ситуация наблюдается на протяжении последних пяти лет. Как заметил Алексей Киселев, менеджер Kaspersky DDoS Prevention в России, злоумышленники тоже не прочь устроить себе отпуск. Однако, если сравнивать с аналогичным периодом предыдущего года, сложность атак продолжает расти: в «Лаборатории Касперского» отмечают рост числа атак с использованием шифрования, что соответствует тенденции усложнения DDoS-атак, которые становится нелегко обнаружить стандартными защитными инструментами.

## ЦОД с акцентом на безопасности

В Москве введен в эксплуатацию ЦОД SafeDC, который ориентирован на предоставление облачных сервисов безопасности.



**Игорь Калайда:**  
«Примерно два года назад компания приняла решение предоставлять услуги на базе своих продуктов, для чего и было начато строительство ЦОДа»

В середине мая компания «НИИ СОКБ» объявила о запуске коммерческого ЦОДа SafeDC, который будет специализироваться на предоставлении услуг Security as a Service (SecaaS), реализованных на базе собственных решений компании и на платформах ее партнеров. По сути, это первый профильный ЦОД в России, ориентированный на сервисы защиты данных и информационной безопасности.

Как рассказывает Игорь Калайда, генеральный директор НИИ СОКБ, будучи одним из лидеров российского рынка информационной безопасности, примерно два года назад компания приняла решение о предоставлении услуг на базе своих разработок, для чего и было начато строительство ЦОДа. Он называет две основные причины для принятия такого решения. Во-первых, это стремление многих российских заказчиков переложить свои расходы с капитальных затрат (CAPEX) на текущие (OPEX). Во-вторых — тенденция к импортозамещению, которая дает новые возможности российским разработчикам.

ЦОД SafeDC расположен в Москве, в районе метро «Калужская», на подземных этажах бизнес-центра. Помещения ЦОДа находятся в собственности НИИ СОКБ. Общая площадь ЦОДа — 240 м<sup>2</sup>, подведенная электрическая мощность — 1 МВт, ЦОД способен вместить до 120 стоек с ИТ-оборудованием. Объект спроектирован с учетом требований, предъявляемых к ЦОДам уровня Tier III, однако в получении соответствующего сертификата (от Uptime Institute) представители НИИ СОКБ необходимости пока не видят. Вместе с тем SafeDC аттестован на соответствие первому классу и первому уровню защищенности ИС для работы с государственными информационными ресурсами и персональными данными граждан.

SafeDC имеет собственный оптический канал до М9. Прямая оптическая связь реализована и с резервной площадкой, которая также располагается в Москве. Серверная инфраструктура ЦОДа основана на решениях Flex System компании Lenovo, а сетевая инфраструктура — на оборудовании Juniper Networks.

Одним из первых сервисов безопасности, доступных на базе SafeDC, стал сервис защищенной мобильной связи, построенный на базе MDM-системы SafePhone, разработанной НИИ СОКБ. Это решение обеспечивает управление корпоративными мобильными устройствами и приложениями, а также оперативное реагирование на различные связанные с ними инциденты (утрача, кража и пр.). Защищенная связь для этого сервиса предоставляется на базе решений «ИнфоТеКС».

Кроме того, на базе SafeDC уже доступны или будут доступны в самое ближайшее время целый ряд других сервисов SecaaS. В частности, сервис PayControl на базе решений компании SafeTech для безопасной аутентификации на порталах и в системах, а также для подписи документов с использованием мобильных устройств. На платформе Skybox будет развернута система постоянного контроля сетевой безопасности клиентов ЦОДа — с информированием о наличии уязвимостей и выработкой рекомендаций по их устранению.

Решение еще одного партнера НИИ СОКБ — компании Group-IB — стало основой для предоставления услуг по предупреждению киберпреступлений. А компания Qualys планирует развернуть на базе SafeDC облачный сервис по управлению уязвимостями и контролю соответствия отраслевым стандартам, требованиям регуляторов и корпоративным политикам безопасности.

Важным преимуществом проекта SafeDC является то, что сервисы безопасности могут применяться в связке, что позволит комплексно решать задачи по защите ИТ-ресурсов заказчика. Одним из примеров применения сразу нескольких решений является защита сервиса «Медкарта 24» — облачной платформы для врачей и пациентов, которая также будет развернута в SafeDC.

НИИ СОКБ планирует расширять набор предоставляемых на базе ЦОДа сервисов. Владимир Бычек, директор по развитию НИИ СОКБ, заявил о том, что компания намерена превратить SafeDC в «конвейер услуг информационной безопасности». Кроме того, в планах НИИ СОКБ — формирование «коробочных решений», чтобы облачные сервисы безопасности могли предоставлять и другие коммерческие ЦОДы. Таким образом, в других ЦОДах руководители НИИ СОКБ видят не конкурентов, а скорее потенциальных партнеров.

Помимо сервисов безопасности, на базе SafeDC предоставляются и классические услуги коммерческого ЦОДа, включая размещение оборудования, аренду стоек, предоставление виртуальных серверов и т. д. Для дополнительной защиты устанавливаемого в ЦОДе оборудования НИИ СОКБ предлагает вариант «ЦОД в ЦОДе» на базе сейфовых шкафов Lampertz. Однако, учитывая небольшие размеры SafeDC, предоставлять облачные сервисы выгоднее, так как они дают гораздо больший доход с единицы площади.

Руководители НИИ СОКБ не раскрывают объема инвестиций в новый ЦОД, но надеются, что они окупятся в течение 4–5 лет.

Александр Барсков

## ZyXEL меняет бизнес-модель

Тайваньская компания ZyXEL решила сфокусироваться на решениях для SMB и операторов связи. Марка интернет-центров Kinetic будет выделена в отдельный бизнес.

Сетевое оборудование потребительского класса превращается в ширпотреб, а значит, основным дифференцирующим фактором становится цена. И поскольку конкурировать с китайскими производителями тяжело даже тайваньским, осенью прошлого года ZyXEL приняла решение о трансформации своего бизнеса: производитель оборудования превратится в поставщика решений и сосредоточится на продуктах для малых и средних предприятий и операторов связи. О том, как новая стратегия скажется на деятельности компании на российском рынке, рассказал Дмитрий Танюхин, назначенный руководителем канала продаж в России и СНГ.

Для лучшей сфокусированности на целевых направлениях в июне-июле планируется открыть в Москве новый офис продаж, штат которого будет состоять из 5–10 человек. При продвижении продукции ставка будет делаться на системных интеграторов и VAR, причем, как рассчитывают в компании, для них удастся обеспечить привлекательную маржу — до 30% по определенным линейкам продуктов. Наряду с организацией подменного фонда рассматривается возможность осуществлять замену техники в течение 24 ч по крайней мере в крупных городах. Для облегчения работы с госорганами оборудование планируется сертифицировать во ФСТЭК.

Отмечается, что, несмотря на кризисный спад, компании удалось увеличить свою долю на российском рынке сетевого оборудования для SMB, и теперь ее главная задача — довести оборот до 10 млн долларов (без учета потребительского оборудования). Конечно, в первую очередь достижение этой цели будет зависеть от усилий сформированной команды, но, по мнению Дмитрия Танюхина, поможет и использование европейских ресурсов компании в части логистики, сервиса и финансов. К тому же в Европе компания давно фокусируется на решениях для SMB и операторов связи и имеет там большой склад оборудования. К слову, на европейский рынок приходится половина бизнеса ZyXEL, объем которого — в мировом масштабе — составляет около 500 млн долларов.

ZyXEL намерена сосредоточиться на пяти продуктовых направлениях (для SMB): сетевая безопасность (межсетевые экраны ZyWall), коммутаторы, контроллеры и точки доступа Wi-Fi, промышленные коммутаторы и облачный сервис Nebula для управления сетями Wi-Fi. На все эти пять продуктовых линеек будет приходиться, согласно предварительной оценке, три четверти оборота обновленной компании в России (оставшаяся четверть — на устройства CPE, которые будут поставляться операторам). Ключевыми

направлениями являются коммутаторы и устройства безопасности. Как утверждается, на российском рынке компания занимает третье место по продажам аппаратных межсетевых экранов.

К числу своих целевых отраслей ZyXEL относит гостиничный и ресторанный бизнес, где обслуживание гостей уже нельзя представить без беспроводного доступа Wi-Fi. Как рассчитывают в компании, наряду с беспроводным оборудованием будет востребован и облачный сервис Nebula по управлению сетью, поскольку он позволяет сократить расходы на администрирование сети, что для отелей и ресторанов является к тому же непрофильной деятельностью. Nebula позволяет управлять как беспроводными, так и проводными устройствами, причем не только внутри одного офиса, но и в рамках распределенной сети, охватывающей сотни площадок. При покупке оборудования будет предоставляться бесплатная двухгодичная подписка на сервис. Впрочем, возможность использования сервиса в России пока детально не прорабатывалась.

Согласно данным компании, ее оборудование используют примерно 700 тыс. предприятий из разных стран мира, поэтому у ZyXEL накоплен немалый опыт предоставления решений для выбранного целевого сегмента. Однако тенденция применения стандартного, типового оборудования охватывает уже не только потребительский сегмент, но и корпоративный. К тому же конкуренция в сегменте SMB достаточно высока, да и маржа обычно не намного больше, чем на рынке потребительского оборудования. Так что достижение поставленных при ребрендинге целей представляется непростой задачей.

Дмитрий Ганьжа



Фото: Дмитрий Ганьжа

**Продвижением решений ZyXEL для SMB и операторов будет заниматься отдельная команда, которую набирает Дмитрий Танюхин**

### МСЭ с поддержкой VPN

Новинка от ZyXEL, МСЭ SG2200-VPN, предназначена для предприятий SMB, имеющих несколько офисов. Межсетевой экран SG2200-VPN способен поддерживать множество соединений VPN (до 3000 туннелей IPSec/SSL/L2TP over IPSec) благодаря наличию интегрированного концентратора VPN. Входящие и исходящие соединения защищаются новейшим шифрованием SHA-2.



## Dell EMC обновила решения для резервного копирования

В дополнение к Data Domain, Dell EMC теперь предлагает интегрированные устройства для резервного копирования Integration Data Protection Appliance.

Данные лежат в основе цифровой трансформации. Их безопасность и доступность представляются ключевыми факторами для успеха последней. Одним из элементов обеспечения сохранности и, следовательно, доступности данных являются их резервное копирование и восстановление. Как заявил Михаил Саркисов, руководитель направления «Системы резервного копирования и восстановления данных» Dell EMC в России и странах СНГ, представляя соответствующие решения, «Dell EMC — единственная компания, для которой защита данных является фокусным рынком». Dell EMC занимает более 60% рынка специализированных устройств для резервного копирования и восстановления данных, а по продажам соответствующего программного обеспечения уступает только Veritas. При этом общий объем поставок — устройств и ПО — в 2016 году превысил 3 млрд долларов. Компания активно инвестирует в разработку новых решений для данного рынка — с 2003 по 2016 год на эти цели потрачено 5 млрд долларов.

Тивные последствия от инфекций наподобие нашумевшего вируса-шифровальщика WannaCry. Однако данные можно будет восстановить, если только не пострадают резервные копии. Для защиты наиболее критичной информации в прошлом году Dell EMC предложила решение Isolated Recovery Solution, предусматривающее изоляцию системы, где хранится «золотая копия» данных. Соединение с сетью активируется на непродолжительное время для синхронизации последних версий файлов. Во избежание компрометации каждая новая «золотая копия» проходит проверку на целостность. При обнаружении повреждений система блокируется. При необходимости восстановление осуществляется в изолированной области.

При организации резервного копирования EMC традиционно делает ставку на дисковые системы. «Резервное копирование данных сходит на нет в силу медленного восстановления данных с ленты», — заявил Михаил Саркисов. Однако данное утверждение представляется все же не вполне справедливым. Спрос на ленточные накопители остается достаточно стабильным, появляются новые продукты и технические решения. Более того, по целому ряду показателей ленты предпочтительнее дисков. Например, при потоковом резервном копировании больших объемов данных современные ленточные накопители способны обеспечить неплохую скорость записи (до 120 Мбайт/с), при этом лента остается самым дешевым носителем. Как отмечается в отчете «Рынок ленточных систем: анализ отрасли и прогноз на 2017–2025 годы» аналитического агентства Persistent Market Research, спрос на ленту будет сохраняться благодаря таким факторам, как потребность в длительном хранении данных для соответствия нормативным требованиям.

На форуме Dell EMC World 2017 производитель представил свое первое интегрированное устройство для резервного копирования Integrated Data Protection Appliance (IDPA) в пакете с ПО — ранее программное обеспечение для резервного копирования предлагалось отдельно от целевых устройств Data Domain. Модельный ряд включает четыре модели: DP5300, DP5800, DP8300 и DP8800 (от 34 Тбайт до 1 Пбайт полезной емкости). В качестве аппаратной платформы используются серверы Dell EMC Power Edge. Как и Data Domain, IDPA поддерживают дедупликацию на лету — утверждается, что средний уровень дедупликации составляет 55 к 1. Среди других функций — встроенное резервирование в облако, шифрование и аналитика данных.



Источник: Dell EMC

В отличие от Data Domain, для интегрированного устройства защиты данных IDPA не придется приобретать программное обеспечение для резервного копирования

Для резервного копирования и восстановления данных Dell EMC предлагает портфель решений Data Domain, куда входят СХД, ПО и ОС. По словам Михаила Саркисова, на эти решения приходится около 15% продаж в России. СХД Data Domain представлены пятью различными моделями: DD2200 — для небольших компаний, DD6300 и DD6800 — для средних, DD9300 и DD9800 — для крупных. Среди прочих их функций представители Dell EMC выделяют дедупликацию на лету, благодаря которой можно снизить потребность в физической емкости хранения в 10–30 раз. Кроме того, год назад EMC представила программную версию своих систем Data Domain Virtual Edition. Это виртуальное устройство устанавливается на гипервизор VMware, а заказчик может использовать любое оборудование по своему выбору.

Регулярное резервное копирование представляет собой прекрасный способ минимизировать нега-

Дмитрий Ганьжа



# Avanpost WebSSO аутентифицирует пользователей в Web

Новый продукт Avanpost WebSSO обеспечивает единый вход в мобильные, традиционные и Web-приложения.

В текущем году десятилетие своей деятельности отмечает компания Avanpost. Как заявил ее генеральный директор Андрей Конусов, компания является лидером российского рынка в области решений идентификации и управления доступом к информационным ресурсам (IDM). В прошлом году число пользователей продукта для PKI, созданного этим разработчиком, перевалило за 1 млн человек. В 2016 году общий рост продаж компании составил более 40%, имеющийся задел проектов позволяет рассчитывать на увеличение оборотов еще в 1,5 раза в 2017 году.

Другой продукт компании, Avanpost IDM, успешно конкурирует на российском рынке с решениями таких мировых вендоров, как IBM и Oracle. По словам Андрея Конусова, за последнее время компания не проиграла ни одного тендера. Ослаблению позиций западных вендоров способствуют удвоение стоимости лицензий в результате роста курса доллара и негибкая политика этих производителей в отношении обновления своих продуктов. Так, у Oracle переход на новую версию продукта по сути предполагает его повторное внедрение, что оказывается далеко не простой задачей. Если же клиенты решают оставить прежнюю версию продукта, то через какое-то время сталкиваются с тем, что ее поддержка прекращается.

В результате создаются объективные предпосылки для перехода пользователей на продукты других вендоров (не обязательно Avanpost). Кроме того, спросу на российские системы обеспечения безопасности способствуют санкционные риски — например, торгово-промышленная палата США запретила компании SailPoint продавать ее IDM-решение «Роснефти».

Несмотря на кризис, компания Avanpost не прекращала вкладывать силы и средства в разработку собственных решений и в середине марта представила новый программный продукт Avanpost WebSSO для безопасной регистрации в SaaS-, мобильных и традиционных приложениях после однократной аутентификации (Single Sign-On, SSO). Работа над ним началась в 2015 году. Компания уже реализовала пилотный проект по аутентификации пользователей на региональном портале крупной федеральной структуры.

В рамках пилотного проекта обеспечивается обработка до 1,5 тыс. запросов на аутентификацию в минуту, при этом обслуживается 5 млн человек. После ввода учетных данных и подтверждения личности, что в среднем занимает менее 3 с, пользователь получает доступ ко всем сервисам портала, то есть фактически ко всем информационным системам, обеспечивающим работу этих сервисов. За автоматическую регистрацию в данных системах и отвечает Avanpost WebSSO. После

перевода в промышленную эксплуатацию будет осуществляться поддержка 12 млн пользователей.

У Avanpost уже есть продукт для единого входа в традиционные приложения — Avanpost SSO. Новое решение, ориентированное на обеспечение автоматической регистрации в среде Web, рассчитано на такие сценарии применения, как общая аутентификация в приложениях пользователей распределенной организации, федеративная аутентификация для нескольких организаций на базе одной из них и аутентификация в SaaS-приложениях в частном облаке. Avanpost WebSSO может использоваться как отдельно, так и совместно с Avanpost IDM. Применение последнего позволяет полностью автоматизировать управление каталогом учетных записей системы WebSSO.



Корпоративные системы все больше переориентируются на Web. Web-приложения становятся стандартом де-факто в современных информационных системах. Признавая, что степень проникновения Web в корпоративный сегмент тем не менее еще невелика, в Avanpost уверены в незаменимости решения. «Через 5–10 лет организаций, не работающих в среде Web, практически не останется. Web-приложения проникнут даже в самые консервативные отрасли и сферы применения ИТ, — уверен Андрей Конусов. — При постоянно увеличивающемся объеме взаимодействия с клиентами через корпоративные Web-решения аутентификация на основе Web-стандартов и технологий станет ключевым, основным и едва ли не единственным способом входа в информационные системы».

По утверждению представителей компании, в России нет аналогов подобных решений, а Avanpost WebSSO не только представляет собой пример импортозамещающего решения (в ближайшее время будет подана заявка на внесение его в реестр российского ПО), но и облегчает разработку других российских программных продуктов, поскольку позволяет обойтись без создания отдельной подсистемы доступа пользователей.

**Avanpost WebSSO обеспечивает защищенную регистрацию пользователей в Web-приложениях после прохождения однократной аутентификации**

Дмитрий Ганьжа

## Allied Telesis: 30 лет на сетевом рынке

В марте японская компания Allied Telesis отпраздновала 30-летие своей деятельности.

На российском рынке компания работает более 20 лет (первоначально под маркой Allied Telesyn). С самого начала компания позиционировала себя как производителя «кирпичиков» для построения сетевой инфраструктуры и во многом придерживается выбранной стратегии до сих пор. У Allied Telesis шесть центров исследований и разработок и три завода (в Сингапуре, Китае и Индонезии).



Фото: Дмитрий Ганьжа

**Allied Telesis фокусируется на предоставлении качественных компонентов для построения сетевой инфраструктуры**

В магическом квадранте Gartner поставщиков инфраструктурных решений для локальных проводных и беспроводных сетей Allied Telesis находится среди нишевых игроков. В отчете отмечается наличие у компании трех линеек продуктов для беспроводного доступа: традиционного беспроводного портфолио в составе Unified Wireless Controller и точек доступа TQ, облачной системы управления AlliedView Cloud с точками доступа, а также решения Extricom, укомплектованного контроллером, ультратонкими ТД и коммутаторами.

Компания Extricom была приобретена Allied Telesis в 2015 году. Во избежание интерференции сигналов в ее решении применяется технология Channel Blanket. Как утверждает, это позволяет одновременно использовать точки доступа стандартов n и a/b/g без потери производительности. «Для обеспечения комфортной коммуникационной беспроводной среды в эпоху Интернета вещей» Allied Telesis совместно с Киотским университетом разрабатывает автономное решение для беспроводных локальных сетей, способное автоматически предотвращать интерференцию радиоволн.

Среди сильных сторон решений компании Gartner выделяет систему управления сетью Allied Telesis Management Framework (AMF). AMF позволяет автоматизировать и упростить многие повседневные задачи администрирования, обеспечивая управление всеми устройствами как одним. Дополнительный бонус — возможность настроить сеть с помощью RESTful API, так что корпоративные пользователи могут добавить соб-

ственные функции или использовать решения сторонних разработчиков. Компания даже позиционирует это решение как SDN для небольших компаний. Впрочем, поддерживается и «классический» подход к реализации программно определяемых сетей — на базе OpenFlow.

Allied Telesis предлагает решения для различных отраслей и сегментов: здравоохранения, транспорта, центров обработки данных и др. Особое внимание уделяется инфраструктуре для видеонаблюдения. Чтобы предлагать клиентам комплексные решения, компания сотрудничает с производителями видеокамер и NVR. Это направление активно развивается и в России. Так, по словам Юрия Бельского, главы представительства Allied Telesis в России, недавно завершены проекты по построению сети для видеонаблюдения в ТРЦ «Ривьера» в Москве и супермаркетах сетей «Магнит» и «Фреш 25».

При создании сети безопасности в ТРЦ «Ривьера» в качестве коммутаторов уровня доступа была выбрана линейка коммутаторов Web-smart серии GS950. Питание подключенных камер видеонаблюдения (несколько десятков) осуществляется с помощью технологии PoE, что упрощает монтаж и эксплуатацию. С помощью технологии стекирования VCSStack коммутаторы серии x510, установленные на уровне распределения, были объединены в одно виртуальное устройство с единым управлением, нумерацией портов и агрегированием каналов до коммутаторов доступа. Это позволило повысить отказоустойчивость всей сети и ее пропускную способность.

Относительно новым для Allied Telesis является направление промышленных коммутаторов. Недавно портфель решений Industrial Ethernet пополнился многофункциональными гигабитными коммутаторами серии IE300. Оборудование рассчитано на работу в суровых погодных условиях и обеспечивает подачу питания по технологии PoE+ (до 30 Вт) и пока не стандартизованной Hi-PoE (до 60 Вт). Благодаря применению технологии High Availability Network Power (HANP) подача питания на подключенные устройства не прерывается при перезагрузке коммутатора, и питаемое устройство, например камера, может записывать видео на карту памяти.

Помимо HANP, в оборудовании Allied Telesis реализуются и другие оригинальные технологии — например, Active Fiber Monitoring для выявления «прослушки» оптических линий. Компания активно ищет возможности выхода на новые рынки. В частности, для Интернета вещей была разработана платформа, обеспечивающая поддержку периферийных вычислений EtherGRID.

Дмитрий Ганьжа

Алексей Севастьянов,  
первый заместитель  
генерального директора,  
DataLine



Фото: DataLine

**В** преддверии форума «МИР ЦОД – 2017» аналитическое агентство OSP Data и «Журнал сетевых решений/LAN» провели исследование текущего состояния и перспектив развития российского рынка коммерческих ЦОДов. С этой целью были опрошены руководители ведущих коммерческих центров обработки данных. Вашему вниманию предлагаются ответы Алексея Севастьянова, первого заместителя генерального директора DataLine.

Александр Барсков

## Как себя чувствует рынок КЦОД

**Журнал сетевых решений/LAN:** Каковы общая оценка ситуации в российской отрасли коммерческих ЦОДов и основные тенденции? Какие вы видите факторы роста и факторы риска?

**Алексей Севастьянов:** Рынок коммерческих центров обработки данных остается высококонкурентным вследствие вывода на рынок новых мощностей за последние два года. В результате на рынке появился переизбыток предложения. Сами операторы коммерческих ЦОДов больше не ограничиваются предоставлением классической услуги по размещению оборудования (colocation) и стараются запускать облачные сервисы, услуги по администрированию ОС и приложений.

Основным фактором роста остается улучшение экономической ситуации в стране. С точки зрения спроса за последний год ситуация выправилась: бизнес постепенно выходит из режима жесткой экономии, количество запросов и их объем планомерно увеличиваются.

**LAN:** Приведите, пожалуйста, общие характеристики ваших ЦОДов и показатели бизнеса.

**Севастьянов:** На текущий момент сеть DataLine включает семь ЦОДов на двух площадках (OST и NORD) в Москве. Общая площадь серверных залов составляет 7515 м<sup>2</sup>, они вмещают 3703 стойки. Большая часть центров обработки данных загружена более чем на 90%, свободные мощности остаются в новом ЦОДе NORD-4. Две его новые очереди будут запущены до конца 2017 года.

По итогам 2016 финансового года доход компании вырос на 59%, количество клиентов увеличилось до 545.

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

**Севастьянов:** По итогам 2016 финансового года структура сервисов DataLine выглядит следующим образом:

- размещение оборудования — 61%, 2015 год — 66%;
- облачные сервисы — 22%, 2015 год — 16%;
- телекоммуникационные услуги — 9%, 2015 год — 11%;
- администрирование — 2%, 2015 год — 2%;
- аренда оборудования — 6%, 2015 год — 5 %.

**LAN:** Поделитесь, пожалуйста, планами по развитию: расширение/увеличение числа площадок, предложение новых сервисов.

**Севастьянов:** В 2017 году будут введены оставшиеся две очереди ЦОДа NORD-4 на 1008 стоек. В планах — сертификация процессов эксплуатации по стандарту Uptime Institute Tier III.

Кроме того, в этом году мы планируем представить целый набор сервисов по обеспечению информационной безопасности, катастрофоустойчивые (DisasterRecovery) решения для облачных и физических инфраструктур, облачное объектное хранилище. Также продолжим развивать направление по администрированию и технической поддержке информационных систем наших заказчиков.

**LAN:** Какие вы видите перспективы расширения деятельности? Планируется ли начать предоставлять услуги интеграции, консалтинга, комплексного решения ИТ-задач заказчика?

**Севастьянов:** Планов по развитию услуг интеграции пока у нас нет, зато активно развивается ИТ-консалтинг. Одно из направлений — проектирование, строительство и наладка службы эксплуатации для центров обработки данных и серверных заказчиков. В рамках ИТ-консалтинга наши специалисты также помогают клиентам провести аудит действующих информационных систем, определиться с объемом необходимых виртуальных или физических ресурсов под проект, составить план миграции и поддержки системы на мощностях DataLine. **LAN**



Владимир Рубанов,  
управляющий директор,  
«Росплатформа»



Фото: «Росплатформа»

**К**омпания «Росплатформа» предлагает программное обеспечение для серверной виртуализации вычислений и хранения данных, в основу которого положены разработки компаний Parallels и Virtuozzo. Ей были переданы все права на исходный код, истоки которого лежат в разработках российских программистов еще в стенах альма-матер основателей Parallels, так что и де-факто, и де-юре это ПО российской разработки. Хотя официальный статус российского оно получило совсем недавно: в самом начале мая два основных продукта — «Р-Виртуализация» и «Р-Хранилище» — были включены в Реестр российского ПО Минкомсвязи РФ. «Росплатформа» продолжает тесно сотрудничать с компаниями группы Parallels, но юридически полностью от них независима. Кроме того, в отличие от них, ее продукты разрабатываются для других потребителей: «Росплатформа» ориентируется на корпоративный рынок и государственные организации. О стратегии и предложениях компании в контексте обеспечения цифрового суверенитета мы поговорили с ее управляющим директором Владимиром Рубановым.

Дмитрий Ганьжа

## «“Росплатформу” МОЖНО СЧИТАТЬ образцом российского производителя»

**Журнал сетевых решений/LAN:** При создании компании звучали заявления о намерении создать российский аналог Amazon Cloud или Microsoft Azure до конца 2016 года...

**Владимир Рубанов:** На самом деле это недоразумение. Оно возникло из-за публикации в «Коммерсанте», где были воспроизведены некоторые случайно опубликованные предварительные идеи, обсуждавшиеся в ходе мозгового штурма относительно возможных направлений деятельности «Росплатформы». Построение российского облака было одним из рассматриваемых вариантов, но от этой идеи очень быстро отказались. Мы — программисты. И наша главная сила — в разработке программного обеспечения. Построением облаков с помощью наших решений пусть занимаются соответствующие профильные компании.

«Росплатформа» — российский вендор программного обеспечения, предназначенного для оснащения центров обработки данных, внутренней ИТ-инфраструктуры предприятий и построения публичных и частных облаков. Никаких собственных ЦОДов у нас нет, и к числу сервис-провайдеров мы не принадлежим. Сервис-провайдеры входят в число наших клиентов, но никак не конкурентов.

**LAN:** Что в таком случае понимается под платформой и что в ней российского?

**Рубанов:** Речь идет о системной части программного обеспечения, то есть о системном ПО, на котором работают прикладные системы. Наш продукт устанавливается на «голое железо» и сам по себе является операционной системой, которая становится платформой для виртуальных окружений, других операционных систем и приложений.

Что касается «российскости», большая часть кода наших продуктов написана именно российскими программистами, однако первоначальное авторство не столь

существенно. В контексте цифрового суверенитета конструктивным становится владение необходимыми юридическими и техническими правами на продукт: распоряжение полным исходным кодом, владение инструментами для работы с ним и наличие специалистов, разбирающихся в этих кодах и инструментах.

Иначе говоря, значение имеет не первоначальное авторство, а наличие юридических прав и организационно-технических возможностей самостоятельно исправлять ошибки в коде, поддерживать пользователей и выпускать новые версии продукта. Это гарантирует, что никакие санкции не повлияют ни на возможность использования и развития такого программного обеспечения, ни на позицию самого вендора.

По этим критериям «Росплатформу» можно считать образцом российского производителя. В нашем распоряжении находится 100% исходных кодов наших продуктов, и мы владеем исключительными правами на выпускаемые решения. У нас имеются собственная инфраструктура для работы с этим кодом и штат высококвалифицированных опытных специалистов.

**LAN:** Не получится ли так, что «Росплатформа» и Parallels параллельно ведут одни и те же разработки?

**Рубанов:** У «Росплатформы» российские владельцы, и она не аффилирована с Parallels и Virtuozzo, хотя является их стратегическим партнером. Вопрос о возможной конкуренции вполне естественен, но ответ на него достаточно прост.

Несмотря на значительную общность технологической базы, предлагаемые продукты ориентированы на разные целевые сегменты. Если Parallels и Virtuozzo нацелены на взаимодействие с сервис-провайдерами и хостерами, то «Росплатформа» разрабатывает программные решения для использования в корпоративном сегменте и государственных структурах. Кроме



того, у «Росплатформы» фокус на рынках России и дружественных стран, для которых фактор обеспечения цифрового суверенитета является дополнительным преимуществом.

**LAN:** *Разработкой вы тоже занимаетесь полностью независимо?*

**Рубанов:** У нас есть общая часть разработок, открытая для всех в полном соответствии с принципами Open Source в рамках международного сообщества программистов. Другая общая часть доступна для совместной работы над ней только нам и нашим партнерам. В каком-то смысле это внутренняя Open-Source-разработка, за которую отвечают специалисты компаний-участников. На базе этих компонентов каждая компания затем собирает свои продукты, добавляя собственный уникальный код. Исключительные права на эти итоговые продукты принадлежат соответствующим компаниям.

Вести разработки совместными усилиями и при этом иметь все права на использование полученных результатов — это отличный механизм. И чем больше участников, тем лучше. В мире часто дублируют усилия в разных отраслях, и в сфере программирования особенно. Каждый (неопытный) программист считает своим долгом написать что-то с нуля. Некоторые компании тоже любят изобретать велосипед.

Люди, которые считают деньги и реально стремятся создавать инновационные системы, все чаще используют модель Open Source — как публичную, так и применяемую внутри группы участников консорциума. Работая над общедоступными открытыми технологиями, мы, по сути, сотрудничаем со всем миром. Если проект является мировым и в нем участвуют лучшие специалисты из ведущих компаний, там рождаются действительно прогрессивные решения. Почему такого же эффекта сложно добиться в рамках одной организации? Как известно, в обособленных популяциях отмечается вырождение генов. То же и с инновациями. В открытом проекте происходит взаимное «опыление» идеями от гораздо более широкого спектра специалистов.

В этой связи важно отметить: если российская компания использует открытый код, ей необходимо участвовать в соответствующих мировых проектах, а не просто заимствовать результаты. Только когда она является активным участником

сообщества разработчиков открытого кода и имеет авторитет и влияние в соответствующем международном проекте, такой открытый код можно использовать для создания российских продуктов, способных укреплять цифровой суверенитет страны. Простая пересборка открытого кода в России — это профанация цифрового суверенитета.

**LAN:** *Каковы приоритетные направления деятельности «Росплатформы»?*

**Рубанов:** Как я уже говорил, целевыми для нас являются корпоративный и государственный сегменты. Мы ориентируемся на организации, у которых есть собственные серверные мощности, на которых и разворачиваются наши решения. При установке нашего системного ПО набор серверов фактически превращается в частное облако IaaS и одновременно отказоустойчивое хранилище данных.

Это тот самый модный сценарий гиперконвергенции, когда задача обеспечения отказоустойчивости и надежности платформы решается с помощью не дорогостоящего оборудования, а типовых относительно дешевых серверов x86 и нашего ПО, которое берет на себя все заботы по надежной распределенной виртуализации вычислений и хранения данных на таком наборе серверов. Благодаря такому подходу удастся отказаться от дорогостоящей аппаратуры и выделенных специализированных систем хранения данных, сохранив все выгоды отказоустойчивости.

За счет переноса функций на умное ПО система продолжит работать даже при отказе диска, сервера или целой группы серверов, а пользователь этого не заметит: перераспределение нагрузки и восстановление данных выполняются автоматически. Таким образом, задача обеспечения работоспособности отдельного сервера теряет свое критическое значение, а значит, можно использовать более дешевое оборудование. В итоге при построении такой виртуализированной инфраструктуры общее решение получается существенно дешевле, а управлять им проще, чем отдельными СХД и серверами разных производителей.

**LAN:** *Первоначально основным приложением для гиперконвергентных решений была поддержка инфраструктуры VDI. Насколько востребованы решения VDI и для каких задач предназначена ваша платформа?*

**Рубанов:** Такой сценарий использования нашего продукта, как организация удаленного доступа к виртуальным рабочим столам, возможен — с его помощью можно легко и быстро развернуть инфраструктуру VDI в контейнерах или VM. Однако мы не позиционируем нашу платформу как специфическое решение для VDI, она имеет более широкое применение, и конкретной специализации у нее нет — прикладные нагрузки могут быть самими разными.

Если при построении гиперконвергентной инфраструктуры задействовать достаточно большое количество серверов, ее можно использовать для самых разных сценариев применения, без ограничений. При достаточном количестве серверов в кластере удастся добиться очень высоких показателей производительности за счет правильного распараллеливания доступа к множественным источникам. В новых версиях мы научились не только осуществлять классическое дублирование дисков, но и использовать умные алгоритмы Erasure Coding — они гораздо эффективнее, чем резервирование по схеме 2+1.

Если говорить о примерах, то в Объединенной строительной корпорации наше решение применяется для документооборота, в нескольких российских университетах на нем развернута система управления вузом, сейчас на базе «Росплатформы» строится большая федеральная информационная система и т. п.

**LAN:** *Многие поставщики гиперконвергентных решений предлагают уже готовые специализированные устройства (appliance), что позволяет быстрее и проще осуществлять развертывание инфраструктуры...*

**Рубанов:** Мы отличаемся тем, что предоставляем своим клиентам большую свободу выбора. Известные вендоры гиперконвергентных решений предлагают готовые программно-аппаратные комплексы, но поставить ПО на уже имеющиеся у заказчика серверы они не могут, а мы такой сценарий поддерживаем. К тому же при нашем подходе заказчик может приобрести серверы у предпочтительного поставщика и установить на них наше программное обеспечение.

Если же заказчик не хочет сам заниматься закупкой оборудования, он может обратиться к нашим партнерам и приобрести у них готовый программно-аппаратный

комплекс (ПАК). Например, с компанией IBS мы сделали ПАК «СКАЛА-Р»: системный интегратор объединил наше ПО с оборудованием российского производителя «Депо компьютерс» и добавил свои компоненты по управлению и мониторингу. «СКАЛА-Р» представлена линейкой ПАК разного масштаба, которые в начальной конфигурации подойдут даже для небольших компаний.

**LAN:** Исторически провайдеры предпочитают контейнеры, а корпоративные пользователи — виртуальные машины. Ваше решение поддерживает и ВМ, и контейнеры. Зачем корпоративным пользователям, вашим основным заказчикам, нужны контейнеры?

**Рубанов:** Это мой любимый вопрос. В части внедрения передовых технологий Россия обычно отстает от передовых стран на несколько лет, это касается и использования контейнеров в корпоративном сегменте. Так, по данным отчета Linux Foundation, еще в далеком 2014 году около трети корпоративных CIO (россияне в опросе не участвовали) заявили, что их компании уже применяют контейнеры, а две трети — что они собираются это сделать в следующем году.

Почему это происходит? Ответ очень простой. Предприятия считают деньги, а контейнеры позволяют на том же оборудовании создать гораздо больше виртуальных окружений, то есть запускать больше прикладных задач. Кроме того, расположив в контейнере отдельную специализированную часть своей системы (микросервис), можно повысить гибкость управления. Это позволяет добиться высокой маневренности бизнеса (agility). А для современных предприятий быстрая адаптация ИТ-инфраструктуры является вопросом как получения конкурентных преимуществ, так и выживания. Построение корпоративных систем на базе микросервисов как раз и позволяет добиться пластичности бизнеса. Эта возможность давно высоко оценена за рубежом, в России компании только присматриваются к ней. Надеюсь, что в ближайшие годы мы станем свидетелями того, как эта технология начнет широко применяться и в России.

Раз уж зашла речь о контейнерах, хотелось бы отметить, что они бывают двух видов: системные и прикладные. Системный контейнер сравним с легкой виртуальной машиной. Примером же прикладного контейнера может служить

Docker. Мы поддерживаем оба вида — внутри наших системных контейнеров могут размещаться и контейнеры Docker.

Но еще раз подчеркну, что мы поддерживаем не только контейнеры. Это лишь одна из возможностей виртуализации в рамках нашей системы, которая может использоваться параллельно с классическими виртуальными машинами. Выбор делают сами клиенты.

**LAN:** Если говорить о перспективах гиперконвергентных решений, насколько широкое распространение они могут получить в качестве универсальной инфраструктуры?

**Рубанов:** На прошедшем недавно Russian Open Source Summit директор SuSe категорически заявил, что через два года все новые ИТ-инфраструктуры будут строиться по гиперконвергентному принципу, то есть приобретать дорогие серверы и СХД перестанут. Возможно, он хотел эпатировать публику, но вот, например, Gartner официально прогнозирует ежегодный рост продаж гиперконвергентных решений на 46%. Это серьезные аналитики, и такие цифры — это очень много по сравнению с общим ростом ИТ-отрасли.

**LAN:** В любом случае для программного обеспечения необходима аппаратная платформа. Насколько реально достижение цифрового суверенитета при отсутствии собственной элементной базы?

**Рубанов:** Москва не сразу строилась — надо стремиться увеличивать российское влияние и вклад в используемые технологические стеки, особенно в критически важных и государственных системах. Если система полностью построена на американском программном и аппаратном обеспечении, ни о каком цифровом суверенитете говорить не приходится. А когда на том же оборудовании установлено российское ПО, это уже улучшает ситуацию, поскольку возможность повлиять на такую систему посредством санкций сокращается.

Степень цифрового суверенитета повышается еще больше, если серверы и используемые в них платы проектируются и собираются в России. Для критических систем могут использоваться процессоры «Эльбрус» и «Байкал», правами на дизайн которых располагают отечественные компании. Так, государственная система управления паспортами построена на «Эльбрусе». Но нужно ли стремиться к полной автономии, при которой все

аппаратное обеспечение было бы придумано и изготовлено в России, — вопрос дискуссионный.

В нашей стране достаточно много производителей ПО (в том же Реестре Минкомсвязи уже больше 3000 позиций), но есть и компании, выпускающие аппаратное обеспечение (с той максимальной степенью локализации, которая возможна в текущих условиях). Все продукты можно объединять в партнерские стеки: (условно) российское оборудование, потом виртуализация, например, на базе нашей платформы, поверх нее российские операционные системы (они уже имеются), и венчают стек российские прикладные продукты.

На основе такой кооперации уже сейчас можно строить импортозамещающие программно-аппаратные комплексы, охватывающие весь стек — от оборудования до прикладных программ.

**LAN:** Так в чем же заключаются основные преимущества предложения «Росплатформы»?

**Рубанов:** Я бы выделил три пункта. Во-первых, российское происхождение де-факто и де-юре, то есть российские программисты и инфраструктура разработки, исключительные права на продукты в России и вот теперь официальное включение в Реестр российского ПО Минкомсвязи. Это важный аргумент прежде всего для государственных заказчиков, хотя и многие российские коммерческие компании начинают ценить отечественную продукцию, так как вендор «под боком» гораздо отзывчивее на их запросы, не говоря уже о предсказуемых ценах в рублях и пользе сохранения средств в экономике страны.

Во-вторых, экономическая привлекательность. Решение, созданное на основе «Росплатформы», заметно дешевле, чем системы, собранные на базе зарубежных аналогов.

В-третьих, технологическое превосходство. Мы предлагаем ряд уникальных функций и возможностей — в частности, объединение контейнерной и гипервизорной виртуализации в рамках одного унифицированного решения, дополненное поддержкой современных гиперконвергентных сценариев для построения ИТ-инфраструктур «по последнему слову науки и техники». **LAN**

# Cisco Connect 2017: навстречу цифровой трансформации

Реализация современной сетевой инфраструктуры на базе решений Cisco позволяет улучшить адаптивность бизнеса и вдобавок сократить время обнаружения угроз.

Дмитрий Ганжа,  
главный редактор «Журнала сетевых решений/LAN»



Открывая Cisco Connect 2017, Джонатан Спэрроу, вице-президент Cisco по России и СНГ, заявил, что на российском рынке компании удалось преодолеть негативную динамику и возобновить рост продаж по всем основным продуктовым направлениям (правда, никаких конкретных цифр названо не было — ни уровня предшествующего снижения, ни достигнутых темпов роста).

Предыдущий форум Cisco Connect проводился полтора года назад, и за это время интерес к решениям компании, несмотря на определенные трудности, с которыми она столкнулась в силу известных причин, не угас: в конференции приняло участие около 3000 человек. По мнению Джоната Спэрроу, это может служить косвенным подтверждением оздоровления ситуации на российском рынке.

К традиционным тематическим потокам, таким как «Центры обработки данных» и «Технологии для совместной работы», добавились два новых: DevNet и Cyber Range. Первый стал результатом активизации деятельности компании в области программных решений, а второй — в сфере компьютерной безопасности. Последняя тема, наряду с цифровой трансформацией бизнеса, стала ключевой на форуме. Всего же было запланировано более 100 докладов и мастер-классов.

## ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПО-РУССКИ

Компании удается предложить рынку востребованные решения. Косвенно это подтверждается ростом

ее капитализации: за последние три года он составил 50%. Однако, чтобы оставаться на гребне волны цифровой трансформации, собственных разработок недостаточно, поэтому Cisco активно приобретает перспективных технологических игроков. Только за последние два года совершено 17 таких сделок, причем самым крупным вложением стала покупка AppDynamics, разработчика систем для контроля и мониторинга производительности корпоративных приложений. AppDynamics удалось «перехватить» за 3,7 млрд долларов буквально накануне IPO.

Влияние цифровизации ощущается все сильнее. Некоторые компании весьма озадачены быстротой происходящих изменений и не знают, что предпринять. Организации меняются медленнее, чем технологии, и в России это отставание проявляется особенно заметно. Как заявил в своем выступлении профессор Майкл Уэйд из бизнес-школы IMD в Швейцарии, в России воздействие цифровой трансформации ощущается меньше, чем в среднем по миру. Это утверждение опирается на выводы, сделанные работающим под его руководством исследовательским центром, который создан при участии Cisco.

Согласно данному исследованию, и в России, и в мире примерно одинаковая доля компаний (около трети) занимают выжидательную позицию в отношении цифровой трансформации, однако в нашей стране задачами, связанными с цифровизацией, активно занимается только каждая шестая компания, тогда как в среднем по миру — каждая четвертая. Это объясняется в первую очередь текущими экономическими трудностями и, как следствие, недостатком инвестиций.

Более половины российских компаний не осознают угрозы. Такое пассивное отношение к цифровой трансформации может объясняться также тем, что основная доля ВВП приходится на компании с госучастием, а они менее подвержены влиянию рыночных факторов и поэтому могут себе позволить подождать и посмотреть, что из всего этого «выкристаллизуется». Подобный подход окажется оправданным, если позже удастся быстро наверстать упущенное благодаря внедрению уже отработанных решений, как это было, например, с развертыванием в России сотовой связи 3G. Правда, можно и прогадать: темпы изменений настолько ускорились, что отставание может оказаться необратимым.

Однако, как показала дискуссия «Цифровизация: российский опыт», отечественным компаниям есть чем похвастаться. Удивительно, но одной из наиболее передовых (с точки зрения ИТ) отраслей является агропромышленный комплекс. Как заявил Владислав Беляев, директор по ИТ «Группы Черкизово», в Кашире строится мясоперерабатывающий завод, где реализуются принципы Industry 4.0 — уровень автоматизации будет самым высоким для подобных предприятий в Европе.





Фото: Дмитрий Ганьжа

**Джонатан Спарроу (на фото в центре): «Все, что может быть подключено к сети, будет к ней подключено»**

Цель проводимой трансформации состоит в ликвидации разрыва между принятием решения (с помощью информационных систем) и его исполнением (посредством производственных систем). «Мы должны объединить наши производственные системы — машины, роботы и автоматы — с информационными, причем сделать это таким образом, чтобы они составляли единое целое, — поясняет Владислав Беляев. — Мы создаем систему, когда решение о производстве той или иной партии продукции, перенастройка оборудования и отгрузка товара будут выполняться полностью автоматически. Это как раз и есть Industry 4.0».

По мнению Майкла Уэйда, вопрос должен формулироваться не «как нам повысить уровень цифровизации», а «как повысить свою продуктивность».

**В последние год-полтора Cisco уделяла большое внимание развитию средств аналитики для сети и ЦОДа**

#### СЕТЬ В КАЧЕСТВЕ БАЗИСА, ИЛИ ЧТО ПРЕДЛАГАЕТ CISCO

Как идти в ногу с изменениями и при этом обеспечить требуемый уровень информационной безо-

пасности? Именно эти две темы, по словам Майкла Гэнзера, старшего вице-президента Cisco по работе в Центральной и Восточной Европе, России/СНГ, волнуют руководителей компаний в первую очередь.

В гиперподключенном мире сеть приобретает ключевое значение. Однако существующие сети не были рассчитаны на поддержку настолько быстрого изменения требований со стороны пользователей. Так, до 95% всех перенастроек сети до сих пор производится вручную или при участии человека (например, запуск сценария). Подключение же к сети всего, что только можно подключить, многократно повышает риск успешной атаки, а опасение компрометации сдерживает цифровую трансформацию.

Только у каждой пятой компании стратегия развития сети согласована со стратегией цифровизации. Между тем корпоративные сети должны обеспечивать ту же степень гибкости предоставления сервисов и удобство использования, что и Интернет. Как отметил во время круглого стола о технологических инновациях Cisco Андрей Кузьмич, директор «Сиско Системс» по технологиям, корпоративные сети отстают от Интернета по уровню внедрения инноваций, в то время как десять лет назад ситуация была прямо противоположной.

Имея самую обширную на сетевом рынке экспертизу, Cisco хорошо представляет, каковы слабые места сетевой инфраструктуры, как ее перестроить и в каком направлении двигаться. Комплектуя свой портфель решений, компания особое внимание уделяет созданию архитектуры цифровых сетей (Digital Network Architecture, DNA). Эта инфраструктура следующего поколения должна обеспечить гибкое и удобное предоставление сервисов за счет максимальной автоматизации и виртуализации, дополненных аналитикой.

Как указывает Андрей Кузьмич, в расширенном толковании DNA охватывает всю необходимую цифровую инфраструктуру — от сети доступа до сети ЦОДа. Cisco предлагает компоненты для построения как физической, так и виртуальной инфраструктуры, в том числе для операторов связи. Например, виртуальный маршрутизатор CSR 1000v позволяет запустить все нужные сетевые функции в ЦОДе оператора. Это дает возможность отказаться от нескольких аппаратных решений в пользу одного виртуализированного.

Портфель предложений Cisco для построения DNA постоянно пополняется. Так, в феврале компания представила пять новых продуктов, в том числе сетевую и вычислительную платформу для филиалов Enterprise Network Compute System (ENCS) 5400, на которую уже установлены гипервизор и виртуальный маршрутизатор. Благодаря поддержке виртуальных сетевых функций одно устройство может заменить множество специализированных, таких как МСЭ, оптимизатор WAN и др.



Фото: Дмитрий Ганьжа



У всех новых аппаратных продуктов Cisco имеются интерфейсы программирования, как правило, на базе REST API. Это позволяет сделать инфраструктуру открытой и программно управляемой, то есть оборудованием Cisco можно управлять с помощью внешних контроллеров. Компания выпускает такие контроллеры — APIC для сетей ЦОДов и APIC-EM для кампусных и территориально распределенных сетей. Объединение сетей на базе APIC и APIC-EM позволяет получить полностью управляемую программную среду для построения автоматизированной корпоративной ИТ-инфраструктуры. При необходимости пользователи могут загрузить на контроллеры собственные приложения, что тоже помогает ускорить реагирование на новые запросы бизнеса.

Согласились бы вы лететь на самолете, который состоит из 50 не согласованных между собой компонентов? Однако компании используют до 50 различных решений в области информационной безопасности, и зачастую они никак не взаимодействуют. По словам Майкла Гэнзера, Cisco фокусируется на создании целостной архитектуры безопасности, способной обеспечивать максимально быстрое обнаружение вторжения. Как утверждается, в первые три минуты она позволяет выявить 91,8% всех угроз, тогда как ближайший конкурент — только 17,1%.

Для автоматизации доступа в сеть компания предлагает технологию TrustSec и контроллер управления политиками доступа ISE. Как поясняет Андрей Кузьмич, с ее помощью создается такая сетевая среда, в которой при перемещении пользователей выполнять переконфигурацию не требуется. В результате удается добиться программной сегментации сети и тем самым минимизировать последствия инцидентов безопасности (см. подробнее статью Сергея Полищука «Новый подход к сегментации сети и его ценность для бизнеса» в «Журнале сетевых решений/LAN» за январь-февраль 2017 года).

При наличии полномасштабной среды под управлением контроллеров APIC и сети доступа под управлением контроллера ISE можно реализовать автоматическое присвоение права пользоваться новым развертываемым приложением и в конечном итоге отказаться от политики применения «черных» списков в пользу «белых». Иначе говоря, в такой сети все, что не разрешено явным образом, запрещено. Этот подход позволяет избавиться от множества списков доступа и, таким образом, снижает вероятность ошибки, улучшая защиту.

### АНАЛИТИКА СЕТИ: ОТ Wi-Fi ДО ЦОДА

В последние год-полтора Cisco уделяла большое внимание развитию средств аналитики для сети и ЦОДов. Так, платформа сетевой аналитики для ЦОДа Cisco Tetration Analytics позволяет видеть



Фото: Дмитрий Ганжа

всю картину взаимодействия приложений в центре обработки данных (см. подробнее статью автора «Тяжелые» решения от Cisco облегчают жизнь операторам ЦОДа» в ноябрьском номере «Журнала сетевых решений/LAN» за 2016 год). Как отмечает Андрей Кузьмич, зачастую люди не знают, что у них происходит в сети ЦОДа. Например, перед тем как развернуть программируемую сеть на базе ACI, необходимо определить политики, а для этого нужно знать, с чем именно взаимодействуют те или иные компоненты приложений. Полученная с помощью Tetration информация позволяет правильно сформулировать политики для ACI.

Решение недавно вошедшей в состав Cisco компании WebDynamics позволяет проанализировать работу приложения не внутри ЦОДа (как Tetration), а между клиентской (front-end) и серверной (back-end) частями. Система StealthWatch, которую Cisco приобрела вместе с компанией Lapscore полтора года назад, обеспечивает выявление и анализ потоков данных в сети с помощью NetFlow. Зная типичную картину сетевых потоков, проще обнаруживать небезопасные аномалии. Аналитические средства CMX для Wi-Fi на основании собранных данных о регистрирующихся беспроводных устройствах формируют статистику о посетителях магазина.

Реализация современной сетевой инфраструктуры, дополненная решениями для анализа данных, позволяет улучшить адаптивность бизнеса и ускорить обнаружение угроз — иногда, как утверждают эксперты Cisco, почти в 100 раз. Кроме того, согласно опросу заказчиков, проведенному IDC, через пять лет возврат инвестиций может составить 400% (срок окупаемости — девять месяцев).

Техническая платформа для IIoT разрабатывается в тесном сотрудничестве с производителем промышленных роботов FANUC

## AIM — теперь в стандарте

Компания CommScope провела в Москве конференцию, посвященную автоматизации управления и обслуживания инфраструктуры передачи данных, — CommScope Intelligence Day 2017.

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



Фото: Александр Барсков

**Ханс-Юрген Нитхаммер:**  
«Главное в стандарте ISO/IEC 18598 на системы AIM — требование к наличию открытых программных интерфейсов для интеграции с другими системами»

Системы управления КС, для обозначения которых в разные периоды их развития применялись разные термины, похоже, наконец обрели общепринятое название: Automated Infrastructure Management (AIM). Именно термин AIM фигурирует в недавно принятом стандарте ISO/IEC 18598 на такие системы. Примечательно, что от маркетингового названия «интеллектуальные КС» отрасль переходит к более практически понятному понятию «автоматизированное управление инфраструктурой».

Глава российского представительства CommScope Роман Китаев выделил три основные тенденции, во многом определяющие развитие рынка решений для кабельных инфраструктур. Это увеличение скоростей передачи данных, потребность в повышении удобства эксплуатации кабельных систем и ценовая оптимизация предлагаемых решений. Повышение удобства эксплуатации особенно важно в связи с ростом сложности и увеличением плотности кабельных инсталляций, и именно на решение этой задачи и нацелены системы AIM. «Основные цели внедрения AIM — сделать эксплуатацию более удобной и надежной», — подчеркнул представитель CommScope.

Особую ценность прошедшей в Москве конференции придало участие в ней в качестве ключевых докладчиков сотрудников CommScope, участвовавших в разработке стандарта ISO/IEC 18598: ведущего эксперта по архитектуре ЦОДов Ханса-Юргена Нитхаммера и руководителя глобальной службы поддержки интеллектуальных решений Майкла Германа.

Вспоминая историю развития систем AIM, Ханс-Юрген Нитхаммер отметил, что первое поколение таких решений появилось около 15 лет назад в ответ на просьбы заказчиков помочь им в администрировании сложных систем КС. Эти решения предназначались только для офисных инсталляций, они обеспечивали документирование всех изменений на кроссовом поле КС в реальном времени, а также упрощали планирование и выполнение заданий при работе с кабельной системой.

За прошедшее время системы AIM получили определенное распространение (у той же CommScope в России доля «интеллектуальных» КС в продажах уже составляет порядка 20%), однако речь об их массовом применении не шла. Этому мешал ряд про-

блем. По словам Ханса-Юргена Нитхаммера, чаще всего заказчики жаловались на то, что предлагаемые решения являлись проприетарными. Кроме того, им не нравились существенный разброс в функциональности систем разных вендоров и отсутствие четких путей интеграции с другими имеющимися системами управления. Сложностей добавляло и то, что мало кто из производителей комплексно подходил к созданию системы AIM: как правило, поставщик КС обеспечивал аппаратную часть, а написанием ПО занимался его партнер.

Разработчики стандарта ISO/IEC 18598 ставили цель устранить указанные выше проблемы. Стандарт состоит из трех основных частей. В первой части описаны общие требования к таким системам: система должна автоматически определять наличие соединений на кроссовом поле, обеспечивать в месте установки стойки доступ к электронным нарядам на выполнение работ, к трассировочной и другой информации, а также выдавать звуковые/визуальные предупреждения о некорректном выполнении задач по подключению и отключению коммутационных шнуров.

Очень важная часть стандарта (Ханс-Юрген Нитхаммер вообще считает ее главной) — требование наличия открытых программных интерфейсов для интеграции с другими системами. Выполнение этого требования смягчает проблему «привязки» к конкретному производителю, поскольку позволяет относительно просто интегрировать системы AIM разных поставщиков. Кроме того, открытый API или другой формат обмена данными упрощает интеграцию AIM с другими системами управления, например с DCIM.

Заметим, что стандарт не оговаривает технологию физического определения факта соединения, которая у разных производителей разная. Например, в системе imVision компании CommScope (ранее она называлась iPatch) на специальной накладке (она монтируется на коммутационную панель) установлены фотоэлементы, которые и фиксируют факты подключения и отключения вилки коммутационного шнура. Это относительно простой (читай, недорогой) способ, который, что особенно важно, позволяет использовать любые стандартные коммутационные шнуры.

Одним из альтернативных методов является применение меток RFID. Комментируя использование этого метода, Степан Большаков, технический директор CommScope Enterprise Solutions в России и СНГ, указал на то, что если метка RFID встраивается в вилки шнуров на этапе их изготовления, то все работает хорошо, но это означает необходимость использования специальных шнуров. Если же метка добавляется на концевик вилки в полевых условиях, то она может оказаться относительно далеко от гнезда, из-за чего при изгибах шнура возникают проблемы со считыва-

## Преимущества AIM — согласно стандарту ISO/IEC 18598

Для иллюстрации возможностей систем AIM в стандарте ISO/IEC 18598 приведены непосредственные (внутренне присущие) и косвенные преимущества их использования.

Внутренне присущие преимущества обеспечиваются функциональностью самой системы AIM. К ним относятся:

- точное и автоматическое документирование вместо подверженной ошибкам трассировки вручную;
- управление изменениями для снижения стоимости обеспечения перемещений, добавлений и изменений;
- управление инцидентами для снижения времени простоя и восстановления;
- управление емкостью для улучшения планирования и повышения процента использования портов;
- управление активами.

Косвенные преимущества обеспечиваются другими системами, которые используют получаемые от системы AIM данные. К числу таких систем относятся:

- различные ИТ-системы (например, системы управления IP-телефонией, поддержки пользователей, обеспечения информационной безопасности и пр.);
- системы управления зданием (средства управления энергообеспечением, освещением, системы безопасности и контроля доступа);
- системы управления инфраструктурой ЦОДа — Data Center Infrastructure Management (DCIM);
- приложения, связанные с базами данных управления конфигурациями — Configuration Management Database (CMDB).

нием метки. Особенно остро эта проблема проявляется в оптических системах высокой плотности.


Довольно необычным (для стандарта) разделом ISO/IEC 18598 стало перечисление основных преимуществ использования систем AIM. Как пояснил «Журналу сетевых решений/LAN» Ханс-Юрген Нитхаммер, вопрос о включении этого раздела вызвал жаркие дебаты среди разработчиков стандарта, но в конечном счете было решено добавить эту информацию, чтобы у заказчиков было четкое понимание пользы соответствующих решений. Приведенные в стандарте преимущества делятся на «непосредственные» (обеспечиваются самой AIM) и «косвенные» (обеспечиваются другими системами благодаря получаемым от AIM данным) (см. врезку

«Преимущества AIM — согласно стандарту ISO/IEC 18598»).


Говоря об аргументах в пользу использования систем AIM в офисных инсталляциях, помимо общих плюсов в части повышения надежности, оперативности и удобства эксплуатации, Ханс-Юрген Нитхаммер указал на то, что они позволяют быстро определить наличие свободных портов и при необходимости локализовать неисправность. Это особенно важно в условиях, когда все больше коробок подключения различных устройств, включая точки доступа Wi-Fi, датчики инженерных систем, средства «интеллектуального» освещения и пр., выносятся в подпотолочное пространство, где визуально трудно определить состояние СКС. Кроме того, все популярнее стано-


22 июня

Организатор




**ОТКРЫТЫЕ СИСТЕМЫ**  
Open Systems Publications






# ТЕХНОЛОГИИ БОЛЬШИХ ДАННЫХ




**ПРАКТИЧЕСКИЕ  
СЕМИНАРЫ  
И КОНФЕРЕНЦИИ**

Регистрация открыта

По вопросам участия: Ольга Пуркина

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

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

Реклама 12+

Специальная цена участия до 31 мая

## 7950 руб.





В новой версии системы imVision (выпущена в декабре 2016 года) обеспечена поддержка архитектуры leaf-spine и многоволоконных соединений

вится технология подачи электропитания по Ethernet (PoE), а мощность соответствующих систем растет, что налагает дополнительные требования на СКС. В следующей версии стандарта ISO/IEC 18598 разработчики обещают добавить раздел, посвященный планированию внедрения решений PoE.

Тенденции развития сетевых инфраструктур ЦОДов стимулируют внедрение систем AIM и на этих объектах. Если в стандартной трехуровневой архитектуре каждый коммутатор доступа подключался, как правило, только к двум вышележащим устройствам, то в набирающей популярность архитектуре spine-leaf такой коммутатор (leaf) подсоединяется уже ко всем коммутаторам spine. Это увеличивает число кабелей и усложняет кабельную инфраструктуру, делая системы AIM более востребованными.

Нельзя не отметить и увеличение числа вариантов подключений с использованием двухволоконных (дуплексных LC) и многоволоконных (MPO) соединителей, предполагающих применение разнообразных гибридных шнуров (с MPO на одном конце и несколькими LC — на другом). При таких подключениях очень важно обеспечить совпадение типов портов и полярности. Задача может оказаться весьма трудоемкой. Здесь опять на помощь приходит AIM. Как рассказал Майкл Герман, в новой версии системы imVision (выпущена в декабре 2016 года) предусмотрена поддержка архитектуры leaf-spine и многоволоконных соединений. Система обеспечивает контроль и мониторинг многоволоконных соединений в реальном времени, включая соединения «точка — многоточка». Кроме того, она гарантирует соблюдение правил обеспечения полярности, в частности, предотвращая соединение портов MPO12 с портами MPO24, а также портов с разной скоростью. Важно и то, что imVision позволяет планировать кабельные тракты при миграции с одной скорости на другую.

Важным вопросом является «взаимоотношение» между системами AIM и системами управления инфраструктурой ЦОДа DCIM. Как отмечают эксперты CommScope, отслеживая изменения на физи-

ческом уровне, средства AIM способны предоставлять в систему DCIM чрезвычайно важные данные о кабельных подключениях и состоянии монтажных шкафов, что делает такие системы более полезными. В частности, задав общие характеристики таких шкафов (число посадочных мест, максимально допустимая нагрузка на пол, мощность и т. д.) и соответствующие характеристики устанавливаемых в них серверов и другого оборудования, можно контролировать их текущий уровень загруженности, мощности и т. д.

Опытом эксплуатации систем AIM на конференции поделились специалисты МТС. Как рассказал Александр Ежов, руководитель группы инженерно-технического обеспечения ЦОДов МТС, ввиду наличия большого числа офисных зданий с развитыми СКС, первым делом специалисты компании решили «навести порядок в кабельном хозяйстве» офисов. В ходе процедуры выбора было решено остановиться на системе iPatch (теперь, как уже говорилось, она называется imVision) компании CommScope. (Например, решение iTracs не подошло по причине высокой стоимости.)

Опыт использования iPatch оказался весьма успешным, и было принято решение о внедрении такой системы и в ЦОДах. В одном из них как раз намечалась модернизация СКС, и в ходе этого процесса сразу были установлены «интеллектуальные» панели CommScope. Среди преимуществ используемого решения Александр Ежов назвал существенное сокращение времени выполнения заявок на подключение нового оборудования и развертывания новых сервисов. Если раньше на обработку подобных заявок уходил в среднем час, то благодаря решению AIM это время сократилось до 5 мин. Важными для МТС стали также оперативность нахождения неисправностей, автоматическое протоколирование коммутации на кроссах, получение информации о состоянии коммутации и оповещение в случае его изменения.

В настоящий момент в МТС реализуется проект по интеграции трех используемых систем управления. Это собственно AIM-система imVision, система Remedy ITSM (она консолидирует информацию о всех заявках и инцидентах по всем системам ИТ) и система инвентаризации Inventory Management System.

В ходе дискуссии делегаты конференции обсуждали, какие аргументы необходимо представить руководству компаний для обоснования необходимости покупки системы класса AIM. Ясно, что для собравшихся, представляющих технические подразделения, удобство эксплуатации чрезвычайно важно, но этот аргумент может оказаться недостаточно весомым для руководства. А вот снижение времени реакции на инциденты (и сокращение возможных финансовых потерь благодаря этому) и обеспечение непрерывности бизнеса — весомые аргументы для обоснования выделения средств на AIM.



# Новые точки доступа Wi-Fi — новые возможности

Рост пропускной способности Wi-Fi — одна из ключевых тенденций развития этой технологии, благодаря которой современные беспроводные сети вышли на гигабитный уровень и по скорости уже мало чем уступают проводным «собратьям». Но наряду с высокой скоростью, немаловажна и экономическая составляющая построения и эксплуатации сетей Wi-Fi. Они должны быть доступны по цене, функциональны, удобны в обслуживании.

Оборудования для сетей Wi-Fi становится все больше. Наряду с классическими универсальными решениями, появляются продукты, «заточенные» под конкретное применение, а также инновационные продукты, в которых интегрированы возможности ранее отдельных устройств. Рассмотрим некоторые тенденции развития продуктов Wi-Fi на примере двух новых точек доступа, выпущенных компанией Extreme Networks.



Одна из них — ExtremeWireless WiNG 7602 — ориентирована на использование в гостиницах. При невысокой стоимости, это решение обладает всеми характеристиками продукта корпоративного класса. Производитель рекомендует

устанавливать точки доступа WiNG 7602 непосредственно в номерах, а не в коридоре, что гарантирует гораздо более качественную связь, а значит, и удовлетворение гостей услугами отеля в целом. Не секрет, что именно качество работы Wi-Fi зачастую становится главным при общей оценке гостиницы посетителями и определяет их рекомендации по ее выбору.

Важной особенностью точки доступа WiNG 7602 является возможность одновременной работы в диапазонах 2,4 и 5 ГГц. Как известно, диапазон 2,4 ГГц сильно зашумлен. Кроме того, в нем доступно меньше частотных каналов, чем в диапазоне 5 ГГц. Поэтому для обеспечения лучшего качества связи предпочтительнее использовать более высокочастотный диапазон. Но далеко не все конечные устройства способны работать на 5 ГГц. Этот фактор особенно важен для таких объектов, как гостиница, где заранее неизвестно, с каким смартфоном или планшетом придет тот или иной гость. Поэтому желательно поддерживать оба частотных диапазона Wi-Fi.

Работая только на частоте 2,4 или 5 ГГц, точка доступа WiNG 7602 поддерживает режим MIMO 2x2 с двумя пространственными потоками, что позволяет в стандарте 802.11ac обеспечивать скорость до 870 Мбит/с. Если же используются сразу оба частотных диапазона, то в каждом из них поддерживается только один пространственный поток: 1x1 (2,4 ГГц) + 1x1 (5 ГГц). При оборудовании точками доступа WiNG 7602 номеров в гостинице двухдиапазонный режим можно включать только на нескольких точках на этаже: благодаря лучшему прохождению сквозь стены и большей «дальнобойности» низкочастотного сигнала, одна точка доступа сможет в диапазоне 2,4 ГГц обслужить сразу несколько комнат. При этом обслуживание на 5 ГГц будет «индивидуальным» для каждого номера. Такое использование точек доступа WiNG 7602 позволит экономично решить задачу охвата всех номеров сразу в двух частотных диапазонах.

Точка WiNG 7602 оснащена дополнительным портом Ethernet, куда можно подключить, например, гостиничный телевизор или ноутбук гостя. Кроме того, встроенный в WiNG 7602 интерфейс Bluetooth поддерживает технологию Apple iBeacon для взаимодействия с мобильными устройствами гостей. Используя технологию Google Eddystone, можно отправлять на мобильные устройства гостей или делегатов проводимых в гостинице конференций различные уведомления или рекламные предложения без необходимости устанавливать какое-то специальное предложение.

Точка доступа WiNG 7602 выполнена в стиле Wall Plate и монтируется, например, на место обычной розетки буквально за пять минут. Никакого радиоблестования объекта при этом проводить не надо. Эти точки доступа используют операционную систему WiNG 5, которая поддерживает несколько вариантов развертывания. Точку доступа можно использовать вообще без контроллера, можно применять виртуальный контроллер или установить полноценный контроллер, который способен централизованно управлять работой до 25 тыс. таких точек доступа.

Тенденция к интеграции в одном устройстве все большего числа функций и появлению решений «все в одном» проявляется во многих областях. Точки доступа Wi-Fi не исключение. В своем новом продукте AP3916 инженеры Extreme Networks интегрировали точку доступа Wi-Fi с камерой видеонаблюдения. По задумке разработчиков, такое решение должно снизить общую стоимость

кабельной системы на объекте, причем как слаботочной (СК), так и силовой, поскольку для подключения точки доступа Wi-Fi и камеры видеонаблюдения используется один интерфейс Ethernet, а электропитание устройства осуществляется через него же (технология PoE).



Сама точка доступа AP3916 соответствует самому современному стандарту 802.11ac Wave 2, и при использовании режима MIMO 2x2:2 она способна обеспечить передачу по радиоканалу 1,2 Гбит/с. Решение поддерживает работу терминалов Wi-Fi в диапазонах 2,4 и 5 ГГц, а также имеет интегрированный радиомодуль BLE/802.15.4 (Bluetooth Low Energy) для подключения различных датчиков и других устройств Интернета вещей (IoT).

Входящая в состав продукта AP3916 широкоугольная видеокамера способна снимать с разрешением вплоть до 1920 x 1080 пикселей и поддерживает форматы H.264 (по умолчанию) и MJPEG. Для съемок в ночное время она оснащена 24 инфракрасными светодиодами (IR LED). Кроме того, камера оборудована микрофоном. Регулировка ориентации камеры в пространстве осуществляется в ручном режиме. Для просмотра и архивирования снятого камерой видео могут использоваться любые цифровые видеорегистраторы, соответствующие спецификации ONVIF (Open Network Video Interface Forum).

У подобного комбо-устройства — широкая сфера потенциального применения: медицинские учреждения, гостиницы, магазины, офисы и пр. Главное задача installатора — грамотно выбрать место установки, чтобы оно одинаково хорошо подошло и для точки доступа Wi-Fi, и для камеры видеонаблюдения. Возможно, на объектах, где это условие выполнить сложно или видеонаблюдение является критически важной задачей, продукты AP3916 могут применяться для организации дополнительной или резервной системы видеонаблюдения. Там же, где с установкой выделенных видеокамер возникают сложности, AP3916 может выручить. В любом случае применение такого интегрированного продукта — это существенное снижение общих расходов на инфраструктуру и установку.

Подробнее: [www.extremenetworks.com](http://www.extremenetworks.com)

## IoT как инструмент цифровой экономики

Интернет вещей, безусловно, является одной из наиболее обсуждаемых тем в отрасли ИКТ. Для одних это просто множество датчиков, подключенных к Интернету, для других — чуть ли не синоним цифровой экономики. Как показала проведенная IDC конференция IoT Forum 2017, даже находясь на начальной стадии, рынок Интернета вещей в России уже достаточно заметен и имеет отличные перспективы развития.

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

По данным IDC, к 2020 году в Центральной и Восточной Европе будет насчитываться 1,4 млрд подключенных устройств, а объем рынка Интернета вещей составит 24 млрд долларов. На Россию, по прогнозу, придется порядка 36% от этой суммы — 8,76 млрд долларов. До указанного уровня рынок вырастет с объема 3,92 млрд, который был зафиксирован аналитиками IDC в 2016 году. Средние темпы роста рынка Интернета вещей в России в период 2016–2020 годов составят 21,3% (см. рис. 1).

Лидерами по объему инвестиций в Интернет вещей в России к 2020 году, по прогнозу IDC, будут производственный сектор и транспортные компании. Кроме того, в первую пятерку по инвестиционной активности войдут энергетика, потребительский сегмент и госсектор. Примечательно, что наибольшие темпы роста покажут кросс-индустриальные решения. Это и понятно: именно на стыке отраслей часто формируются наиболее инновационные разработки, демонстрирующие наилучшую рентабельность. Да и сам Интернет вещей сформировался на стыке ИТ, коммуникационных технологий и «умных» устройств.

Из чего складывается рынок Интернета вещей? Аналитики IDC делят его на четыре составляющие: оборудование, ПО, услуги и связь. По состоянию на 2016 год доли всех названных компонент сопоставимы (см. рис. 2), но при этом продажи оборудования (29%)

и услуг (30%) по объемам все же превосходят затраты на ПО (22%) и коммуникационные каналы (19%).

На текущий момент большинство внедряемых решений в области IoT эксперты относят к бизнес-модели первого поколения — Интернету вещей 1.0. Для этой модели характерен акцент на установке различных датчиков и сенсоров и на организации их подключения. Сервисы и приложения по анализу собираемой информации, конечно, тоже используются, однако «глубина» проработки данных невелика.

При переходе к модели Интернета вещей 2.0 акцент будет смещаться на аналитику. Все шире станут использоваться преимущества облачной модели, средства машинного обучения и когнитивные вычисления. При этом в платформах IoT активнее будут применяться открытые программные интерфейсы API для обмена данными с другими системами, а также различные приложения с открытым программным кодом. Для поколения 2.0 будет характерно увеличение обратных связей, что существенно расширит возможности систем.

Важной тенденцией станут перенос интеллекта ближе к конечным устройствам и наделение их все большими возможностями. Несмотря на эффективность облачной модели, ситуация, когда анализ данных и выработка управляющих воздействий происходят где-то далеко в крупном ЦОДе, для многих задач является нежелательной. Передача трафика до ЦОДа и обратно может привести к недопустимым задержкам там, где требуется быстрая реакция (производственные процессы, системы безопасности, взаимодействие автомобиля с дорожной инфраструктурой и пр.).

Как следствие, наряду с переносом интеллекта в мегаЦОДы нарастает обратный процесс, получивший название «периферийные вычисления» (fog computing), когда анализ собираемых данных и выработка управляющих воздействий происходят в узлах, максимально приближенных к конечным устройствам. В будущем все в большей степени анализ будет производиться самими устройствами, что позволит минимизировать задержку на принятие решений и повысит автономность устройств.

Хотя по своему объему рынок Интернета вещей уже достаточно весом, он только в начале пути. Более половины (54%) из 150 опрошенных руководителей в России пока даже не планируют использовать «подключенные» устройства для сбора информации, мониторинга и автоматизации (см. рис. 3). Интересно и то, что 15% опрошенных уже внедрили подключенные устройства, но не планируют дальнейшего расширения. Возможно, эти руководители считают, что они уже прошли этап цифровой трансформации и перевели свои предприятия на рельсы новой экономики. В таком случае, боюсь, они заблуждаются.

Нередко приходится слышать мнение о том, что Интернет вещей является базисом для новой, циф-

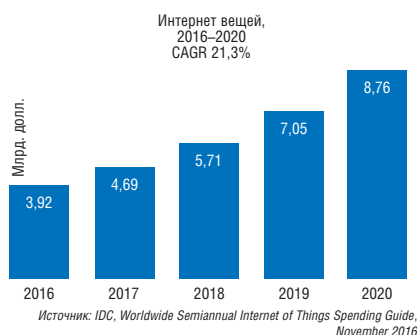


Рис. 1. Развитие рынка Интернета вещей в России в период 2016–2020 годов

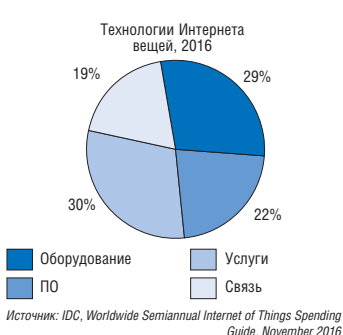


Рис. 2. Основные составляющие рынка Интернета вещей в России

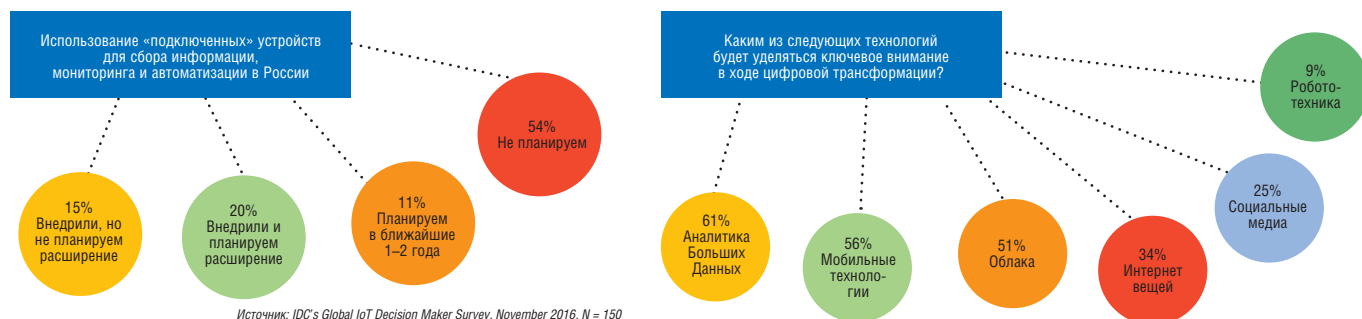


Рис. 3. Состояние Интернета вещей в России

ровой экономики. Несомненно, эта технология для реализации новых бизнес-моделей — важная, но далеко не единственная и не самодостаточная. В ходе опроса, проведенного в 2016 году аналитической группой OSP Data в рамках совместного исследования с Hitachi Data Systems, Интернет вещей был поставлен только на четвертое место по степени важности в деле цифровой трансформации предприятий. Выше оказались аналитика Больших Данных, мобильные и облачные технологии (см. рис. 4). Хотя, конечно, именно комплексное применение названных технологий позволит достичь наибольшего эффекта. Тот же Интернет вещей бессмыслен без средств анализа собираемых данных, тогда как средства аналитики превращаются в ничто при отсутствии источников этих данных (подключенных устройств).

Возвращаясь к Интернету вещей, нельзя не упомянуть множество пока еще не решенных проблем, начиная с отсутствия отечественных стандартов и заканчивая острыми вопросами безопасности. Но это не значит, что можно ничего не делать, ожидая их разрешения. Опыт пионеров показывает, что уже сегодня удается реализовывать действительно эффективные проекты. Возможно, следует начинать с небольших тестовых реализаций, которые позволят избежать больших рисков и вместе с тем «почувствовать» новые возможности. Тем более что современные технологии дают возможность быстро и с минимальными инвестициями «попробовать» IoT: зачастую достаточно расставить недорогие датчики, а саму платформу и средства анализа арендовать в облаке.

Рис. 4. Результаты ответа на вопрос «Каким из следующих технологий будет уделяться ключевое внимание в ходе цифровой трансформации?»

## Fortinet сертифицировала МСЭ по первому классу защищенности

Межсетевые экраны FortiGate Enterprise Firewall были сертифицированы ФСТЭК в соответствии с новыми требованиями.

Компания Fortinet получила сертификат соответствия ФСТЭК по первому классу защищенности на свои МСЭ FortiGate Enterprise Firewall. Сертификат № 3720 подтверждает, что FortiGate Enterprise Firewall под управлением операционной системы FortiOS с версией программного обеспечения 5.4.1 является программно-техническим средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, и соответствует требованиям нормативных документов.

Сертификация позволяет продавать FortiGate Enterprise Firewall государственным организациям, банкам, страховым компаниям — всем предприятиям, где применяются информационные системы первого класса защищенности. «На сегодняшний день мы практически единственная компания на российском рынке, обладающая сертификатами, соответствующими новым требованиям ФСТЭК, утвержденным в сентябре 2016 года, — гово-

рит Алексей Андрияшин, ведущий системный инженер Fortinet. — Для нас очень важно, чтобы все заказчики, нуждающиеся в высокоэффективных межсетевых экранах для защиты персональных данных своих клиентов, получили доступ к нашим решениям в России. Именно поэтому мы хотим соответствовать нормам российского законодательства и активно занимаемся вопросами сертификации».

Сертифицированная версия программного обеспечения FortiOS 5.4.1 позволяет обеспечить адекватную защиту от современных угроз и сегодня, и в будущем — до тех пор, пока данная версия будет поддерживаться компанией Fortinet (как минимум до окончания срока действия сертификата 16 марта 2020 года). Пользователи сертифицированного решения могут быть уверены в его актуальности, так как производителем предусмотрен механизм своевременного обновления баз обнаружения и предотвращения угроз.



Источник: Fortinet

## «Абитех» подписала соглашение с GE о выпуске ИБП под маркой «А-ИСТ»

Источники бесперебойного питания «А-ИСТ» будут собираться в России из комплектующих GE.

Дмитрий Ганжа,  
главный редактор «Журнала сетевых решений/LAN»

### РОССИЙСКИЙ ИБП ПОД МАРКОЙ «А-ИСТ»

На юбилейной 15-й партнерской конференции «Абитех» объявила о подписании лицензионного соглашения «Assembly License and Sale Agreement» с GE Industrial Solutions, в соответствии с которым будут реализовываться ИБП под маркой «А-ИСТ» («Абитех-источник»). Как видно из названия соглашения, оно предусматривает организацию сборочного производства и право на продажи оборудования. «В этом году мы сделали следующий шаг в нашем сотрудничестве с GE — создали платформу для бесперебойного питания, где объединены решения GE и наработанный опыт «Абитех», — отметил Евгений Михеев, руководитель компании «Абитех» — С подписанием лицензионного соглашения у нас появятся совершенно законные основания для российского производства источников бесперебойного питания».

Модельный ряд ИБП «А-ИСТ» предусматривает поддержку широкого диапазона мощностей — от 10 до 160 кВА. Источники будут собираться на площадке «Абитех» из тех же комплектующих, что и ИБП под маркой GE. Для тщательной проверки и тестирования продукции GE поставит свое тестовое оборудование. Первые ИБП мощностью от 10 до 40 кВА (аналог GE SG 10-40) планируется выпустить до конца текущего года. Согласно предварительному прогнозу, объемы продаж источников «А-ИСТ» и GE со временем сравняются.

Из-за таможенных пошлин импорт комплектующих обходится дороже, чем готовых устройств, к тому же масштабы производства меньше, поэтому и себестоимость ИБП окажется выше, чем, например, при производстве в Польше, однако цены на ИБП «А-ИСТ» и аналогичные ИБП под маркой GE будут одинаковыми. Это позволит «Абитех» участвовать в проектах,

где обязательным или приоритетным условием является производство оборудования в России. Кроме того, при закупках в рамках 223-ФЗ товары российского происхождения получают 15-процентный гандикап (приоритет) по цене, что повышает шансы выиграть тендер.

### МАСШТАБИРУЕМЫЕ, НО НЕ МОДУЛЬНЫЕ

В GE в целом скептически относятся к идее модульной конструкции применительно к ИБП, хотя соответствующая линейка у компании есть. «Главное достоинство модульных решений — простота масштабирования, — объясняет позицию компании Кас Розенберг, директор по работе с вертикальными рынками GE Industrial Solutions в регионе EMEA. — Однако для их обслуживания все равно приходится привлекать сервисные компании, что во многом нивелирует названное преимущество». Как показывает практика, заказчики часто осуществляют замену не сами — обращаются к специализированной компании. При этом, несмотря на наличие возможности «горячей замены», нагрузка обычно отключается от ИБП.

В результате компания предложила промежуточное решение, которое нашло воплощение в бестрансформаторных ИБП серии TLE мощностью от 40 до 120 кВА (всего пять моделей разной мощности с шагом 20 кВА). Источники этой серии получили обозначение Scalable, то есть расширяемые или наращиваемые — их мощность можно увеличить путем добавления силовых модулей. Однако выполнять замену и добавление блоков в «горячем режиме», как в случае модульных устройств, нельзя. До шести источников могут быть объединены в параллель. Эти источники средней мощности дополняют линейку TLE «снизу» (до этого серия TLE включала ИБП на 160–800 кВА).

Как и в серии SG третьего поколения, в новых ИБП предусматривается аппаратная поддержка «черного ящика» — платы обновленной системы управления FLEX DSP. Соответствующий модуль позволяет фиксировать переходные процессы и фактически записывает осциллограмму для ряда параметров. Система отслеживает 16 аналоговых характеристик и 16 параметров состояния ИБП в интервале 50 мс до и после возникновения события. В случае нештатной ситуации эта информация может быть использована сервисной службой для более точной оценки причины ее возникновения и для выдачи рекомендаций заказчику, чтобы не допустить повторных инцидентов.

Наряду с линейкой TLE Scalable были анонсированы две модели моноблочных ИБП TLE мощностью 30 и 40 кВт с возможностью установки АКБ в корпусе устройства. На все ИБП предоставляется гарантия сроком 2 года, а срок их службы составляет 12 лет. В качестве бонуса покупателям предлагается сервис iUPSGuard (см. подробнее раздел «Сервис от «Абитех»»).

### РЕЗЕРВИРОВАНИЕ С ПОМОЩЬЮ КОЛЬЦЕВОЙ ШИНЫ

Надежность системы бесперебойного энергоснабжения можно увеличить разными способами: посредством дублирования систем (2N), параллельного резервирования (N+1) и т. п. GE предложила использовать для статических ИБП то же решение, что и для систем с динамическими ИБП большой мощности, —



Фото: «Абитех»



изолированную параллельную кольцевую систему (Isolated Parallel Ring Bus, IPRB).

Как считают в GE, при таком подходе реализуются основные преимущества всех остальных способов резервирования: обеспечивая необходимую степень отказоустойчивости, это решение позволяет распределить всю имеющуюся нагрузку между всеми источниками бесперебойного питания. При этом оно отличается простотой и эффективностью, позволяя минимизировать капитальные затраты.

Суть решения состоит в том, что все ИБП подключаются к кольцевой шине. Например, для защиты ЦОДа мощностью 10 МВт с избыточностью N+2 можно подключить 12 источников по 1 МВт. Все они подают питание в шину, а нагрузка делится между ними поровну. При возникновении проблем с каким-либо источником кольцо можно разомкнуть и изолировать неисправный ИБП. Таким образом, для проведения обслуживания отключать нагрузку не потребуется.

### ИБП С МАХОВИКОМ ВМЕСТО БАТАРЕЙ

GE представила интегрированное решение для бесперебойного питания, где вместо традиционных батарей для хранения энергии используются маховики (flywheel) производства VYCON. У GE уже было подобное решение, в котором применялись маховики другого поставщика. В силу ряда причин компания от него отказалась, но ввиду роста интереса, прежде всего на рынке США, в конце прошлого года вновь начала выпускать такие системы. Возможность подключения маховика предусматривается в ИБП серий SG и TLE мощностью от 60 кВА, причем на весь комплект предоставляется единая гарантия (маховик поставляется под маркой GE).

Для центров обработки данных одним из преимуществ маховика перед батареями является экономия на охлаждении: маховик, как и ИБП, может работать при температуре в помещении до 35–40°C, тогда как батареям требуется не более 20–22°C. Другой тенденцией (помимо повышения средней температуры в помещениях ЦОДа), которая способствует росту популярности таких решений, является виртуализация, в результате чего достаточно обеспечить меньшее время автономной работы.

Как отмечает Алексей Савкин, директор по продажам GE Industrial Solutions в странах СНГ, 99% всех инцидентов с качеством питания длятся менее 10 с: обеспечение таких длительных сроков автономной работы, как раньше, во многих сценариях использования теперь не требуется. Маховик же способен поддерживать питание в течение 10 с — этого вполне достаточно для того, чтобы запустить современный дизель-генератор (средний показатель 4 с). При необходимости до шести маховиков могут быть установлены параллельно, и, таким образом, длительность

работы от накопителя энергии увеличивается до одной минуты.

### СЕРВИС ОТ «АБИТЕХ» И GE

«Абитех» обслуживает оборудование GE на всей территории России — в штате компании более 30 сервисных инженеров. Как заявил Иван Качалкин, начальник сервисного центра «Абитех», «наша задача — обслуживать все проданные и установленные в России источники бесперебойного питания, чтобы не было забытого оборудования». Конечно, такую задачу тяжело решить в одиночку, поэтому «Абитех» заявляет о желании увеличить количество сервисных партнеров, к которым предъявляются весьма жесткие требования по теоретической и, главное, практической подготовке.

Компания намерена увеличить число сервисных партнеров до 20–30. Помимо повышения доступности сервиса, это должно позволить сократить время реакции на нештатные ситуации (менее 3 ч в любое время дня и ночи). Чтобы восстановить работу оборудования, необходимые комплектующие должны быть оперативно доступны. На складе имеются запчасти на все модели ИБП (причем даже те, которые уже сняты с производства) в общей сложности на сумму около 1 млн евро.

Эффективную эксплуатацию современного оборудования трудно представить без средств мониторинга и удаленного доступа. Для облегчения обслуживания и эксплуатации ИБП компания GE предлагает глобальную систему мониторинга и диагностики iUPSGuard, которая позволяет своевременно информировать ее сотрудников, партнеров и заказчиков о нештатных ситуациях и выявлять неблагоприятные тенденции в функционировании ИБП. Помимо источников GE, система может контролировать устройства других производителей (при наличии стандартного интерфейса SNMP). В первый год использования ИБП соответствующий сервис предоставляется бесплатно (для ИБП мощностью от 160 кВА).

Информация передается по защищенным каналам только в одном направлении — от источника в ЦОД GE, где и аккумулируется. Иначе говоря, с ее помощью нельзя воздействовать на ИБП извне — например, отключить его. Анализ ежеквартальных отчетов позволяет давать заказчикам рекомендации по режимам эксплуатации оборудования — в частности, по изменению настроек системы кондиционирования для оптимизации температурного режима и предотвращения его выхода из строя. Информация из базы данных iUPSGuard может выводиться на экран смартфона.

В Москве создан тренинговый учебный центр для проведения теоретических и практических занятий, где представлена вся линейка актуального оборудования GE.



Источник: GE

С помощью мобильного приложения iUPSGuard сервисный инженер оперативно получит все данные о текущем состоянии и истории функционирования ИБП

Вместо аккумуляторов с ИБП GE серий SG и TLE теперь можно использовать маховики



Источник: GE

## С акцентом на EcoStruxure

Первый день саммита инноваций, проведенного Schneider Electric в Москве, был посвящен решениям для ИТ-рынка и ЦОДов.

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

Открывая Innovation Summit 2017, Йохан Вандерплаетсе, президент Schneider Electric в России и СНГ, отметил, что современные тенденции провоцируют увеличение спроса на электроэнергию: по прогнозу, в ближайшие 40 лет ее потребление вырастет в 1,5 раза. Вместе с тем, чтобы затормозить изменение климата, необходимо за тот же период снизить выбросы углекислого газа в два раза. Для решения обеих задач придется существенно повысить эффективность производства, доставки и потребления электроэнергии.

Это вполне возможно. Во-первых, все более широкое распространение получают возобновляемые источники энергии и новые системы ее аккумуляции, причем стоимость их постоянно сокращается. Во-вторых, степень централизации производства и распределения электроэнергии неуклонно снижается. Отрасль будет постепенно переходить от традиционной централизованной модели (когда энергия вырабатывается только крупными генерирующими центрами) к распределенной модели активно-адаптивной сети и использованию небольших локальных генерирующих систем, установленных рядом с потребителями. По словам Йохана Вандерплаетсе, уже сегодня есть примеры «умных» домов, которые не только полностью обеспечивают

свои потребности в электричестве, но и готовы передавать ее избыток другим.

Третьим важным направлением повышения энергоэффективности является все более широкое использование цифровых технологий. Эксперты отмечают конвергенцию традиционных средств доставки, распределения и управления электроэнергией с современными ИТ-технологиями. Эта тенденция наглядно воплощена в EcoStruxure — новой архитектуре

активного управления электроэнергией, разработанной Schneider Electric.

По словам Наталии Макарочкиной, вице-президента подразделения IT Division в России и СНГ, эта комплексная архитектура позволяет активно управлять энергией на всем ее пути — от электростанции до розетки. Она состоит из трех уровней. На первом — наделенное интеллектуальными средствами сбора и передачи данных оборудование электрической инфраструктуры: трансформаторы, ИБП, электрощиты, блоки распределения и т. д. На втором — программные средства мониторинга и управления StruxureWare. На третьем — приложения и сервисы StruxureOp, обеспечивающие более глубокий анализ собранных данных.

Одной из ключевых областей применения решений EcoStruxure являются современные центры обработки данных. Характеризуя ситуацию в данной области, Филипп Арсено, старший вице-президент подразделения IT Division, отметил, что наряду с развитием мегацифров наблюдается интерес к развитию периферийных вычислений — edge computing. «Небольшие региональные ЦОДы будут развиваться так же активно хотя бы из-за ограничений в пропускной способности каналов связи с мегацифрами», — сказал он. Используя интеллектуальные функции EcoStruxure, можно, например, обеспечить эффективное управление удаленными малыми ЦОДами.

На Innovation Summit был продемонстрирован ряд новинок компании — в частности, ИБП Galaxy VM, укомплектованные литий-ионными батареями. Такие батареи позволяют минимизировать операционные расходы за счет большого количества (до 5000) циклов заряда-разряда и увеличенного до 15 лет срока службы. Их можно использовать и с другими ИБП Schneider Electric, в том числе с выпущенными в этом году устройствами Galaxy VX мощностью от 500 до 1500 кВт. На стендах были также представлены защищенные промышленные ИБП Gutor, новые внутрирядные кондиционеры для высокоплотных ЦОДов и различные стоечные конструктивы. Среди прочих новинок отметим большой фальшпольный кондиционер мощностью 140 кВт, рядом с которым демонстрировался макет современного модульного фальшпола.

На саммите было заключено стратегически важное соглашение о локализации производства стоечного оборудования: входящая в производственную группу Remer компания «ЦМО» займется выпуском серверных шкафов по лицензии Schneider Electric. Кроме того, подписан меморандум о намерениях сотрудничества с сетью центров обработки данных 3Data. Schneider Electric станет технологическим партнером российской компании в проектах по строительству ЦОДов, поставляя ИБП, системы кондиционирования и другие компоненты инженерной инфраструктуры.

ИБП Galaxy VM  
с литий-ионными  
батареями



Фото: Александр Барсков

# Schneider Electric будет способствовать развитию российского рынка IIoT

Второй день Schneider Electric Innovation Summit 2017 был посвящен промышленной автоматизации и Промышленному интернету.

Дмитрий Ганьжа,  
главный редактор «Журнала сетевых решений/LAN»

Интернет вещей лежит в основе разворачивающейся четвертой промышленной революции — Industry 4.0. По некоторым оценкам, к 2030 году вклад IIoT в мировую экономику составит 14 трлн долларов. Это, по выражению Грега Конари, старшего вице-президента Schneider Electric по стратегии, «одна из главных мегатенденций сегодня, оказывающая глубокое влияние на рынок».

Широкомасштабное внедрение IIoT и IIoT ведет к коренным изменениям в бизнес-практике, операционных процедурах и общих подходах к решению проблем, однако Schneider Electric рассматривает Промышленный интернет как эволюционное явление, а не революционное. Первое решение, которое соответствовало принципам IIoT в современном понимании (цифровизация и подключенность), появилось у компании в далеком 1987 году, еще до возникновения Всемирной паутины, — это была цифровая распределенная система управления.

Как заявил Леонид Мухамедов, исполнительный вице-президент Schneider Electric по региону Европа, в своем выступлении на пленарной сессии Innovation Summit 2017, до 70% всего производимого Schneider Electric оборудования имеет отношение к Промышленному интернету. По его словам, красота Промышленного интернета состоит в том, что, решая с его помощью одни задачи, заказчики совершенно неожиданно для себя параллельно справляются со множеством других. Так, благодаря автоматизации учета повышается прозрачность операций, что создает препятствия для воровства.

Schneider Electric подписала соглашение с «Лабораторией Касперского» по совместным исследованиям и разработке решений в области промышленной кибербезопасности



Фото: Дмитрий Ганьжа

Согласно исследованию Schneider Electric, в Европе более 50% компаний уже используют Промышленный интернет вещей, в России же соответствующий рынок только начинает формироваться. Как отметил Виталий Недельский, президент Национальной ассоциации Промышленного интернета, российские предприятия «запаздывают с внедрением интеллектуальных сетей». Вступление в НАПИ Schneider Electric должно способствовать ускорению этого процесса, в чем компания весьма заинтересована.

Заявления о значимости для Schneider Electric российского рынка — отнюдь не пустые слова. По обороту он занимает четвертое место — после США, Китая и Франции. Только за шесть последних лет — с 2010 по 2016 год — инвестиции в него превысили 1 млрд евро. В России у компании пять заводов, а в Сколково функционирует центр НИОКР по разработке программных решений для Smart Grid.

Правда, как отметил во время пресс-конференции Йохан Вандерплаетсе, президент Schneider Electric в России и СНГ, этот центр специализируется на адаптации решений для «умной» передачи энергии для российского рынка. Подписанное же соглашение об открытии еще одного центра НИОКР в Иннополисе (Республика Татарстан) предусматривает в числе прочего создание решений, которые будут использоваться на глобальном рынке. В первую очередь речь идет о разработках для нефтегазовой отрасли и для защиты критической инфраструктуры.

Вопросы информационной безопасности при использовании технологий IIoT по-прежнему интересуют заказчиков в первую очередь. О потенциальных последствиях говорят такие инциденты, как DDoS-атаки с использованием ботнета Mirai, состоящего из подключенного к Интернету устройств (и это еще не самый плохой сценарий). Так что о мерах безопасности необходимо побеспокоиться заранее, и желательно, чтобы соответствующие функции уже присутствовали в предлагаемом решении. «Системы безопасности должны быть интегрированы, — подчеркнул Андрей Духвалов, руководитель департамента перспективных технологий «Лаборатории Касперского». — Мы считаем, что лучше говорить не об информационной безопасности, а об информационной устойчивости».

Schneider Electric заключила соглашение с «Лабораторией Касперского» по разработке решений в области промышленной кибербезопасности. У «Лаборатории Касперского» уже имеется центр компетенций в Иннополисе, на базе которого и планируется осуществлять сотрудничество. Взаимодействие компаний началось еще в рамках Консорциума Промышленного интернета (Industrial Internet Consortium), членами которого они обе являются.



# Как экономить на хранении данных ЦОДа

Все современные ЦОДы сталкиваются с проблемой постоянного увеличения объемов данных разной степени критичности, которые обязательно нужно надежно хранить. Это могут быть данные продуктивных систем конечных заказчиков ЦОДов, к которым предъявляются повышенные требования к доступности (как правило, более чем 99,9% доступности) или архивные данные, к которым требования доступности ниже, но которые следует долго хранить (например, архивы видеонаблюдения или резервные копии продуктивных систем). Также каждый тип данных имеет свои специфические требования к производительности дисковых подсистем.

В этих условиях на первый план выходят две следующие задачи:

1. Как правильно организовать хранение данных с учетом различных требований к их доступности и производительности?
2. Как при этом оптимизировать затраты в условиях постоянно растущих объемов данных?

Традиционным подходом является использование классических аппаратных систем хранения данных с вертикально масштабируемой архитектурой (scale-up) и сетью хранения данных на базе протокола Fibre Channel. При таком подходе в зависимости от типа задачи приходится использовать разные системы хранения данных различных производителей. Этот подход позволяет организовать хранение данных с учетом различных требований, но при этом имеет ряд существенных минусов:

- Высокая стоимость покупки и обслуживания аппаратных СХД (особенно после трех лет эксплуатации, когда нужно продлевать контракт на поддержку СХД по сильно завышенной стоимости либо покупать новую СХД).
- Большое количество разных СХД различных производителей повышает сложность администрирования (на профессиональном сленге: «зоопарк»).
- Серьезные ограничения при масштабировании систем (предел вертикального масштабирования СХД обычно только 8 контроллеров, и если он достигнут, нужно покупать новую СХД).
- Нет возможности задействовать оборудование сторонних производителей для оптимизации стоимости (так называемый vendor-lock).
- Высокая стоимость SAS-дисков (особенно SSD) и невозможность использования SATA- дисков в отказоустойчивых конфигурациях.

Данный подход позволяет решить задачу корректного хранения данных с учетом различных требований к доступности и производительности, но при этом стоимость такого подхода является слишком высокой, а отсутствие гибкости при масштабировании и управлении СХД не позволяет оперативно реагировать на постоянно возрастающие требования заказчиков ЦОДов.

На сегодняшний день существуют два подхода к решению данной проблемы (которые можно комбинировать), и оба подхода

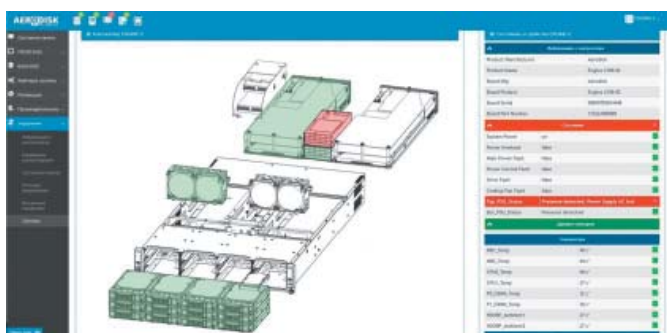
основаны на применении программно-определяемых систем хранения данных.

## Подход №1. Использование программных СХД с архитектурой scale-up

Суть подхода — постепенно заменить аппаратные СХД программными с архитектурой scale-up.

На текущий момент программно-определяемые СХД по надежности и функциональности не уступают классическим аппаратным решениям. К примеру, СХД AERODISK ENGINE российской разработки поставляется как в аппаратном варианте, так и в программном. При этом программный вариант СХД AERODISK ENGINE с точки зрения надежности, производительности и функциональности ничуть не уступает аппаратному, но дает следующие преимущества:

- Возможность резко снизить затраты на покупку и эксплуатацию СХД, используя собственное x-86-совместимое оборудование и диски.
  - Обычные x-86 серверы (которые применяются в качестве контроллеров программных СХД) и дисковые полки значительно дешевле (обычно в 2–3 раза) аналогичного оборудования, поставляемого в аппаратных СХД.
  - Оригинальные Enterprise-диски от их производителей (HGST, Seagate, WD) также в 2–3 раза дешевле, чем аналогичные диски (по сути те же самые), поставляемые в рамках аппаратных СХД.
  - По истечении 3 лет эксплуатации нет надобности продлевать гарантию на аппаратную СХД по завышенной стоимости:
    - вместо продления гарантии на устаревшие диски лучше использовать новые современные диски, что в итоге получается дешевле и при этом объем новых дисков всегда больше;
    - жизненный цикл контроллеров СХД (серверов x-86) — 5 лет, в течение этого срока стоимость их аппаратного обслуживания находится на умеренном уровне.
  - Лицензирование программных СХД (во всяком случае AERODISK) выполняется по количеству контроллеров и по количеству дисков (объем дисков неважен), поэтому данные затраты можно нести по мере необходимости (с учетом фактического роста объема данных и нагрузки). Также, если есть потребность в снижении CAPEX-затрат на лицензии ПО AERODISK ENGINE, можно получать СХД как услугу.
- Стандартизация и снижение сложности управления инфраструктурой хранения данных осуществляются за счет использования единого программного решения.
  - В данный момент ПО AERODISK ENGINE может закрыть большинство потребностей, в частности:
    - высокопроизводительное гибридное хранилище для продуктивных систем (виртуализация, СУБД, электронная



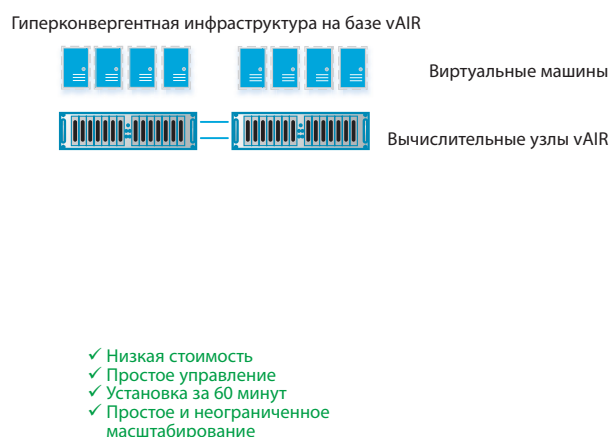
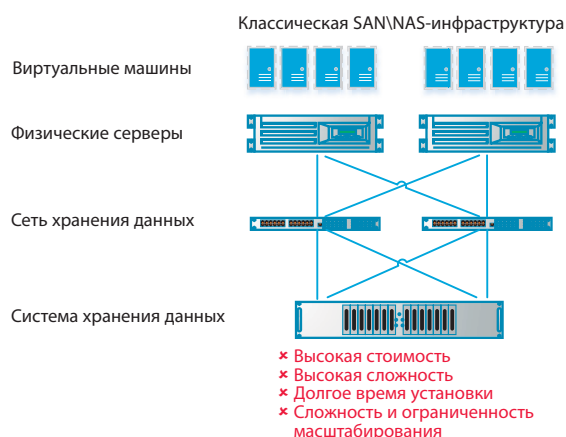
Интерфейс управления программно-определяемой СХД AERODISK ENGINE



- почта) с использованием SSD-дисков для ускорения производительности;
- облачное файловое хранилище с использованием дисков большого объема;
- СХД для видеонаблюдения с большим постоянным потоком записи и с возможностью длительного хранения;
- хранилище архивов и резервных копий с поддержкой компрессии и автоматической дедупликацией для экономии места на дисках.

ских СХД с архитектурой scale-up, будет организована на базе растянутых между контроллерами томов и файловых систем, что позволит использовать недорогие SATA-диски (в том числе и SSD), количество контроллеров в СХД не будет иметь логических ограничений.

На схеме ниже приведено наглядное сравнение двух подходов к созданию ИТ-инфраструктуры на примере небольшого кластера высокой доступности (HA-cluster).



Такой подход позволит в несколько раз снизить стоимость владения инфраструктурой СХД за счет снижения затрат на оборудование и повышения стандартизации инфраструктуры. При этом остаются актуальными следующие издержки архитектуры scale-up:

- ограничение при масштабировании (до 8 контроллеров на одну логическую систему);
- невозможность использования недорогих SATA-дисков для отказоустойчивых конфигураций;
- остается актуальной проблема большого количества различных элементов ИТ-инфраструктуры, которыми нужно управлять (то .есть. серверы, сеть хранения, СХД, системы виртуализации и т. п.).

## Подход №2. Использование гиперконвергентных вычислительных комплексов с архитектурой scale-out

Использование гиперконвергентных систем является наиболее инновационным подходом к созданию ИТ-инфраструктур ЦОД-ов любого масштаба и сложности, который позволяет объединить scale-out СХД и систему виртуализации в одну легко масштабируемую систему с централизованным управлением.

В отличие от вертикального масштабирования (scale-up), принцип горизонтального масштабирования (scale-out) снимает ограничения по количеству контроллеров СХД и позволяет использовать недорогие SATA-диски в отказоустойчивых конфигурациях СХД. Для реализации данного подхода компания AERODISK разработала гиперконвергентный комплекс AERODISK vAIR, сочетающий в себе СХД с архитектурой scale-out и систему виртуализации. Этот комплекс будет доступен в конце 2017 года и позволит в полной мере устранить текущие экономические издержки умного хранения данных.

Продукт AERODISK vAIR, как и ENGINE, будет поставляться как в аппаратном варианте, так и в программном. Отказоустойчивость в данной системе, в отличие от классиче-

Как видно из схемы, использование гиперконвергентных систем, объединяя в себе виртуализацию, серверы, СХД и сеть хранения в одном масштабируемом решении, радикально упрощает эксплуатацию и масштабирование ИТ-инфраструктуры.

Дополнительную гибкость системе придает возможность использования различных систем виртуализации. На текущий момент поддерживается встроенная виртуализация на базе KVM, а также популярные системы VMware vSphere и MS Hyper-V, что позволяет максимально гибко подходить к планированию инфраструктуры и при необходимости использовать существующие (уже купленные) лицензии на сторонние системы виртуализации.

Кроме того, использование данного подхода решает проблемы, связанные с высокой стоимостью и низкой степенью гибкости традиционных инфраструктур хранения данных.

## Вывод

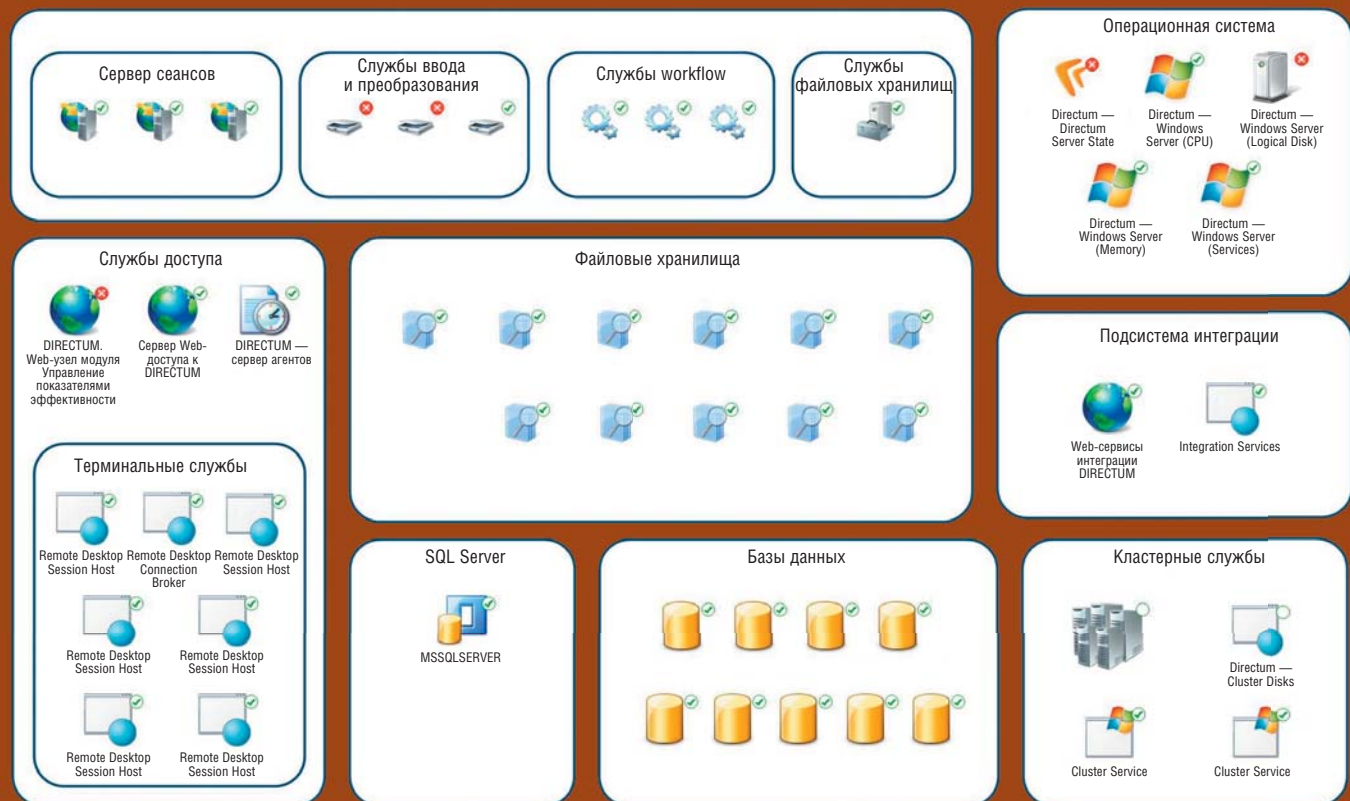
На сегодняшний день оптимальным вариантом развития систем хранения данных ЦОДов, с учетом эффективного подхода к затратам, несомненно является использование гиперконвергентных программно-определяемых СХД, так как они позволяют серьезно снизить затраты на инфраструктуру, более гибко и оперативно реагировать на новые требования и продлить жизненный цикл оборудования систем хранения данных.

Для инфраструктур, в которые уже вложены серьезные средства в сеть хранения данных на базе Fibre Channel или в которых есть задачи по дезагрегации отдельных хранилищ (дезагрегация — противоположность гиперконвергентности), разумным будет совмещать программные scale-up СХД с гиперконвергентными системами там, где это возможно.

# Системный мониторинг: сопровождаем СЭД проактивно

Одной из первоочередных задач, на которую следует выделить ресурсы и время при сопровождении системы электронного документооборота, является организация процесса мониторинга. Инструменты мониторинга облегчают решение и предупреждение проблем. При этом в долгосрочной перспективе проактивный подход более эффективен, чем реактивный, и может быть реализован с помощью доступных средств.

**Алексей Корепанов,**  
руководитель проектов внедрения DIRECTUM



Объекты системного мониторинга



После внедрения системы электронного документооборота (СЭД) процессы в компании необходимо развивать и адаптировать с учетом меняющегося окружения.

Чтобы избежать дисбаланса между ростом запросов со стороны сотрудников бизнес-подразделений и возможностью развития системы электронного документооборота, важно в самом начале определить требования, причем не только функциональные (какие действия должна выполнять система), но и нефункциональные (доступность, быстродействие, целостность, возможности доработки/настройки и др.). В частности, для крупных компаний могут быть актуальными поддержка круглосуточной работы, одновременное подключение тысяч пользователей, масштабируемость системы, сохранность и безопасность данных.

Еще на старте проекта следует обозначить целевые показатели для этих параметров с учетом потенциального роста масштаба решаемых задач. Помимо системного ПО и оборудования, необходимо позаботиться о формировании команды сопровождения и поддержки.

## ОРГАНИЗАЦИЯ МОНИТОРИНГА

В числе прочих первоочередных мер необходимо выделить ресурсы и время на организацию процесса мониторинга. Системный мониторинг состоит из нескольких уровней. В этой статье рассматриваются основные инструменты, используемые в рамках этого процесса.

На верхнем уровне мониторинга осуществляется контроль внедрения в СЭД новых процессов. Допустим, на старте проекта определены ключевые показатели: какие задачи предстоит решать, сколько пользователей будет работать и сколько документов создаваться за год. Исходя из этого, выбирается определенное оборудование, в котором, с учетом возможного расширения системы, предусматривается определенный «запас» производительности на случай непредвиденной загрузки.

Дальнейшее развитие СЭД потребует мониторинга нагрузки на оборудование. Контроль за производительностью позволит определить, способно ли имеющееся «железо» поддерживать новые процессы. Если показатели загрузки приближаются к 60–80%, то без обновления оборудования автоматизировать новые задачи

будет крайне сложно, так как возникает риск неработоспособности уже внедренных процессов и остановки системы.

В идеале такой сценарий развития событий следует принять во внимание еще на нулевом этапе внедрения и реализации системы. Нагрузку на оборудование рекомендуется указывать в плане внедрения новых процессов на 1–3–5 лет (или аналогичном документе).

На следующем уровне системного мониторинга необходимо отслеживать текущие процессы:

- загрузку оборудования;
- длительность выполнения операций пользователями, поскольку этот показатель не всегда коррелирует с загрузкой оборудования (например, нагрузка на SQL-сервер может быть низкой, но работа пользователей затруднена вследствие длительных задержек из-за проблем с каналами или конкретной рабочей станцией);
- динамику инцидентов.

Рассмотрим каждый из них более подробно и определим оптимальную периодичность и необходимые инструменты мониторинга.

## КОНТРОЛЬ ЗАГРУЗКИ ОБОРУДОВАНИЯ

Если СЭД имеет клиент-серверную архитектуру, как, например, система DIRECTUM, то речь идет об отслеживании только уровня загрузки серверной части системы. Контроль загрузки оборудования на клиентских местах администраторы осуществляют локально.

Ключевое значение для достижения требуемой производительности имеет SQL-сервер. Основными контролируемыми показателями при мониторинге являются следующие:

- Нагрузка на ЦПУ. Согласно рекомендациям Microsoft, значение этого показателя не должно превышать 80%. Если же постоянная нагрузка составляет 60–80%, необходимо либо оптимизировать процессы, либо менять оборудование.
- Нагрузка на диски (IOPS). Microsoft рекомендует в качестве идеальных показателей отсутствие очереди на дисках и отработку запроса к диску не более чем за 25 мс. В конечном итоге от времени выполнения запроса зависит длительность осуществления операции с точки зрения пользователя.

- Блокировки запросов. Они тоже оказывают влияние на длительность выполнения операций у пользователей.
- Кеш планов запросов.
- Время нахождения страницы в оперативной памяти.

Другие показатели уже не так явно сказываются на длительности выполнения операций и не так быстро изменяются, поэтому их можно анализировать реже.

При организации мониторинга серверной части нельзя забывать о «слоне» — о работоспособности сервисных служб. Если обратиться к примеру DIRECTUM, то в этой системе используется множество подобных служб: сервис интеграции (DISI), сервис захвата и преобразования (DCTS), workflow, сервер сеансов. SQL-сервер в данном контексте тоже является службой. Рекомендуется отслеживать работу всех имеющихся служб.

Какие инструменты используются:

- SCOM, Zabbix или аналоги;
- счетчики Windows Server для контроля показателей сервера за длительный период и отслеживания их динамики;
- инструменты SQL-сервера;
- инструменты центра администрирования DIRECTUM для мониторинга служб.

Периодичность контроля:

- Нагрузку на диски и процессор желательно отслеживать постоянно. С помощью SCOM можно настроить предельные значения, при достижении которых администратор получит оповещение.
- Общий контроль работоспособности служб на уровне системы тоже осуществляется постоянно — с помощью оповещений SCOM. В ходе мониторинга на основе эмпирических данных для каждого сервера устанавливается максимально допустимая нагрузка за единицу времени. Исходя из этого, вычисляется граница, при достижении которой потребуется принимать какие-либо меры. Если нагрузка долго держится на предельном уровне, команда сопровождения должна рассмотреть возможность замены оборудования.
- Динамику изменения нагрузки на серверную часть необходимо фиксировать один раз в месяц и один раз в квартал. Для выявления причин отклонения следует установить, что изменилось внутри системы: количество поддерживаемых пользователей, интенсивность их работы, внедрение новых решений.

Накапливая и анализируя такую информацию, можно заранее прогнозировать, какие последствия будут иметь те или иные изменения.

### КОНТРОЛЬ ДЛИТЕЛЬНОСТИ ОПЕРАЦИЙ

В системе выполняется множество операций: сохранение карточек документов, отправка задач, формирование отчетов, открытие записей справочников и т. д. На этапе формирования требований определяется типовая длительность выполнения каждой операции, которая затем контролируется. Этот показатель важен для команды сопровождения, так как от него зависит общее впечатление пользователя о системе наравне с удобством интерфейса.

**Инструменты мониторинга.** Мониторинг осуществляется при помощи средств пользовательского профилирования (профайлинга), а также (частично) журнальных файлов системы, где фиксируется время выполнения конкретных операций. Затем информация по всем пользователям агрегируется и анализируется.

### Классификация информации и анализ.

В крупных компаниях накапливается большой объем данных, что позволяет делать репрезентативные прогнозы на основе средних значений. Поэтому в первую очередь следует выделить однотипные операции и вычислить среднее значение. Это позволяет сделать вывод о том, насколько удовлетворительно работает система при выполнении тех или иных операций, и понять, как повлияли изменения конкретного процесса на его среднюю продолжительность.

Затем составляется список самых длительных операций — первых кандидатов на оптимизацию. Далее выявляются пользователи, у которых система работает медленней, чем у других. Работу конкретного пользователя могут затруднять внешние помехи, слабый ПК, вирусы, плохо настроенная сеть. В любом случае профайлинг поможет решать такие проблемы проактивно и устранять их еще до поступления жалоб в службу поддержки.

Помимо классификации по видам операций, необходима классификация групп пользователей по бизнес-ролям. К примеру, делопроизводители преимущественно работают со справочниками и документами, а руководители — с задачами.

От особенностей работы пользователя зависит, какие операции будут наиболее критичными для выполнения его роли в системе — их следует контролировать в первую очередь.

Кроме того, можно выделить группы пользователей, которые часто выполняют одну и ту же операцию. Это позволяет определить приоритеты для оптимизации. Помимо этого, отслеживание длительности операций по бизнес-ролям помогает выявить ситуацию, когда конечный пользователь работает с системой не так, как рекомендовано. Это может стать поводом для обучения его оптимальному способу выполнения той или иной операции.

В профайлинге, кроме прочего, содержится информация о работе служб DIRECTUM. Фиксация отклонений от рекомендуемой длительности выполнения операций поможет выявить ошибки в прикладной разработке и улучшить функционирование службы.

**Периодичность контроля.** В случае профайлинга речь идет об обработке очень большого объема информации, поэтому постоянный мониторинг невозможен. В связи с этим рекомендуется один раз в неделю анализировать список длительных операций, ежемесячно осуществлять полный профайлинг по всем перечисленным срезам и ежеквартально отслеживать динамику.

### КОНТРОЛЬ ДИНАМИКИ ИНЦИДЕНТОВ

В случае возникновения инцидентов мониторинг осуществляется по нескольким направлениям. В первую очередь следует проанализировать журнальные файлы системы. Собирать их надо централизованно и затем обрабатывать с помощью автоматических инструментов.

Некоторые ошибки фиксируются в журналах в фоновом режиме и не требуют каких-то действий со стороны пользователя, но влияют на длительность выполнения операций. Задача состоит в том, чтобы отслеживать те ошибки, которые возникают достаточно часто и могут критичным образом повлиять на работу системы. В случае разовых ошибок, происходящих примерно в одно и то же время у большого количества пользователей, необходимо вмешательство

команды сопровождения. Это же касается большого количества однотипных ошибок, появляющихся в течение короткого промежутка времени. Кроме того, стоит контролировать объем файлов с журналами — как правило, его заметное увеличение указывает на наличие какой-то проблемы.

На этапе сопровождения системы в службу Service Desk поступают обращения пользователей. Их можно классифицировать следующим образом:

- Обращения, связанные с длительностью операций. Эта информация анализируется вместе с результатами профайлинга.
- Непосредственно инциденты. В этом случае вычисляются средние значения их частоты (количество за день), которые сравниваются с целевым показателем. Если в ходе развития СЭД отмечается рост числа инцидентов по одному компоненту или бизнес-процессу, значит, последние доработки могли оказать негативное влияние и нужно оптимизировать работу системы.

Проанализировав характер обращений, можно выделить проблемные компоненты и «проблемных» пользователей, а также объединить инциденты по месту возникновения (отдел, филиал, здание). Имея такую информацию, проще выявить первоисточник проблем, который не всегда очевиден при реактивной работе с обращениями. Пользователи могут столкнуться с одной и той же ошибкой при выполнении разных операций и по-разному их описать. Классификация даст возможность разрешить тысячу инцидентов у тысячи пользователей путем устранения общей для них проблемы.

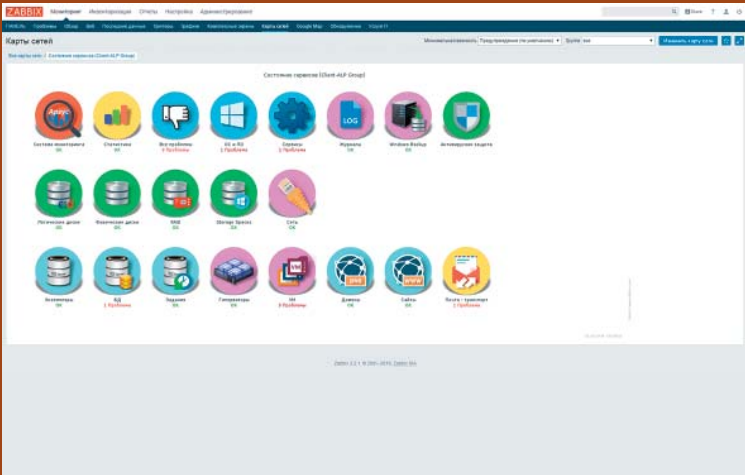
\* \* \*

Итак, существуют два подхода к поддержке и сопровождению системы. Возникшие проблемы можно решать по мере поступления (реактивно) или предсказывать и предупреждать их с помощью описанных инструментов (проактивно). Второй подход позволит уменьшить количество нештатных ситуаций, накопить исторические данные и спрогнозировать, как будет вести себя система при тех или иных изменениях. Проактивный подход более эффективен в долгосрочной перспективе и может быть реализован с помощью доступных средств. Наш опыт работы с крупными компаниями целиком это подтверждает. **LAN**

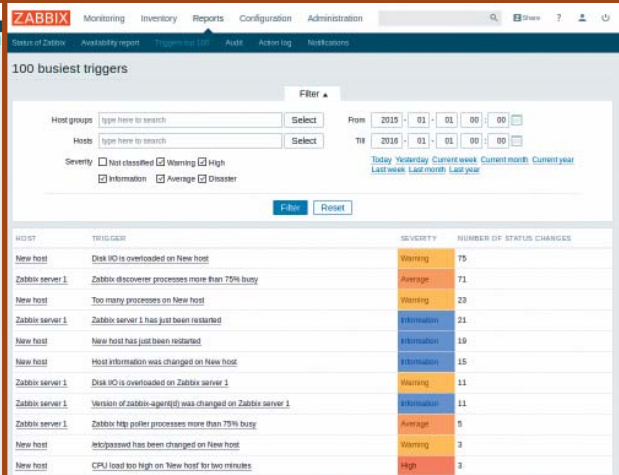
# Проблемы стандартного и выгоды нестандартного мониторинга здоровья ИТ-инфраструктуры

Традиционный подход к мониторингу ИТ-инфраструктуры не соответствует ее сложности, изменчивости и степени влияния на работу всей организации. Это ставит под угрозу все уровни поддержки ИТ-инфраструктуры: от планирования до оперативного обслуживания. Зачастую компании начинают реагировать на такое несоответствие только в том случае, когда оно приводит к крайне болезненным последствиям. Что можно сделать уже сегодня, чтобы эти проблемы остались в прошлом?

**Павел Рыцев,**  
ИТ-директор, руководитель Центра компетенции  
по импортозамещению и Open Source в ALP Group



Интерфейс сервиса централизованного мониторинга и контроля



Отчет о триггерах ИТ-инцидентов в Zabbix



Качественная поддержка современной ИТ-инфраструктуры — многоплановый процесс, сложный для любой средней и уж тем более крупной компании. На этом пути необходимо преодолеть немало препятствий, чтобы достичь стабильно высоких результатов, но получается это далеко не у всех. Среди многих проблем выделяется одна — отсутствие целостного подхода к мониторингу ИТ-инфраструктуры. А между тем на основе такого подхода выстраивается вся система реагирования на инциденты и их предотвращения.

С этой проблемой постоянно сталкиваются большинство компаний независимо от их размера и сферы деятельности. Причем ее важность и даже наличие не всегда осознаются, поэтому борьба идет со следствиями, а не с причиной. Результат — нестабильность и низкое качество работы не только самой ИТ-инфраструктуры, но и ИС в целом. Более того, под угрозой оказываются основная деятельность, финансовое положение и репутация организации. К счастью, сегодня проблему можно не только идентифицировать, но и эффективно решить. Этому и посвящен данный материал.

Традиционный подход к мониторингу ИТ-инфраструктуры не соответствует ее сложности, изменчивости и степени влияния на работу всей организации. Это ставит под угрозу все уровни поддержки ИТ-инфраструктуры: от планирования (ошибки при выделении необходимых ресурсов, неадекватные затраты на отдельные сервисы и т. д.) до оперативной деятельности (долгое выяснение причин инцидентов и их неверная классификация, снижение уровня доступности сервисов, устранение последствий вместо определения причин, отсутствие проактивности).

Зачастую на сложившееся несоответствие начинают реагировать, когда оно уже принимает крайне болезненные формы, но даже в этом случае мало кто пытается решить проблему кардинально! Почему? И что можно сделать уже сегодня, чтобы все это осталось в прошлом? Ниже я постараюсь ответить на эти вопросы. Но сначала давайте разберемся, какие именно устаревшие идеи (стереотипы) не дают реализовать потенциал технологий мониторинга.

## ЧЕТЫРЕ СТЕРЕОТИПА ОТНОСИТЕЛЬНО МОНИТОРИНГА

*Мониторинг ИТ-инфраструктуры воспринимается как побочный, а не основной процесс.* Он не продумывается и не планируется стратегически. В лучшем случае этот тонкий инструмент служит только для «латания дыр», причем исключительно на оперативном уровне (в итоге сложные или трудноопределимые ИТ-проблемы будут повторяться). Между тем система мониторинга способна предоставить достаточно точных и актуальных данных, чтобы можно было проактивно выявлять проблемы, дорого обходящиеся бизнесу, и предотвращать их.

Но даже если данные собираются в нужном объеме, их необходимо своевременно обрабатывать и анализировать. А этого как раз и не происходит. Загвоздка состоит в том, что развитие мониторинга ИТ — почти всегда непрофильный и дополнительный для владельца компании процесс, который обычно никак не планируется и не развивается. В результате система мониторинга устанавливается, но не дорабатывается и совсем не улучшается. А это не тот инструмент, который можно оставить без внимания.

*Мониторинг ИТ-инфраструктуры затрагивает только технический контур.* Поэтому обычно имеется лишь возможность оповещать ИТ-персонал об уже случившихся проблемах по почте или SMS, а также получать скудные статистические данные о нагрузке на оборудование и об использовании вычислительных ресурсов. Но даже эти потенциально ценные сведения, скорее всего, будут лежать мертвым грузом — ниже будет показано, почему.

*Не хватает компетенций и экспертизы для правильной интерпретации собираемых данных.* Даже внедрив довольно развитую и недорогую систему мониторинга (от HP, IBM или Microsoft), можно не получить желаемого результата из-за недостатка квалификации персонала. За аксиому принимается утверждение, что для работы с такими системами особых компетенций не требуется, но это

в корне неверно. Нужно иметь специфический опыт, чтобы не просто «выхватывать» самые очевидные проблемы «верхнего уровня», а уметь выявлять их еще на этапе зарождения и своевременно предотвращать, пока они еще не повлияли на работу критичных бизнес-сервисов и не обернулись дорогостоящими (и постоянно повторяющимися!) сбоями и простоями, вводящими в ступор и ИТ-службу, и бизнес-подразделения.

*В ИТ-службе, занятой одновременно и мониторингом, и устранением инцидентов и проблем, неизбежно наблюдается конфликт интересов.* Такое положение дел складывается, когда за проведение мониторинга, выдачу рекомендаций и коррекцию ситуации отвечают одни и те же специалисты. Например, если ИТ-специалист должен гарантировать доступность CRM в течение 95% времени, то оповещение о проблеме «портит» ему статистику.

**Традиционный подход к мониторингу ИТ-инфраструктуры не соответствует ее сложности, изменчивости и степени влияния на работу всей организации. Это ставит под угрозу все уровни поддержки ИТ-инфраструктуры.**

В итоге оповещение просто не регистрируют в системе, хотя проблему, возможно, устранят. Или более банальный, но не менее печальный пример: специалисту всего лишь «неохота» разбираться с обнаруженным инцидентом, особенно непродолжительным и не слишком заметным. Следовательно, ошибки будут повторяться и копиться, приводя к появлению слабых мест в инфраструктуре, а на их устранение будет требоваться все больше сил и средств.

Нештатные ситуации, возникающие в результате небрежности или влияния человеческого фактора, тоже зачастую остаются незарегистрированными. Все это может скрывать системные проблемы — причем не только в инфраструктуре, но и в самом процессе ИТ-поддержки (особенно в тех компаниях, где ИТ-служба вынуждена обслуживать большое число филиалов). Такие проблемы могут оставаться незамеченными до тех пор, пока мониторинг не станет окончательно бесполезным.

Эту ситуацию можно изменить путем внедрения не просто технической системы, а полноценного сервиса централизованного мониторинга и контроля (СЦМК).

## СЕРВИС ЦЕНТРАЛИЗОВАННОГО МОНИТОРИНГА И КОНТРОЛЯ

СЦМК — это сервис, состоящий не только из технического, но и из экспертного контура, то есть он подкрепляется регулярно пополняемой базой знаний из экспертного центра и мощной экспертизой выделенной многопрофильной команды. Специалисты последней непрерывно анализируют поток данных, предоставляемых средствами мониторинга, и могут заблаговременно предупредить о проблемах, предложив способы их решения. Так что же принципиально меняется в этой надоевшей всем схеме?

*Корпоративный заказчик получает готовый бизнес-процесс мониторинга и контроля состояния ИТ.* Этот процесс достаточно просто и быстро (подключение и автоматическая настройка занимают всего несколько часов) адаптируется в соответствии с потребностями конкретной организации. Инкорпорированная внутрь процесса технология обкатана на сотнях корпоративных клиентов. Более того, в процессе задействуется такой объем компетенций и экспертизы, которым даже крупная компания почти наверняка не располагает (нанимать и удерживать в штате специалистов такого уровня слишком дорого, поскольку в одной организации не реализуется столько релевантных для их уровня проектов).

*Начало сбора и накопления нужных данных не откладывается на неопределенный срок.* Заказчику не придется рассматривать и согласовывать отдельный бюджет на закупку лицензий, долго внедрять продукт, собирать и обучать специалистов, так как при создании СЦМК ставка делается на использование собственных наработок и компонентов, функционирующих на базе свободного ПО. Вся настройка уже автоматизирована, за нее отвечают выделенные ИТ-менеджеры и специалисты.

*Первые результаты можно получить уже через несколько дней или недель (многое зависит от масштаба компании, целей и задач бизнеса, а также от*

*текущего состояния инфраструктуры).* Большие затраты и неочевидные результаты просто исключены, причем независимо от того, подключается ли СЦМК время от времени (например, перед сезонными пиками продаж или для поддержки сложного и дорогого внедрения) или постоянно (для экономного регулярного ИТ-аудита инфраструктуры или части инфраструктуры, например региональной).

*Процесс мониторинга и контроля ИТ все время актуализируется.* Сервис автоматически и безошибочно обнаруживает новые объекты мониторинга. Он позволяет решить проблемы, которые только что проявились (вместе с внедрением новых ИТ-продуктов или угрозами ИБ), или закрыть те, которые решены и больше никогда не проявятся в инфраструктуре клиента.

*Заказчик получает возможность более объективно регистрировать не только ИТ-инциденты (мгновенный и правильный результат), но и — по мере накопления данных — любую информацию об узких местах в серверном ландшафте (отложенный, стратегический результат).* Кроме того, он получит всю информацию о самых проблемных ИТ-сервисах, на которые нужно обратить внимание в первую очередь. Все сведения собираются и объединяются опытными специалистами и экспертами, для которых эта деятельность является основной. Предложения, формируемые на основе полученной информации, позволяют более эффективно использовать имеющиеся средства и точнее планировать ИТ-бюджет.

*Вместе с СЦМК заказчик получает готовую базу лучших практик.* Несмотря на специфику, свойственную каждой компании, большинство имеющихся ИТ-сервисов построено на основе хорошо изученных и во многом стандартизированных решений, особенно если это типовые предложения вендоров или аутсорсеров, что позволяет консолидировать опыт, полученный при работе с разными организациями. В результате решение даже сложной, уникальной, с точки зрения клиента, проблемы окажется, скорее всего, уже глубоко проработанным. Иначе говоря, заказчик перестает быть «площадкой для экспериментов», он начинает пользоваться плодами опыта тех, кто подключил для него СЦМК —

неважно, на постоянной основе или временно.

*СЦМК ориентируется на недопущение проблем, а не на устранение уже возникших сбоев.* Особенно, если речь идет о сбоях и простоях, вызванных некачественными или устаревшими архитектурными решениями. Такой подход позволяет минимизировать потери благодаря раннему обнаружению и исправлению потенциальных недостатков и проблем разной степени критичности еще до того момента, когда они могли бы нанести урон бизнесу.

*СЦМК может быть не революционным, а дополнительным решением, поддерживающим и контролирующим работу внутренней ИТ-службы.* Например, такой подход выгоден фармацевтическим или торгово-розничным компаниям, то есть тем отраслям, где финансовая ответственность бизнеса крайне высока и действуют глобальные ограничения, делающие невозможной или болезненной смену модели ИТ-поддержки. Для таких предприятий чрезвычайно важны двойной контроль качества работы ИТ, отсутствие конфликта интересов, грамотная техническая и организационная экспертиза, широкий диапазон знаний (за счет возможностей сильного экспертного центра).

*СЦМК может стать временной страховкой для бизнеса.* Если, например, не устраивает работа внутренней ИТ-службы или поставщика внешних ИТ-услуг, очень полезной может оказаться возможность опереться на плечи команды экспертов, которая уже знает все об инфраструктуре компании и в любой момент способна прийти на помощь.

Таким образом, встраивание СЦМК в фундамент организационно-технической системы поддержки ИТ-инфраструктуры организации не только позволяет за сравнительно небольшие деньги решить указанные выше проблемы, но и дает дополнительные преимущества: качественный, хорошо спланированный и грамотно реализованный процесс по поиску, правильному определению, классификации, регистрации и решению ИТ-проблем; необходимые технические и экспертные инструменты, гарантирующие результат, причем без создания зачастую неэффективных внутренних механизмов мониторинга и контроля ИТ. **LAN**

# ИБП: тенденции и новинки

Общее улучшение экономической ситуации сказалось и на рынке ИБП, на котором намечается рост на фоне увеличения числа игроков и ужесточения конкуренции. В плане техники эксперты отмечают повышение интереса к модульным решениям, а также начало применения в ИБП литий-ионных аккумуляторов.

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





Большинство производителей сдержанны в своих ожиданиях относительно перспектив рынка на ближайший год. «Рынок уже адаптировался к новым экономическим условиям и изменившемуся курсу рубля, а клиенты постепенно возвращаются к отложенным ранее ИТ-проектам. Если в ближайшем будущем не произойдет никаких больших потрясений и сохранится текущая макроэкономическая ситуация, то по итогам 2017 года можно ожидать роста российского рынка ИБП примерно на 10–15%», — дает свой прогноз Алексей Бурочкин, директор по маркетингу компании Eaton.

«Исходя из данных о продажах ИБП в России в 2016 году, можно утверждать, что после трех лет падения рынка сформировалась тенденция к росту, — говорит Анатолий Маслов, технический эксперт Tripp Lite. — По нашим прогнозам, рынок ИБП продолжит расти и в 2017 году за счет вакуума продаж в 2013–2015 годах. Мы видим возвращение отложенного спроса: начинают выделяться бюджеты на модернизацию ИТ-инфраструктуры, реализуются старые проекты».

Надежды на рост рынка ИБП многие эксперты связывают с активным развитием отрасли ЦОДов, для которых критически важно качественное электропитание. «Рост потребности в энергоэффективных и высокопроизводительных центрах обработки данных обусловлен как органическим ростом потребностей бизнеса, так и недавними изменениями в российском законодательстве, — считает Алексей Бурочкин. — Эти изменения предполагают, в частности, обязательное хранение персональных данных россиян на территории РФ, а также создание сотовыми операторами и интернет-провайдерами архивов трафика абонентов за несколько месяцев на серверах, находящихся в России».

### УСИЛЕНИЕ КОНКУРЕНЦИИ

Конкуренция на российском рынке ИБП обостряется, в том числе за счет выхода на него новых игроков, причем не только из Китая и Юго-Восточной Азии. Так, в 2017 году свои источники бесперебойного питания представила чешская компания Conteg. Начиная с производства серверных шкафов, Conteg уже достаточно давно позиционирует себя в качестве поставщика комплексной инженерной инфраструктуры для ЦОДов. Однако до 2017 года в портфеле ее продукции был

один серьезный изъян — не хватало собственных ИБП. Теперь этот изъян ликвидирован.

«Время сейчас достаточно сложное, — комментирует ситуацию Дмитрий Куликов, менеджер по развитию бизнеса компании Conteg. — В условиях спада экономики и санкций строительство новых ЦОДов идет достаточно сдержанно, однако мы видим положительные тенденции в этом сегменте и уверены, что новые качественные ИБП по привлекательной цене будут положительно восприняты рынком и пользоваться хорошим спросом».

Ряд экспертов говорят о том, что заказчики все активнее рассматривают решения новых игроков. «На смену традиционным поставщикам приходят новые игроки, такие как Huawei и Legrand, которым уже удалось “отъесть” достаточно большой кусок рынка у лидеров», — считает Александр Веприцкий, главный технический пресейл-эксперт дистрибьюторского центра «Радистр». При этом он предупреждает, что, хотя та же Huawei заявила о себе достаточно громко и не намерена сбавлять темпов развития, только время покажет, насколько хорошо проявят себя ее ИБП, проработав хотя бы 5–7 лет.

Оценивая текущую ситуацию на рынке, Анатолий Маслов полагает, что «ИБП А-брендов [имеются в виду ведущие поставщики. — Прим. ред.] в текущей ситуации для многих заказчиков дороги, а китайские бренды еще не имеют стабильного качества и отлаженной сервисной поддержки». В этих условиях наиболее привлекательными для заказчиков становятся предложения компаний, сочетающие высокое качество оборудования с отличной сервисной поддержкой и приемлемой ценой.

### КОГДА НАДО БЫСТРЕЕ

Одна из серьезных проблем современного рынка ИБП, по мнению Анатолия Маслова, — предложение сырых решений: «Острая конкуренция не оставляет времени на долгую и кропотливую разработку ИБП, из-за чего страдает качество выпускаемой продукции». Как утверждает представитель Tripp Lite, дабы избавить заказчика от приобретения сырого продукта, эта компания тщательно тестирует и испытывает свои новинки в течение года с целью улучшения алгоритмов работы,

а также оптимизации и упрощения инсталляции и сервиса.

Традиционные процедуры реализации обновлений не подходят для современного динамичного рынка: проектирование, разработка, тестирование, сертификация — все это требует времени. Как отмечает Павел Пономарев, менеджер по развитию направления «Трехфазные ИБП» компании Schneider Electric, частично ускорить внесение изменений в продукты для реализации пожеланий заказчиков компании Schneider Electric удалось благодаря широкому внедрению систем автоматизированного тестирования при разработке ИБП.

### ОПТИМИЗАЦИЯ СТОИМОСТИ

Как полагает Мария Митюрёва, руководитель отдела маркетинга Delta Electronics, ключевой тенденцией в области ИБП на российском рынке в этом году будет стремление заказчиков просчитывать все возможные расходы по проекту наперед: «Они перейдут с подсчета операционных расходов (ОРЕХ) на расчет всей суммы операционных расходов и капитальных вложений по проекту (CAPEX) в целом. Это значит, что заказчики даже будут готовы вкладывать больше средств на начальном этапе, конечно, если эти вложения смогут окупиться в будущем».

Михаил Саликов, директор направления ЦОДов компании Huawei в России, указывает на стремление покупателей к оптимизации стоимости решений: «Если раньше многие заказчики практически не обращали внимания на стоимость устройств, приобретая их “с запасом на развитие”, то сейчас учитывается каждая копейка и во главу угла встают возможность расширения систем в будущем по мере необходимости и общая стоимость владения». В этих условиях растет интерес к модульным решениям, обеспечивающим возможность расширения «по запросу». По данным Михаила Саликова, этот интерес стимулируется еще и тем обстоятельством, что за последние годы стоимость модульных решений стала сопоставимой со стоимостью моноблочных устройств.

Тенденцию увеличения доли модульных ИБП отмечает целый ряд экспертов. «Многие заказчики оценили надежность и гибкость конфигурации таких систем, что позволяет подобрать идеальное решение для конкретных задач и избежать

переплаты», — говорит Артем Хохлов, продакт-менеджер компании Powerscom. «Если раньше модульные ИБП в основном предлагались в среднем сегменте мощностей, то теперь многие производители имеют мощные модульные системы, которые успешно применяются в крупных ЦОДах», — добавляет Анатолий Маслов. Он указывает на такие преимущества модульных систем (по сравнению с моноблочными), как снижение времени простоя при сбое (за счет быстрой замены модуля) и недорогая реализация резерви-

рования N+1 (за счет избыточного модуля во фрейме).

Другим проявлением тенденции к оптимизации стоимости является упрощение решений, на что указывают в компании Tripp Lite. «Если ранее заказчик делал серверную на базе выделенной комнаты с отдельным мощным трехфазным ИБП и с системой прецизионного кондиционирования, то сейчас он строит свой серверный кластер на базе стойки или нескольких стоек в общих помещениях

с бытовым или полупромышленным кондиционированием с использованием стоечных однофазных ИБП или сверхкомпактных трехфазных ИБП с ценником однофазного ИБП», — приводит пример Анатолий Маслов.

Как отмечает Василий Лапшин, заместитель генерального директора российского офиса Makelsan, ужесточение конкуренции приводит к снижению средневзвешенной стоимости ИБП на рынке. «Кроме того, государственный курс на

## Новинки ИБП малой мощности

### Eaton

Весной 2016 года Eaton представила новые ИБП 9PX мощностью 2,2 и 3 кВт. По мнению представителей компании, данные устройства идеально подходят для обеспечения высокого качества защиты электропитания малых и средних ЦОДов, хранилищ данных, сетевого и телекоммуникационного оборудования, а также объектов ИТ-инфраструктуры предприятий и медицинских учреждений.



Ключевая особенность 9PX — выходной коэффициент мощности, равный 1. КПД устройства составляет до 94% в режиме двойного преобразования и до 98% в высокоэффективном режиме. В ИБП реализована технология управления аккумуляторными батареями АВМ с уникальным трехступенчатым алгоритмом заряда, продлевающим срок службы батарей на 50%.

### Delta

Среди новинок прошлого года можно выделить однофазный ИБП малой мощности семейства Ampron серии RT мощностью 1–3 кВА. К этому ИБП с двойным преобразованием можно подключать ПК, серверы и телекоммуникационную аппаратуру. Модель имеет компактную архитектуру и отличается высоким коэффициентом мощности на выходе (0,9). КПД устройства равно 94%, что является одним из лучших показателей для таких ИБП. К ИБП можно подключать дополнительные внешние батарейные модули для повышения продолжительности работы от резервного питания.

Кроме того, в 2016 году вышла обновленная версия ИБП семейства Ampron серии N на 1–3 кВА. Эти компактные ИБП с двойным преобразованием могут быть использованы для снабжения бесперебойным электропитанием рабочих

станций, PoS-терминалов, банкоматов. Система обеспечивает стабильную подачу напряжения синусоидальной формы и обладает выходным коэффициентом мощности 0,9. Жидкокристаллический дисплей значительно облегчает управление устройством.

Кроме того, компанией был представлен обновленный линейно-интерактивный ИБП семейства Agilon серии VX с микропроцессорным контроллером. Он призван обеспечить защиту электропитания ПК, мониторов или, например, кассовых терминалов. Отличительной чертой этой модели стало наличие ЖК-дисплея, благодаря которому, как и в новой модели N, значительно упростился процесс самостоятельной настройки и управления системой.

### IPPON

В середине 2016 года была представлена первая модель самых бюджетных ИБП IPPON серии Back Basic — IPPON Back Basic 650. По состоянию на апрель 2017 года в линейку входят шесть моделей, три из которых имеют стандартный компьютерный разъем (для одновременного подключения и защиты до трех устройств) и три оснащены евророзетками (для одновременного подключения и защиты двух устройств).

Как отмечают в компании, серия Back Basic уже пользуется успехом и у домашних пользователей, и у корпоративных заказчиков.

IPPON не забывает и об обновлении популярной серии линейно-интерактивных ИБП Comfo. В скором времени в этой серии должна появиться новая модель мощностью 1 кВА.



импортозамещение подталкивает поставщиков к попыткам переноса сборочных производств на территорию нашей страны, что, возможно, приведет в будущем к появлению собственных ИБП, полностью разрабатываемых и производимых в России», — говорит он.

### СМЕЩЕНИЕ АКЦЕНТОВ

По мнению Артема Хохлова, на российском рынке прослеживаются две основные тенденции, которые с перво-

го взгляда могут показаться взаимоисключающими. Первая — это рост продаж дешевых резервных (off-line) ИБП и самых базовых моделей линейно-интерактивных устройств. Это можно объяснить последствиями колебаний валютного курса и кризиса в целом, что привело к желанию многих компаний максимально уменьшить издержки на ИТ-инфраструктуру. Вторая — рост продаж ИБП с двойным преобразованием. «Онлайн-ИБП до 3 кВА все чаще устанавливаются вместо аналогичных линейно-

интерактивных устройств, что объясняется сокращающимся ценовым различием между этими двумя технологиями, тем более что первые обеспечивают более качественное и надежное электропитание», — отмечает эксперт Powercom.

А вот Владимир Русаков, директор по продажам IPPON, видит тенденцию смещения потребительского спроса в пользу корпоративных решений. Не случайно компания, будучи одним из лидеров сегмента массовых ИБП на российском рынке, в 2015

### Schneider Electric

В компании Schneider Electric выделяют две новинки, относящиеся к категории ИБП малой мощности: BC750-RS и SMT2200RMI2UNC. Первая относится к семейству ИБП APC Back-UPS, имеет мощность 750 ВА и оснащена розетками Schuko. Продукт пришел на смену BC650-RS. Его главное преимущество, по словам Святогора Гавриленко, менеджера по работе с розничными партнерами подразделения IT Division компании Schneider Electric, — увеличение мощности по сравнению с предыдущей моделью при сохранении цены.



SMT2200RMI2UNC — дополнительный вариант исполнения основной модели (SMT2200RMI2U). Этот ИБП семейства Smart-UPS с ЖК-экраном в стоечном шасси высотой 2U имеет мощность 2200 ВА. Нововведение — встроенная плата сетевого управления (AP9631) для удаленного управления. Устройство обеспечивает мониторинг окружающей среды. «Эта новинка — ответ на запрос рынка, нуждающегося в надежных стоечных ИБП с возможностью удаленного управления», — отмечает Святогор Гавриленко.

### Powercom

В 2016 году в категории ИБП малой мощности Powercom представила устройства INFINITY-500/800/1100/1500. ИБП серии INFINITY не содержат в своем составе внутренних АКБ, но позволяют подключать внешние АКБ большой емкости на 12 В (500, 800) или 24 В (1100, 1500) для обеспечения длительного времени автономной работы. Данные ИБП выдают выходное напряжение в виде чистой синусоиды, что позволяет им обеспечивать бесперебойным электроснабжением такое оборудование, как котлы отопления, насосы водоснабжения и другие устройства, предъявляющие высокие требования к качеству электропитания.



В 2017 году планируется выпуск новой линейки ИБП с двойным преобразованием мощностью до 3 кВт — устройств серии MRT, выполненных в форм-факторе Rack/Tower и оснащенных обновленным поворотным LCD-дисплеем. Отличительной особенностью

данной серии станет коэффициент мощности, равный 1. Впоследствии планируется расширение данной линейки до 10 кВА.

### Tripp Lite

Компания выпустила новые однофазные ИБП двойного преобразования малой мощности серии SmartOnline — модели SUINT1000 (2000, 3000) XLCD. Эти ИБП настольного и настольного размещения подходят для защиты мощных расчетных и графических компьютеров и серверов, ответственного исследовательского и лабораторного оборудования (расположенного там, где нет 19-дюймовой стойки для размещения).



Для защиты серверного оборудования и размещения в 19-дюймовой стойке компания предлагает полностью обновленную в 2016 году линейку стоечных ИБП малой мощности серии SmartOnline — модели SUINT1000 (1500, 2200, 3000LCD2U). Все обновленные модели имеют улучшенные технические характеристики и подходят для защиты всех типов современного серверного и сетевого оборудования.



году взяла курс на «утяжеление» своих продуктов. Так, в 2017 году она выпустила следующие новинки: трехфазные онлайн-новые ИБП серии Innova RT Tower 3/1 10 и 20 кВА.

Корпоративные решения — это в первую очередь системы с двойным преобразованием энергии, рост спроса на которые отмечают в компании «Связь инжиниринг». «Это связано с повышением требований к оборудованию по качеству

электропитания, а также с постепенной заменой персональных моделей ИБП для компьютеров на системы для централизованной защиты электропитания всего офиса или серверной. Такое решение при более высоких качественных характеристиках надежнее и удобнее в обслуживании, а его система управления может интегрироваться в корпоративную среду заказчика», — говорит Алексей Морозов, руководитель направления «Маркетинг» этого отечественного производителя.

Эксперт компании «Радистр» отмечает «отраслевую ориентацию» предлагаемых на рынке ИБП. Так, по его мнению, ИБП Huawei изначально были разработаны для защиты ИТ-оборудования в ЦОДах и серверных помещениях, но они не являются оптимальным выбором для защиты медицинской аппаратуры или оборудования, установленного на промышленных предприятиях. Для таких применений лучше поискать специализированные ИБП. Например,

## Новинки ИБП большой мощности

### Conteg

В этом году Conteg вышла на рынок ИБП, представив продукты Miracle M3. Эта модульная система бесперебойного питания с общей максимальной мощностью 1,2 МВт специально создана для применения в ЦОДах и призвана обеспечить гарантированную защиту современного ИТ- и технологического оборудования. Благодаря применению самых современных технологий данные ИБП объединяют в себе все плюсы распределенной логики управления и предусматривают масштабирование от 30 до 300 кВт (в одном устройстве) с возможностью резервирования N+1.



Как утверждают в Conteg, сочетающие в себе возможности по организации батарейной поддержки и гибкости системы распределения электропитания ИБП Miracle M3 обладают универсальным конструктивом, который с легкостью адаптируется к требуемой инженерной инфраструктуре

заказчика. Miracle M3 полностью совместимы с решениями Conteg по кондиционированию, оптимизации воздушных потоков и организации кабельной проводки. Они выполнены в едином дизайне с серверными шкафами Conteg RSF и внутрирядными кондиционерами CoolTeg.

Conteg планирует расширять портфель ИБП. В частности, уже сейчас идут работы над ИБП с силовыми модулями мощностью 50 кВА. Как считают в компании, данные разработки позволят удовлетворить потребности клиентов в ИБП большой мощности для крупных ЦОДов.

### Eaton

Представители Eaton выделяют устройство 9PHD для защиты электропитания в сложных и экстремальных условиях экс-

плуатации с диапазоном мощности 30–200 кВт, которое совсем недавно было впервые представлено российскому рынку. Его высокотехнологичная модульная конструкция обеспечивает высокий КПД (97% в режиме двойного преобразования и свыше 99% в режиме экономии электроэнергии), а также простоту ввода в эксплуатацию. Новое устройство оснащено несколькими интеллектуальными технологиями для обеспечения максимальной надежности функционирования. ИБП комплектуется датчиками параметров окружающей среды для дистанционного мониторинга температуры и влажности, защищенным сенсорным ЖК-дисплеем, специальными воздушными фильтрами, а также резервными управляемыми вентиляторами охлаждения для каждого силового модуля.



### Delta

Среди новинок Delta Electronics — модульные ИБП серии DPH мощностью 500 кВА, обеспечивающие одну из самых высоких плотностей мощности (55 кВА на один модуль 3U). КПД новинки — 96,5% для преобразования AC-AC, а в экономичном режиме этот показатель доходит до 99%.

Кроме того, в компании выделяют новые ИБП серии DPS мощностью от 600 кВА до 1,2 МВА, которые также обеспечивают высокую плотность мощности (600 кВА/м²). Эти ИБП предназначены для



специально для промышленности предназначен ИБП Gutor компании Schneider Electric.

### МЕНЬШЕ МЕСТА, БОЛЬШЕ МОЩНОСТЬ

Сегодня заказчики все больше обращают внимание на решения, с помощью которых удастся оптимизировать использование площадей ЦОДов благодаря значительной плотности мощности ИБП.

Даже несмотря на то, что уже сложно еще больше увеличить плотность мощности ИБП, как считает Михаил Саликов из Huawei, работы в этом направлении будут продолжаться. Еще одно важное направление усилий разработчиков — увеличение надежности устройств. «Уже сейчас ИБП Huawei сложно вывести из строя даже намеренно, — утверждает он. — Вероятность же отказа в результате выхода из строя каких-либо элементов устройства минимальна, так как все

ключевые элементы ИБП дублированы и имеют функцию горячей замены».

Все больше внимания российские заказчики уделяют энергоэффективности приобретаемых технических решений. «Все меньшим спросом пользуются решения с КПД ниже 96%, ведь каждый процент КПД в будущем влечет за собой экономию по проекту, — отмечает Мария Митюрёва. — Даже увеличение общего КПД системы на 1% (с 95 до 96%) может

крупных ЦОДов и позволяют значительно сократить площадь, занимаемую системой бесперебойного электропитания. Коэффициент выходной мощности этих систем равен 1, а КПД достигает значения 96,5%.

### Huawei

В 2016 году компания Huawei представила новые серии модульных ИБП Huawei UPS5000E со встроенными батареями. Как отмечают эксперты компании, такие решения весьма популярны среди заказчиков, поскольку позволяют не только существенно экономить место, необходимое для размещения ИБП и батарей, но также обслуживать и заменять батареи в режиме реального времени.

Изменения не обошли стороной и традиционную линейку модульных ИБП Huawei UPS5000E. Помимо системы беспроводного мониторинга батарей, доступной в этой серии ИБП, они также получили силовые модули 50 кВА. При этом габаритные размеры и стоимость модулей не изменились. «Для наших заказчиков это значит, что за те же деньги они могут получить большую мощность, а в некоторых случаях и сэкономить место в ЦОДе для размещения дополнительных стоек с ИТ-оборудованием», — отмечает Михаил Саликов, директор направления ЦОДов компании Huawei в России.

Еще одна новинка Huawei — UPS5000S с КПД, достигающим 97,5%. Следует обратить внимание на то, что такая высокая эффективность достигается уже при нагрузке около 40%, с которой обычно работают большинство ИБП. «Заказчики, которым необходимо обеспечить бесперебойным питанием большие нагрузки, очень быстро заметят экономию на оплате электроэнергии, которую они могут получить за счет новых источников бесперебойного питания, — рассказывает Михаил Саликов. — Так, в одном из проектов, в соответствии с представленными заказчиком данными, после замены старого ИБП на новый, Huawei UPS5000S, он окупится в течение четырех лет исключительно за счет разницы в ежемесячно потребляемой электроэнергии».

### IPPON

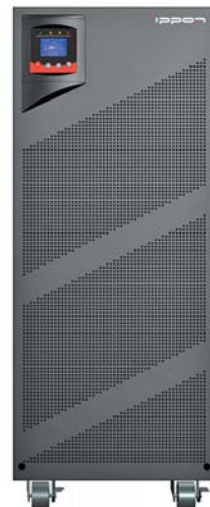
IPPON на протяжении многих лет является одним из лидеров сегмента массовых ИБП российского рынка ИБП. Однако планы развития компании связаны не только с массовыми

моделями — она продолжает придерживаться взятого в 2015 году курса на «утяжеление» решений (тогда вышли онлайн-ИБП IPPON Innova RT 6/10 KVA). В апреле 2017 года на российском рынке представлены трехфазные онлайн-ИБП Innova RT Tower 3/1 10 и 20 кВА для надежной защиты сложного и дорогостоящего оборудования. «В связи с этим компания расширила компетенцию своих технических центров и готова предоставлять полный спектр услуг по установке и техническому обслуживанию тяжелых решений IPPON», — отмечает Владимир Русаков, директор по продажам IPPON.

### Makelsan

В 2016 году модельный ряд Makelsan остался без глобальных изменений в техническом плане. Но при этом в компании отмечают расширение мощностного ряда серии LevelUPS до 800 кВА. Это самая «продвинутая» с технической точки зрения серия, оснащаемая выпрямителями и инверторами на IGBT с трехуровневым преобразованием. Она характеризуется КПД до 96% и высоким выходным коэффициентом мощности. Данная серия способна работать в режиме рекуперации энергии в сеть.

Кроме этого, модернизирован дизайн корпусов ИБП Boxer и LevelUPS — теперь можно заказать устройства в опциональном корпусе со встроенным выходным трансформатором гальванической изоляции. Производитель изменил цветовое оформление ИБП, теперь оборудование штатно поставляется в ярко-оранжевом исполнении, под заказ доступны любые другие цвета.



позволить в перспективе сэкономить десятки тысяч долларов».

Важная тенденция повышения эффективности ИБП — переход на использование литий-ионных аккумуляторов. Пионером здесь выступила компания Schneider Electric, которая готова предлагать такие аккумуляторы для основных моделей ИБП большой мощности: Symmetra PX, Galaxy 7000, Galaxy VM, Galaxy VX. «Мы с 2011 года проводили исследования и внедрения подобных решений, что позволило накопить солидный опыт и вывести на рынок отработанный продукт, — рассказывает Павел Пономарев. — Это решение в корне

отличается от батарей, которые используются в смартфонах и ноутбуках: начиная от технологии и длительности разработки и тестирования, заканчивая архитектурой самих ячеек и их системой мониторинга».

Предлагаемый Schneider Electric батарейный шкаф площадью менее 0,4 м<sup>2</sup> может поддерживать автономную работу в течение 10 мин нагрузки мощностью 180 кВт, имея при этом вес 550 кг. Идентичное по времени автономной работы традиционное решение (свинцово-кислотные АКБ) занимало бы вдвое большую площадь и имело бы вдвое больший вес. «Возможность быстрой перезарядки,

поблочный мониторинг множества параметров батарей с их балансировкой, количество циклов заряда-разряда, измеряющееся тысячами, — все это позволяет нам говорить о сроке службы подобных систем в 15 лет», — добавляет специалист Schneider Electric.

### ОТ КОРОБОК К РЕШЕНИЯМ

Важным требованием со стороны покупателей Мария Митюрёва называет расширение возможностей самостоятельной работы с системой: «Заказчики хотят самостоятельно проводить определенные операции с системой (изменять величину

## Новинки ИБП большой мощности



### Schneider Electric

Специалисты компании выделяют несколько новинок в области ИБП большой мощности. Одна из них — ИБП для промышленного применения Gutor PXC. «ИБП Gutor известны, в том числе в России, благодаря своей надежности — они применяются в АСУТП промышленных предприятий, для питания систем противоаварийной защиты и иных критичных нагрузок заводов, — рассказывает Павел Пономарев, менеджер по развитию направления «Трёхфазные ИБП» компании Schneider Electric, — эта линейка традиционно разрабатывалась на заказ для конкретных проектов, что влияло на срок поставки. Мы взяли все лучшее из решений популярного сегмента мощностей 10–80 кВА и выпустили ИБП Gutor PXC, который конфигурируется на заказ из готовых блоков, что удобнее и быстрее».



ИБП Gutor PXC имеют срок службы 15–20 лет, выполнены в форм-факторе Sarel, сейсмостойки, могут работать при температуре до +40°C, причем даже при столь высокой температуре имеют многолетний межсервисный интервал. Внутренняя архитектура ИБП построена по модульному принципу, что минимизирует время восстановления, а возможность дополнительной комплектации различными трансформаторами (до трех штук, часть может быть встроена внутрь корпуса) позволяет создавать решения, наиболее востребованные в промышленности.

Другая новинка — выпущенный в начале 2017 года ИБП Galaxy VX мощностью до 1500 кВт. Этот ИБП построен с использованием технологий, отлично себя зарекомендовавших в ИБП Galaxy VM: это блочно-модульная архитектура с делением ИБП на силовую часть и блоки ввода-вывода (куда подводятся все кабели); четырехуровневый инвертор, в несколько раз снижающий вероятность отказов полупроводниковых компонентов; мощное зарядное устройство, позволяющее до 40% от номинала мощности ИБП использовать на зарядку батарей. Для пользователя также важным является энергоэффективность в широком диапазоне нагрузок, включая наличие эффективного режима есconversion. Использование этого режима позволяет, с одной стороны, работать с КПД до 99%, а с другой — заряжать батареи, корректировать коэффициент мощности ИБП по входу и без пауз переключаться на двойное преобразование в случае проблем во внешней сети электропитания.

### Powercom

В категории ИБП большой мощности компания представила в 2016 году продукты ONL-M. Они выпускаются в двух форм-факторах (42U и 30U) и поставляются как с внешними батарейными шкафами, так и с внутренними, что позволяет соз-





выходного напряжения, просматривать время автономной работы и т. п.), не прибегая к помощи партнеров или вендоров». Это удобно делать через LCD-дисплей, поэтому даже в случае однофазных ИБП небольшой мощности пользователи отдадут предпочтение решениям, оснащенным таким дисплеем.

Одной из наиболее актуальных тенденций на рынке ИБП в компании Eaton считают переориентацию вендоров на комплексный подход при обслуживании клиентов. «Это означает, что теперь заказчик получает не только максимально широкий ассортимент продукции, охватывающий

весь спектр задач в рамках того или иного проекта, но и приобретает гарантию и сервисное обслуживание, учитывающее полный жизненный цикл оборудования», — поясняет Алексей Бурочкин. Кроме того, он отмечает курс на рост интеллектуальности ИБП, что позволяет повысить качество управления ИТ-инфраструктурой, улучшить энергоэффективность и избежать нештатных ситуаций.

Михаил Саликов из Huawei вообще считает основной тенденцией то, что все больше заказчиков заинтересованы в покупке не какого-то конкретного устройства, а полноценного решения по организации

питания, включая различные уровни сервиса и постгарантийной поддержки. «Не исключено, что в ближайшем будущем мы все чаще и чаще сможем видеть на рынке предложения вида “бесперебойное питание как сервис”», — считает он.

Большая доля государственных закупок в России серьезно тормозит внедрение новых технологий бесперебойного электропитания. Тем не менее модульные конструкции, литий-ионные батареи, «продвинутые» средства управления и комплексные предложения будут пользоваться все большим спросом у российских заказчиков. **LAN**

давать решения как для малых помещений, так и для больших машинных залов. При этом в зависимости от потребностей заказчика решения по обеспечению бесперебойного питания можно собирать из модулей мощностью 20 или 30 кВА, представленных в линейке ONL-M. Такой набор номиналов предоставляет возможность получить любую мощность, как «четную», так и «нечетную».

Линейка модульных ИБП ONL-M разработана с учетом современных требований заказчиков, в том числе к снижению расходов на первичную закупку, модернизацию и обслуживание оборудования. В результате устройства серии ONL-M оказываются на треть дешевле в эксплуатации по сравнению с моноблочными трехфазными аппаратами серии ONL-II.

В этом году планируется выпуск новой серии трехфазных решений VGD-II в диапазоне мощностей от 10 до 500 кВА с возможностью параллельной работы. Данные ИБП будут доступны в варианте как с внутренними АКБ, так и с внешними — для обеспечения длительного времени автономной работы.

### Tripp Lite

2016 год оказался очень продуктивным для Tripp Lite с точки зрения вывода на рынок новых серий ИБП. В первую очередь в компании отмечают моноблочные трехфазные ИБП серий SVT и SUT в диапазоне мощностей от 10 до 40 кВА для серверных и небольших ЦОДов. «Выпуск этих ИБП позволил нам конкурировать в нишах, в которых ранее мы конкурировать не могли, имея только модульные решения, которые обходятся дороже», — отмечает Анатолий Маслов, технический эксперт Tripp Lite.

Главное преимущество новой серии SVT (10, 20, 30 кВА), по мнению эксперта Tripp Lite, — это функциональность современного ИБП в суперкомпактном корпусе со встроенными АКБ за минимальные деньги. Старшую серию SUT (20, 40 кВА) компания позиционирует как ИБП для обеспечения более длительной автономной работы. Серия SUT не такая компактная,



как SVT, но обеспечивает больший срок автономной работы от встроенных АКБ с возможностью его удлинения до нескольких часов.

В этом году Tripp Lite выпускает на рынок новую модульную серию ИБП SVX большой мощности от 30 до 210 кВА. Эти ИБП способны запитать нагрузку 210 кВА (210 кВт), имея при этом габариты, как у стандартной серверной стойки.

### «Связь инжиниринг»

В 2016 году компания обновила дизайн модульных трехфазных ИБП серии СИП380А МД, повысив надежность и ремонтнопригодность серии. В обновленном кабинете ИБП обеспечен удобный доступ к внутренним компонентам для сервисного обслуживания. Теперь доступны силовые модули с коэффициентом мощности, равным 1, что позволяет подключать к ИБП оборудование с большей активной мощностью. ИБП этой серии относятся к системам большой мощности и предназначены для применения в серверных, ЦОДах и на других объектах с повышенными требованиями к отказоустойчивости.

В текущем году специалисты компании «Связь инжиниринг» планируют расширить возможности коммуникации и дистанционного управления ИБП с использованием различных интерфейсов. Большое внимание уделяется защищенности управления ИБП и возможности интеграции их в системы заказчиков.

# Как организовать видеонаблюдение «по уму»

Чтобы система видеонаблюдения была установлена не для галочки, а действительно справлялась со своей задачей фиксации событий, проект ее реализации должен быть тщательно проработан. Наряду с выбором камер критическое значение имеет инфраструктура для передачи и хранения данных. На форуме «Бизнес-Видео — 2017» интегрированное решение для организации видеонаблюдения представили компании Zavio, Allied Telesis и Synology.

Дмитрий Ганьжа,  
главный редактор «Журнала сетевых решений/LAN»



Камеры Zavio поддерживают широкий динамический диапазон 120 дБ. С помощью функции Zavio WDR Extreme можно детализировать изображение на затененных и засвеченных участках



Программное обеспечение Synology Surveillance Station позволяет нормализовать изображение с камер «рыбий глаз»

## ВИДЕОНАБЛЮДЕНИЕ НЕ ДЛЯ ГАЛОЧКИ

По числу камер видеонаблюдения на душу населения Москве пока еще далеко до Лондона, но их становится все больше и больше. Однако значительная часть установленных камер используется неэффективно и не справляется со своими задачами. Более того, как отметил в своем выступлении Ярослав Кузьмицкий, директор по развитию бизнеса компании InPrice Distribution, дистрибьютора Zavio, в 80% случаев видеонаблюдение никому не нужно и о нем вспоминают только при наступлении нештатной ситуации: «Во многих инфраструктурных проектах видеонаблюдение подключается едва ли не в последний день. На таких системах предпочитают экономить, устанавливая для галочки, но все это до тех пор, пока что-то не случится: пожар, ограбление и т. п.».

Основными задачами при установке систем видеонаблюдения являются обеспечение оперативного реагирования на события и их фиксация. Однако решить их можно лишь в том случае, если приняты необходимые меры, в частности, продуманы процессы обработки поступающих сигналов с поста видеонаблюдения. Сама по себе система видеонаблюдения бесполезна, если за ней не стоит организационная структура. Между тем, по опыту реализации проектов компанией InPrice Distribution, лишь 10% всех заказчиков устанавливают систему видеонаблюдения в рамках реализации тщательно выверенной стратегии обеспечения безопасности.

Наряду с ошибками при проектировании стремление к максимальной экономии (на качестве камер, видеопотоке, емкости хранилища и т. п.) оборачивается тем, что система видеонаблюдения оказывается неработоспособной. Так, например, полученное изображение не позволяет распознать затененный номер машины на КПП, потому что камера не поддерживает технологию WDR. Или для сокращения объема архива нередко видеопоток ограничивается всего 5 кадрами в секунду. В результате при каком-либо происшествии записанный архив оказывается бесполезен, поскольку не удастся разглядеть детали, которые зачастую имеют решающее значение для идентификации.

Таким образом, как указывает Ярослав Кузьмицкий, если видеонаблюдение устанавливается формально, для галочки (чтобы только было!), то лучше просто

купить муляжи, так как подобная экономия неизбежно приведет к повторным инвестициям. Он выделяет следующие типовые проблемы при реализации видеонаблюдения:

- экономия на качестве камер;
- покупка по спецификации без тестирования на реальном объекте;
- экономия на архиве за счет скорости потока: менее 10 кадров в секунду;
- экономия на архиве за счет снижения разрешения потока видео;
- экономия на длине архива и качестве NVR;
- наличие мертвых зон наблюдения и другие огрехи проектирования и монтажа.

Чтобы их избежать, необходимо четко ставить задачу и понимать, для чего будет использоваться видеонаблюдение. Например, для гарантированного фиксирования событий с детализацией, достаточной для последующей идентификации причины и объекта события, когда все перечисленные пункты выполняются при любых обстоятельствах. В частности, идентификация объекта должна обеспечиваться при любой погоде: в солнце, ливень, туман, пургу или мороз. Если это не так, значит, на каком-то из этапов было принято неверное решение и видеонаблюдения у вас, по сути, нет. Чтобы система отвечала заявленным требованиям, следует тщательно проработать проект и проконсультироваться со специалистами. Как считает Ярослав Кузьмицкий, эффективное видеонаблюдение должно быть частью онлайн-мониторинга и обязательно интегрироваться с системами СКУД для идентификации объектов в реальном времени и подтверждения обоснованности факта возникновения события или тревоги.

Однако, чтобы все реализовать «по уму», нужны деньги. Применение современных технологий позволяет не экономить на качестве видео. Например, с помощью алгоритмов сжатия, таких как H.265, можно получить высокое разрешение при сокращении требований к пропускной способности и записывать поток с частотой 60 кадров в секунду, что важно для детализации фиксируемых камерой событий. Дополнительное сокращение потока достигается за счет выделения в кадре областей, представляющих наибольший интерес. Для этого в интерфейсе камеры определяется, какие зоны кадра следует передавать с низким битрейтом, а какие с высоким, и суммарный поток удается уменьшить. В результате при использова-

нии правильных зон развертки оператор будет видеть все что нужно, а на передачу изображения излишних областей поток тратиться не будет.

Тайваньский производитель Zavio одним из первых стал поддерживать в своих видеокамерах кодек H.265. Более того, он оптимизировал алгоритмы сжатия в своей технологии динамического анализа кадра Zavio SmartCodec за счет выделения статичных и динамичных зон в течение всего времени съемки. Если в зоне наблюдается движение, степень сжатия уменьшится и потери деталей не будет. Таким образом, и без того весьма компактный поток с H.265 удастся сжать практически вдвое. Это позволяет уменьшить объем архива при заданной длине или увеличить его длину при той же емкости хранения.

Правда, пока эта технология реализована только в камерах ZAVIO серии x8000 Extreme, на которых установлены мощные процессоры. Кроме того, если вы хотите воспользоваться преимуществами этой проприетарной технологии, придется применять либо «родное» ПО ZAVIO CamGraba, либо NVR того же производителя.

Выбор камеры имеет значение. Ярослав Кузьмицкий советует выбирать ее как монитор — глазами, то есть убедиться в качестве получаемого изображения в реальных условиях работы. Кроме того, в зависимости от предполагаемых задач и области применения камеры должны поддерживать такие умные алгоритмы и современные функции, как уже описанный алгоритм выделения областей интереса (Region of Interest, ROI), коридорный формат, режим антитумана, адаптивная ИК-подсветка, широкий динамический диапазон (Wide Dynamic Range, WDR), программно оптимизированная диафрагма (P-Iris), специализированная LPR-экспозиция и т. д. Например, при уличной установке камеры функция антитумана в наших широтах практически обязательна — она позволяет устранить размытость в кадре и очистить изображение даже при очень слабой видимости с помощью алгоритма исправления изображения.

Однако камера — это лишь элемент общей инфраструктуры видеонаблюдения. Если при реализации проекта вы сэкономили на сетевом оборудовании, сеть может оказаться неработоспособной в самый неподходящий момент. Качество сетевой инфраструктуры и ее стабиль-



ность могут как иметь фатальное значение для результата в целом, так и стать решающим фактором успеха. Если у вас установлены ненадежные регистраторы, не оснащенные средствами защиты на уровне хранения, например однодисковые NVR, то при поломке диска, чтобы извлечь всего лишь 10-секундный ролик, вам придется отдать его на восстановление, а это не менее 70 тыс. руб. Ценность видеонаблюдения зависит от длительности хранения архива и его целостности — попустительское отношение к выбору системы видеорегистрации и хранения приводит к утере доказательной базы.

Завершая свое выступление, Ярослав Кузьмицкий дал простые советы для заказчиков, заинтересованных в том, чтобы инвестиции не были потрачены зря:

- покрытие зон, предназначенных для видеонаблюдения, планируйте с запасом;
- устанавливайте камеры в контруклах и в самых неожиданных местах;
- крепите камеру прочно, чтобы ее нельзя было отвернуть, либо подключайте уличные камеры через гиродатчики к системе тревожного оповещения;
- экономьте не за счет разрешения и потока, а за счет правильного выбора технологий;
- при выборе камер обязательно тестируйте их на реальном объекте;
- выбирайте камеры из списка совместимых устройств для вашего NVR или ПО с учетом решаемой задачи;
- не бойтесь использовать панорамные камеры — существующие алгоритмы позволяют восстановить «нормальное» изображение; совокупная эффектив-

ность этих камер выше, а цена сравнима с обычными.

## СЕТЬ ДЛЯ ВИДЕОНАБЛЮДЕНИЯ

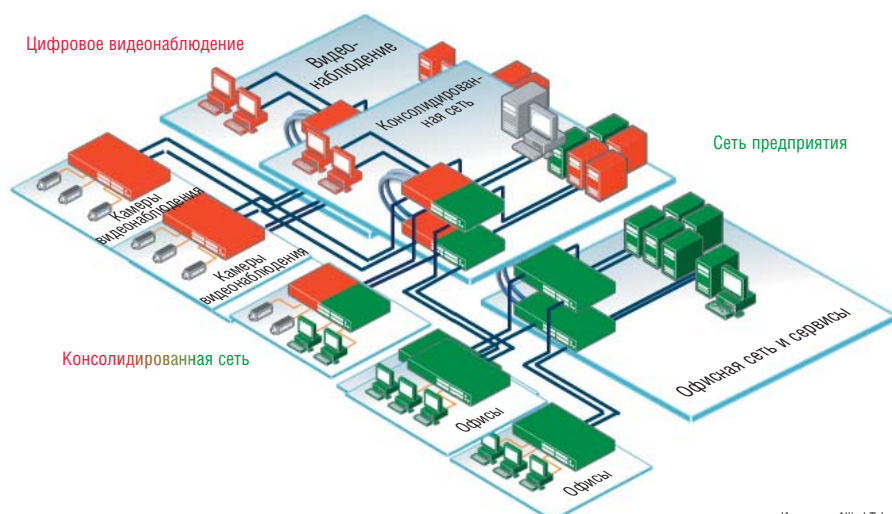
Если не уделять должного внимания всей системе видеонаблюдения, в том числе инфраструктуре, по которой данные будут передаваться, то должного уровня эффективности добиться не удастся. Современные комплексы видеонаблюдения предъявляют свои требования и к сети передачи данных. С учетом объемов передаваемого трафика сеть должна обеспечивать высокую пропускную способность, быть надежной, защищенной и достаточно интеллектуальной, чтобы самостоятельно реагировать на угрозы и поддерживать свою работоспособность. Это важно, потому что содержать штат персонала для круглосуточного контроля за работой каждого устройства в сети мало кто может себе позволить.

Часто в сети предприятия присутствуют две обособленные инфраструктуры: сеть предприятия и сеть безопасности (для видеонаблюдения). Однако, как отмечает Алексей Мельчаков, менеджер по работе с партнерами компании Allied Telesis, сегодня в большинстве проектов используются цифровые камеры, информацию с которых можно передавать по сети передачи данных, обслуживающей само предприятие. Это позволяет две обособленные сети заменить одной. Такое объединение приводит к оптимизации затрат и при построении, и при обслуживании сетей. А благодаря используемой технологической базе сотрудники службы безопасности могут быть уверены в том, что они станут

получать стабильный, высококачественный видеопоток, доступный в режиме 24/7. В то же время такая же надежная и производительная работа гарантируется и для других отделов — бухгалтерии, кадров, разработки и т. п., при этом доступ к разным данным и сервисам будет разграничен и защищен.

Для японского производителя сетевого оборудования Allied Telesis видеонаблюдение — особый рынок. Компания очень много инвестировала в развитие этого направления и активно сотрудничает с поставщиками видеокамер, в частности Axis и Panasonic, осуществляя, например, совместное тестирование для обеспечения наилучшей передачи видео. Компания предлагает решения для построения сетей разного масштаба — от небольших на 10–20 камер и средних на 50–200 камер до масштабных мультисервисных сетей, которые обычно проектируются с перспективой расширения и увеличения количества видеоустройств с учетом потребностей заказчика. К каждой из этих топологий предъявляются свои технологические требования, и каждая из них имеет уникальную архитектуру.

В небольших сетях популярностью пользуются недорогие, простые и функциональные решения, которые, будучи один раз настроены, уже не требуют внимания — «настроил и забыл». В ответ на подобные запросы Allied Telesis предлагает реализовать сеть на базе одного коммутатора, к которому подключаются рабочие места и камеры, — «решение в одной коробке». Зачастую в качестве такого коммутатора используются высо-



При использовании IP-камер, вместо двух отдельных сетей — для видеонаблюдения и передачи данных — достаточно одной

Источник: Allied Telesis

копроизводительные устройства серии AT-x930 и AT-x510 с поддержкой питания по Ethernet (PoE+). Благодаря неблокируемой архитектуре коммутаторов можно безболезненно добавлять камеры и рабочие места без потери в производительности и отказоустойчивости. Более того, на коммутаторе реализованы механизмы контроля доступа, имеется встроенный сервер RADIUS и поддерживается тройная аутентификация (802.1x, MAC, Web). Это позволяет сэкономить на приобретении отдельного сервера безопасности. Если изначально в сети были установлены коммутаторы серии AT-x510 (коммутатор второго уровня), при расширении инфраструктуры и необходимости формирования ядра сети их функциональность может быть расширена с L2 до L3 за счет дополнительной программной лицензии.

Масштабные сети имеют многоуровневую структуру. В сети, где установлено несколько десятков камер, уже есть и уровень доступа, куда подключаются камеры, и уровень агрегации, куда сходятся потоки, а далее производится запись на устройства хранения. Большие распределенные сети изначально рассчитаны на масштабирование — они способны поддерживать нелимитированное количество камер. Для обеспечения надежной работы предусматривается необходимая степень резервирования и избыточности, при этом камеры можно подключать вживую — сеть будет сохранять работоспособность. Подобные сети применяются в крупных проектах вплоть до таких, как «Безопасный город».

Для построения сетевой инфраструктуры системы видеонаблюдения Allied Telesis рекомендует использовать гигабитные коммутаторы серии x510. При их создании за основу был взят коммутатор третьего уровня старшего класса, из которого исключили функциональность динамической маршрутизации, достаточно редко используемую в сетях видеонаблюдения. Это позволило удешевить устройство, хотя оно поддерживает такие необходимые функции, как питание PoE+. Среди других возможностей, востребованных при построении сетей видеонаблюдения, — технологии резервирования и стекирования, в том числе удаленного, когда коммутаторы могут территориально находиться в разных местах, а управляться как одно устройство. По словам Алексея Мельчакова, технологическая база Allied

Telesis достаточна для построения масштабных решений с перспективой роста.

Технология Ethernet Protection Switched Ring (EPSRing) позволяет восстановить соединение в случае разрыва сети за минимальное время — менее чем за 50 мс. Эта задержка, если брать поток видео, незаметна человеческому глазу. Раньше эта технология была доступна на устройствах старшего класса (коммутаторы третьего уровня) и использовалась в крупных проектах, таких как «Безопасный город», а теперь она поддерживается и на бюджетных коммутаторах L2 и поэтому встречается даже в проектах организации видеонаблюдения в торговых центрах. Другой способ обеспечения отказоустойчивости сети — применение механизмов стекирования.

Allied Telesis поддерживает как локальный, так и удаленный стеки. В первом случае два коммутатора, находящиеся в одном месте, могут быть объединены в стек специальным кабелем, при этом нагрузка распределяется между ними динамически. При выходе одного из строя второй тут же возьмет нагрузку на себя. Allied Telesis использует подход к стекированию Active-Active, когда оба устройства постоянно работают, поэтому нет опасности, что при отказе одного из устройств другое не запустится. При построении кампусной сети коммутаторы могут быть объединены с помощью механизмов удаленного стекирования через SFP-модули. Управление коммутаторами в стеке тоже осуществляется как одним устройством.

Современную систему видеонаблюдения невозможно представить без питания по Ethernet (Power over Ethernet, PoE). Это позволяет обойтись без еще одной сети — для обеспечения питания камер. Как правило, для камер достаточно менее 30 Вт, то есть PoE+, но некоторым требуется мощность до 60 Вт. Не так давно Allied Telesis выпустила коммутаторы с поддержкой пока не стандартизированной технологии High PoE. Это промышленные коммутаторы серии AT-IE300, они предназначены для ситуаций, когда требуется обеспечить удаленное питание камер в сложных условиях. «При выборе коммутатора встает вопрос о суммарном бюджете PoE, от которого зависит максимальное количество питаемых камер, — объясняет Алексей Мельчаков. — В настоящее время наблю-



Источник: Allied Telesis

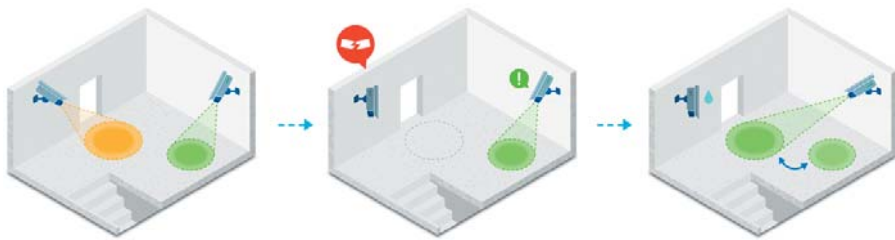
**Промышленные коммутаторы Allied Telesis IE3000 способны обеспечить питание подключенных устройств мощностью до 60 Вт**

дается тенденция оптимизации камер по потреблению питания, поэтому, на наш взгляд, существующие стандарты 802.3af и 802.3at, или PoE и PoE+, останутся актуальными и достаточными».

## ХРАНЕНИЕ ЗАПИСЕЙ

Еще один краеугольный камень системы видеонаблюдения — система для записи и хранения данных. До того как IP-камеры получили распространение, организация видеонаблюдения предполагала приобретение и установку дорогостоящих устройств DVR для записи видео, к которым камеры подключались напрямую. С распространением IP-камер на смену цифровым видеорекордерам (Digital Video Recorder, DVR) пришли сетевые (Network Video Recorder, NVR). Однако проблема хранения сделанных записей только усугубилась с увеличением доступности и востребованности соответствующих решений.

По сравнению с другими типами данных объемы видеоданных растут наиболее быстро. Согласно прогнозам аналитической компании IHS, в текущем году камерами видеонаблюдения будет сгенерировано более 6000 Пбайт данных, а к 2019 году совокупный ежегодный объем видеонаблюдения составит 3,3 трлн часов. Кроме того, сроки хранения видеозаписей все более удлиняются. Это связано как с ужесточением нормативного регулирования, так и со все более активным использованием записей не только для обеспечения безопасности, но и для аналитических задач, что становится причиной выдвижения



Источник: Synology

Если одна из установленных поворотных камер выходит из строя, то можно заранее задать параметры второй камеры, чтобы она изменила позицию и снимала заданный сектор постоянно или по заданному расписанию

дополнительных требований к функциональности NVR.

В своих проектах InPrice Distribution использует решения Synology, которая с 2007 года предлагает решения для хранения видеозаписей. В то время камеры были преимущественно аналоговыми, но уже тогда Synology сумела оценить потенциал нового рынка, что позволило этой компании расти вместе с ним и совершенствовать свои решения. Все выпускаемые ею NAS наряду с функциями файлового сервера, принт-сервера, почтового сервера и другими возможностями поддерживают и видеорегиистратор — независимо от модели функциональность устройств одинакова. Помимо продуктов для SOHO и SMB, Synology предлагает решения для корпоративного сегмента. Модели серий XS и XS+ предназначены для сегмента SME и способны поддерживать запись с 70 и 100 камер соответственно. В них можно устанавливать диски емкостью до 10 Тбайт.

NAS имеют возможность увеличения дискового пространства за счет подключаемых корзин. В некоторых случаях возможно более чем двукратное масштабирование. Установив необходимое количество дисков, потом можно добавлять и другие без остановки рабочих процессов. Максимальная возможная емкость хранения, составляющая 1,8 Пбайт при установке 180 дисков по 10 Тбайт, достигается в случае моделей RC18015xs+ (с 15 модулями расширения RXD1215sas) и RS1816xs+ (с 14 модулями расширения RX1216sas). При этом имеются ограничения по тому и разделу: максимальный размер одного тома — 200 Тбайт.

У Synology есть и специализированная модель: NVR216 с поддержкой просмотра и записи видео от девяти IP-камер. Ее основное отличие — наличие возможности прямого подключения монитора/ТВ и управляющих периферийных устройств

без использования ПК. Устройство поставляется с четырьмя бесплатными лицензиями и возможностью расширения их числа до девяти камер. В NVR216 устанавливаются два HDD, при подключении модуля расширения DX513 их число можно увеличить до семи. Таким образом, базовая конфигурация оптимизирована под потребности большинства малых и средних офисов или точек розничной торговли.

Вместе с NAS предлагается система управления для видеонаблюдения Surveillance Station. С ее помощью, например, можно сконфигурировать и настроить сразу все камеры одной модели. Surveillance Station поддерживает более 5500 моделей камер 90 разных производителей, в том числе с разрешением 4K. Поддержка стандарта ONVIF 2.6, профилей S и G гарантирует интероперабельность со множеством камер, отсутствующих в списке совместимых, что упрощает процесс планирования и закупки. В последней версии ПО Surveillance Station 8.0 добавилась возможность поддержки и других видов устройств, таких как контроллеры управления дверями.

Встроенные функции Surveillance Station позволяют сэкономить дисковое пространство при записи. Это можно сделать разными способами — например, записывать видео только при детектировании движения. В версии 8.0 добавилась функция Advanced Continuous Recording: когда ничего не происходит, запись ведется в низком разрешении, а при обнаружении движения осуществляется переключение на другой поток с более высоким разрешением. Как только действие заканчивается, происходит возврат к низкому разрешению.

Поддержка многоадресной передачи позволяет снизить нагрузку и на NAS, и на сеть. Трансляция видео нескольким клиентам в одном потоке позволяет,

например, службе охраны просматривать видео в реальном времени одновременно из нескольких мест. Для вывода изображения на экран можно воспользоваться терминалом VS360HD. Это узкоспециализированное устройство для визуализации изображения с камер без возможности нецелевого использования (охраннику не удастся поиграть в компьютерные игры). VS360HD оснащен мощным видеodecoderом и может считывать «живой» видеопоток с Surveillance Station или напрямую с камеры и выводить его на устройства HDMI.

С помощью правил на Surveillance Station можно настраивать различные варианты событий и действий. При наступлении таких событий, как обнаружение движения, появление/исчезновение объекта, расфокусировка/загораживание камеры и т. п., могут инициироваться поиск в архиве, запись изображения с камеры (в том числе с повышением разрешения), вывод отдельной таблицы событий на монитор оператора, отправление push-уведомлений и сообщений по SMS и электронной почте и т. д. Например, если одна из установленных поворотных камер ломается, можно заранее задать параметры второй камеры, чтобы она изменила позицию и снимала заданный сектор постоянно или по расписанию до тех пор, пока первая не будет восстановлена.

Для обеспечения гарантированной доступности Synology предлагает решение Synology High Availability. Оно предполагает использование двух идентичных серверов NAS, которые объединены в кластер (в качестве временной меры возможно подключение различных серверов). Один из серверов в кластере является активным, другой находится в резерве. Все данные с дисков активного устройства копируются на второй сервер. В случае отказа основного запасной берет на себя выполнение его функций. Однако, как отмечает Николай Варламов, руководитель





Источник: Synology

При использовании модулей расширения и дисков емкостью 10 Тбайт максимальная емкость хранения Synology RackStation RC18015XS+ составляет 1,8 Пбайт

отдела сервисно-технической поддержки компании Synology, такая конфигурация обходится в два раза дороже.

Новая версия программного обеспечения поддерживает конфигурацию с выделенными серверами (N+M): один (или несколько) находится в резерве, и после отказа запись с камер, которые обслуживал вышедший из строя сервер, продолжается на резервный. При восстановлении данные переносятся обратно. Один резервный сервер может быть соединен с несколькими основными, и наоборот —

один основной с несколькими резервными. Очевидно, в такой конфигурации архив записей на неисправном сервере будет недоступен до его восстановления, зато новые записи не будут потеряны. Такой вариант резервирования, естественно, обходится дешевле, чем дублирование каждого NAS по отдельности.

Развертывание сотен IP-камер представляет собой трудоемкую задачу. Для проектов распределенного видеонаблюдения с несколькими площадками Synology предлагает Synology Central Management

System (CMS). Реализация этого решения предполагает наличие выделенного главного сервера (host server), который осуществляет контроль за всеми серверами записи на различных площадках. CMS позволяет организовать видеонаблюдение филиалов при их соединении, например через Интернет. Один хост-сервер способен контролировать до 300 удаленных площадок и 5000 камер. Таким образом, из центрального офиса можно следить за состоянием и просматривать архивы как локальных камер, так и удаленных — в филиалах. LAN



## ОТКРЫТЫЕ СИСТЕМЫ

Open Systems Publications

Открыты для вас. 25 ЛЕТ

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

## ДОБАВЬТЕ ВЕСЬ МИР ИТ В СВОЙ ПЛАНШЕТ

Издания для профессионалов, деловых людей и энтузиастов

12+

Реклама



## Директор информационной службы (CIO.RU)

Ежемесячное бизнес-издание, адресованное руководителям ИТ-подразделений и бизнес-руководителям, активно участвующим в принятии решений по реализации ИТ-проектов.



## Windows IT Pro/RE

Журнал предоставляет детализированную информацию о практическом использовании технологий корпорации Microsoft.



## Бюджетное пополнение линейки ИБП Smart-UPS On-Line

Линейка источников бесперебойного питания Smart-UPS On-Line компании Schneider Electric пополнилась моделями серии SRC средней ценовой категории, причем цена некоторых из них на 40% ниже, чем у устройств «старшей» серии SRT со схожими мощностными (вольт-амперными) характеристиками. Заказчикам доступны модели с диапазоном мощности от 1 до 10 кВА. Все ИБП этой серии выпускаются только в напольном исполнении.

От серии SRT новые ИБП заимствовали все основные функции: поддержку широкого диапазона входных напряжений, жесткую регулировку выходного

напряжения, частотное регулирование, внутренний байпас и коррекцию фактора силы входного сигнала. Для Smart-UPS On-Line серии SRC мощностью от 3 кВА доступна возможность подключения внешних батарей, что позволяет увеличить время автономной работы.

Заменить необслуживаемые герметичные свинцово-кислотные батареи с загущенным электролитом и защитой от утечек заказчики могут самостоятельно. Точная интеллектуальная зарядка повышает их эффективность и продлевает срок эксплуатации до 3–5 лет. На алфавитно-цифровом дисплее отображаются системные параметры и аварийные сообщения. Кроме того, после установки специальной платы появляется возможность удаленного управления ИБП через последовательный интерфейс, порт USB или сеть. Корректировка коэффициента мощности на входе позволяет минимизировать затраты на установку за счет применения генераторов меньшей мощности и использования кабелей меньшего сечения.

ИБП Smart-UPS On-Line серии SRC полностью совместимы с программным решением APC InfraStruXure Manager.



## Многофункциональное устройство iBoot-PoE для управления питанием

iBoot-PoE компании Dataprobe представляет собой решение «три в одном»: удлинитель PoE, инжектор и устройство для удаленного управления питанием. При этом оно отличается небольшими размерами, прочным корпусом и удобством использования.

С помощью iBoot-PoE пользователь может удаленно управлять питанием (включение, выключение, перезапуск) систем безопасности, камер и других устройств с поддержкой PoE. Кроме этого, iBoot-PoE может выступать в роли удлинителя PoE с поддержкой стандартов IEEE 802.3af и 802.3at и доступной мощностью 25,5 Вт, а при подключении отдельного источника питания — в качестве гигабитного инжектора.

Всеми установленными устройствами iBoot можно управлять централизованно через любой Web-браузер. Web-интерфейс, предоставляющий доступ к управлению, информации о состоянии устройства и жур-



налу событий, поддерживается и мобильными браузерами, поэтому устройство можно включить, выключить или перезапустить буквально на ходу. Два типа паролей, для пользователя и администратора, обеспечивают необходимую защиту от нежелательного доступа.

iBoot-PoE может быть настроен на автоматический перезапуск устройств, в том числе при появлении неполадок. Пользователям доступно создание расписаний для быстрого утреннего перезапуска устройств или выключения питания на ночь в целях экономии.

## Взрывозащищенные тепловизионные камеры Axis

Три новые взрывозащищенные тепловизионные сетевые камеры Axis с температурной сигнализацией позволяют операторам производственных предприятий контролировать удаленные, труднодоступные зоны повышенной ответственности, оперативно реагировать на происшествия, а также защитить сотрудников, оборудование и критическую промышленную инфраструктуру. Камеры разработаны на основе отраслевых стандартов и открытых протоколов, снабжены высокопрочным кожухом и легко интегрируются с существующими системами диспетчерского управления и сбора данных (SCADA).

Фиксированные взрывозащищенные камеры XF40-Q2901/XF60-Q2901 с температурной сигнализацией предназначены для измерения температуры оборудования, выявления утечек из трубопроводов, обнаружения возгораний, контроля оборудования и защиты периметра. Помимо этого, они упрощают визуальный контроль и проверку надлежащей работы оборудования



и процессов и даже позволяют использовать удаленную поддержку при проведении планового техобслуживания.

Взрывозащищенные тепловизионные сетевые камеры XP40-Q1942 с функциями наклона и панорамирования предназначены для обнаружения людей в зонах ограниченного доступа и обеспечения безопасности персонала на опасных участках. Кроме того, камеры XP40-Q1942 поддерживают электронную стабилизацию изображения, что существенно улучшает качество видеосъемки в условиях вибрации, позволяя получать стабильное и удобное для просмотра видеоизображение в режиме реального времени.



# 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



**КРЕДО-ТЕЛЕКОМ**  
нам доверяют с 1995г.

**8-800-100-8281**

БЕСПЛАТНЫЙ КРУГЛОСУТОЧНЫЙ ТЕЛЕФОН

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

- 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.



Сегодня ЦОДы – это основа информационных систем современных предприятий.

Завтра ЦОДы – ключевые производственные площадки новой, цифровой экономики.



Один день. 6 июня 2017. «МИР ЦОД» – вся необходимая информация для оптимального выбора, грамотного внедрения и бесперебойной эксплуатации технических решений, которые позволят повысить вашу эффективность сегодня и развернуть новые бизнес-модели завтра.

Организатор



- Тенденции мирового рынка ЦОД
- Наилучшие практики построения, эксплуатации и развития ЦОДов
- Новые решения для мега-ЦОДов
- Энергоэффективное охлаждение
- Управление физической инфраструктурой ЦОД
- Виртуализация и гиперконвергентные решения
- Программно-определяемые СХД

Генеральный партнер

Life Is On

Schneider  
Electric

Золотой партнер

ROS  
ПЛАТФОРМА

Партнеры

AERODISK  
faster, higher, safer

АКЦИОНЕРНОЕ ОБЩЕСТВО  
АБИТЕХ

CABERO  
HEAT EXCHANGER

CAREL

CONTEC

FNT

PANDUIT™

RiT

Synology®

telecore

По вопросам участия: Ольга Пуркина



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



kon@osp.ru

Реклама 12+